Pontificia Universidad
JAVERIANA
Cali

Facultad de Ingeniería
y Ciencias
Ingeniería Electrónica

Monografía de Trabajo de Grado

# Sistema electrónico de seguridad y control de acceso para un módulo contenedor orientado al emprendimiento juvenil en el barrio La Isla de Cali

Juan Manuel Montenegro Arturo
Germán Garcés

*Director*
Dr. Luis Eduardo Tobón

25 de agosto de 2026

Nota de Aceptación

Aprobado por el Comité de Trabajo de Grado en cumplimiento de los requisitos exigidos por la Pontificia Universidad Javeriana para optar al título de Ingeniero Electrónico.

---

Dr. Mateo López Victoria
Decano Facultad de Ingeniería y Ciencias

---

Dr. Luis Eduardo Tobón Llano
Director Carrera Ingeniería Electrónica

---

Dr. Luis Eduardo Tobón
Director Trabajo de Grado

---

Dr. Carlos Andrés Giraldo Castañeda
Jurado 1

---

Dr. Manuel Vicente Valencia
Jurado 2

Santiago de Cali, 25 de agosto de 2026

Señores
Pontificia Universidad Javeriana – Cali
Dr. Mateo López Victoria
Decano
Facultad de Ingeniería y Ciencias
Santiago de Cali

Cordial Saludo.

Por medio de la presente nos permitimos presentarle el Trabajo de Grado titulado "Sistema electrónico de seguridad y control de acceso para un módulo contenedor orientado al emprendimiento juvenil en el barrio La Isla de Cali".

Esperamos que este trabajo reúna todos los requisitos académicos, cumpla el propósito para el cual fue creado y sirva de apoyo para futuros proyectos relacionados con la materia.

Atentamente,

Juan Manuel Montenegro Arturo

Germán Garcés

Santiago de Cali, 25 de agosto de 2026

Señores
**Pontificia Universidad Javeriana – Cali**
Dr. Mateo López Victoria
Decano
Facultad de Ingeniería y Ciencias
Santiago de Cali

Cordial Saludo.

Certifico que el presente Trabajo de Grado titulado "Sistema electrónico de seguridad y control de acceso para un módulo contenedor orientado al emprendimiento juvenil en el barrio La Isla de Cali", realizado por Juan Manuel Montenegro Arturo y Germán Garcés, estudiantes de Ingeniería Electrónica, se encuentra terminado y puede ser presentado para su sustentación.

Atentamente,

_____

Dr. Luis Eduardo Tobón
Director Trabajo de Grado

# Agradecimientos

Expresamos nuestro agradecimiento a nuestras familias, por su apoyo constante, comprensión y acompañamiento durante todo nuestro proceso de formación profesional. Su confianza, paciencia y motivación fueron fundamentales para afrontar los retos académicos y personales que hicieron parte del desarrollo de este trabajo de grado.

A nuestro director de trabajo de grado, por su orientación, seguimiento y aportes durante cada etapa del proyecto. Sus observaciones permitieron fortalecer el enfoque técnico de la propuesta, mejorar la organización del documento y consolidar el desarrollo del prototipo de manera más clara, coherente y estructurada.

A la Pontificia Universidad Javeriana Cali y a los docentes que contribuyeron a nuestra formación académica, por brindarnos los conocimientos, herramientas y criterios necesarios para abordar este proyecto desde una perspectiva técnica y responsable. Cada aprendizaje adquirido durante la carrera aportó de manera significativa al diseño, implementación y validación del sistema desarrollado.

A las personas y entidades vinculadas al módulo contenedor en el barrio La Isla de Cali, por su disposición y colaboración durante el planteamiento del proyecto. Su participación permitió comprender mejor el contexto de aplicación y orientar la solución hacia una necesidad real de seguridad, organización y apoyo a las actividades comunitarias y de emprendimiento.

Finalmente, agradecemos a nuestros compañeros y amigos, quienes nos acompañaron durante este proceso mediante su apoyo, consejos y aportes. Su presencia hizo parte importante del camino recorrido para culminar esta etapa académica y profesional.

# Glosario

### Símbolos

**A**: Unidad de corriente eléctrica expresada en amperios.
**Hz**: Unidad de frecuencia expresada en hercios.
**kW**: Unidad de potencia eléctrica equivalente a mil vatios.
**kWh**: Unidad de energía eléctrica utilizada para estimar consumo eléctrico.
**ms**: Unidad de tiempo expresada en milisegundos.
**V**: Unidad de tensión eléctrica expresada en voltios.
**W**: Unidad de potencia eléctrica expresada en vatios.
**Wh**: Unidad de energía eléctrica equivalente al consumo de un vatio durante una hora.

### Acrónimos y Abreviaturas

**AC**: Corriente alterna.
**DC**: Corriente continua.
**ESP32**: Microcontrolador utilizado como unidad central de control del prototipo.
**HTTP**: Protocolo utilizado para realizar solicitudes entre la ESP32 y Google Sheets.
**IDE**: Entorno de desarrollo integrado utilizado para programar la tarjeta de control.
**RC522**: Módulo lector RFID utilizado para leer tarjetas o llaveros de acceso.
**RFID**: Identificación por radiofrecuencia.
**SIM**: Módulo de identificación de suscriptor utilizado para conectividad celular.
**SPI**: Interfaz de comunicación utilizada entre la ESP32 y el módulo RC522.
**UID**: Identificador único de una tarjeta o llavero RFID.
**USB**: Interfaz utilizada para alimentar, programar o comunicar la tarjeta de control.
**Wi-Fi**: Tecnología de comunicación inalámbrica utilizada para consultar la base de datos.

### Términos

**Acceso autorizado**: Condición en la que una credencial RFID se encuentra registrada, activa y con permiso válido.
**Acceso denegado**: Condición en la que el sistema mantiene bloqueada la cerradura porque la credencial no tiene permiso.
**Apps Script**: Herramienta de Google utilizada para conectar Google Sheets con la ESP32 mediante un servicio web.
**Base de datos**: Registro organizado de usuarios, identificadores RFID, estados de autorización y permisos.
**Cerradura electrónica**: Actuador encargado de permitir o restringir físicamente el acceso al módulo contenedor.

**Credencial RFID**: Tarjeta o llavero utilizado por el usuario para solicitar acceso al sistema.
**Google Sheets**: Hoja de cálculo utilizada como base de datos externa del sistema.
**Llave no registrada**: Credencial cuyo identificador no aparece en la base de datos.
**Módulo contenedor**: Espacio físico para el cual se propone el sistema electrónico de control de acceso.
**Prototipo**: Versión funcional del sistema desarrollada para integrar y validar la lógica de acceso.
**Relé**: Dispositivo que permite activar la cerradura electrónica a partir de una señal enviada por la ESP32.
**Señalización**: Respuesta visual o sonora generada mediante LED rojo y buzzer.
**Transformador**: Fuente utilizada para alimentar la cerradura electrónica de 12 V.
**Usuario autorizado**: Usuario registrado en la base de datos con permiso activo de acceso.
**Usuario no autorizado**: Usuario o credencial que no cumple las condiciones de acceso definidas.
**Sistema fotovoltaico**: Conjunto de paneles, inversor y protecciones propuestos para apoyar la alimentación del módulo. **Arreglo fotovoltaico**: Conjunto de paneles solares conectados entre sí para generar energía eléctrica a partir de la radiación solar.
**Caja de protección AC**: Gabinete o conjunto de elementos de protección ubicados en el lado de corriente alterna del sistema energético.
**Caja de protección DC**: Gabinete o conjunto de elementos de protección ubicados en el lado de corriente continua del sistema fotovoltaico.
**Fusible AC**: Elemento de protección utilizado en corriente alterna para interrumpir el circuito ante una condición de sobrecorriente.
**Fusible DC**: Elemento de protección utilizado en corriente continua para proteger el arreglo fotovoltaico ante sobrecorrientes.
**Inversor solar**: Equipo encargado de convertir la energía en corriente continua generada por los paneles solares en corriente alterna utilizable por las cargas del contenedor.
**Inversor *on-grid***: Tipo de inversor solar diseñado para operar conectado a la red eléctrica, permitiendo alimentar cargas y trabajar en conjunto con el suministro convencional.
**Medidor bidireccional**: Dispositivo utilizado en sistemas conectados a red para registrar el flujo de energía entre el sistema fotovoltaico, las cargas internas y la red eléctrica.
**Panel solar**: Módulo encargado de convertir la radiación solar en energía eléctrica de corriente continua mediante celdas fotovoltaicas.
**Protección contra sobretensiones**: Dispositivo utilizado para proteger los equipos eléctricos ante aumentos transitorios de tensión.
**Red eléctrica**: Sistema externo de suministro de energía utilizado como respaldo o complemento para alimentar las cargas del módulo contenedor.
**Seccionador DC**: Dispositivo de maniobra que permite abrir o aislar el circuito de corriente continua proveniente de los paneles solares.

# Resumen

Este trabajo presenta el diseño, implementación y validación funcional de un sistema electrónico de seguridad y control de acceso para un módulo contenedor orientado al emprendimiento juvenil en el barrio La Isla de Cali. La solución se desarrolló con el propósito de regular el ingreso al espacio, proteger los elementos internos del módulo y facilitar una administración más organizada de los usuarios autorizados. El prototipo integra una tarjeta LilyGO A7670 ESP32 como unidad de control, un lector RFID RC522 para la identificación de credenciales, una base de datos en Google Sheets para la gestión de usuarios y permisos, elementos de señalización visual y sonora, y una cerradura electrónica de 12 V activada mediante relé y alimentada por un transformador independiente. La metodología incluyó la definición de criterios de diseño, selección de componentes, estructuración de la lógica de funcionamiento, implementación progresiva por subsistemas y validación mediante pruebas controladas. Los resultados permitieron comprobar que el sistema identifica credenciales autorizadas, rechaza usuarios sin permiso, diferencia llaves no registradas, activa la cerradura únicamente ante una autorización válida y genera señales de advertencia o alarma según la condición evaluada. Además, se verificó que los permisos de acceso pueden modificarse, agregarse o retirarse desde Google Sheets sin reprogramar la ESP32. De manera complementaria, se planteó un diseño general del sistema energético del módulo, basado en una propuesta fotovoltaica conectada a red. En conjunto, el prototipo validado constituye una base técnica para una futura implementación del sistema de seguridad en el módulo contenedor, considerando ajustes físicos, eléctricos y operativos propios de una instalación real.

**Palabras clave:** control de acceso, RFID, ESP32, Google Sheets, cerradura electrónica, módulo contenedor, seguridad electrónica, sistema fotovoltaico.

# Abstract

This work presents the design, implementation, and functional validation of an electronic security and access control system for a container module intended to support youth entrepreneurship in La Isla neighborhood, located in Cali. The solution was developed to regulate entry to the space, protect the internal resources of the module, and support a more organized management of authorized users. The prototype integrates a LilyGO A7670 ESP32 board as the control unit, an RC522 RFID reader for credential identification, a Google Sheets database for user and permission management, visual and audible signaling elements, and a 12 V electronic lock activated through a relay and powered by an independent transformer. The methodology included the definition of design criteria, component selection, operating logic design, progressive implementation by subsystems, and validation through controlled tests. The results showed that the system identifies authorized credentials, rejects users without permission, distinguishes unregistered keys, activates the lock only after a valid authorization, and generates warning or alarm signals according to the evaluated condition. It was also verified that access permissions can be modified, added, or removed from Google Sheets without reprogramming the ESP32. Additionally, a general energy system design was proposed for the module, based on a grid-connected photovoltaic alternative. Overall, the validated prototype provides a technical basis for a future implementation of the security system in the container module, considering the physical, electrical, and operational adjustments required for a real installation.

**Keywords:** access control, RFID, ESP32, Google Sheets, electronic lock, container module, electronic security, photovoltaic system.

# Índice general

# Índice de figuras

# Índice de cuadros

Capítulo 1

# Introducción

## 1.1. Introducción

En la ciudad de Cali, el barrio La Isla, ubicado en la comuna 4, presenta condiciones sociales que dificultan el acceso de la población joven a oportunidades de formación y desarrollo. En este contexto, surge la necesidad de fortalecer espacios comunitarios destinados a actividades formativas y productivas, procurando que estos cuenten con condiciones adecuadas de seguridad, organización y funcionamiento.

Esta situación refuerza los ciclos de desigualdad y desaprovecha el potencial de una comunidad con necesidades urgentes de integración social y económica. En este contexto, el proyecto se articula con los Objetivos de Desarrollo Sostenible (ODS), particularmente con la reducción de desigualdades (ODS 10), al proponer una alternativa tecnológica orientada al fortalecimiento de espacios comunitarios para jóvenes. Sin embargo, para que un módulo destinado a actividades formativas y productivas pueda operar en un entorno de alta vulnerabilidad, no basta con disponer de una infraestructura física; también se requiere un mecanismo que permita regular su uso, proteger los recursos instalados y garantizar condiciones mínimas de seguridad operativa.

Por esta razón, el eje principal del presente trabajo es el diseño, implementación y validación de un sistema electrónico de control y seguridad para el acceso a un módulo contenedor, basado en microcontroladores. Este sistema busca integrar dispositivos de identificación, sensores, actuadores y una lógica de funcionamiento capaz de responder ante diferentes condiciones de uso, como accesos autorizados, intentos de ingreso no permitido y cambios en el estado del acceso. A partir de esta solución, se pretende fortalecer el uso seguro y organizado del espacio, aportando una herramienta tecnológica que contribuya a la protección del módulo y al adecuado desarrollo de las actividades previstas en su interior.

Adicionalmente, el proyecto contempla el diseño de un sistema de energía solar fotovoltaica y de una red eléctrica interna para el módulo contenedor, con el propósito de proyectar su funcionamiento como un espacio energéticamente autónomo. Este componente incluye la definición general de los requerimientos energéticos, la distribución eléctrica interna y los criterios técnicos necesarios para soportar equipos básicos destinados a actividades formativas y productivas. De esta manera, el módulo no solo se concibe como un espacio seguro y controlado, sino también como una infraestructura sostenible que promueve el uso de energía asequible y no contaminante, en línea con el

ODS 7.

El presente trabajo se desarrolla en el área de la Ingeniería Electrónica, con énfasis en la implementación de sistemas embebidos aplicados a la seguridad, el control de acceso y la automatización de espacios físicos. A su vez, incorpora el diseño energético y eléctrico del módulo como soporte para una futura implementación integral. De esta forma, el proyecto busca articular innovación tecnológica, seguridad operativa, sostenibilidad energética e impacto social, en línea con el ODS 9, Industria, innovación e infraestructura, ofreciendo una base técnica replicable para iniciativas orientadas al emprendimiento juvenil y la sostenibilidad comunitaria en contextos vulnerables de la ciudad de Cali.

Capítulo 2

# Planteamiento del Problema

El barrio La Isla, en la ciudad de Cali, presenta condiciones de vulnerabilidad social que afectan las oportunidades de desarrollo de su población joven, particularmente en los ámbitos educativo y laboral, lo que contribuye a las oportunidades educativas y laborales, contribuyendo a que una parte considerable de la población juvenil no acceda a la educación superior ni a espacios productivos, lo que incrementa la atracción hacia la mal denominada "vida fácil" asociada a entornos delictivos o al consumo de diferentes sustancias.

Tal como se señala en el Diagnóstico de Desarrollo Socioeconómico de la Comuna 4, "para el caso de los jóvenes entre 15 y 29 años se tiene que en la Comuna 4 residen 971 jóvenes, de los cuales el 25.6 % no logra conseguir trabajo y el 19.7 % no estudia ni trabaja" (Alcaldía de Santiago de Cali, 2022). En este contexto, se evidencia la ausencia de entornos seguros y sostenibles que promuevan el aprendizaje, el emprendimiento y la responsabilidad social, y que, al mismo tiempo, contribuyan de manera positiva al cuidado del medio ambiente.

Por lo tanto, el problema se centra en la necesidad de diseñar un espacio energéticamente autónomo que, además de contar con alimentación fotovoltaica, incorpore un sistema electrónico de control y seguridad para gestionar el acceso al contenedor. Este espacio funcionará como una plataforma productiva, orientada a que los jóvenes del barrio La Isla puedan desarrollar proyectos de vida fundamentados en la educación, el emprendimiento, la responsabilidad y el respeto, como alternativa a las dinámicas de violencia y a las economías ilegales presentes en el entorno.

## 2.1. Planteamiento del Problema

En el barrio La Isla, en la ciudad de Cali, se presentan condiciones sociales y económicas que afectan el bienestar y las oportunidades de desarrollo de su población. Así como lo informa el Departamento Administrativo de Planeación [1], "Los problemas de violencia intrafamiliar, drogadicción, ausencia de solidaridad, falta de respeto y el desconocimiento de que, además de derechos, existen deberes." Estas problemáticas limitan el acceso a oportunidades de desarrollo, reducen la calidad de vida de los habitantes y generan un círculo de exclusión social difícil de romper.

En este contexto, estas condiciones llevan a muchos jóvenes a abandonar sus estudios, a no continuarlos y a dedicarse a actividades que no contribuyen a su crecimiento personal ni al bienestar comunitario. Así como se muestra en el informe según la Universidad Icesi & Departamento Administrativo de Planeación Municipal [2], El 42 % de la población sólo llegó a la secundaria, el 5.7 %

a estudios técnicos, el 7.2 % alcanzó estudios profesionales y solo el 0.5 % de la población cursó un posgrado.

Ante este panorama, el proyecto considera el módulo contenedor como un espacio destinado al desarrollo de actividades formativas y productivas para los jóvenes del sector. Para que este pueda cumplir adecuadamente su propósito, es necesario contemplar condiciones técnicas que permitan proteger los recursos dispuestos en su interior y favorecer una operación organizada, estableciendo así la seguridad del espacio como uno de los aspectos relevantes dentro de su diseño.

Una de las principales barreras para el funcionamiento de un espacio comunitario de este tipo es la necesidad de garantizar condiciones de seguridad, control y uso organizado. En este marco, el problema se formula en torno a cómo diseñar, implementar y validar un sistema tecnológico de seguridad para un módulo contenedor, capaz de gestionar el ingreso de usuarios autorizados, detectar condiciones de acceso no permitido y activar respuestas de control acordes con la lógica definida. De esta manera, el sistema propuesto permitirá fortalecer la protección del espacio, mejorar la administración de su uso y aportar una solución electrónica funcional para el desarrollo seguro de actividades formativas y productivas orientadas al emprendimiento juvenil.

### 2.1.1. Contexto del Problema

El proyecto se plantea para un módulo contenedor concebido como un espacio de apoyo a actividades formativas y productivas orientadas a jóvenes del barrio La Isla. Su operación supone el uso compartido de una infraestructura en la que pueden disponerse equipos, herramientas y otros recursos necesarios para el desarrollo de las actividades previstas.

Debido a estas condiciones de uso, el funcionamiento del módulo requiere mecanismos que permitan administrar el ingreso, restringir accesos no autorizados y proteger los recursos ubicados en su interior. En este contexto, el control de acceso se establece como una necesidad técnica asociada directamente a la operación del espacio, más que como un elemento independiente de su funcionamiento.

A partir de esta necesidad se define el desarrollo de un sistema electrónico capaz de identificar usuarios, validar permisos y ejecutar respuestas de control sobre el acceso físico. De manera complementaria, el proyecto considera una propuesta general de alimentación eléctrica y generación fotovoltaica, con el fin de proyectar las condiciones energéticas requeridas para una futura implementación integral del módulo.

### 2.1.2. Delimitación del Proyecto

### 2.1.3. Función Principal del Proyecto

La función principal del proyecto es regular electrónicamente el acceso al módulo contenedor, mediante la identificación y validación de los usuarios que solicitan ingresar. A partir de esta validación, el sistema determina si habilita temporalmente el mecanismo de apertura o mantiene el acceso restringido, de acuerdo con los permisos establecidos para cada credencial.

El sistema electrónico de seguridad constituye el componente central del proyecto y su funcionamiento se evalúa mediante pruebas controladas orientadas a verificar la correcta autorización o denegación del acceso. De manera complementaria, se desarrolla una propuesta general del sistema eléctrico y fotovoltaico del módulo, concebida como soporte técnico para una futura implementación integral.

### 2.1.4. Alcance y Limitaciones

El presente proyecto de grado tiene como alcance principal el diseño, implementación y validación de un prototipo electrónico de seguridad para un módulo contenedor destinado al emprendimiento juvenil en el barrio La Isla de Cali. Este componente permitirá evaluar una solución tecnológica basada en microcontroladores, dispositivos de identificación, sensores y actuadores, orientada a fortalecer la seguridad operativa del espacio. De manera complementaria, el proyecto contempla el diseño general de un módulo con energía fotovoltaica, como soporte para el desarrollo de actividades formativas y productivas.

El prototipo de seguridad incluirá la definición de la arquitectura del sistema, la selección de componentes electrónicos, el diseño de la lógica de funcionamiento, la programación del microcontrolador y la integración física de los elementos necesarios para su operación. Su desarrollo estará enfocado en verificar el comportamiento del sistema ante condiciones definidas de uso, como accesos autorizados, intentos de ingreso no permitido, cambios en el estado del acceso y activación de elementos de bloqueo o señalización.

La validación del prototipo se realizará mediante pruebas funcionales controladas, con el fin de comprobar la respuesta del sistema implementado y su coherencia con la lógica de operación definida. Estas pruebas estarán orientadas a verificar el funcionamiento de los mecanismos de identificación, bloqueo, señalización y respuesta ante condiciones de acceso autorizado y no autorizado

Por otro lado, el diseño fotovoltaico y la distribución eléctrica interna se abordarán a nivel técnico y documental, mediante la estimación de requerimientos, definición general de componentes, esquemas y especificaciones. Estos elementos no contemplan instalación física, puesta en marcha ni validación en campo dentro del alcance del proyecto.

### 2.1.5. Síntomas del Problema

En el barrio La Isla se evidencian condiciones que afectan la consolidación de espacios seguros para la formación, el emprendimiento y el desarrollo de actividades productivas orientadas a jóvenes. Entre los principales síntomas se encuentra la limitada disponibilidad de entornos organizados donde la población juvenil pueda participar en procesos educativos, comunitarios o productivos de manera continua y segura. Esta situación se relaciona con problemáticas sociales previamente identificadas en la comuna, como inseguridad, drogadicción, falta de respeto por normas de convivencia y baja continuidad en procesos de formación [1, 2].

Otro síntoma relevante es la exposición de los espacios comunitarios a usos no autorizados o inadecuados cuando no existen mecanismos claros para regular el ingreso. En un módulo destinado al uso compartido, la ausencia de control de acceso puede dificultar la administración del espacio, comprometer la protección de equipos y herramientas, y generar incertidumbre sobre quién puede ingresar, bajo qué condiciones y en qué momento.

Asimismo, la falta de un sistema electrónico de seguridad limita la capacidad de respuesta ante eventos básicos de operación, como intentos de acceso no permitido, apertura no autorizada, cambios en el estado del acceso o necesidad de activar señales de advertencia. Esto evidencia la necesidad de contar con una solución que permita identificar usuarios, supervisar condiciones del acceso y ejecutar acciones de control de forma organizada.

Finalmente, al proyectar el módulo como un espacio de apoyo a actividades formativas y productivas, también se hace evidente la necesidad de prever una alimentación eléctrica adecuada para los sistemas internos. Por esta razón, además del prototipo electrónico de seguridad, se requiere considerar una propuesta general de alimentación y distribución eléctrica que permita orientar una futura implementación sostenible del contenedor.

### 2.1.6. Formulación

El presente proyecto busca responder a la siguiente pregunta fundamental:

¿Cómo desarrollar un sistema electrónico de seguridad basado en microcontroladores para un módulo contenedor de uso comunitario, que integre mecanismos de identificación, monitoreo y actuación, con el fin de regular el acceso y validar su funcionamiento mediante pruebas controladas?

### 2.1.7. Sistematización

Para abordar la problemática de manera estructurada, la pregunta central se descompone en subpreguntas que permiten orientar el desarrollo del sistema electrónico de seguridad. Estas se organizan en cuatro dimensiones: caracterización de requerimientos, diseño del sistema, implementación del prototipo y validación funcional.

**1. Caracterización de requerimientos del módulo**

- ¿Qué condiciones de uso, operación y seguridad debe cumplir el módulo contenedor para funcionar como espacio comunitario orientado al emprendimiento juvenil?
- ¿Qué tipos de usuarios, escenarios de ingreso y condiciones de acceso deben considerarse para definir la lógica de autorización del sistema?
- ¿Qué recursos internos, equipos o elementos del módulo requieren protección mediante un sistema de control de acceso?

**2. Diseño del sistema electrónico de seguridad**

- ¿Qué mecanismos de identificación permiten diferenciar usuarios autorizados y no autorizados de manera funcional y adecuada para el contexto del proyecto?
- ¿Qué sensores, actuadores y elementos de señalización se requieren para monitorear el estado del acceso y ejecutar acciones de control?
- ¿Qué arquitectura basada en microcontroladores permite integrar la identificación, el monitoreo y la actuación dentro de una misma lógica de funcionamiento?

**3. Implementación del prototipo**

- ¿Qué componentes electrónicos deben seleccionarse para construir un prototipo funcional del sistema de seguridad?
- ¿Cómo debe programarse el microcontrolador para responder ante accesos autorizados, intentos de ingreso no permitido y cambios en el estado del acceso?
- ¿Cómo puede incorporarse una dinámica estratégica de uso, como el registro de participación o elementos de gamificación, para incentivar la apropiación responsable del espacio?

**4. Validación funcional del sistema**

- ¿Qué pruebas controladas permiten verificar el funcionamiento de los mecanismos de identificación, monitoreo y actuación del prototipo?
- ¿Cómo se evalúa la respuesta del sistema ante escenarios de acceso autorizado, acceso no autorizado, apertura, cierre y activación de señales de control?

- ¿Qué resultados permiten determinar si el prototipo cumple con la función de regular el acceso y fortalecer la seguridad operativa del módulo?

Estas subpreguntas permiten abordar la problemática desde una secuencia lógica de desarrollo, partiendo de la identificación de necesidades del módulo, continuando con el diseño e implementación del sistema electrónico, y finalizando con la validación de su funcionamiento mediante pruebas controladas.

Capítulo 3

# Justificación

## 3.1. Justificación

El desarrollo del presente proyecto responde a la necesidad de proporcionar condiciones técnicas que favorezcan la operación segura y organizada de un módulo contenedor destinado a actividades formativas y productivas para jóvenes del barrio La Isla. Las condiciones sociales del sector evidencian limitaciones en las oportunidades educativas y laborales de la población joven; de acuerdo con el diagnóstico socioeconómico de la comuna 4, el 25.6 % de los jóvenes entre 15 y 29 años no logra conseguir trabajo y el 19.7 % no estudia ni trabaja [3]. En este contexto, la disponibilidad de espacios orientados al emprendimiento requiere no solo una infraestructura física, sino también mecanismos que permitan administrar su utilización y proteger los recursos dispuestos en su interior.

Desde el componente de Ingeniería Electrónica, el proyecto se justifica en el desarrollo de un sistema de seguridad y control de acceso que permita gestionar el ingreso al módulo mediante la identificación y validación de usuarios. La implementación de una solución basada en un sistema embebido permite integrar los mecanismos de identificación, actuación y señalización necesarios para responder ante diferentes condiciones de acceso. De esta manera, el sistema busca reducir la dependencia de mecanismos manuales de supervisión y proporcionar una alternativa programable para administrar los permisos de ingreso y controlar físicamente el acceso al espacio.

La construcción de un prototipo permite evaluar esta propuesta antes de considerar una implementación definitiva en el módulo contenedor. Mediante pruebas funcionales controladas es posible verificar el comportamiento del sistema ante accesos autorizados, usuarios sin permiso y credenciales no registradas, así como comprobar la actuación de la cerradura, la señalización y la actualización de permisos desde la base de datos. Este proceso permite obtener evidencia sobre el funcionamiento de la arquitectura propuesta e identificar ajustes necesarios para una futura implementación en condiciones reales.

De manera complementaria, el proyecto considera el diseño general de la alimentación eléctrica y de un sistema fotovoltaico conectado a red para proyectar las condiciones energéticas requeridas por el módulo. Esta propuesta parte de una estimación preliminar de las cargas y contempla los principales elementos de generación, conversión, distribución y protección eléctrica. Su planteamiento considera criterios técnicos y de seguridad establecidos en el Reglamento Técnico de Instalaciones Eléctricas (RETIE) [4] y en la NTC 2050 [5], como referencia para una eventual implementación

física.

En conjunto, el trabajo permite establecer una base técnica para la futura implementación del módulo contenedor, integrando como eje principal un sistema electrónico de seguridad y control de acceso implementado y validado, y como componente complementario una propuesta general de alimentación eléctrica y generación fotovoltaica. El desarrollo obtenido aporta una arquitectura funcional, criterios de selección de componentes, lógica de operación y resultados de pruebas que pueden utilizarse como referencia para continuar el proceso de adecuación del sistema a las condiciones reales del espacio.

Capítulo 4

# Objetivos

## 4.1. Objetivos

### 4.1.1. Objetivo General

Diseñar, implementar y validar un sistema electrónico de seguridad basado en microcontroladores para un módulo contenedor de uso comunitario, integrando mecanismos de identificación, monitoreo y actuación que permitan regular el acceso al espacio y verificar su funcionamiento mediante pruebas controladas.

### 4.1.2. Objetivos específicos

- Caracterizar las condiciones de uso, operación y seguridad del módulo contenedor, identificando los requerimientos funcionales, técnicos y de acceso necesarios para el desarrollo del sistema de control y seguridad.
- Diseñar la arquitectura del sistema electrónico de seguridad, definiendo los mecanismos de identificación, sensores, actuadores, señales de respuesta y lógica de operación basada en microcontroladores.
- Implementar un prototipo funcional del sistema de control y seguridad, integrando los componentes electrónicos seleccionados, la programación del microcontrolador y los mecanismos físicos de identificación, monitoreo y actuación.
- Validar el funcionamiento del prototipo mediante pruebas controladas, verificando su respuesta ante accesos autorizados, intentos de ingreso no permitido, cambios en el estado del acceso y activación de los elementos de control o señalización.
- Diseñar una propuesta general de sistema fotovoltaico para el módulo contenedor, considerando los requerimientos básicos de alimentación, la estimación de demanda energética y los criterios técnicos necesarios para proyectar su autonomía energética.

Capítulo 5

# Marco de Referencia

## 5.1. Áreas Temáticas

Para las áreas propias de la disciplina se emplea la taxonomía IEEE [6]. En el marco de este proyecto, las áreas temáticas se relacionan principalmente con el diseño, implementación y validación de un sistema tecnológico de seguridad basado en microcontroladores, dispositivos de identificación, sensores, actuadores y lógica de control. También se incluyen áreas asociadas a la autonomía energética mediante sistemas fotovoltaicos. A continuación se listan las áreas temáticas relevantes:

- Security – Access control.
- Security – Access control – Authorization.
- Security – Computer security – Authentication.
- Security – Computer security – Identity management systems.
- Human factors – Identification of persons.
- Control systems – Control design.
- Control systems – Control equipment – Microcontrollers.
- Sensors – Sensor systems and applications.
- Sensors – Sensor systems and applications – Radiofrequency identification
- Computer software – Software – Embedded software.
- Computers and information processing – Embedded systems.
- Security and privacy – Access control.
- Power, energy, and industry applications – Power generation – Solar power generation.
- Power, energy, and industry applications – Power generation – Solar power generation – Photovoltaic systems.
- Power, energy, and industry applications – Power systems – Power distribution.

## 5.2. Marco Teórico

El marco teórico del presente proyecto se fundamenta en conceptos y principios relacionados con los sistemas de energía solar fotovoltaica autónomos, la generación distribuida, el almacenamiento de energía, el diseño de redes eléctricas internas y los sistemas electrónicos de control, integrados en un contexto social y normativo específico. Estos elementos permiten comprender el alcance técnico del diseño propuesto y las restricciones ambientales, sociales, económicas y normativas que condicionan su desarrollo.

#### 5.2.0.1. Sistemas embebidos

Los sistemas embebidos son sistemas computacionales diseñados para cumplir con funciones específicas dentro de un dispositivo o aplicación mayor. A diferencia de un computador de propósito general, un sistema embebido se desarrolla para ejecutar tareas concretas, interactuar con elementos físicos del entorno y responder de acuerdo con una lógica previamente definida.

Estos sistemas suelen estar compuesto por hardware, software, entradas, salidas y en muchos casos, elementos de sensado y actuación que permiten tomar información del entorno y ejecutar acciones sobre él. En la literatura los sistemas embebidos se asocian con soluciones basadas en microprocesadores o microcontroladores, controladas por software y orientadas a operación confiable, frecuentemente bajo restricciones de tiempo o respuesta.[7]

El uso de microcontroladores permite integrar en un mismo sistema funciones de lectura, procesamiento y control. Plataformas de prototipado como Arduino, se emplean ampliamente para crear objetos electrónicos interactivos y conectar sensores, actuadores y módulos externos mediante entradas y salidas digitales o analógicas, permitiendo validas la lógica y función del sistema antes de una implementación a escala real.

#### 5.2.0.2. Sistemas electrónicos de control de acceso

Los sistemas electrónicos de control de acceso permiten regular y monitorear el uso de espacios físicos mediante tecnologías digitales, contribuyendo a la organización, seguridad y uso responsable de la infraestructura. En proyectos comunitarios, estos sistemas pueden integrarse como herramientas de corresponsabilidad social cuando se diseñan bajo esquemas que incentivan la participación y el cumplimiento de normas de uso.

Desde el punto de vista tecnológico, los sistemas de control de acceso basados en microcontroladores permiten implementar soluciones flexibles y escalables, integrando sensores, actuadores y dispositivos de identificación. En aplicaciones que emplean mecanismos de identificación sin contacto, los estándares internacionales, como la familia ISO/IEC 14443, establecen los principios generales

de funcionamiento y comunicación de tarjetas de proximidad [8].

#### 5.2.0.3. Tecnologías de identificación de usuarios

Las tecnologías de identificación de usuarios permiten reconocer o verificar a una persona antes de concederle acceso a un sistema o espacio físico. En los sistemas electrónicos de control de acceso, estos mecanismos proporcionan la información necesaria para determinar posteriormente si el usuario cuenta con autorización para ingresar.

De acuerdo con el National Institute of Standards and Technology (NIST), los mecanismos de autenticación pueden clasificarse según tres factores: algo que el usuario conoce, como una contraseña o un código PIN; algo que el usuario posee, como una tarjeta, credencial o dispositivo; y algo inherente al usuario, como una característica biométrica. Esta clasificación permite diferenciar las tecnologías de identificación según el tipo de información utilizada para comprobar la identidad o posesión de una credencial. En el caso del presente proyecto, la identificación mediante RFID corresponde al factor de posesión, debido a que el usuario debe presentar una credencial física previamente asociada al sistema.

**RFID:** Una de las tecnologías más usadas es la identificación por radiofrecuencia RFID. Esta tecnología permite reconocer una tarjeta, etiqueta o dispositivo mediante comunicación inalámbrica de corto alcance entre un lector y un identificador. En este tipo de aplicaciones, el lector actúa como un dispositivo de entrada, enviando al sistema la información del identificador detectado, para que la lógica programada determine si el acceso debe ser autorizado o restringido.

**Teclado matriciales:** Otra alternativa es el uso de códigos de acceso mediante teclados o interfaces similares. En este caso, la identificación se basa en un dato conocido por el usuario, como una clave numérica previamente configurada. Esta solución de bajo costo, es fácil de implementar, sin embargo presenta limitaciones relacionadas con la posibilidad de compartir, olvidar o comprometer la clave.

**NFC:** También existen tecnologías de proximidad como NFC, que permiten la comunicación inalámbrica entre dispositivos a muy corta distancia. Esta tecnología esta diseñada para operar por proximidad muy cercado y se usa en aplicaciones de conexión rápida entre dispositivos como pagos sin contacto o intercambio de información.

**QR:** El código QR es una tecnología de identificación visual basada en un código bidimensional que permite almacenar información en un patrón gráfico legible mediante una cámara o lector óptico. La norma ISO/IEC 18004:2024 define los requisitos de la simbología QR, incluyendo sus características, métodos de codificación de datos, formatos, corrección de errores y parámetros de lectura. En sistemas de control de acceso, el código QR puede utilizarse como una credencial

visual asignada a un usuario. El sistema captura el código mediante una cámara o módulo lector, interpreta la información contenida y la compara con una lógica de autorización previamente definida.

**Credenciales digitales:** Las credenciales digitales son mecanismos de autenticación que permiten comprobar la identidad o autorización de un usuario mediante información electrónica. Estas pueden adoptar diferentes formas, como códigos temporales, identificadores únicos, enlaces de acceso, claves dinámicas, tokens digitales o permisos asociados a una cuenta o dispositivo.

**Biometricos:** Las tecnologías biométricas permiten reconocer o verificar a una persona a partir de características físicas o comportamentales. La norma ISO/IEC 2382-37:2022 establece una descripción sistemática de los conceptos relacionados con biometría aplicada al reconocimiento de seres humanos. Entre las modalidades biométricas más conocidas se encuentran la huella dactilar, el reconocimiento facial, el iris o la voz.

#### 5.2.0.4. Topología de los sistemas de energía solar fotovoltaica

Existen múltiples configuraciones para la implementación de paneles solares. Los sistemas on-grid están pensados para funcionar en conjunto con los servicios de energía cotidianos, donde al final del mes se paga la energía eléctrica consumida a lo largo de ese tiempo. El sistema de paneles solares aquí busca reducir el costo final, aportando en la generación de energía eléctrica durante el día. Funciona con un vatímetro que sirve para medir la entrada o consumo y la generación de la vivienda. El panel solar convierte la radiación solar en energía eléctrica en forma de corriente continua que pasa por el inversor que la transforma en corriente alterna y se envía a la red. De esta forma, el excedente de energía producida se descuenta (A un precio inferior al consumido) de la factura del usuario.

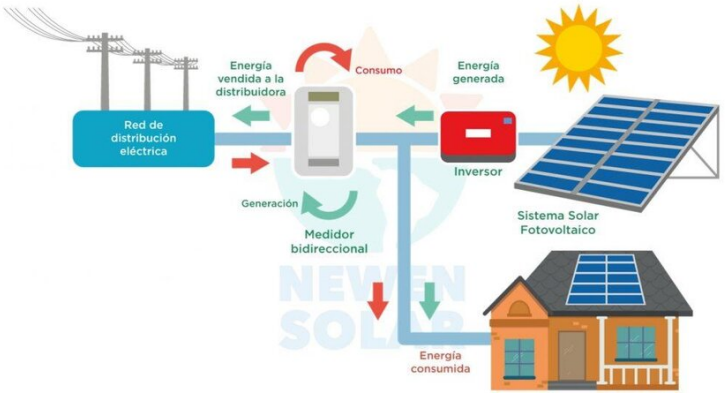


Figura 5.1: Sistema fotovoltaico on-grid

Los sistemas de energía solar fotovoltaica autónomos, también conocidos como sistemas *off-grid*,

son configuraciones diseñadas para suministrar energía eléctrica sin depender de una red convencional mediante la conversión directa de la radiación solar en energía eléctrica y su posterior almacenamiento en baterías para ser utilizadas cuando no hay sol, ya sea por situaciones climáticas o por el horario. Estos sistemas off-grid se componen principalmente de módulos fotovoltaicos, reguladores de carga, sistemas de almacenamiento, inversores y dispositivos de protección eléctrica, los cuales deben ser dimensionados de manera coordinada para garantizar un suministro confiable y seguro [9].

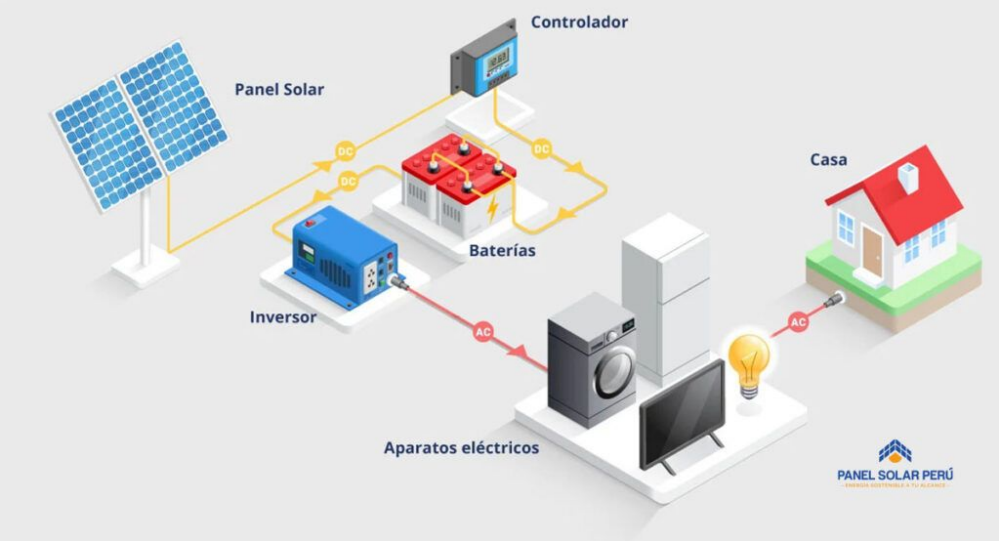


Figura 5.2: Sistema fotovoltaico off-grid

Finalmente, existen sistemas híbridos que se caracterizan por contar con un inversor híbrido que tiene la capacidad de trabajar conectado a la red y, al mismo tiempo, funcionar con baterías solares. Es la mezcla de las dos configuraciones anteriores, donde se integran baterías para situaciones puntuales y el consumo excedente es proporcionado por un servicio externo.

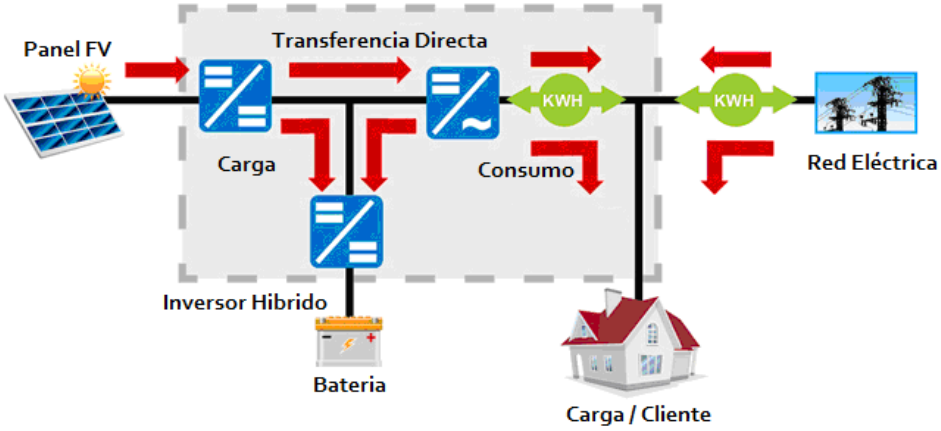


Figura 5.3: Sistema fotovoltaico híbrido

Dentro de los sistemas off-grid, diversos estudios han señalado que los sistemas fotovoltaicos autónomos constituyen una alternativa técnicamente viable para el suministro energético en contextos comunitarios y productivos donde el acceso a la red es limitado o inexistente, contribuyendo a la sostenibilidad operativa de infraestructuras sociales y económicas [10]. Su diseño adecuado requiere considerar factores como la disponibilidad del recurso solar, los perfiles de carga, la eficiencia de los componentes y las condiciones ambientales del sitio de aplicación.

#### 5.2.0.5. Tipos de paneles solares

La energía solar es una fuente limpia, renovable e inagotable que no genera contaminación ni emisiones durante su uso. Existe una variedad de tipos de paneles solares disponibles en el mercado y catalogados según su función, voltaje, corriente y tecnología.

**Paneles térmicos:** Estos dispositivos están diseñados para aprovechar la radiación solar, pero no generan electricidad; sino que la convierten en calor para luego ser usada en la calefacción de agua caliente sanitaria o en algunos procesos industriales. Estos paneles funcionan al absorber la radiación y transferirla a un fluido, pueden ser de colector plano o de tubos al vacío.

Figura 5.4: Panel Térmico

**Paneles fotovoltaicos:** Estos dispositivos están diseñados para convertir la energía solar en electricidad mediante el proceso fotovoltaico. Estos paneles se componen de células fotovoltaicas, hechas de silicio, capaces de producir corriente continua al ser impactadas por los fotones provenientes del sol. Sin embargo, para el consumo de casas o empresas, la energía es transformada en corriente alterna mediante un inversor, para ser usada en diferentes dispositivos como televisores, ventiladores, motores, computadores, etc. Además, pueden ser catalogados según su voltaje: 12 Voltios para instalaciones más pequeñas o 24 voltios para instalaciones medianas o grandes, dependiendo del número de células y de la potencia que estos puedan generar.

Figura 5.5: Paneles fotovoltaicos

Dentro de los paneles fotovoltaicos existen una gran cantidad de variantes y tipos, cada uno con sus características que los hacen idóneos para ciertas situaciones o necesidades.

- Paneles monocristalinos: Este tipo de paneles se caracteriza por su fabricación en un único cristal de silicio, lo que le permite ofrecer un mayor rendimiento en comparación con otros tipos de paneles. El panel monocristalinos destaca en su alta eficiencia, logrando entre un 18 % y 23 %, lo que significa mayor electricidad en menos espacio. Además de ofrecer una larga vida útil y es fácil identificarlo por su color negro o azul oscuro. Usados en espacios reducidos como tejados residenciales.
- Paneles Policristalino: Este tipo de paneles se fabrican a partir de varios fragmentos de silicio que se funden para su integración. Ofrecen una eficiencia entre el 13 % y el 18 % y se diferencian por su color azul con textura. Este panel es más económico por su proceso de fabricación más sencillo, teniendo una buena relación costo -beneficio. Usados en proyectos más grandes con un espacio más amplio, como granjas solares o techos industriales.
- Película delgada: Los paneles de película delgada, o también conocidos como Thin-film, son un tipo de panel fabricado en capas delgadas de varios materiales semiconductores. Este tipo de paneles se caracteriza por su flexibilidad y ligereza, permitiendo su instalación en estructuras curvas, pero con una eficiencia mucho menor, entre 8 % y el 12 %. Usados en fachadas, vehículos o techos con bajo soporte estructural.
- Paneles bifaciales: Este tipo de paneles ofrece una mezcla de tecnologías y la capacidad de captar luz por ambas caras, por lo que ofrece una mayor eficiencia entre un 20 % y 30 %. La cara frontal recibe la luz directa del sol, como cualquier panel. Pero la cara trasera aprovecha la luz que rebota en el suelo o en superficies cercanas. Usados en grandes plantas solares a gran escala sobre suelos de grava clara o arena que reflejan mucha luz.

#### 5.2.0.6. Generación distribuida y sistemas energéticos descentralizados

La generación distribuida se refiere a la producción de energía eléctrica a pequeña y mediana escala, ubicada cerca de los puntos de consumo. En el contexto de sistemas fotovoltaicos autónomos, la generación distribuida permite reducir pérdidas energéticas, mejorar la confiabilidad del suministro y fortalecer la resiliencia energética de comunidades y espacios productivos [11].

Desde una perspectiva social y económica, los sistemas energéticos descentralizados han sido identificados como herramientas que facilitan la inclusión social, el desarrollo comunitario y el fortalecimiento del tejido productivo local, al permitir el acceso a energía limpia y estable para actividades educativas y de emprendimiento [12, 13]. Estos sistemas adquieren especial relevancia en proyectos orientados a poblaciones juveniles en contextos de vulnerabilidad social.

#### 5.2.0.7. Almacenamiento de energía en sistemas fotovoltaicos

En el contexto de sistemas solares, una batería es un dispositivo electroquímico que almacena energía eléctrica en forma química para liberarla posteriormente.

El almacenamiento de energía es un componente esencial en los sistemas fotovoltaicos autónomos, dado que permite compensar la variabilidad del recurso solar y garantizar la continuidad del suministro energético. Las baterías constituyen la tecnología de almacenamiento más utilizada en este tipo de aplicaciones, y su selección debe considerar parámetros como la capacidad, la profundidad de descarga, la vida útil y la compatibilidad con los demás componentes del sistema [14].

Es importante destacar que la profundidad de descarga (DoD, por sus siglas en inglés) representa el porcentaje de la capacidad nominal de la batería que puede ser utilizada durante un ciclo de descarga sin comprometer significativamente su vida útil. Este parámetro es determinante en el diseño de los sistemas fotovoltaicos, ya que establece la fracción de energía realmente aprovechable del banco de almacenamiento. Las tecnologías como el plomo-ácido presentan profundidades de descarga recomendadas cercanas al 50 %. Al mantener las baterías en este rango, se puede extender el número de ciclos de Carga-Descarga y, con ello, la vida útil. Por ende, es recomendable hacer un buen dimensionamiento del sistema con una capacidad que supere lo requerido para evitar daños.

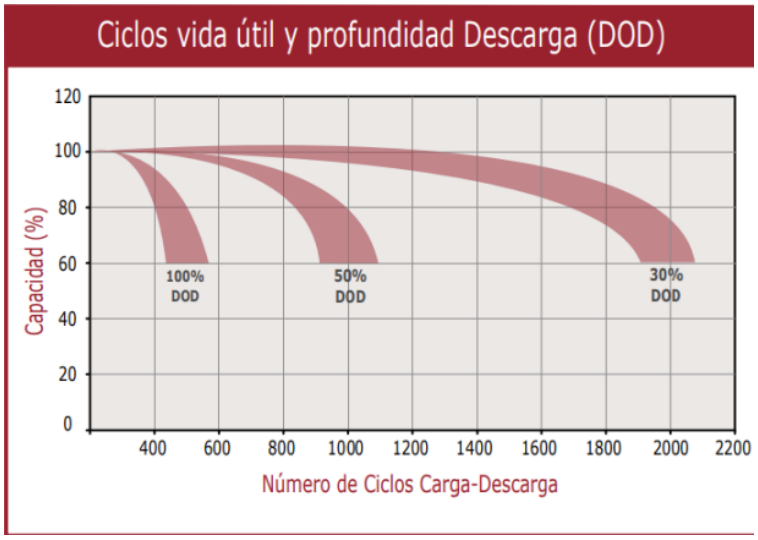


Figura 5.6: Profundidad de descarga de una batería GEL 12 V

Por otro lado, las baterías de ion-litio, particularmente las de fosfato de hierro-litio (LiFePO4), permiten valores entre el 80 % y 95 %, lo que mejora el aprovechamiento energético y reduce el sobredimensionamiento del sistema.

La profundidad de descarga se define como:

$$DoD = \frac{E_{descargada}}{E_{Nominal}} x100\,\%$$

Donde:

$$E_{descargada} = Energia\ extraida$$

$$E_{nominal} = Capacidad\ total\ nominal\ de\ la\ batera$$

En consecuencia, un dimensionamiento inadecuado del sistema de almacenamiento puede comprometer la operación del sistema fotovoltaico, generando interrupciones en el suministro o reduciendo la vida útil de los equipos. Por esta razón, el análisis de la demanda energética y de los perfiles de consumo resulta fundamental en la etapa de diseño [15].

Existen una variedad de tipos de baterías en el mercado, cada una con características especiales para cada tipo de situación.

- Plomo-Ácido: Es la tecnología de las baterías de automoviles, pero se puede adaptar. Basadas en la reacción electroquímica entre placas de plomo y dióxido de plomo en presencia de ácido sulfúrico. Además, tienen unas subclases:
  - Abiertas/inundadas: Tienen un bajo costo inicial, pero son muy sensibles a las descargas profundas y requieren que se les rellene el liquido cada cierto tiempo.
  - AGM (Absorben Glass Mat): Están selladas y no requieren mantenimiento, además de ser mas resistentes a las vibraciones y son más eficientes que las abiertas.
  - GEL: El electrolito en este caso está gelificado haciéndolas muy seguras y duraderas, con mayor estabilidad térmica y mejor tolerancia a ciclos profundos, ideales para espacios con poca ventilación
- Baterías de Litio: Basadas en el movimiento reversible de iones de litio entre el ánodo y el cátodo durante los procesos de carga y descarga. Son las más comunes y muy seguras, además de tener un ciclo de vida mucho más largo. Dentro de las desventajas asociadas, se encuentra un mayor costo inicial y requieren de electrónica de gestión más especializada.
- A tener en cuenta: El mercado de las baterías esta en constante movimiento y cada año implementan nuevas tecnologías, baterías de Sodio-Ion son una nueva tentativa, ya que funcionan de manera similar a las de litio pero usan sodio en su lugar. Baterías de flujo o de estado sólido son algunas tentativas.

#### 5.2.0.8. Energía, sostenibilidad y emprendimiento juvenil

El acceso a energía confiable y asequible ha sido reconocido como un factor habilitador del desarrollo social y económico, especialmente en iniciativas orientadas al emprendimiento juvenil. La literatura especializada señala que la disponibilidad de energía limpia favorece la creación de entornos productivos sostenibles, mejora las oportunidades de formación y contribuye a la reducción de

desigualdades [14, 11].

En este sentido, el diseño de espacios energéticamente autónomos se alinea con los Objetivos de Desarrollo Sostenible, particularmente con el ODS 7 (energía asequible y no contaminante), el ODS 9 (industria, innovación e infraestructura) y el ODS 10 (reducción de desigualdades), al integrar soluciones tecnológicas con impacto social positivo [16, 17, 18]. Este enfoque refuerza la pertinencia del proyecto desde una perspectiva técnica, social y ambiental.

## 5.3. Trabajos Relacionados

El análisis de trabajos relacionados permite identificar cómo ha sido abordado el problema del diseño de espacios energéticamente autónomos orientados a usos comunitarios, formativos y productivos, así como los enfoques técnicos y contextuales utilizados en estudios previos. Para esta revisión se consideran como criterios de comparación el tipo de infraestructura propuesta, la solución energética empleada, el contexto social de aplicación y el nivel de integración técnica del sistema.

Diversos trabajos han analizado la relación entre el espacio urbano y los procesos de exclusión social, destacando el papel que tienen los entornos físicos en la reproducción o mitigación de desigualdades, especialmente en contextos urbanos vulnerables. En este sentido, Álvarez y Ramírez, desde una reflexión crítica sobre la ciudad y el territorio, abordan cómo los espacios urbanos pueden convertirse en escenarios de inclusión o exclusión social, visibilizando las limitaciones estructurales que enfrentan poblaciones marginadas y la necesidad de repensar la infraestructura urbana como un medio para promover ciudadanía y equidad. [19].

En relación con la provisión energética para infraestructuras comunitarias, diversos trabajos han analizado el uso de sistemas fotovoltaicos autónomos como soporte para actividades sociales, educativas y productivas en contextos con limitaciones de acceso energético. Mandelli presentan una revisión exhaustiva de sistemas energéticos off-grid aplicados a infraestructura comunitaria, evidenciando que estas soluciones permiten mejorar la disponibilidad energética y apoyar procesos de desarrollo local. No obstante, el estudio se centra en la clasificación de sistemas y en el análisis comparativo de experiencias previas, sin abordar el diseño técnico detallado de la red eléctrica interna, la coordinación de protecciones ni la aplicación de normativas eléctricas específicas, aspectos que resultan fundamentales en el presente proyecto [20].

Otros trabajos han abordado el acceso a la energía como un factor habilitador del emprendimiento juvenil y del desarrollo económico local, destacando su impacto en la generación de oportunidades productivas sostenibles. En este sentido, la Agencia Internacional de Energías Renovables (IRENA) señala que la disponibilidad de energía renovable confiable puede fortalecer iniciativas productivas lideradas por jóvenes, especialmente en contextos vulnerables, al reducir barreras de entrada y favorecer la creación de empleo y autoempleo. No obstante, estos análisis se desarrollan principalmente

desde una perspectiva socioeconómica y de políticas públicas, sin incorporar criterios técnicos de diseño energético, ni consideraciones normativas propias de la Ingeniería Electrónica aplicadas a infraestructuras específicas, aspectos que constituyen el foco del presente proyecto [21].


Figura 5.7: Impacto laboral de las energías renovables en países en desarrollo

A nivel internacional, organismos multilaterales han documentado el uso de soluciones energéticas descentralizadas como soporte para infraestructura comunitaria, destacando su contribución a la resiliencia social y económica de las comunidades. En particular, el programa ESMAP del Banco Mundial analiza el papel de los sistemas energéticos descentralizados en el fortalecimiento de servicios comunitarios y productivos, señalando su potencial para mejorar la sostenibilidad operativa y el acceso a energía en contextos vulnerables. No obstante, estos reportes presentan un enfoque general orientado a políticas energéticas y modelos de adopción, sin abordar en detalle los procesos de diseño eléctrico, la coordinación de protecciones ni la integración técnica de sistemas energéticos autónomos en infraestructuras específicas, aspectos que son desarrollados en el presente proyecto [22].

Diversos estudios recientes han analizado el papel de las microredes eléctricas como una solución eficaz para mejorar la autosuficiencia energética y facilitar la integración de fuentes renovables en sistemas de pequeña y mediana escala. En particular, Bielecki presenta un análisis detallado de las microredes como herramientas para la autosuficiencia energética, destacando su capacidad para operar de forma conectada o aislada de la red principal mediante la integración de generación distribuida, almacenamiento energético y sistemas de control. El estudio resalta que este tipo de arquitecturas permite reducir pérdidas en transmisión, mejorar la confiabilidad del suministro y disminuir la dependencia de redes centralizadas, aspectos especialmente relevantes para proyectos locales y comunitarios. Asimismo, se señala que la incorporación de sistemas de monitoreo y control, basados en sensores eléctricos, resulta fundamental para garantizar la estabilidad y el balance energético del sistema. No obstante, el autor identifica desafíos asociados a los costos iniciales de inversión y a la necesidad de marcos regulatorios adecuados, lo que evidencia la importancia de realizar estudios de viabilidad técnica y económica en aplicaciones específicas.[23]

En el contexto colombiano, los desafíos regulatorios mencionados adquieren una relevancia par-

ticular debido a la obligatoriedad del cumplimiento del Reglamento Técnico de Instalaciones Eléctricas [4], así como de normas técnicas internacionales aplicables a sistemas fotovoltaicos [24]. Esto implica que cualquier propuesta de sistema energético distribuido o esquema tipo microred, aun en aplicaciones de pequeña escala, debe concebirse desde su etapa de diseño bajo criterios formales de seguridad eléctrica, coordinación de protecciones, puesta a tierra y calidad del suministro. En consecuencia, la articulación entre arquitectura técnica, viabilidad económica y cumplimiento normativo no constituye un elemento complementario, sino un componente estructural del proceso de diseño, especialmente en proyectos orientados a contextos comunitarios donde la confiabilidad y la seguridad resultan determinantes.

El estudio titulado *"Performance of a Photovoltaic Solar Container Under Mediterranean and Arid Climate Conditions"* analiza el comportamiento energético de un contenedor equipado con un sistema fotovoltaico autónomo sometido a condiciones climáticas mediterráneas y áridas. La investigación evalúa parámetros como la producción eléctrica, el rendimiento del generador fotovoltaico, el comportamiento térmico del sistema y la influencia de la radiación solar y la temperatura ambiente sobre la eficiencia global del sistema. Los resultados muestran que la configuración en contenedor permite una solución modular, transportable y adaptable a diferentes entornos climáticos, manteniendo niveles de desempeño adecuados incluso bajo altas temperaturas. El trabajo concluye que los contenedores solares representan una alternativa viable para aplicaciones remotas y descentralizadas, particularmente en contextos donde se requiere suministro energético autónomo y rápida implementación. [25]

Además de los estudios relacionados con la viabilidad energética de los contenedores, también se identificaron investigaciones orientadas a comprender las necesidades de seguridad desde la perspectiva de los usuarios. En esta línea, Frimpong analiza la relación entre diferentes mecanismos de control de acceso y la percepción del riesgo frente a delitos como el robo y el hurto en barrios residenciales de Sekondi-Takoradi, Ghana. El estudio considera elementos como cercas, alarmas contra intrusión y barreras físicas, y emplea una metodología basada en encuestas realizadas a residentes de tres barrios y entrevistas a actores clave, con el propósito de relacionar las condiciones de seguridad de los espacios con la percepción de quienes los utilizan. Este trabajo resulta relevante para el presente proyecto no solo por abordar el control de acceso en un contexto con problemáticas de seguridad, sino también por su aproximación metodológica, ya que la consulta directa a usuarios y actores vinculados al entorno permite identificar necesidades, percepciones y condiciones de uso que pueden orientar posteriormente la definición de requerimientos de una solución de seguridad. En este sentido, el estudio constituye un referente para considerar al usuario y al contexto de aplicación durante las etapas iniciales de caracterización y diseño, aunque su aplicación se concentre en propiedades residenciales y en mecanismos físicos de protección. [26]

Además de la viabilidad energética de los contenedores solares, otros estudios han señalado la importancia de incorporar criterios de seguridad y control de acceso en infraestructuras ubicadas en contextos urbanos con percepción de riesgo. En esta línea, Frimpong analiza si las características de control de acceso en propiedades residenciales reducen la percepción de riesgo frente a delitos

como robo y hurto en barrios de Sekondi-Takoradi, Ghana. El trabajo examina elementos como cercas, alarmas contra intrusión y barreras físicas como estrategias utilizadas por la comunidad para reducir el riesgo de victimización. La investigación combina encuestas realizadas a residentes con entrevistas a actores clave, permitiendo relacionar las condiciones de seguridad de los espacios con la percepción y las necesidades de sus usuarios.

Este enfoque constituye un referente metodológico para la caracterización de las necesidades asociadas al uso y la seguridad de espacios comunitarios, ya que evidencia la importancia de considerar la percepción de los usuarios y de los actores vinculados al contexto antes de establecer criterios de diseño. Para el presente proyecto, este antecedente resulta pertinente tanto por su aproximación al control de acceso en contextos con problemáticas de seguridad como por el uso de técnicas de consulta a usuarios para orientar la identificación de necesidades y requerimientos. [26]

Otro trabajo relacionado es el de Imoize y Alabi, quienes desarrollan un sistema de control de acceso de bajo costo basado en RFID y contraseña, orientado a responder a preocupaciones de seguridad en hogares y espacios industriales. La propuesta integra un lector RFID, tarjetas de identificación, teclado matricial, microcontrolador, pantalla LCD, buzzer, motor driver y fuente de alimentación, configurando un sistema de doble autenticación para permitir o denegar el acceso. Este estudio se relaciona con el presente proyecto porque aborda la implementación de una solución electrónica de seguridad enfocada en restringir el ingreso de personas no autorizadas mediante tecnologías accesibles y compatibles con sistemas embebidos. A diferencia del presente trabajo, su aplicación se enfoca en hogares y espacios industriales, mientras que este proyecto orienta el sistema de seguridad hacia un módulo contenedor comunitario destinado al emprendimiento juvenil en un contexto de vulnerabilidad social. [27]

Un antecedente relevante es el trabajo de Palma, Agudo, Sánchez y Macías, quienes presentan un sistema de control de acceso para salones de clase mediante tecnología NFC e Internet de las Cosas. El sistema permite identificar usuarios, registrar el uso de los espacios y publicar la información en una plataforma web, facilitando la supervisión de aulas desde un centro de administración. Este trabajo resulta pertinente porque evidencia la posibilidad de integrar mecanismos de identificación de usuarios con sistemas de registro y supervisión remota, permitiendo administrar de manera más organizada el acceso y uso de infraestructuras compartidas. Asimismo, constituye un referente para considerar la gestión de usuarios y el almacenamiento de información como funciones complementarias dentro de un sistema electrónico de control de acceso. [28]

Otro trabajo relacionado es el de Abdulshaheed, Abbas, Al Barazanchi y Hashim, quienes desarrollan un sistema de control y alerta para puertas mediante RFID e IoT. La propuesta integra diferentes métodos de acceso, como tarjeta RFID, contraseña temporal y apertura remota por administrador, además de funciones de bloqueo ante intentos no válidos y alertas mediante conexión Wi-Fi. Este antecedente aporta al presente proyecto porque evidencia una arquitectura de seguridad electrónica que combina identificación de usuarios, mecanismos de bloqueo, comunicación remota

y respuesta ante accesos no permitidos. Sin embargo, su enfoque se orienta a una solución general de puerta inteligente, sin abordar su integración en una infraestructura comunitaria destinada a actividades formativas y productivas. [29]

En síntesis, los trabajos revisados evidencian avances relevantes tanto en el desarrollo de sistemas electrónicos de control de acceso como en el uso de soluciones fotovoltaicas aplicadas a infraestructuras modulares o comunitarias. Por un lado, los estudios sobre seguridad muestran la viabilidad de implementar tecnologías de identificación, autenticación, sensado y actuación para regular el ingreso a espacios físicos; por otro, los trabajos sobre contenedores solares y sistemas energéticos descentralizados permiten reconocer la importancia de proyectar una infraestructura con soporte energético sostenible. Sin embargo, se identifica que estos enfoques suelen abordarse por separado: algunos se centran en la seguridad electrónica y otros en la disponibilidad energética. En este sentido, el aporte del presente trabajo radica en asumir la seguridad del módulo como eje central de desarrollo, mediante un prototipo electrónico funcional orientado al control del acceso y a la protección del espacio, mientras que el componente fotovoltaico y la red eléctrica interna se plantean como soporte técnico para una futura implementación integral.

Capítulo 6

# Materiales y Métodos

## 6.1. Enfoque general del desarrollo

El desarrollo de la solución se estructuró a partir del diseño, implementación y validación funcional de un sistema electrónico de seguridad y control de acceso para un módulo contenedor de uso comunitario. El proceso inició con la definición de los criterios de diseño del sistema, continuó con la selección de los componentes electrónicos, la elaboración de diagramas funcionales, la programación del microcontrolador y la integración física del prototipo. Finalmente, se definió un conjunto de pruebas controladas para verificar la respuesta del sistema ante escenarios de acceso autorizado, acceso no autorizado, monitoreo del estado del acceso y activación de los mecanismos de actuación o señalización.

## 6.2. Criterios de diseño del sistema de seguridad

Los criterios de diseño del sistema de seguridad se definieron a partir de la necesidad de regular el acceso al módulo contenedor, proteger los recursos ubicados en su interior y facilitar una operación organizada del espacio. Para ello, se establecieron criterios funcionales, técnicos, de seguridad y de uso comunitario, los cuales orientaron la selección de componentes, la arquitectura del sistema y la lógica de funcionamiento del prototipo.

Desde el punto de vista funcional, el sistema debía permitir la identificación de usuarios, la validación del acceso y la activación de una respuesta según la condición evaluada. En este sentido, la solución debía diferenciar entre ingresos autorizados y no autorizados, habilitar el mecanismo de apertura únicamente cuando se cumpliera la condición de autorización y mantener restringido el acceso en caso contrario. Además, debía permitir el monitoreo del estado del acceso, de manera que el sistema pudiera reconocer condiciones como apertura, cierre o intento de ingreso no permitido.

En cuanto a los criterios técnicos, se priorizó una arquitectura basada en microcontrolador, debido a su capacidad para integrar entradas, salidas y lógica de control en un solo sistema. También se consideró la compatibilidad eléctrica entre los módulos de identificación, sensores, actuadores y elementos de señalización, así como la disponibilidad comercial de los componentes, la facilidad de programación, el bajo consumo energético y la posibilidad de realizar ajustes durante la etapa de pruebas.

Los criterios de seguridad se orientaron a garantizar que el sistema respondiera de forma controlada ante diferentes escenarios de operación. Por esta razón, se contempló la respuesta ante acceso autorizado, acceso denegado, intentos fallidos consecutivos, activación de señales de advertencia y retorno al estado inicial. Esta lógica busca evitar que el acceso dependa únicamente de una supervisión manual y permite que el prototipo actúe de manera coherente frente a eventos definidos.

Finalmente, se consideraron criterios de uso comunitario, dado que el sistema está destinado a un espacio compartido por usuarios con diferentes niveles de familiaridad tecnológica. Por ello, la operación debía ser sencilla, comprensible e intuitiva, apoyándose en señales visuales o sonoras que indicaran claramente el estado del sistema. Asimismo, se tuvo en cuenta que el control de acceso puede convertirse en un medio para promover el uso responsable del módulo, especialmente si se articula con dinámicas de participación, registro de uso o estrategias de gamificación que incentiven la apropiación del espacio por parte de la comunidad.

Cuadro 6.1: Criterios funcionales del sistema de seguridad

| **Criterio funcional** | **Justificación** |
|---|---|
| Control de acceso | Regula el ingreso al módulo y reduce la dependencia de supervisión manual. |
| Identificación de usuarios | Permite diferenciar usuarios autorizados y no autorizados antes de permitir el ingreso. |
| Validación de autorización | Define si la información ingresada cumple las condiciones para habilitar el acceso. |
| Apertura controlada | Asegura que el mecanismo de apertura solo se active con una autorización válida. |
| Restricción de ingreso | Mantiene el acceso bloqueado cuando el usuario no cumple los criterios establecidos. |
| Monitoreo del estado del acceso | Permite reconocer si la puerta se encuentra abierta, cerrada o si cambia de estado. |
| Señalización del estado del sistema | Informa si el sistema está en espera, autorizó el ingreso, negó el acceso o activó una alerta. |
| Manejo de intentos fallidos | Contabiliza accesos no autorizados consecutivos y ejecuta una respuesta al superar el límite definido. |
| Activación de alarma o advertencia | Genera una respuesta visual o sonora ante condiciones anómalas del acceso. |
| Apropiación del espacio | Permite integrar dinámicas de participación o gamificación para incentivar el uso responsable del módulo. |

Cuadro 6.2: Criterios técnicos cuantificables del sistema de seguridad

| **Criterio técnico** | **Parámetro evaluado** | **Criterio que se debe cumplir** |
|---|---|---|
| Tiempo de respuesta del sistema | Tiempo entre identificación y respuesta | El sistema debe generar una respuesta de autorización, rechazo o advertencia en un tiempo menor o igual a 2 segundos después de recibir la credencial o dato de acceso. |
| Tiempo de activación del acceso | Duración de apertura | El mecanismo de apertura debe permanecer activo durante un intervalo definido entre 3 y 5 segundos antes de retornar al estado inicial. |
| Intentos fallidos permitidos | Número máximo de intentos | El sistema debe permitir máximo 3 intentos consecutivos no autorizados antes de activar una señal de advertencia o bloqueo lógico. |
| Señalización visual | Número mínimo de estados indicados | El sistema debe diferenciar al menos 3 estados mediante señalización: espera, acceso autorizado y acceso denegado o alerta. |
| Señalización sonora | Activación de advertencia | El sistema debe activar una señal sonora cuando se alcance el límite de intentos fallidos o se detecte una condición no autorizada. |
| Monitoreo del estado del acceso | Detección de apertura/cierre | El sensor de acceso debe permitir distinguir al menos dos estados físicos: puerta abierta y puerta cerrada. |
| Reinicio del sistema | Tiempo de retorno al estado inicial | Después de una autorización, rechazo o advertencia, el sistema debe retornar automáticamente al estado de espera en un tiempo definido menor o igual a 5 segundos. |

| Criterio técnico | Parámetro evaluado | Criterio que se debe cumplir |
|---|---|---|
| Validación funcional | Escenarios mínimos de prueba | El prototipo debe verificarse en al menos 3 escenarios: acceso autorizado, acceso no autorizado, tres intentos fallidos, apertura/cierre del acceso y activación de señalización. |

### 6.2.1. Criterios de seguridad

Los criterios de seguridad se definieron con el propósito de garantizar que el sistema respondiera de manera controlada ante las diferentes condiciones de acceso al módulo contenedor. Estos criterios orientaron la lógica de funcionamiento del prototipo, especialmente en los casos de ingreso autorizado, ingreso no autorizado, intentos fallidos consecutivos y activación de señales de advertencia.

El primer criterio considerado fue que el acceso debía permanecer restringido mientras no existiera una autorización válida. Por esta razón, el sistema no debía activar el mecanismo de apertura hasta que el usuario fuera identificado y validado correctamente. Esta condición permite evitar aperturas accidentales o ingresos no permitidos durante el estado de espera del sistema.

El segundo criterio fue la respuesta diferenciada ante accesos autorizados y no autorizados. Cuando el usuario cumple las condiciones de autorización, el sistema debe permitir la apertura durante un tiempo definido y generar una señal de confirmación. En caso contrario, el acceso debe permanecer bloqueado y el sistema debe indicar el rechazo mediante una señal visual o sonora.

También se estableció como criterio el manejo de intentos fallidos consecutivos. Esta condición permite que el sistema no solo rechace accesos no autorizados, sino que también identifique la repetición de intentos inválidos como un evento de advertencia. Para ello, la lógica de control debe contar los intentos fallidos y ejecutar una respuesta definida cuando se alcance el límite establecido.

Otro criterio de seguridad corresponde al monitoreo del estado del acceso. El sistema debe permitir reconocer si la puerta se encuentra abierta o cerrada, de manera que la lógica de operación no dependa únicamente de la identificación del usuario, sino también de la condición física del acceso. Esto permite complementar el control de ingreso con una supervisión básica del estado del módulo.

Finalmente, se definió que el sistema debe retornar a un estado inicial estable después de cada evento de autorización, rechazo o advertencia. Este criterio permite que el prototipo quede nuevamente disponible para una nueva operación de acceso, evitando estados indefinidos que puedan afectar la continuidad del funcionamiento.

#### 6.2.1.1. Criterios de uso comunitario

Los criterios de uso comunitario se definieron considerando que el sistema de seguridad está orientado a un módulo contenedor destinado a actividades formativas y productivas para jóvenes del barrio La Isla. Por esta razón, el diseño no debía enfocarse únicamente en el funcionamiento técnico del acceso, sino también en la facilidad de uso, la comprensión del sistema y la apropiación del espacio por parte de la comunidad.

Un primer criterio fue que la operación del sistema debía ser clara e intuitiva para usuarios sin conocimientos técnicos. Esto implica que el proceso de identificación, autorización y respuesta del sistema debe poder comprenderse fácilmente mediante señales visuales o sonoras, evitando secuencias complejas que dificulten el uso cotidiano del módulo.

También se consideró necesario que el sistema apoyara el uso organizado del espacio. Al regular el ingreso de usuarios autorizados, el control de acceso contribuye a establecer una dinámica de administración más ordenada, donde el uso del módulo pueda asociarse a condiciones previamente definidas y no dependa únicamente de supervisión manual.

Otro criterio importante fue promover la corresponsabilidad en el uso del módulo. Al existir un sistema que identifica, valida y responde ante cada intento de ingreso, los usuarios pueden percibir el espacio como un recurso compartido que requiere cuidado, respeto por las normas y uso responsable de los elementos instalados en su interior.

Finalmente, se tuvo en cuenta que el sistema puede integrarse con estrategias que incentiven la participación de los jóvenes. En este sentido, dinámicas como el registro de uso, metas de participación o elementos de gamificación pueden fortalecer la apropiación del espacio, motivar la asistencia continua y promover una relación más activa entre los usuarios y el módulo comunitario [30].

## 6.3. Arquitectura general del sistema

La arquitectura del sistema electrónico de seguridad se definió para organizar las funciones necesarias para el control de acceso al módulo contenedor. El sistema considera la interacción de los usuarios y del administrador, así como los procesos de identificación, procesamiento, monitoreo, actuación y señalización requeridos durante su operación.

La Figura 6.1 presenta el entorno de operación del sistema y su relación con los elementos externos. Los usuarios interactúan con el sistema mediante la información de identificación, mientras que el administrador gestiona los usuarios y las condiciones de acceso. Asimismo, se representa la

interacción con el módulo contenedor, sobre el cual se ejecutan las acciones de apertura, bloqueo y señalización, y con la fuente encargada de suministrar la energía necesaria para el funcionamiento del sistema.

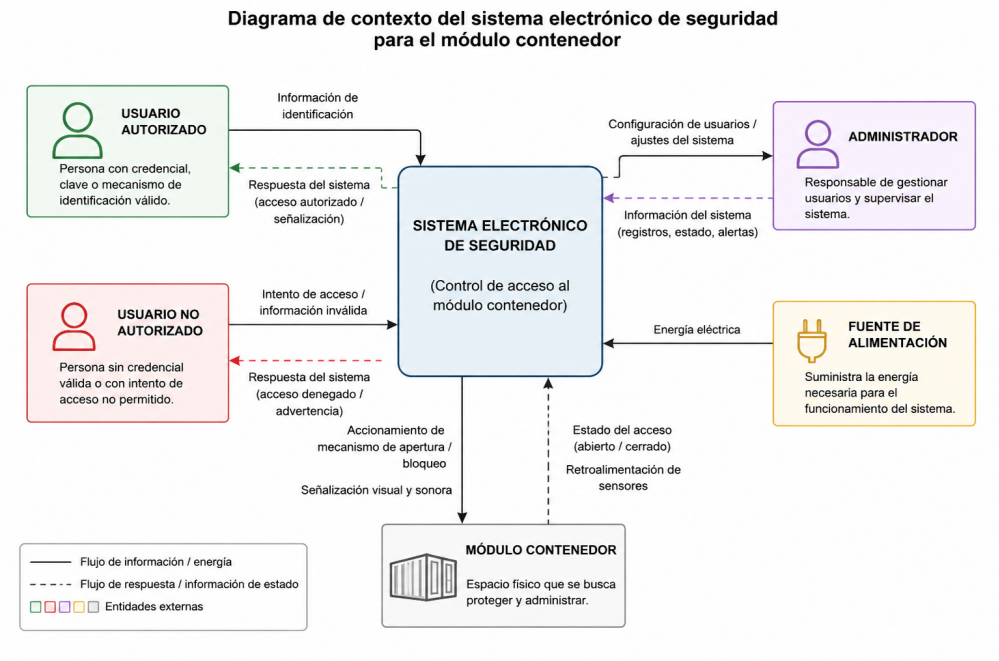


Figura 6.1: Diagrama de contexto del sistema electrónico de seguridad.

La organización funcional del sistema se presenta en la Figura 6.2. Las entradas proporcionan la información correspondiente a la identificación del usuario y al estado del acceso; posteriormente, la unidad de control procesa estas señales de acuerdo con la lógica establecida y genera las acciones correspondientes sobre el mecanismo de apertura o bloqueo y los elementos de señalización. Esta estructura permite establecer claramente el flujo de información entre los diferentes subsistemas antes de realizar su selección e integración física.

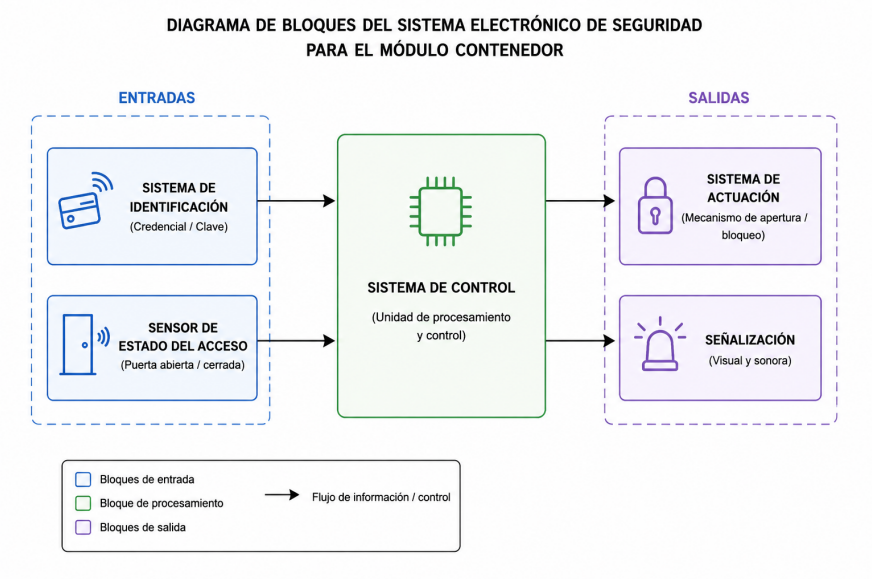


Figura 6.2: Diagrama de bloques del sistema electrónico de seguridad.

## 6.4. Selección de Materiales

La selección de los principales dispositivos del sistema se realizó mediante matrices de evaluación comparativa, en las cuales se analizaron diferentes alternativas disponibles para cada función del prototipo. Para esta comparación se consideraron criterios técnicos y funcionales relacionados con la compatibilidad con el sistema, facilidad de integración, características de operación, disponibilidad y adecuación a los requerimientos definidos previamente. A partir de los resultados obtenidos en cada matriz se seleccionaron los dispositivos con mayor pertinencia para la implementación del prototipo, cuya elección se justifica en los apartados siguientes.

### 6.4.1. Unidad de control

Para la selección de la unidad de control se compararon cuatro alternativas: Arduino Uno, ESP32-C3, Raspberry Pi Pico y LilyGO A7670 ESP32. La evaluación se realizó mediante una matriz de selección considerando cinco criterios relacionados con las necesidades del prototipo: conectividad Wi-Fi, integración de batería de respaldo, posibilidad de expansión hacia LTE y GNSS, capacidad de procesamiento y memoria, y facilidad de implementación e integración. Para cada criterio se asignó una valoración de 0 a 2, donde 0 indica que la alternativa no cumple el criterio, 1 que lo cumple parcialmente y 2 que presenta un cumplimiento favorable.

Cuadro 6.3: Matriz de selección de la unidad de control.

| **Criterio** | **Arduino Uno** | **ESP32-C3** | **Raspberry Pi Pico** | **LilyGO A7670 ESP32** |
|---|---|---|---|---|
| Conectividad Wi-Fi | 0 | 2 | 2 | **2** |
| Integración directa de batería de respaldo | 1 | 1 | 0 | **2** |
| Escalabilidad futura LTE y GNSS | 0 | 0 | 0 | **2** |
| Capacidad de procesamiento y memoria | 1 | 2 | 2 | **2** |
| Facilidad de implementación e integración | 2 | 2 | 1 | 1 |
| **Puntaje total** | **4** | **7** | **5** | **9** |

A partir de la matriz de selección, la LilyGO A7670 ESP32 obtuvo el mayor puntaje, con 9 de 10 puntos posibles. Su elección se relaciona principalmente con la integración de conectividad Wi-Fi, la posibilidad de utilizar una batería de respaldo y la capacidad de expansión hacia funciones de conectividad celular LTE y GNSS, características que ofrecen mayor flexibilidad para el desarrollo y posterior ampliación del sistema. Aunque otras alternativas presentan ventajas en facilidad de implementación, la LilyGO ofrece un conjunto de prestaciones más adecuado para los requerimientos definidos en el proyecto.

La tarjeta incorpora un microcontrolador ESP32 y, de acuerdo con la documentación técnica de LilyGO, las versiones T-A7670E ESP32, T-A7670SA ESP32 y T-A7670G ESP32 emplean un módulo ESP32-WROVER-E con 4 MB de memoria Flash y 8 MB de PSRAM [31]. Estas capacidades son suficientes para ejecutar la lógica de control, gestionar los periféricos conectados y realizar la comunicación requerida para la consulta de usuarios y permisos. En el prototipo desarrollado, la conectividad Wi-Fi se utiliza para establecer la comunicación con la base de datos externa, mientras que las capacidades adicionales de la plataforma permiten considerar futuras ampliaciones sin sustituir la unidad de control.

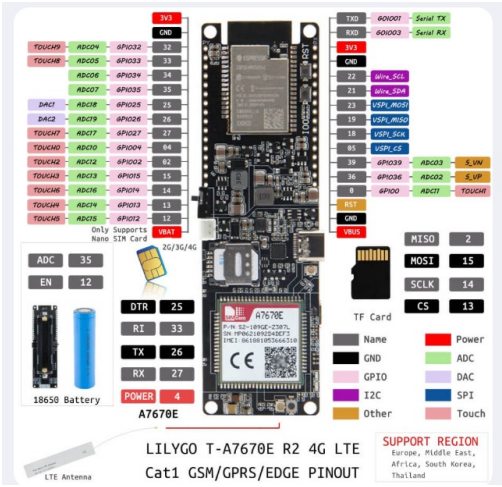


Figura 6.3: Diagrama de conexiones Lilygo T-A7076 ESP32

### 6.4.2. Sistema de identificación

Para seleccionar el mecanismo de identificación se evaluaron cuatro alternativas: teclado matricial, código QR, huella dactilar y RFID. La comparación consideró criterios relacionados con la identificación sin contacto, identificación individual del usuario, integración con el microcontrolador, costo y disponibilidad, y facilidad de uso. Se utilizó una escala de 0 a 2, donde 0 indica que la alternativa no cumple el criterio, 1 que lo cumple parcialmente y 2 que presenta un cumplimiento favorable.

Cuadro 6.4: Matriz de selección del sistema de identificación.

| **Criterio** | **Teclado matricial** | **Código QR** | **Huella dactilar** | **RFID** |
|---|---|---|---|---|
| Identificación sin contacto | 0 | 2 | 2 | **2** |
| Identificación individual | 1 | 2 | 2 | **2** |
| Integración directa con microcontrolador | 2 | 1 | 1 | **2** |
| Bajo costo y disponibilidad | 2 | 1 | 0 | **2** |
| Uso sencillo e intuitivo | 1 | 2 | 2 | **2** |
| **Puntaje total** | **6** | **8** | **7** | **10** |

De acuerdo con la matriz de selección, RFID obtuvo el mayor puntaje, con 10 de 10 puntos posibles. Esta alternativa presentó un cumplimiento favorable en todos los criterios considerados, al permitir una identificación sin contacto mediante credenciales individuales, facilitar su integración con sistemas basados en microcontroladores y ofrecer una solución de bajo costo, disponible y sen-

cilla para el usuario.

Para la implementación se seleccionó el módulo RFID RC522, basado en el integrado MFRC522. Este dispositivo permite leer tarjetas y llaveros de proximidad que operan a una frecuencia de 13,56 MHz y puede comunicarse con la unidad de control mediante interfaz SPI [32]. Cada credencial proporciona un identificador que posteriormente puede ser utilizado por la lógica del sistema para consultar la autorización asociada al usuario. Estas características permitieron incorporar el módulo como mecanismo de identificación dentro del prototipo de control de acceso.


Figura 6.4: Lector RFID RC522

### 6.4.3. Sistema de actuación

Para la selección del mecanismo de actuación se evaluaron cuatro alternativas: cerradura electrónica de 12 V, electroimán de retención, servomotor con pestillo y cerradura mecánica. La comparación consideró criterios relacionados con la integración electrónica, el bloqueo del acceso, el consumo energético, la capacidad de realizar apertura y bloqueo automáticos y la facilidad de implementación en el prototipo. Se utilizó una escala de 0 a 2, donde 0 indica que la alternativa no cumple el criterio, 1 que lo cumple parcialmente y 2 que presenta un cumplimiento favorable.

Cuadro 6.5: Matriz de selección del sistema de actuación.

| Criterio | Cerradura electrónica 12 V | Electroimán de retención | Servomotor con pestillo | Cerradura mecánica |
|---|---|---|---|---|
| Integración con la ESP32 mediante relé | **2** | 2 | 1 | 0 |
| Mantiene el acceso bloqueado sin autorización | **2** | 1 | 1 | 2 |
| Consumo energético solo durante la apertura | **2** | 0 | 2 | 2 |
| Apertura y bloqueo automáticos | **2** | 2 | 1 | 0 |
| Facilidad de implementación en el prototipo | **2** | 1 | 1 | 0 |
| **Puntaje total** | **10** | **6** | **6** | **4** |

De acuerdo con la matriz de selección, la cerradura electrónica de 12 V obtuvo el mayor puntaje, con 10 de 10 puntos posibles. Esta alternativa presentó un cumplimiento favorable en todos los criterios evaluados, especialmente por su capacidad de mantener restringido el acceso mientras no exista una autorización, realizar la apertura mediante una señal de control y consumir energía principalmente durante su accionamiento. Asimismo, su integración mediante una etapa de conmutación permite controlar el mecanismo desde la unidad de procesamiento sin alimentar directamente la carga desde el microcontrolador.

Para la implementación se seleccionó una cerradura electrónica con alimentación de 12 V, diseñada para aplicaciones de control de acceso [33]. Debido a sus requerimientos eléctricos, su activación se realiza mediante un relé y una fuente de alimentación independiente, permitiendo separar la etapa de control de la etapa de potencia. Esta configuración permite que la unidad de control determine la activación del mecanismo sin suministrar directamente la corriente requerida por la cerradura.

Es importante aclarar que la cerradura seleccionada no constituye por sí sola un mecanismo de seguridad física absoluta. Dentro del alcance del prototipo, su función es permitir la validación del control electrónico del acceso, manteniendo el mecanismo restringido mientras no exista una autorización y habilitando su apertura cuando el sistema genera la señal correspondiente. La resistencia frente a intentos de apertura forzada depende de factores adicionales, como las características mecánicas de la cerradura, su forma de instalación y las condiciones estructurales de la puerta. Por esta razón, para una implementación definitiva en el módulo contenedor sería necesario seleccionar y dimensionar un mecanismo de cierre acorde con el nivel de seguridad requerido y con las condiciones reales de instalación.

Figura 6.5: Cerradura Electrónica.

### 6.4.4. Sistema de señalización

Para el sistema de señalización se seleccionaron LED de color rojo y un buzzer con rango de operación entre 5 V y 24 V. Estos elementos cumplen la función de informar al usuario sobre condiciones relevantes del sistema, especialmente eventos de acceso no autorizado, intentos fallidos o activación de una condición de advertencia.

Los LED rojos se emplean como señal visual para indicar estados de alerta o rechazo de acceso. Su uso permite que el usuario identifique de manera inmediata que la autorización no fue válida o que el sistema se encuentra en una condición de advertencia. Para su conexión al sistema de control, cada LED debe incorporar una resistencia limitadora de corriente, con el fin de proteger tanto el indicador como la salida del microcontrolador.

El buzzer se utiliza como señal sonora de alarma ante eventos definidos por la lógica de seguridad, como ingresos no autorizados o acumulación de intentos fallidos. Debido a que su rango de alimentación puede estar entre 5 V y 24 V, su conexión debe realizarse de acuerdo con la tensión seleccionada para el prototipo.

Dentro de la lógica de funcionamiento, la señalización se activa cuando el sistema detecta una condición no autorizada o una alerta. En estos casos, los LED rojos y el buzzer permiten generar una respuesta visible y audible, reforzando la función de seguridad del prototipo y facilitando la interpretación del estado del sistema por parte de los usuarios o responsables del módulo.

## 6.5. Diseño de la lógica de funcionamiento

El diseño de la lógica de funcionamiento se definió con el propósito de establecer la secuencia de operación del sistema electrónico de seguridad desde el estado inicial hasta la respuesta final ante cada evento de acceso. Esta lógica permite que el sistema evalúe la información recibida, determine si el usuario cumple las condiciones de autorización y active la respuesta correspondiente de apertura, bloqueo, señalización o advertencia.

El funcionamiento general del sistema parte de un estado de espera, en el cual el sistema permanece atento a la presentación de una credencial mediante el módulo RFID. Cuando se detecta una tarjeta o llavero, la información leída es enviada al sistema de control, donde se compara con los identificadores previamente definidos como autorizados.

Si la credencial es válida, el sistema activa la cerradura electrónica durante un intervalo determinado para permitir el acceso al módulo. Al mismo tiempo, puede generar una señal visual que indique la autorización del ingreso. Una vez finalizada la secuencia de apertura, el sistema retorna al estado inicial para quedar disponible ante una nueva solicitud de acceso.

En caso de que la credencial no sea válida, el sistema mantiene la cerradura en estado restringido y activa una señal de rechazo mediante los elementos de señalización definidos. Además, la lógica contempla el conteo de intentos fallidos consecutivos, de manera que, al superar el límite establecido, se active una condición de advertencia mediante el buzzer y los LED rojos.

Esta lógica permite estructurar el comportamiento del prototipo de forma ordenada, diferenciando claramente los escenarios de acceso autorizado, acceso no autorizado, advertencia y retorno al estado inicial. De esta manera, el sistema no depende únicamente de una acción manual, sino de una secuencia programada que integra identificación, decisión, actuación y señalización.

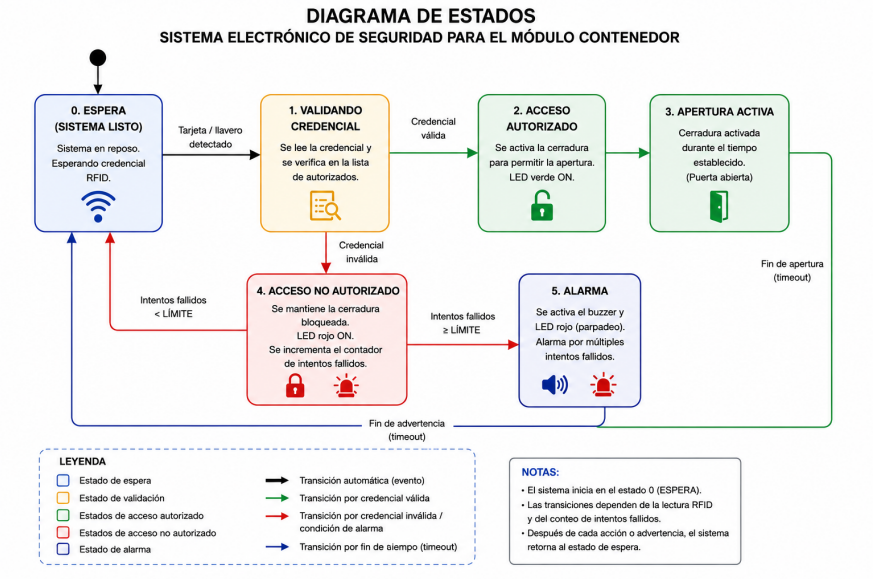


Figura 6.6: Diagrama de estados.

### 6.5.1. Secuencia de operación

### 6.5.2. Diagrama de flujo

El diagrama de flujo presenta la secuencia de operación del sistema electrónico de seguridad desde su inicialización hasta el retorno al estado de espera después de cada evento. Como se observa en la Figura **??**, el sistema permanece inicialmente con el acceso bloqueado mientras espera la lectura de una credencial y supervisa las condiciones definidas para la operación.

Cuando se detecta una credencial, el sistema verifica su autorización. Si el usuario cuenta con permiso vigente, se habilita temporalmente la cerradura electrónica para permitir el ingreso y, posteriormente, el sistema retorna a la condición inicial. Si la credencial no cumple con las condiciones de autorización, el acceso permanece bloqueado, se genera la señalización correspondiente y se incrementa el contador de intentos fallidos. Al alcanzar tres intentos consecutivos, se activa una advertencia mediante el LED rojo y el buzzer antes de restablecer el sistema.

El diagrama permite representar de manera gráfica la lógica general de funcionamiento del prototipo, facilitando la comprensión de las decisiones que toma el sistema ante cada condición de acceso. Su utilización permite sintetizar el comportamiento programado y establecer una referencia clara para la posterior implementación y validación funcional del sistema electrónico de seguridad.

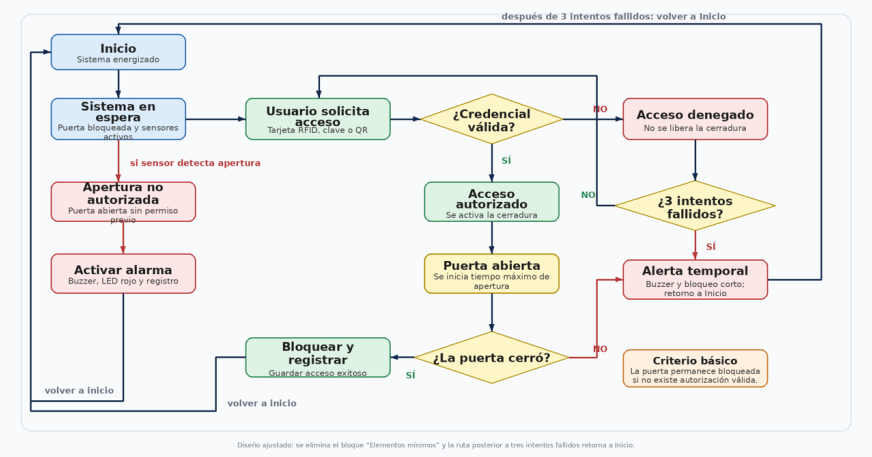


Figura 6.7: Diagrama de flujo.

## 6.6. Proceso de implementación del prototipo

El proceso de implementación del prototipo se planteó como una etapa posterior al diseño funcional y a la selección de los componentes del sistema de seguridad. Su propósito fue integrar progresivamente los elementos definidos, verificar su conexión básica y consolidarlos en una solución electrónica capaz de ejecutar la lógica de control de acceso propuesta.

La implementación se organizó por bloques funcionales, iniciando con la unidad de control y continuando con el sistema de identificación RFID, la etapa de actuación mediante relé y cerradura electrónica, los elementos de señalización y las condiciones de alimentación necesarias para el funcionamiento del conjunto. Esta organización permitió ordenar el montaje, reducir errores de conexión y facilitar la depuración del sistema durante las pruebas iniciales.

Dentro de esta etapa se consideró la conexión física de los componentes, la asignación de pines, la programación de la tarjeta de control y la verificación inicial de las respuestas esperadas ante diferentes eventos de operación. La validación detallada del comportamiento del prototipo se presenta posteriormente en el apartado de resultados, a partir del plan de pruebas definido para el sistema.

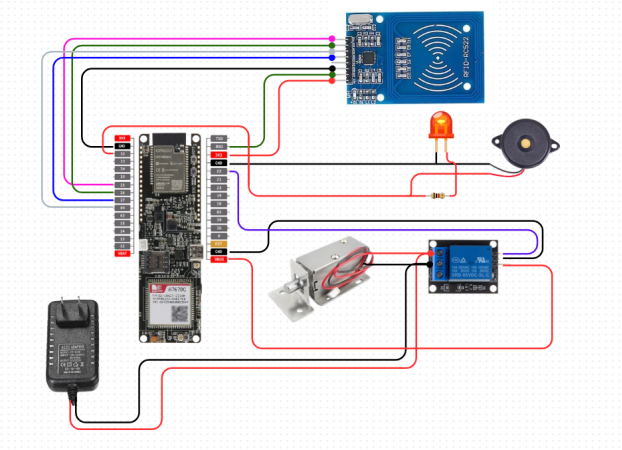

Figura 6.8: Diagrama de conexión del prototipo del sistema electrónico de control de acceso.

En la Figura 6.8 se presenta el diagrama general de conexión del prototipo. En este se observa la integración entre la tarjeta LilyGO A7670 ESP32, el módulo RFID RC522, el relé, la cerradura electrónica de 12 V, el LED rojo, el buzzer y la fuente de alimentación utilizada para la etapa de actuación.

El diagrama permite identificar la separación entre la etapa de control y la etapa de potencia. La ESP32 se encarga de leer la credencial RFID, procesar la lógica de acceso y enviar las señales de control, mientras que la cerradura electrónica es alimentada mediante una fuente externa de 12 V y activada a través del relé. Esta configuración evita que el microcontrolador alimente directamente el actuador y permite un funcionamiento más seguro del sistema.

### 6.6.1. Montaje inicial

El montaje inicial consistió en la conexión básica de la tarjeta LilyGO A7670 ESP32 y la verificación de su alimentación, con el fin de asegurar que la unidad de control pudiera operar de manera estable antes de integrar los demás componentes del sistema. Esta etapa permitió comprobar el encendido de la tarjeta, la comunicación con el computador y la posibilidad de cargar programas de prueba desde el entorno de desarrollo seleccionado.

Durante esta fase se identificaron los pines disponibles para la conexión de los módulos externos, teniendo en cuenta que algunos pines de la tarjeta pueden estar asociados a funciones de alimentación u otros recursos internos. Por esta razón, la asignación de entradas y salidas se realizó de manera preliminar antes de conectar el lector RFID, la cerradura, el LED y el buzzer.

También se verificaron las condiciones básicas de alimentación del prototipo, diferenciando la alimentación de la unidad de control y de los elementos de actuación. Debido a que la cerradura

electrónica opera a 12 V, esta no debe alimentarse directamente desde la tarjeta de control, sino mediante una etapa de conmutación que permita activar la carga de forma segura a partir de una señal lógica.

Una vez confirmada la operación inicial de la tarjeta y la disponibilidad de pines, se procedió a preparar la integración progresiva de los subsistemas. Esta organización permitió reducir errores de conexión y facilitar la revisión individual de cada bloque antes de consolidar el montaje completo del sistema electrónico de seguridad.

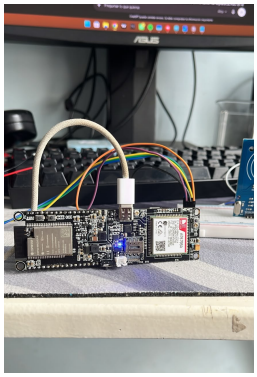

Figura 6.9: Montaje inicial.

### 6.6.2. Integración del sistema de identificación

La integración del sistema de identificación se realizó mediante la conexión del módulo RFID RC522 a la tarjeta LilyGO A7670 ESP32. Este módulo fue incorporado como entrada principal del sistema de seguridad, ya que permite leer tarjetas o llaveros RFID y entregar al sistema de control el identificador asociado a cada credencial.

Para su conexión se consideró la interfaz de comunicación SPI utilizada por el módulo RC522, por lo que fue necesario asignar los pines correspondientes a las señales de comunicación, alimentación y referencia común. Esta asignación se realizó teniendo en cuenta los pines disponibles de la tarjeta de control y evitando interferir con funciones internas propias de la LilyGO A7670 ESP32.

Durante esta etapa se contempló que el módulo RFID funcionara como el primer punto de interacción entre el usuario y el sistema. Cuando una credencial es aproximada al lector, el módulo obtiene su identificador y lo envía al sistema de control, donde posteriormente se compara con los identificadores autorizados dentro de la lógica programada.

La integración de este subsistema permitió establecer la base del proceso de autorización, ya que la decisión de permitir o negar el acceso depende inicialmente de la lectura correcta de la credencial

RFID. Por esta razón, el módulo de identificación fue integrado antes de los elementos de actuación y señalización, asegurando que la lógica de validación pudiera construirse a partir de una entrada definida.

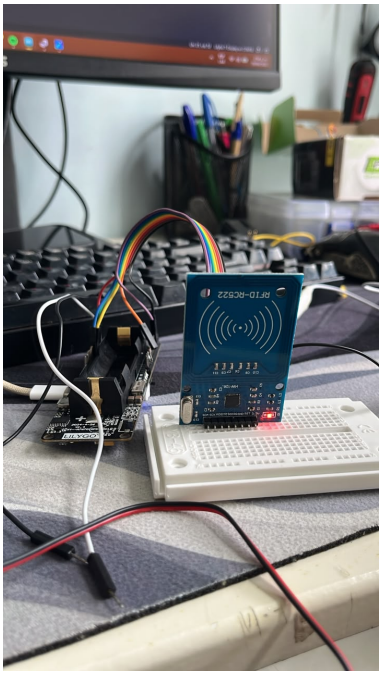


Figura 6.10: Prueba con lector RC522.

### 6.6.3. Integración de señalización

La integración de señalización se realizó con el propósito de comprobar las respuestas visuales y sonoras del sistema ante diferentes condiciones de operación, sin conectar todavía la cerradura electrónica. En esta etapa se incorporaron el LED rojo y el buzzer como elementos encargados de indicar eventos relacionados con acceso denegado, intentos fallidos o estados anómalos del sistema.

Inicialmente, cada elemento de señalización fue probado de forma individual desde la tarjeta de control. El LED rojo se utilizó como indicador visual, mientras que el buzzer permitió generar una señal sonora de advertencia. Estas pruebas permitieron verificar que ambos componentes respondieran correctamente a las señales digitales enviadas desde la LilyGO A7670 ESP32.

Además de la activación de los elementos físicos, se utilizó el monitor serial como herramienta de seguimiento durante las pruebas. A través de este medio se visualizaron mensajes asociados al estado de la puerta, lo que permitió comprobar si el sistema reconocía correctamente condiciones como puerta abierta o puerta cerrada antes de accionar cualquier mecanismo de apertura.

Esta verificación permitió relacionar la lectura del estado de la puerta con las respuestas de señalización del sistema. De esta manera, cuando el sistema detectaba una condición determinada, el monitor serial mostraba el estado correspondiente y, al mismo tiempo, se podía comprobar la activación del LED rojo o del buzzer según la lógica programada.

La integración de señalización permitió validar una parte importante de la lógica de seguridad sin depender todavía del sistema de actuación. Con ello se comprobó que el prototipo podía informar visual y sonoramente sus estados principales, dejando preparada la lógica para su posterior integración con la cerradura electrónica y el control físico del acceso.

### 6.6.4. Integración del sistema de actuación

La integración del sistema de actuación se realizó a partir de la cerradura electrónica de 12 V seleccionada para controlar físicamente la apertura del acceso. Antes de incorporarla al sistema completo, la cerradura se probó de manera independiente con una fuente de alimentación adecuada, con el fin de verificar su funcionamiento básico y confirmar que respondiera correctamente al suministro de tensión.

Esta prueba inicial permitió comprobar que la cerradura ejecutara la acción mecánica esperada antes de conectarla a la lógica de control. De esta manera, se redujo el riesgo de atribuir fallas del actuador al código, al microcontrolador o a los demás componentes del sistema durante la integración general del prototipo.

Después de validar su funcionamiento individual, la cerradura fue integrada al sistema mediante una etapa de conmutación con relé, debido a que no puede ser alimentada directamente desde la tarjeta LilyGO A7670 ESP32. La cerradura requiere una alimentación de 12 V con capacidad de corriente suficiente, por lo que se descartó el uso de un elevador de voltaje, ya que este no entregaba la potencia necesaria para activar correctamente el actuador.

Para su alimentación se consideró el uso de una fuente o transformador de 12 V independiente, mientras que la tarjeta de control únicamente entrega la señal lógica encargada de activar el relé. De esta forma, se separa la etapa de control de la etapa de potencia, protegiendo la tarjeta y permitiendo que la cerradura reciba la energía requerida para su operación.

Dentro de la lógica del sistema, la cerradura permanece en estado restringido mientras no exista una credencial autorizada. Cuando el sistema de control valida un acceso permitido, activa el relé durante un tiempo definido, energizando la cerradura con la fuente de 12 V y permitiendo la apertura del módulo contenedor.

Una vez finalizado el intervalo de apertura, la señal de control se desactiva, el relé abre el circuito de alimentación de la cerradura y el acceso retorna a su condición de bloqueo. Posteriormente, el sistema vuelve al estado inicial de espera, quedando preparado para evaluar una nueva solicitud de acceso.

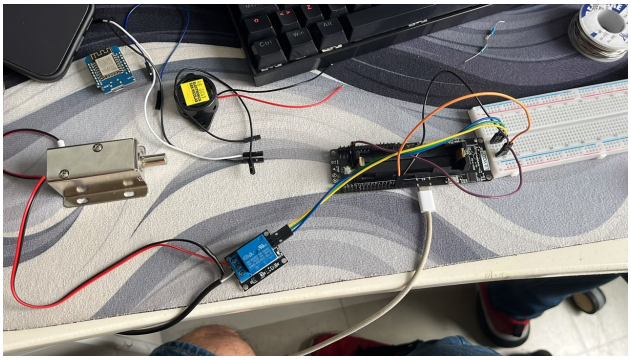

Figura 6.11: Montaje sistema de actuación.

### 6.6.5. Base de datos de usuarios

Para la gestión de usuarios del sistema de control de acceso se planteó el uso de una base de datos organizada en Google Sheets, almacenada en Google Drive. Esta hoja de cálculo permite registrar las credenciales RFID asociadas a cada usuario y definir si una llave se encuentra autorizada, no autorizada o no registrada dentro del sistema.

La selección de Google Sheets se realizó debido a que permite organizar la información en formato tabular, facilitar la edición de usuarios y actualizar los permisos de acceso sin modificar directamente el código cargado en la ESP32. De esta manera, la lista de usuarios autorizados puede administrarse desde una plataforma externa y consultarse durante la operación del prototipo.

La estructura de la base de datos se definió mediante campos básicos como identificador de la llave RFID, nombre o referencia del usuario, estado de autorización y observaciones. El identificador RFID corresponde al código leído por el módulo RC522 cuando el usuario aproxima una tarjeta o llavero al lector. Este dato se utiliza como criterio principal de búsqueda dentro de la hoja de cálculo.

Durante el funcionamiento del sistema, la ESP32 se conecta a una red Wi-Fi y realiza la consulta de la base de datos alojada en Google Sheets. Cuando una credencial es leída por el módulo RFID, el sistema compara el identificador obtenido con los registros disponibles en la hoja de cálculo, determinando si la llave corresponde a un usuario autorizado, a un usuario registrado sin permiso de acceso o a una credencial no registrada.

Si el identificador RFID se encuentra en la base de datos y su estado corresponde a autorizado, el sistema permite la activación del mecanismo de apertura mediante el relé y la cerradura electrónica. Si el identificador aparece registrado pero no cuenta con permiso de acceso, el sistema mantiene la cerradura bloqueada y activa la señalización de rechazo. En caso de que la llave no exista en la base de datos, el sistema la clasifica como no registrada y también niega el acceso.

Esta organización permite diferenciar tres condiciones dentro de la lógica de control: acceso autorizado, acceso denegado por usuario no autorizado y acceso denegado por llave no registrada. Esta diferenciación es importante porque permite que el sistema no solo rechace credenciales inválidas, sino que también distinga entre usuarios registrados sin permiso y llaves completamente desconocidas.

El uso de una base de datos externa también permite proyectar el sistema hacia una administración más flexible, en la cual los permisos puedan actualizarse desde Google Sheets sin intervenir físicamente el prototipo. De esta manera, la base de datos funciona como un componente de apoyo para la lógica de autorización, integrando la identificación RFID con una fuente externa de consulta y gestión de usuarios.

Como ejemplo de la estructura propuesta, la base de datos en Google Sheets se organizó con los campos *uid*, *usuario*, *activo* y *permiso*. El campo *uid* corresponde al identificador leído por el módulo RFID; el campo *usuario* permite asociar la llave con una persona; el campo *activo* indica si la credencial tiene autorización vigente; y el campo *permiso* define el tipo de acceso asignado dentro del sistema.

Cuadro 6.6: Ejemplo de estructura de la base de datos de usuarios en Google Sheets

| **uid** | **USUARIO** | **ACTIVO** | **PERMISO** |
|---|---|---|---|
| 7E1BFA05 | Sergio | NO | CONTENEDOR |
| EC60F105 | Juan | SI | CONTENEDOR |

A partir de esta organización, la ESP32 consulta el identificador RFID leído y lo compara con la columna *uid*. Si el identificador existe y el campo *ACTIVO* se encuentra en 'SI", el sistema permite el acceso según el permiso asignado. Si el identificador existe pero el campo *ACTIVO* se encuentra en 'NO", el sistema reconoce la llave como registrada, pero no habilitada para ingresar. En caso de que el identificador no se encuentre en la hoja de cálculo, la llave se clasifica como no registrada y el acceso permanece bloqueado.

G5 fx

| | A | B | C | D |
|---|---|---|---|---|
| 1 | **uid** | **USUARIO** | **ACTIVO** | **PERMISO** |
| 2 | 7E1BFA05 | Sergio | NO | CONTENEDOR |
| 3 | EC60F105 | Juan | SI | CONTENEDOR |
| 4 | | | | |

Figura 6.12: Base de datos.

### 6.6.6. Integración completa

La integración completa del prototipo se enfocó en consolidar los subsistemas previamente conectados dentro de una operación conjunta, verificando que las entradas, salidas y respuestas del sistema funcionaran de forma coordinada. En esta etapa no se evaluó cada componente de manera aislada, sino la interacción entre ellos dentro de una misma secuencia de control.

Para realizar esta integración, se organizó el cableado final del prototipo y se revisó la correspondencia entre los pines asignados en el código y las conexiones físicas realizadas en la tarjeta de control. Esta revisión permitió evitar conflictos entre señales de entrada, salidas de señalización y activación del relé, especialmente considerando que la cerradura requiere una etapa de potencia independiente.

También se ajustó la lógica general para que el sistema respondiera de manera ordenada ante eventos consecutivos. Por esta razón, se definieron prioridades de funcionamiento, de modo que la validación de credenciales, el monitoreo del estado de la puerta, el conteo de intentos fallidos y la activación de alarmas no generaran respuestas contradictorias durante la operación.

Durante la integración se empleó el monitor serial como herramienta de depuración, permitiendo observar la secuencia interna del sistema mientras se ejecutaban los eventos de prueba. A través de estos mensajes fue posible verificar el paso entre estados, confirmar la lectura de credenciales, revisar el conteo de intentos fallidos y comprobar que las salidas se activaran en el momento correspondiente.

Un aspecto importante de esta etapa fue la coordinación entre la señalización y la actuación. El sistema debía diferenciar claramente entre una advertencia por intento fallido, una alarma por acumulación de intentos no autorizados y una activación válida del mecanismo de apertura. Para ello, se ajustaron los tiempos de activación del LED, el buzzer y el relé, evitando que las respuestas se superpusieran o dificultaran la interpretación del estado del sistema.

Finalmente, la integración completa permitió dejar el prototipo preparado para su validación funcional mediante un plan de pruebas. A partir de esta etapa, el sistema quedó organizado para evaluar escenarios de acceso autorizado, acceso no autorizado, intentos fallidos consecutivos, activación de alarma, apertura controlada y retorno al estado inicial, los cuales se analizan posteriormente

en el apartado de resultados.

Figura 6.13: Integración completa

### 6.6.7. Pruebas con usuarios potenciales

Con el propósito de evaluar la interacción entre los usuarios y el prototipo, se plantean pruebas con personas que presenten características similares a las de los usuarios previstos del sistema. Estas pruebas permitirán identificar dificultades de uso, verificar la comprensión de las funciones disponibles y reconocer posibles mejoras relacionadas con la operación, la accesibilidad y la experiencia de usuario.

La evaluación se realizará mediante escenarios de uso previamente definidos, en los cuales cada participante deberá ejecutar las principales funciones del prototipo siguiendo las instrucciones proporcionadas. Durante el desarrollo de la prueba se observarán aspectos como la correcta ejecución de las tareas, los errores presentados, la necesidad de asistencia y la claridad de los elementos de interacción.

Al finalizar, se escucharán los comentarios de los participantes donde podrán expresar su apreciación sobre el dispositivo, comentando aspectos como la facilidad de uso, la claridad de las instrucciones, la utilidad del sistema y su nivel de satisfacción. La información obtenida será utilizada exclusivamente para evaluar el funcionamiento y la usabilidad del prototipo, sin que estas pruebas

correspondan a una validación comercial o a una implementación definitiva en el contexto de aplicación.

La participación será voluntaria y se informará previamente a cada participante sobre el propósito de la actividad. Asimismo, se evitará recopilar información personal que no sea necesaria para el desarrollo de la evaluación.

## 6.7. Diseño general del sistema energético

El diseño general del sistema energético se desarrolló como un componente complementario del proyecto, con el propósito de proponer una alternativa de alimentación eléctrica para el módulo contenedor. Este apartado no corresponde a una implementación física del sistema fotovoltaico, sino a una aproximación técnica que permite identificar los elementos principales requeridos para una futura instalación.

Para la elaboración del esquema energético se utilizó la aplicación QElectroTech, mediante la cual se representó la conexión general entre los paneles solares, las protecciones eléctricas, el inversor, el medidor bidireccional, la red eléctrica y las cargas internas del contenedor. Esta representación permitió visualizar de manera ordenada la relación entre los componentes del sistema y su posible integración dentro del módulo.

La propuesta se planteó bajo una configuración solar conectada a red, en la cual los paneles solares entregan energía a un inversor *on-grid*. Este inversor permite convertir la energía generada por los paneles en energía utilizable para las cargas del contenedor, manteniendo la posibilidad de apoyo desde la red eléctrica cuando la generación solar no sea suficiente.

Para estimar la carga del sistema se identificaron los consumos eléctricos básicos que podrían estar asociados al funcionamiento del módulo, como iluminación, sistema electrónico de seguridad, cerradura eléctrica, equipos de comunicación y cargas auxiliares de tomacorriente. La energía diaria se calculó multiplicando la potencia de cada carga por el tiempo estimado de uso diario.

Cuadro 6.7: Estimación preliminar de cargas del módulo contenedor

| **Carga considerada** | **Cantidad** | **Potencia estimada** | **Tiempo de uso** | **Energía diaria** |
|---|---|---|---|---|
| Sistema electrónico de seguridad | 1 | 0,7 W | 24 h | 16,8 Wh |
| Cerradura electrónica de 12 V | 1 | 12 W | 0,1 h | 1,2 Wh |

| Carga considerada | Cantidad | Potencia estimada | Tiempo de uso | Energía diaria |
|---|---|---|---|---|
| Iluminación LED interna | 4 | 18 W | 6 h | 432 Wh |
| Equipo de comunicación | 1 | 10 W | 8 h | 80 Wh |
| Equipo de apoyo | 1 | 300 W | 4 h | 1200 Wh |
| Carga auxiliar de tomacorriente | 1 | 200 W | 2 h | 400 Wh |
| **Total estimado** | – | – | – | **2129,5 Wh** |

A partir de la estimación anterior, la demanda diaria aproximada del módulo corresponde a 2129,5 Wh, equivalente a 2,12 kWh/día. Este valor se tomó como referencia preliminar para orientar la selección general de los elementos del sistema energético, sin que represente un dimensionamiento definitivo de instalación.

El diseño también contempló la inclusión de protecciones en corriente continua y corriente alterna, con el fin de representar una conexión más segura entre los paneles solares, el inversor, las cargas internas y la red eléctrica. Entre estos elementos se consideraron fusibles, seccionadores, protecciones contra sobretensiones e interruptores de protección general.

Finalmente, se aclara que el sistema energético propuesto tiene un carácter preliminar y documental dentro del proyecto. Por esta razón, cualquier implementación física futura deberá ser revisada por personal competente, considerando las condiciones reales del sitio, la carga definitiva del contenedor, la normativa aplicable y los criterios de seguridad eléctrica correspondientes.

Capítulo 7

# Resultados y Discusión

En este capítulo se presentan los resultados obtenidos a partir del desarrollo del sistema electrónico de seguridad y del diseño general del sistema energético propuesto para el módulo contenedor. La información se organiza con base en el proceso de implementación, el plan de pruebas definido y el análisis de los datos obtenidos durante la verificación funcional del prototipo.

Los resultados del sistema de seguridad se obtuvieron mediante pruebas controladas orientadas a comprobar el comportamiento de los subsistemas de identificación, monitoreo, señalización y actuación. Estas pruebas permitieron evaluar la respuesta del prototipo ante escenarios como acceso autorizado, acceso no autorizado, intentos fallidos consecutivos, activación de alarma, apertura controlada y retorno al estado inicial.

Además de los resultados experimentales asociados al funcionamiento del prototipo, se incluyen resultados empíricos derivados de la observación directa del comportamiento del sistema durante las pruebas. También se consideran resultados documentales y teóricos relacionados con la selección de componentes, el diseño energético, la estimación de cargas y el dimensionamiento general de la alimentación eléctrica del módulo.

El análisis de los resultados se presenta mediante descripciones técnicas, tablas, fotografías, diagramas y demás figuras de apoyo, con el fin de facilitar la interpretación de la información obtenida. De esta manera, el capítulo permite relacionar el diseño planteado con el comportamiento observado del prototipo y con los criterios definidos para la solución propuesta.

## 7.1. Plan de pruebas sistema de seguridad

### 7.1.1. Objetivo del plan de pruebas

El objetivo del plan de pruebas fue verificar el funcionamiento del prototipo electrónico de seguridad bajo escenarios controlados, con el fin de comprobar que los subsistemas de identificación, monitoreo, señalización y actuación respondieran de acuerdo con la lógica de control definida durante el diseño.

Este plan permitió evaluar si el sistema era capaz de diferenciar entre credenciales autorizadas y no autorizadas, activar la cerradura electrónica únicamente cuando existiera una autorización válida, generar señales visuales y sonoras ante eventos de rechazo o alarma, y retornar al estado inicial

después de cada operación.

Asimismo, el plan de pruebas buscó comprobar el comportamiento del sistema frente a condiciones específicas de seguridad, como intentos fallidos consecutivos, activación temporal de alarma y verificación del estado de la puerta. De esta manera, las pruebas permitieron obtener evidencia funcional sobre la respuesta del prototipo antes de analizar su desempeño en el apartado de resultados.

### 7.1.2. Condiciones generales de prueba

Las pruebas del prototipo se realizaron bajo condiciones controladas, con el fin de verificar el comportamiento funcional del sistema electrónico de seguridad antes de considerar su aplicación en un entorno real. Para ello, el montaje se mantuvo energizado de forma estable y se evaluó la respuesta del sistema ante eventos definidos previamente, evitando variaciones externas que pudieran afectar la interpretación de los resultados.

El sistema de control estuvo conformado por la tarjeta LilyGO A7670 ESP32, programada desde el entorno de desarrollo seleccionado y conectada al computador para el seguimiento mediante el monitor serial. Esta herramienta permitió visualizar mensajes relacionados con la lectura de credenciales RFID, la consulta de permisos, el conteo de intentos fallidos, la activación de salidas, el estado del relé y el retorno del sistema a la condición inicial.

La validación se organizó mediante una matriz de pruebas funcionales repetibles. En total se emplearon 4 credenciales RFID, distribuidas entre credenciales autorizadas, credenciales registradas sin permiso activo y credenciales no registradas en la base de datos. Cada escenario de prueba se ejecutó de forma individual y se repitió 50 veces, con el propósito de verificar la consistencia de la respuesta del prototipo y reducir la posibilidad de concluir el funcionamiento del sistema a partir de un único evento de prueba.

Para cada evento evaluado se registró la respuesta esperada, la respuesta obtenida, el estado del relé, el estado de la cerradura electrónica, la activación de los elementos de señalización, el mensaje mostrado en el monitor serial y la condición final del sistema. Adicionalmente, cuando aplicó, se registró el tiempo de respuesta entre la lectura de la credencial RFID y la activación o rechazo del acceso, con el fin de contar con una medida cuantitativa del comportamiento del sistema.

Para las pruebas de identificación se utilizaron credenciales RFID con diferentes condiciones de autorización. Las credenciales autorizadas permitieron verificar la apertura controlada del acceso; las credenciales registradas sin permiso activo permitieron comprobar la negación de ingreso a usuarios deshabilitados; y las credenciales no registradas permitieron evaluar el comportamiento del sistema ante intentos de acceso no reconocidos.

Cuadro 7.1: Condiciones generales de validación funcional del prototipo

| **Aspecto evaluado** | **Condición definida** | **Evidencia de verificación** |
|---|---|---|
| Entorno de prueba | Pruebas realizadas bajo condiciones controladas, con el prototipo energizado de forma estable y sin variaciones externas intencionales durante la ejecución de los escenarios. | Observación directa del montaje y registro de ejecución de pruebas. |
| Unidad de control | Uso de la tarjeta LilyGO A7670 ESP32 como unidad central del sistema, encargada de procesar la lectura RFID, consultar permisos y activar las salidas correspondientes. | Mensajes del monitor serial y respuesta física del sistema. |
| Credenciales RFID | Uso de 4 credenciales RFID distribuidas entre credenciales autorizadas, credenciales registradas sin permiso activo y credenciales no registradas. | Lectura del UID en el monitor serial y comparación con la base de datos. |
| Variables observadas | Estado del relé, activación de la cerradura, señalización mediante LED rojo, activación del buzzer, mensaje en monitor serial y retorno al estado inicial. | Observación física del prototipo, capturas del monitor serial y fotografías del montaje. |
| Tiempo de respuesta | Cuando aplicó, se registró el tiempo entre la lectura de la credencial RFID y la activación o rechazo del acceso. | Registro temporal generado desde el sistema y verificación en monitor serial. |
| Sistema de actuación | La cerradura electrónica de 12 V fue alimentada mediante un transformador independiente y activada a través de un relé controlado por la ESP32. | Activación controlada del relé y comprobación física del estado de la cerradura. |
| Señalización | El LED rojo y el buzzer se utilizaron para diferenciar eventos de advertencia, acceso denegado y alarma por intentos fallidos consecutivos. | Observación directa de la activación visual y sonora durante cada escenario. |
| Base de datos | Se verificó la modificación de permisos desde Google Sheets mediante activación, desactivación, adición y retiro de credenciales. | Capturas de la base de datos, lectura RFID posterior al cambio y respuesta del sistema. |
| Retorno seguro | Después de cada evento de acceso autorizado, rechazo o alarma, el sistema debía regresar al estado de espera y quedar disponible para una nueva lectura RFID. | Mensaje de estado inicial en monitor serial y verificación de nueva lectura. |

Cada credencial fue aproximada al módulo RFID RC522 y la respuesta obtenida fue observada tanto en los elementos físicos del prototipo como en los mensajes generados por el monitor serial.

Los elementos de señalización estuvieron conformados por el LED rojo y un buzzer, utilizados para representar estados de advertencia, acceso denegado y alarma. Estas salidas permitieron observar de forma directa la respuesta del sistema ante eventos no autorizados y verificar la diferencia entre un aviso breve por intento fallido y una alarma repetitiva después de alcanzar el límite de intentos definido.

La cerradura electrónica de 12 V se alimentó mediante un transformador independiente y fue activada a través de un relé controlado por la tarjeta ESP32. Esta configuración permitió separar la etapa de control de la etapa de potencia, evitando que la cerradura fuera alimentada directamente desde el microcontrolador y garantizando que recibiera la energía necesaria para su operación. Durante las pruebas se verificó que la cerradura se activara únicamente ante una credencial autorizada y que permaneciera bloqueada ante credenciales no autorizadas, inactivas o no registradas.

También se evaluó la actualización de permisos desde la base de datos externa en Google Sheets. Para ello, se realizaron cambios en el estado de algunas credenciales, agregando, desactivando o retirando registros, y posteriormente se presentó la credencial correspondiente ante el lector RFID. Esta prueba permitió comprobar que la respuesta del prototipo dependiera de la información vigente en la base de datos y no únicamente de valores fijos cargados en el código del microcontrolador.

Durante las pruebas se mantuvo una secuencia de evaluación ordenada, iniciando con el sistema en estado de espera y ejecutando cada escenario de forma individual. Después de cada evento, se verificó que el prototipo retornara al estado inicial, permitiendo repetir la prueba y comparar el comportamiento obtenido con la respuesta esperada. La evidencia de verificación estuvo compuesta por observación directa del montaje, capturas del monitor serial, registro de eventos de prueba, fotografías del prototipo y comprobación física del estado de la cerradura.

### 7.1.3. Escenarios de prueba

Los escenarios de prueba se definieron con el propósito de evaluar el comportamiento del prototipo ante las condiciones principales de operación del sistema electrónico de seguridad. Cada escenario permitió verificar una parte específica de la lógica de control, considerando la identificación de usuarios, la respuesta ante accesos autorizados y no autorizados, la activación de señalización, el conteo de intentos fallidos, el accionamiento de la cerradura, la actualización de permisos desde la base de datos y el retorno al estado inicial.

Las pruebas se organizaron de manera secuencial, iniciando con la verificación del estado de

espera del sistema y continuando con eventos de acceso permitido, acceso rechazado, actualización de permisos y condiciones de alarma. Esta organización permitió comprobar que el prototipo respondiera de forma ordenada ante cada evento y que las salidas físicas coincidieran con los mensajes observados mediante el monitor serial.

Cuadro 7.2: Escenarios definidos para la validación funcional del prototipo

| **Escenario de prueba** | **Acción realizada** | **Respuesta esperada** |
|---|---|---|
| Estado inicial del sistema | Energizar el prototipo y observar su condición de arranque. | El sistema debe iniciar en estado de espera, sin activar la cerradura, el relé, el buzzer ni la señal de alarma. |
| Lectura de credencial autorizada | Aproximar al lector RFID una tarjeta o llavero registrado en la base de datos con permiso activo. | El sistema debe reconocer la credencial, activar el relé y habilitar la cerradura durante el tiempo definido. |
| Lectura de credencial registrada sin permiso activo | Aproximar al lector RFID una tarjeta o llavero registrado en la base de datos, pero con el permiso desactivado. | El sistema debe reconocer que la credencial existe, negar el acceso, mantener la cerradura bloqueada y activar la señalización de rechazo. |
| Lectura de credencial no registrada | Aproximar al lector RFID una tarjeta o llavero cuyo UID no se encuentre registrado en la base de datos. | El sistema debe clasificar la credencial como no registrada, denegar el acceso, mantener el relé desactivado y conservar la cerradura bloqueada. |
| Activación de alarma por intentos fallidos | Completar tres intentos fallidos consecutivos. | El sistema debe activar el LED rojo y el buzzer de forma repetida durante un tiempo determinado, diferenciando esta alarma del aviso breve por intento fallido. |
| Activación de cerradura electrónica | Validar una credencial autorizada y observar la respuesta del relé y de la cerradura. | El relé debe activar la alimentación de la cerradura de 12 V durante el tiempo definido para permitir la apertura. |

| Escenario de prueba | Acción realizada | Respuesta esperada |
|---|---|---|
| Actualización de permiso en base de datos | Modificar en Google Sheets el estado de una credencial registrada, cambiando su condición de activa a inactiva o de inactiva a activa. | El sistema debe responder de acuerdo con el permiso vigente en la base de datos durante la siguiente lectura RFID, sin requerir reprogramación de la ESP32. |
| Adición de nueva credencial | Registrar en Google Sheets un nuevo UID con usuario, estado activo y permiso asignado. | El sistema debe reconocer la nueva credencial en la siguiente lectura y permitir o negar el acceso según el permiso definido. |
| Retiro de acceso a una credencial | Desactivar el campo de permiso o retirar el registro asociado a una credencial previamente autorizada. | El sistema debe negar el acceso en la siguiente lectura, mantener la cerradura bloqueada y generar la señalización de rechazo correspondiente. |
| Retorno al estado inicial | Finalizar una secuencia de acceso autorizado, acceso denegado, actualización de permiso o alarma. | El sistema debe desactivar las salidas correspondientes, restablecer las condiciones necesarias y volver al estado de espera para una nueva lectura RFID. |

Los escenarios definidos permitieron cubrir las funciones principales del prototipo y establecer una base ordenada para la validación funcional. A partir de estas pruebas fue posible comparar la respuesta esperada con el comportamiento observado, verificando si cada subsistema actuaba correctamente dentro de la lógica general del sistema de seguridad. Además, la inclusión de escenarios asociados a permisos activos, permisos inactivos, credenciales no registradas y actualización desde la base de datos permitió evaluar no solo la apertura física del acceso, sino también la capacidad del sistema para administrar diferentes condiciones de autorización.

### 7.1.4. Criterios de aceptación

Los criterios de aceptación se definieron para establecer las condiciones mínimas que debía cumplir el prototipo durante las pruebas funcionales. Estos criterios permitieron comparar la respuesta esperada con el comportamiento observado, determinando si cada escenario de prueba podía considerarse satisfactorio dentro de la lógica de control propuesta.

Para considerar una prueba como aceptada, el sistema debía ejecutar la respuesta correspondiente sin generar activaciones indebidas, errores de secuencia o estados indefinidos. La validación se realizó observando el comportamiento físico de los componentes, los mensajes mostrados en el monitor serial y la respuesta de la cerradura, el relé, el LED rojo y el buzzer. Adicionalmente, se consideraron criterios cuantitativos asociados a repetibilidad, ausencia de falsas aperturas, tiempo de respuesta y retorno seguro al estado inicial.

Estos criterios permitieron establecer una base objetiva para analizar los resultados de las pruebas. De esta manera, cada escenario evaluado pudo clasificarse según el cumplimiento de la respuesta esperada, facilitando la identificación de comportamientos correctos, ajustes necesarios o posibles fallas durante la operación del prototipo. La inclusión de criterios asociados a falsas aperturas, actualización de permisos, tiempo de respuesta y repetibilidad permitió fortalecer la validación funcional del sistema más allá de una comprobación básica de apertura y cierre.

## 7.2. Resultados de implementación del prototipo

En este apartado se presentan los resultados obtenidos durante la implementación y evaluación del prototipo, considerando las pruebas realizadas sobre sus componentes, funciones y operación general. Estos resultados permiten evidenciar el cumplimiento de los requerimientos definidos y verificar el funcionamiento integrado del sistema. Como complemento, en los anexos se incluye un enlace a material audiovisual en el que se registra el funcionamiento del prototipo durante cada una de las pruebas efectuadas.

### 7.2.1. Montaje físico del sistema

El montaje físico del sistema electrónico de seguridad se realizó integrando los componentes principales del prototipo en una configuración funcional y organizada, con el propósito de verificar la operación conjunta entre la unidad de control, el sistema de identificación, los elementos de señalización y la etapa de actuación. El montaje incluyó la tarjeta LilyGO A7670 ESP32, el módulo RFID RC522, el relé de activación, la cerradura electrónica de 12 V, los LED rojos, el buzzer y el transformador utilizado para alimentar la cerradura.

La disposición física del prototipo permitió reducir interferencias entre las conexiones de control y potencia, facilitar la observación de los estados del sistema durante las pruebas y comprobar la respuesta de cada subsistema de manera ordenada. Esta organización fue necesaria para validar que la activación de la cerradura dependiera únicamente de una credencial autorizada y que, ante credenciales inactivas, no registradas o rechazadas, el sistema mantuviera el acceso bloqueado.

El montaje permitió comprobar que los componentes quedaran correctamente integrados y que

cada subsistema respondiera de acuerdo con la lógica programada. Las pruebas realizadas sobre el montaje físico evidenciaron que el lector RFID reconoció las credenciales evaluadas, el sistema diferenció accesos autorizados, usuarios sin permiso activo y credenciales no registradas, los LED y el buzzer se activaron según las condiciones definidas, y el relé accionó la cerradura únicamente cuando se presentó una autorización válida.

Asimismo, se verificó que el sistema retornara al estado inicial después de cada evento de operación, manteniendo la cerradura bloqueada cuando no existía una autorización válida. Este comportamiento permitió confirmar que el montaje físico funcionaba de manera coherente con la lógica de control planteada para el prototipo y que las salidas físicas coincidían con los estados reportados mediante el monitor serial.

El resultado de esta etapa fue un prototipo funcional integrado, capaz de ejecutar las acciones principales del sistema de seguridad bajo condiciones controladas. La evidencia visual del montaje físico se presenta mediante fotografías del sistema ensamblado, las cuales permiten observar la disposición general de los componentes, la integración de la cerradura y la conexión entre la etapa de control y la etapa de actuación.

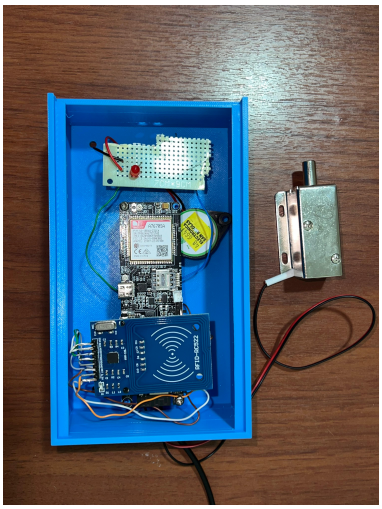

Figura 7.1: Integración de componentes del prototipo de control de acceso.

Figura 7.2: Verificación de la cerradura electrónica durante la prueba funcional.

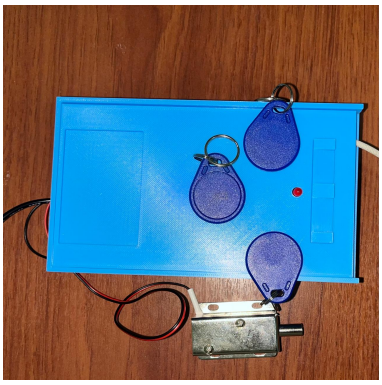

Figura 7.3: Integración de componentes con caja de protección.

### 7.2.2. Integración de componentes

La integración de componentes permitió consolidar el prototipo electrónico de seguridad como un sistema funcional, en el cual cada elemento cumplió una función específica dentro de la lógica de control de acceso. La tarjeta LilyGO A7670 ESP32 operó como unidad central, recibiendo la información del módulo RFID RC522 y generando las señales de salida para la activación del relé, la cerradura electrónica, el LED rojo y el buzzer.

Como resultado de la integración, se comprobó que los componentes trabajaron de manera coordinada durante las pruebas funcionales. El sistema reconoció correctamente las credenciales RFID autorizadas, rechazó las credenciales no registradas, activó las señales de advertencia según la condición evaluada y accionó la cerradura únicamente cuando se presentó una autorización válida.

La etapa de actuación funcionó correctamente mediante la separación entre control y potencia. La ESP32 entregó la señal lógica al relé, mientras que la cerradura electrónica de 12 V recibió alimentación desde un transformador independiente. Esta configuración permitió activar el meca-

nismo de apertura sin exigir corriente directamente al microcontrolador, evitando fallas por falta de potencia en el actuador.

Los elementos de señalización también se integraron de forma satisfactoria. El LED rojo y el buzzer permitieron diferenciar los eventos de acceso no autorizado y alarma por intentos fallidos consecutivos. En el caso de un intento fallido individual, el sistema generó una advertencia breve; mientras que, al alcanzar tres intentos consecutivos no autorizados, se activó una alarma repetitiva durante un tiempo determinado.

En general, la integración de componentes fue exitosa, ya que no se presentaron fallas que impidieran la ejecución de la lógica principal del sistema. El prototipo logró mantener el acceso bloqueado ante credenciales no autorizadas, habilitar la cerradura ante credenciales válidas, activar las señales de advertencia correspondientes y retornar al estado inicial después de cada evento evaluado.

## 7.3. Resultados de pruebas funcionales

### 7.3.1. Prueba de acceso autorizado

La prueba de acceso autorizado se realizó con el propósito de verificar que el sistema permitiera la apertura únicamente cuando se presentara una credencial RFID registrada con permiso activo en la base de datos. Esta prueba permitió comprobar la relación entre el sistema de identificación, la consulta de autorización, la activación del relé y el accionamiento de la cerradura electrónica de 12 V.

Para ejecutar la prueba, el prototipo se mantuvo inicialmente en estado de espera, con la cerradura bloqueada, el relé desactivado y sin señales de alarma activas. Posteriormente, se aproximó al lector RFID RC522 una credencial previamente registrada en Google Sheets con estado activo y permiso de acceso al contenedor. Al detectar la credencial, la tarjeta LilyGO A7670 ESP32 realizó la lectura del identificador, consultó la condición asociada en la base de datos y generó la respuesta correspondiente según la lógica de autorización definida.

La prueba se repitió 25 veces con credenciales autorizadas, con el fin de verificar la consistencia del comportamiento del sistema y evitar que la validación dependiera de un único evento de lectura. En cada repetición se registró la detección RFID, la respuesta de autorización, el estado del relé, la activación de la cerradura, la señalización generada, el mensaje observado en el monitor serial y el retorno del sistema al estado inicial.

Como resultado, el sistema reconoció correctamente la credencial autorizada y activó el relé encargado de alimentar la cerradura electrónica. Durante el intervalo definido en la programación, la cerradura recibió alimentación de 12 V desde el transformador independiente, permitiendo la apertura del acceso. Finalizado este tiempo, el relé se desactivó y el sistema retornó al estado inicial

de espera, quedando disponible para una nueva lectura RFID.

Cuadro 7.3: Resultado de la prueba de acceso autorizado

| **Elemento evaluado** | **Respuesta esperada** | **Resultado obtenido** |
|---|---|---|
| Lectura RFID | El lector debe detectar la credencial autorizada. | La credencial fue detectada correctamente por el módulo RFID RC522. |
| Consulta de autorización | El sistema debe consultar el UID leído y verificar que la credencial se encuentre activa en la base de datos. | La ESP32 identificó la credencial como registrada y con permiso activo. |
| Validación de credencial | El sistema debe clasificar la credencial como autorizada. | El sistema generó la condición de acceso permitido según la información registrada en Google Sheets. |
| Activación del relé | El relé debe activarse únicamente después de validar la credencial autorizada. | El relé se activó correctamente después de la validación del permiso. |
| Accionamiento de cerradura | La cerradura debe recibir alimentación de 12 V durante el tiempo definido. | La cerradura se energizó correctamente mediante el transformador independiente y permitió la apertura. |
| Tiempo de respuesta | El intervalo entre la lectura RFID y la activación del relé debe mantenerse dentro del tiempo esperado para la operación del sistema. | El tiempo de respuesta registrado fue de 4 s aproximadamente. |
| Repeticiones ejecutadas | El comportamiento debe mantenerse consistente durante las repeticiones realizadas con credenciales autorizadas. | Se realizaron 25 repeticiones, de las cuales 25 presentaron activación correcta de la cerradura. |

| Elemento evaluado | Respuesta esperada | Resultado obtenido |
|---|---|---|
| Activaciones indebidas | No debe presentarse activación del relé ni de la cerradura antes de la validación de una credencial autorizada. | No se observaron activaciones indebidas durante el estado de espera ni antes de la validación RFID. |
| Retorno al estado inicial | El sistema debe desactivar el relé y quedar disponible para una nueva lectura. | El relé se desactivó después del tiempo definido y el sistema retornó correctamente al estado de espera. |

La prueba fue satisfactoria, ya que el sistema respondió de acuerdo con la lógica de control definida para un acceso autorizado. La cerradura solo se activó después de reconocer una credencial registrada con permiso activo, y no se presentaron activaciones indebidas durante el estado de espera. Esto permitió confirmar que el mecanismo de apertura quedó condicionado correctamente a la validación RFID y a la información vigente en la base de datos.

La ESP32 no alimentó directamente la cerradura, sino que activó el relé mediante una señal lógica, mientras que el transformador suministró la energía necesaria para el actuador. Esta configuración permitió que la cerradura funcionara de manera estable durante las repeticiones de la prueba.

En términos funcionales, este resultado demuestra que el prototipo cumple con la condición principal de acceso autorizado: identificar una credencial válida, consultar su estado de autorización, activar el mecanismo de apertura durante un tiempo determinado y retornar automáticamente al estado inicial. La evidencia de esta prueba se soportó mediante observación directa del montaje, respuesta física de la cerradura, mensajes del monitor serial y registro de los eventos ejecutados durante la validación.

### 7.3.2. Prueba de acceso no autorizado

La prueba de acceso no autorizado se realizó con el propósito de verificar que el sistema mantuviera restringido el acceso cuando se presentara una credencial RFID sin autorización vigente. Esta condición incluyó credenciales no registradas en la base de datos y credenciales registradas sin permiso activo. La prueba permitió comprobar que la lógica de control negara correctamente el ingreso, evitara la activación de la cerradura electrónica y generara una señal de advertencia ante una condición de acceso rechazado.

Para ejecutar la prueba, el prototipo se mantuvo inicialmente en estado de espera, con la cerra-

dura bloqueada, el relé desactivado y sin señales de alarma activas. Posteriormente, se aproximaron al lector RFID RC522 credenciales que no cumplían la condición de autorización. Al detectar cada credencial, la tarjeta LilyGO A7670 ESP32 realizó la lectura del identificador, consultó su condición en la base de datos y generó la respuesta correspondiente según la lógica de validación definida.

La prueba se repitió 25 veces con credenciales no autorizadas, con el fin de verificar que el sistema mantuviera un comportamiento consistente ante intentos de ingreso no permitidos. En cada repetición se registró la lectura RFID, la condición de autorización, el estado del relé, el estado de la cerradura, la señalización generada, el mensaje observado en el monitor serial y el retorno del sistema al estado inicial.

Como resultado, el sistema identificó correctamente las credenciales sin autorización vigente y mantuvo la cerradura en estado bloqueado. En esta condición, el relé no fue activado, por lo que la cerradura electrónica de 12 V no recibió alimentación desde el transformador. De esta manera, se comprobó que una credencial no autorizada no genera apertura ni desbloqueo del acceso.

Además de negar el acceso, el sistema activó una señal breve de advertencia mediante los elementos de señalización definidos. Esta respuesta permitió diferenciar el acceso rechazado de un estado normal de espera, indicando que la credencial presentada no fue aceptada. El evento también fue observado mediante el monitor serial, donde se evidenció la lectura de la credencial y el mensaje asociado al acceso denegado.

Cuadro 7.4: Resultado de la prueba de acceso no autorizado

| **Elemento evaluado** | **Respuesta esperada** | **Resultado obtenido** |
|---|---|---|
| Lectura RFID | El lector debe detectar la credencial presentada. | La credencial fue detectada correctamente por el módulo RFID RC522. |
| Consulta de autorización | El sistema debe consultar el UID leído y verificar que la credencial no cuenta con autorización vigente. | La ESP32 identificó la credencial como no autorizada, inactiva o no registrada, según la información disponible en la base de datos. |
| Validación de credencial | El sistema debe clasificar la credencial como no autorizada. | El sistema generó la condición de acceso denegado. |

| **Elemento evaluado** | **Respuesta esperada** | **Resultado obtenido** |
|---|---|---|
| Estado del relé | El relé debe permanecer desactivado ante una credencial sin autorización vigente. | El relé permaneció desactivado durante la prueba. |
| Accionamiento de cerradura | La cerradura no debe recibir alimentación ni habilitar la apertura. | La cerradura permaneció bloqueada y no recibió alimentación de 12 V. |
| Señalización del rechazo | El sistema debe generar una advertencia breve ante el acceso denegado. | El LED rojo y/o el buzzer se activaron según la lógica programada para indicar el rechazo. |
| Monitor serial | El sistema debe mostrar el evento de acceso no autorizado. | El monitor serial permitió observar la lectura de la credencial y el mensaje asociado al acceso denegado. |
| Falsas aperturas | No debe presentarse activación del relé ni de la cerradura ante credenciales no autorizadas, inactivas o no registradas. | Se registraron 0 falsas aperturas durante las repeticiones ejecutadas. |
| Repeticiones ejecutadas | El sistema debe mantener el rechazo de acceso de forma consistente durante las repeticiones realizadas. | Se realizaron 25 repeticiones, de las cuales 25 mantuvieron la cerradura bloqueada correctamente. |
| Retorno al estado inicial | El sistema debe quedar disponible para una nueva lectura RFID después del aviso de rechazo. | Después del aviso breve, el sistema retornó correctamente al estado de espera. |

La prueba fue satisfactoria, ya que el sistema respondió de acuerdo con la lógica definida para un acceso no autorizado. La cerradura no se activó, el relé permaneció desactivado y el sistema generó una señal de advertencia sin comprometer el estado de bloqueo del acceso.

Este resultado permitió confirmar que el prototipo diferencia entre una credencial autorizada y una credencial sin autorización vigente. Además, evidenció que el mecanismo de apertura se mantiene condicionado a la validación RFID y a la información registrada en la base de datos, evitando activaciones indebidas ante intentos de ingreso no permitidos.

En términos funcionales, la prueba demuestra que el sistema cumple con la condición de seguridad asociada al rechazo de usuarios no autorizados. La evidencia de esta prueba se soportó mediante observación directa del montaje, estado físico de la cerradura, mensajes del monitor serial, señalización del rechazo y registro de los eventos ejecutados durante la validación.

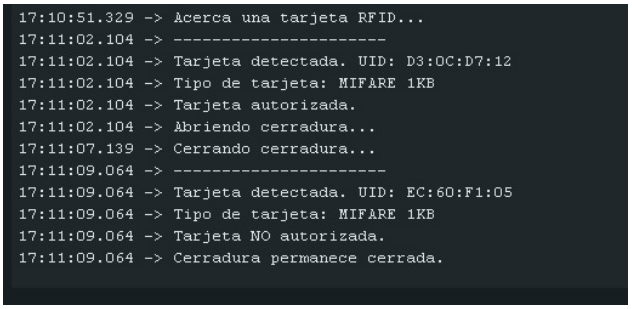


Figura 7.4: Registro en monitor serial durante la prueba de acceso no autorizado.

### 7.3.3. Prueba de actualización de accesos desde la base de datos

La prueba de actualización de accesos desde la base de datos se realizó con el propósito de verificar que el sistema pudiera modificar los permisos de ingreso a partir de los cambios realizados en Google Sheets. Esta prueba permitió comprobar que la autorización de las credenciales RFID no dependía únicamente de valores fijos dentro del código, sino de la consulta realizada por la ESP32 a la hoja de cálculo alojada en Google Drive.

Para ejecutar la prueba, el prototipo se conectó a una red Wi-Fi y se mantuvo en comunicación con la base de datos de usuarios. Posteriormente, se realizaron cambios directamente en Google Sheets, modificando el estado de algunas credenciales, agregando nuevos identificadores RFID y retirando permisos de acceso. Después de cada modificación, se presentó la tarjeta correspondiente ante el lector RFID RC522 para comprobar la respuesta del sistema.

La prueba se repitió 15 veces, considerando diferentes acciones de administración de usuarios: autorización de una credencial registrada, desactivación de una credencial previamente autorizada, adición de una nueva credencial, retiro de acceso y presentación de una llave no registrada. En cada caso se verificó que la respuesta del sistema coincidiera con el estado vigente de la base de datos durante la siguiente lectura RFID, sin necesidad de reprogramar la ESP32.

Uno de los cambios evaluados consistió en modificar el campo *ACTIVO* de una credencial registrada. Cuando el estado se encontraba en “SI”, el sistema permitió el acceso y activó el relé para energizar la cerradura. Al cambiar el mismo campo a “NO”, la ESP32 reconoció que la llave seguía registrada en la base de datos, pero sin permiso activo, por lo que mantuvo la cerradura bloqueada

y generó la señalización de rechazo.

También se verificó la posibilidad de agregar una nueva credencial a la base de datos. Para ello, se incorporó un nuevo identificador RFID en la columna *uid*, junto con el nombre del usuario, el estado activo y el permiso correspondiente. Al presentar esta nueva tarjeta ante el lector, el sistema consultó la hoja de cálculo, reconoció la credencial agregada y respondió según el permiso asignado.

Además, se comprobó el retiro de acceso mediante la modificación o eliminación del registro asociado a una llave. Cuando una credencial previamente autorizada fue desactivada en la base de datos, el sistema negó el ingreso en la siguiente consulta. En caso de que el identificador no estuviera presente en la hoja de cálculo, la llave fue clasificada como no registrada y el acceso permaneció bloqueado.

Durante esta prueba también se observó el comportamiento del sistema después de cada modificación realizada en la base de datos. Para ello, se registró la lectura RFID posterior al cambio, el mensaje mostrado en el monitor serial, el estado del relé, la respuesta de la cerradura y la señalización generada. Esta verificación permitió confirmar que la administración de permisos podía realizarse de forma externa, conservando la lógica de seguridad del prototipo.

Cuadro 7.5: Resultado de la actualización de accesos desde Google Sheets

| **Acción realizada** | **Cambio en la base de datos** | **Resultado obtenido** |
|---|---|---|
| Autorizar una llave registrada | El campo *ACTIVO* se configuró como “SI”. | El sistema reconoció la credencial como autorizada y permitió la activación de la cerradura. |
| Desactivar una llave registrada | El campo *ACTIVO* se cambió de “SI” a “NO”. | El sistema reconoció la credencial como registrada, pero negó el acceso y mantuvo la cerradura bloqueada. |
| Agregar una nueva credencial | Se añadió un nuevo *uid* con usuario, estado activo y permiso asignado. | El sistema identificó la nueva llave y respondió de acuerdo con el permiso registrado. |
| Quitar acceso a una credencial | Se desactivó el campo *ACTIVO* o se retiró el registro de la hoja. | El sistema negó el acceso en la siguiente lectura de la credencial y no activó el relé. |

| Acción realizada | Cambio en la base de datos | Resultado obtenido |
|---|---|---|
| Presentar una llave no registrada | El *uid* leído no existía en la base de datos. | El sistema clasificó la llave como no registrada, mantuvo la cerradura bloqueada y activó la señalización de rechazo. |
| Repeticiones ejecutadas | Se realizaron 15 modificaciones o consultas asociadas a permisos de acceso. | En 15 casos el sistema respondió de acuerdo con el estado vigente de la base de datos. |
| Reprogramación de la ESP32 | Los cambios debían aplicarse desde Google Sheets sin modificar el código cargado en el microcontrolador. | No fue necesario reprogramar la ESP32 para activar, desactivar, agregar o retirar credenciales. |
| Falsas aperturas | No debía activarse la cerradura ante credenciales desactivadas, retiradas o no registradas. | Se registraron 0 falsas aperturas durante la prueba. |

Los resultados de esta prueba fueron satisfactorios, ya que los cambios realizados en Google Sheets se reflejaron en el comportamiento del sistema durante la operación. Esto permitió comprobar que los permisos de acceso podían modificarse, agregarse o retirarse desde la base de datos sin reprogramar la ESP32.

Este resultado representa una ventaja funcional para la administración del módulo contenedor, debido a que permite actualizar los usuarios autorizados de forma externa y flexible. De esta manera, el sistema puede adaptarse a cambios en los permisos de ingreso, incorporación de nuevos usuarios o retiro de accesos sin intervenir físicamente el prototipo ni modificar directamente la lógica cargada en el microcontrolador.

En términos de validación funcional, esta prueba permitió comprobar que la base de datos externa no solo actúa como un registro de usuarios, sino como un elemento activo dentro de la lógica de autorización del sistema. Por lo tanto, la respuesta del prototipo quedó condicionada al estado vigente de cada credencial, fortaleciendo la administración del acceso y reduciendo la necesidad de ajustes manuales sobre el código del microcontrolador.

## 7.4. Resultados de las pruebas con usuarios potenciales

### 7.4.1. Descripción general de las pruebas

Las pruebas se realizaron con propietarios y trabajadores de emprendimientos dedicados a la venta de alimentos en puestos ubicados en el espacio público del barrio Bochalema, en la ciudad de Cali. Estos participantes fueron seleccionados como usuarios potenciales debido a que desarrollan actividades comerciales en condiciones similares al contexto de uso previsto para el proyecto.

Los emprendimientos evaluados presentan características relacionadas con la atención directa al público, el manejo de productos y equipos dentro de espacios reducidos, la necesidad de proteger los elementos almacenados y la operación en zonas de fácil acceso desde la calle. Estas condiciones son comparables con las previstas para los módulos contenedores orientados al emprendimiento juvenil, por lo que permitieron realizar una aproximación al uso del sistema en un entorno semejante al de su aplicación final.

La selección de estos participantes no tuvo como propósito realizar una validación comercial definitiva, sino observar la interacción con el prototipo e identificar apreciaciones, dificultades y oportunidades de mejora relacionadas con su funcionamiento y facilidad de uso.

Al igual que en las pruebas funcionales del prototipo, en los anexos se incluye un enlace a una carpeta de Google Drive que contiene los registros audiovisuales de las pruebas realizadas con los usuarios potenciales. Este material permite evidenciar el desarrollo de las actividades, la interacción de los participantes con el sistema y el funcionamiento del prototipo durante cada prueba.

### 7.4.2. Desarrollo de la interacción con el prototipo

La interacción con el prototipo se llevó a cabo en dos emprendimientos dedicados a la venta de alimentos, ubicados en el barrio Bochalema. En cada establecimiento se presentó el sistema electrónico de seguridad y control de acceso, se explicó su propósito y se describió la secuencia básica de funcionamiento antes de iniciar las actividades prácticas.

Posteriormente, los participantes interactuaron directamente con el prototipo siguiendo la secuencia de operación definida para el sistema. Durante esta actividad se observó la forma en que cada usuario comprendía las instrucciones, utilizaba los elementos de acceso y ejecutaba las funciones disponibles, procurando que la intervención de los desarrolladores fuera mínima.

Las pruebas se realizaron de manera independiente en cada emprendimiento, con el fin de registrar la experiencia particular de los participantes y comparar su interacción con el sistema en dos contextos comerciales similares. Durante el proceso se documentaron las actividades mediante fotografías y videos, como evidencia de la ejecución de las pruebas y del funcionamiento del prototipo.

Figura 7.5: Prueba 1: SuperDeli

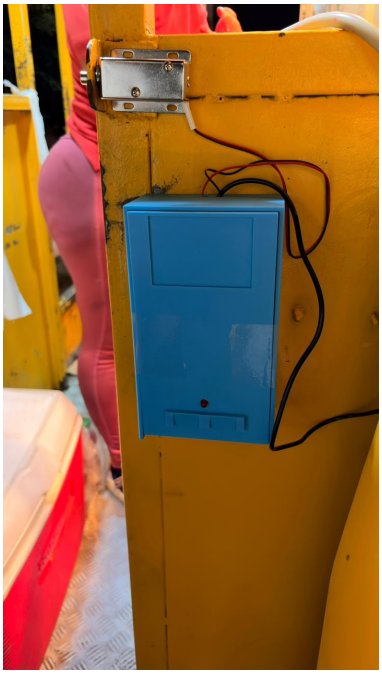

Figura 7.6: Montaje prueba 1

Figura 7.7: Prueba 2: Las Delicias de Manolo

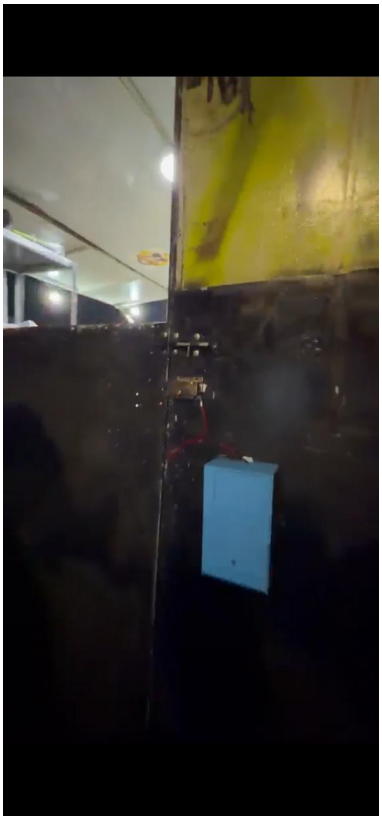

Figura 7.8: Montaje prueba 2

### 7.4.3. Observaciones durante la ejecución de las tareas

Durante las pruebas realizadas en los dos emprendimientos de alimentos, los participantes recibieron una explicación inicial sobre el propósito del prototipo y la secuencia establecida para su operación. Posteriormente, cada usuario interactuó directamente con el sistema, mientras se observaban la comprensión de las instrucciones, la ejecución de las tareas, la respuesta del prototipo y la necesidad de asistencia durante el proceso.

La secuencia de operación inició con el sistema energizado, la puerta bloqueada y los sensores activos. A continuación, el participante solicitó el acceso mediante una tarjeta RFID. El sistema verificó la credencial ingresada y, cuando esta fue válida, liberó la cerradura, permitió la apertura de la puerta y registró el acceso autorizado. Una vez cerrada la puerta, la cerradura volvió a bloquearse y el sistema retornó al estado de espera.

También se verificó el comportamiento del prototipo ante el uso de llaves no registradas y de llaves registradas sin autorización de acceso. En el primer caso, el sistema rechazó la credencial, mantuvo la cerradura bloqueada y contabilizó el intento fallido; al presentarse tres intentos consecutivos

con llaves no registradas, se activó temporalmente la alarma mediante el buzzer y el indicador LED rojo. En el segundo caso, cuando se utilizó una llave registrada pero sin permisos de acceso, el sistema mantuvo la cerradura bloqueada y mostró únicamente el aviso correspondiente, sin activar la alarma.

En ambos emprendimientos, los participantes comprendieron correctamente las instrucciones y completaron la secuencia de operación establecida. La interacción se desarrolló de manera fluida y no fue necesaria una intervención constante por parte de los desarrolladores para orientar el uso del prototipo.

El sistema respondió correctamente ante las acciones realizadas durante las pruebas. Los mecanismos de identificación, la cerradura, los sensores, los indicadores y las alertas funcionaron de acuerdo con el comportamiento esperado, sin presentar interrupciones, fallas ni dificultades que impidieran completar las actividades definidas.

La Tabla 7.6 presenta una síntesis de las principales observaciones registradas durante las pruebas efectuadas en los dos emprendimientos.

Cuadro 7.6: Observaciones registradas durante las pruebas con usuarios potenciales.

| **Aspecto observado** | **Emprendimiento 1** | **Emprendimiento 2** |
|---|---|---|
| Comprensión de las instrucciones | Las instrucciones fueron comprendidas correctamente. | Las instrucciones fueron comprendidas correctamente. |
| Ejecución de las tareas | Se completó la secuencia de operación establecida. | Se completó la secuencia de operación establecida. |
| Respuesta del prototipo | El sistema respondió de acuerdo con lo esperado. | El sistema respondió de acuerdo con lo esperado. |
| Necesidad de asistencia | No se requirió asistencia adicional durante la prueba. | No se requirió asistencia adicional durante la prueba. |
| Fallas o dificultades | No se presentaron fallas ni dificultades observables. | No se presentaron fallas ni dificultades observables. |

En términos generales, los resultados observados en ambos emprendimientos evidenciaron que el prototipo pudo ser utilizado correctamente dentro de los escenarios de prueba definidos y que su secuencia de funcionamiento resultó comprensible para los usuarios potenciales participantes.

### 7.4.4. Oportunidades de mejora identificadas

Durante las pruebas realizadas en los dos emprendimientos no se identificaron fallas que impidieran la operación del prototipo ni fue necesario efectuar modificaciones inmediatas en su funcionamiento. Los participantes completaron correctamente la secuencia de acceso y el sistema respondió

de acuerdo con la lógica implementada para las llaves autorizadas, las llaves registradas sin permiso de acceso y las llaves no registradas.

La percepción de los propietarios de los emprendimientos fue favorable. Ambos manifestaron que les gustó mucho el sistema y valoraron positivamente su capacidad para controlar el acceso y diferenciar las distintas condiciones de las llaves utilizadas durante las pruebas. También mostraron interés en la respuesta de seguridad generada ante los intentos realizados con llaves no registradas.

Los participantes consideraron adecuado que una llave registrada, pero sin autorización, generara un aviso y mantuviera la cerradura bloqueada sin activar la alarma. De igual manera, valoraron que los intentos consecutivos con llaves no registradas fueran contabilizados y que, después del tercer intento, se activaran el buzzer y el indicador LED rojo como mecanismo de alerta.

A pesar de que el funcionamiento fue satisfactorio, se identificó como oportunidad de mejora el fortalecimiento de los avisos visuales y sonoros del sistema. Esto permitiría que el usuario diferencie con mayor facilidad entre un acceso autorizado, una llave registrada sin permiso y una llave no registrada, especialmente en espacios con ruido o alta afluencia de personas.

Como oportunidad de mejora, se plantea complementar el prototipo con una fuente de alimentación de respaldo que permita mantener temporalmente las funciones de control de acceso ante una interrupción del suministro eléctrico. Esta incorporación fortalecería la continuidad operativa del sistema sin modificar la lógica de funcionamiento que fue verificada satisfactoriamente durante las pruebas realizadas.

En términos generales, las oportunidades de mejora planteadas corresponden a complementos orientados a fortalecer la operación y la experiencia de uso del prototipo. Los resultados obtenidos durante las pruebas fueron satisfactorios, tanto en el funcionamiento del sistema como en la interacción de los participantes, quienes expresaron una percepción positiva frente a su utilidad, respuesta y facilidad de uso.

## 7.5. Análisis de resultados del sistema de seguridad

El análisis de los resultados obtenidos permite establecer que el sistema electrónico de seguridad respondió de manera coherente con la lógica de funcionamiento definida durante el diseño. Las pruebas realizadas evidenciaron que el prototipo logró diferenciar entre credenciales autorizadas, credenciales registradas sin permiso activo y credenciales no registradas, activar la cerradura únicamente ante una condición válida de acceso y mantener el bloqueo cuando la credencial presentada no cumplía con los criterios de autorización definidos.

Uno de los resultados más relevantes fue la correcta relación entre la lectura RFID, la consulta

de autorización y la activación del mecanismo de apertura. En las pruebas de acceso autorizado, el sistema identificó la credencial registrada con permiso activo, activó el relé durante el tiempo definido y permitió que la cerradura electrónica de 12 V recibiera alimentación desde el transformador independiente. Este comportamiento confirma que la etapa de control y la etapa de potencia trabajaron de forma coordinada, sin exigir al microcontrolador la alimentación directa del actuador.

En las pruebas de acceso no autorizado, el sistema mantuvo la cerradura bloqueada y evitó la activación del relé, lo cual demuestra que la apertura del acceso quedó condicionada a la validación de una credencial con permiso vigente. Este resultado es importante porque confirma que una credencial inactiva, retirada o no registrada no genera desbloqueo del sistema, manteniendo la función principal de restricción de acceso.

La prueba de actualización de accesos desde Google Sheets permitió comprobar que la administración de permisos puede realizarse de forma externa, sin reprogramar la ESP32. Los cambios realizados en la base de datos, como activar, desactivar, agregar o retirar credenciales, se reflejaron en la respuesta del prototipo durante la siguiente lectura RFID. Esto fortalece la utilidad práctica del sistema, ya que permite modificar los permisos de ingreso sin intervenir físicamente el montaje ni alterar el código cargado en el microcontrolador.

El comportamiento de los elementos de señalización también fue adecuado. El LED rojo y el buzzer permitieron distinguir entre un aviso breve por intento fallido y una alarma generada por la acumulación de tres intentos consecutivos no autorizados. Esta diferenciación mejora la interpretación del estado del sistema, ya que permite reconocer cuándo se trata de un rechazo individual y cuándo se presenta una condición de advertencia más crítica.

El uso del monitor serial facilitó el seguimiento de la lógica interna durante las pruebas. A través de los mensajes observados fue posible confirmar la lectura de credenciales, la validación del identificador, la consulta de permisos, el conteo de intentos fallidos, la activación de salidas y el retorno al estado inicial. Esto permitió verificar que las respuestas físicas del prototipo coincidieran con los estados lógicos definidos en la programación.

Para consolidar el análisis, los resultados de las pruebas se organizaron en una matriz resumen. La tasa de cumplimiento se calculó como la relación entre el número de eventos ejecutados correctamente y el número total de eventos realizados para cada escenario, de acuerdo con la siguiente expresión:

$$\text{Tasa de cumplimiento} = \frac{\text{Eventos correctos}}{\text{Eventos ejecutados}} \times 100$$

Cuadro 7.7: Resumen consolidado de resultados funcionales del sistema de seguridad

| **Escenario evaluado** | **Eventos ejecutados** | **Eventos correctos** | **Fallas** | **Tasa de cumplimiento** |
|---|---|---|---|---|
| Acceso autorizado | 25 | 25 | 0 | 100 % |
| Credencial registrada sin permiso activo | 15 | 15 | 0 | 100 % |
| Credencial no registrada | 10 | 10 | 0 | 100 % |
| Actualización de permisos desde Google Sheets | 15 | 15 | 0 | 100 % |
| Activación de alarma por tres intentos fallidos | 10 | 10 | 0 | 100 % |
| Retorno al estado inicial | 50 | 50 | 0 | 100 % |
| Falsas aperturas ante accesos no autorizados | 50 | 50 | 0 | 100 % |

Las pruebas realizadas fueron satisfactorias, ya que el sistema cumplió con los criterios de aceptación establecidos para los escenarios evaluados. No se evidenciaron activaciones indebidas de la cerradura, respuestas contradictorias entre señalización y actuación, ni permanencia del sistema en estados indefinidos después de una autorización, rechazo, actualización de permiso o alarma. Además, el retorno al estado inicial permitió comprobar que el prototipo quedaba disponible para una nueva lectura RFID después de cada evento.

Desde el punto de vista funcional, los resultados demuestran que el prototipo cumple con el objetivo de regular el acceso mediante una solución basada en microcontrolador, identificación RFID, base de datos externa, señalización y actuación eléctrica. La validación realizada no corresponde a una certificación de seguridad ni a una prueba de operación permanente en campo; sin embargo, permite comprobar la lógica principal del sistema bajo condiciones controladas, con escenarios repetibles, criterios de aceptación definidos y evidencia física del comportamiento del prototipo.

Finalmente, el análisis evidencia que la arquitectura implementada puede servir como base para una futura instalación en el módulo real, siempre que se realicen los ajustes físicos, eléctricos y de montaje necesarios. Entre estos ajustes se incluyen la ubicación definitiva de la cerradura,

la protección del cableado, la instalación segura del transformador, la fijación de los elementos de señalización, la protección de la electrónica y la adecuación del sistema a las condiciones reales de uso del contenedor.

## 7.6. Resultado del diseño general del sistema energético

Como resultado del diseño general del sistema energético, se obtuvo un esquema de conexión preliminar para la alimentación eléctrica del módulo contenedor. Este esquema fue elaborado en la aplicación QElectroTech y permitió representar la relación entre los paneles solares, las protecciones en corriente continua, el inversor solar, las protecciones en corriente alterna, el medidor bidireccional, la red eléctrica y las cargas internas del contenedor.

El esquema propuesto corresponde a una configuración solar conectada a red, en la cual los paneles solares entregan energía a un inversor *on-grid*. Este inversor se encarga de convertir la energía generada por los paneles en energía alterna utilizable por las cargas del módulo, manteniendo la posibilidad de apoyo desde la red eléctrica cuando la generación fotovoltaica no sea suficiente.

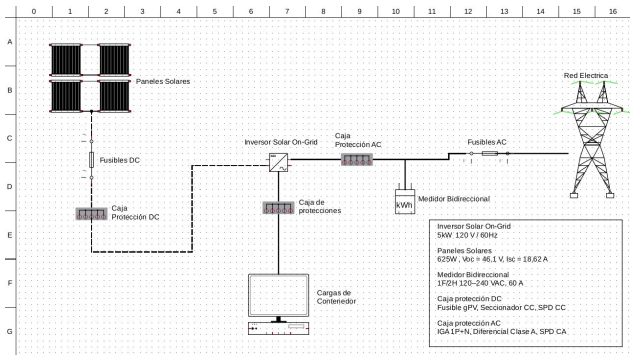


Figura 7.9: Esquema general del sistema energético propuesto para el módulo contenedor.

En la Figura 7.9 se observa la disposición general del sistema energético propuesto. El arreglo fotovoltaico se conecta inicialmente a una etapa de protección en corriente continua, compuesta por elementos como fusibles, seccionador y protección contra sobretensiones. Posteriormente, la energía se dirige hacia el inversor solar, el cual se conecta a la etapa de corriente alterna del sistema.

En el lado de corriente alterna se incluyen protecciones eléctricas antes de la conexión con las cargas del contenedor y con la red eléctrica. También se considera un medidor bidireccional, debido a que la propuesta corresponde a una configuración conectada a red. Este elemento permite representar el intercambio de energía entre el sistema fotovoltaico, las cargas internas y la red eléctrica convencional.

El resultado obtenido no corresponde a una instalación física validada en campo, sino a una representación técnica preliminar que permite orientar una futura implementación energética del módulo. Por esta razón, el esquema debe entenderse como una base de diseño que deberá ser ajustada posteriormente según las condiciones reales del sitio, la carga definitiva del contenedor, la selección final de equipos y la normativa eléctrica aplicable.

Capítulo 8

# Conclusiones

El desarrollo del proyecto permitió responder a la necesidad de contar con un sistema electrónico de seguridad para un módulo contenedor orientado al uso comunitario, integrando mecanismos de identificación, administración de permisos, señalización y actuación bajo una lógica de control basada en microcontrolador. A partir del diseño, implementación y validación funcional del prototipo, se comprobó que la solución propuesta permite regular el acceso al módulo mediante credenciales RFID, diferenciando entre usuarios autorizados, usuarios registrados sin permiso activo y credenciales no registradas.

En relación con el objetivo general, se concluye que fue posible diseñar e implementar un prototipo funcional de control de acceso capaz de activar una cerradura electrónica únicamente cuando se presenta una credencial registrada con permiso vigente. Las pruebas realizadas demostraron que el sistema mantiene el acceso bloqueado ante credenciales no autorizadas, activa el mecanismo de apertura cuando la validación es correcta y retorna al estado inicial después de cada evento de operación.

Respecto al diseño del sistema de seguridad, se logró estructurar una arquitectura organizada por subsistemas, conformada por identificación RFID, control mediante ESP32, consulta de permisos en base de datos, señalización visual y sonora, y actuación eléctrica mediante relé y cerradura. Esta división facilitó la selección de componentes, la integración progresiva del prototipo y la verificación del funcionamiento de cada bloque antes de consolidar el sistema completo.

La implementación del sistema evidenció la importancia de separar la etapa de control de la etapa de potencia. La tarjeta LilyGO A7670 ESP32 permitió ejecutar la lógica de validación, consultar la condición de autorización y enviar señales de control, mientras que la cerradura electrónica de 12 V fue alimentada mediante un transformador independiente y activada a través de un relé. Esta configuración evitó que el microcontrolador alimentara directamente el actuador y permitió una operación más segura y estable del prototipo.

La incorporación de Google Sheets como base de datos externa permitió administrar los permisos de acceso sin modificar directamente el código cargado en la ESP32. Durante las pruebas se verificó que el sistema respondiera a cambios como activación, desactivación, adición o retiro de credenciales, lo cual representa una ventaja funcional para la administración del módulo contenedor, ya que permite actualizar los usuarios autorizados de forma flexible y externa.

Las pruebas funcionales permitieron comprobar que el sistema respondió correctamente ante los escenarios definidos en el plan de validación. El prototipo identificó credenciales autorizadas, rechazó credenciales no autorizadas, mantuvo bloqueada la cerradura ante usuarios sin permiso activo, activó señales de advertencia, contabilizó intentos fallidos consecutivos y generó una alarma diferenciada después de alcanzar el límite establecido. Estos resultados respaldan el cumplimiento de la lógica de seguridad planteada durante el diseño.

La validación funcional se fortaleció mediante la definición de criterios de aceptación, escenarios de prueba repetibles y registro de evidencias asociadas al comportamiento del sistema. A partir de la matriz de pruebas, se evaluó la respuesta del relé, la cerradura, el LED rojo, el buzzer, el monitor serial, el retorno al estado inicial y la ausencia de falsas aperturas ante credenciales sin autorización vigente. Esto permitió analizar el prototipo no solo como una demostración de apertura y cierre, sino como un sistema de control de acceso con condiciones verificables de operación.

El uso de LED rojos y buzzer permitió establecer una señalización clara para los eventos principales del sistema. Se evidenció que el prototipo puede diferenciar entre un aviso breve por intento fallido y una alarma repetitiva por acumulación de intentos no autorizados, lo cual mejora la interpretación del estado del sistema y refuerza su función de advertencia dentro del control de acceso.

En cuanto al componente energético, el proyecto permitió plantear una propuesta general para la alimentación eléctrica del módulo contenedor, considerando la necesidad de suministrar energía al sistema de seguridad y a los elementos internos previstos. Este componente se abordó como un diseño técnico y documental, por lo que constituye una base para una futura implementación, pero no corresponde a una instalación física validada en campo.

De manera general, los resultados obtenidos respaldan el planteamiento del problema, ya que el prototipo desarrollado contribuye a la administración segura del acceso al módulo contenedor y reduce la dependencia de mecanismos exclusivamente manuales. Aunque las pruebas se realizaron bajo condiciones controladas y no en una instalación definitiva dentro del módulo, el comportamiento observado permite validar la lógica principal del sistema y establecer una base técnica para una futura implementación en el espacio real.

Finalmente, el proyecto permitió fortalecer aprendizajes relacionados con el diseño de sistemas embebidos, la integración de componentes electrónicos, la administración externa de permisos, la separación entre control y potencia, la programación de lógica de acceso y la validación funcional mediante pruebas controladas. Estos aprendizajes fueron fundamentales para consolidar una solución técnica coherente con los objetivos planteados y con las condiciones de uso previstas para el módulo contenedor.

Capítulo 9

# Recomendaciones

Se recomienda que, para una futura instalación del sistema en el módulo contenedor real, se realice una adecuación física definitiva de los componentes electrónicos, asegurando que la tarjeta de control, el relé, el transformador, el lector RFID, el buzzer y los LED queden protegidos dentro de cajas o compartimientos adecuados. Esto permitiría reducir la exposición del sistema a golpes, manipulación indebida, humedad, polvo o desconexiones accidentales durante la operación cotidiana del módulo.

También se recomienda organizar el cableado interno del sistema mediante canaletas, borneras o conectores adecuados, con el fin de facilitar el mantenimiento, mejorar la seguridad eléctrica y evitar falsos contactos. Esta recomendación es especialmente importante en la etapa de actuación, debido a que la cerradura electrónica trabaja con una alimentación independiente de 12 V y requiere separación clara entre la etapa de control y la etapa de potencia.

Para mejorar la confiabilidad del sistema, se recomienda realizar pruebas adicionales en condiciones más cercanas al uso real del módulo contenedor. Aunque el prototipo fue validado bajo condiciones controladas, una instalación definitiva permitiría evaluar aspectos como la ubicación del lector RFID, la respuesta de la cerradura instalada en la puerta, la estabilidad de la alimentación eléctrica y el comportamiento del sistema durante jornadas prolongadas de funcionamiento.

Se recomienda fortalecer la gestión de la base de datos en Google Sheets mediante una estructura de administración más controlada. Para ello, es conveniente definir responsables de edición, restringir permisos de modificación y mantener un registro ordenado de los cambios realizados sobre los usuarios, llaves y estados de autorización. Esto permitiría reducir errores al agregar, activar, desactivar o retirar accesos dentro del sistema.

Asimismo, se recomienda complementar la base de datos con campos adicionales que permitan llevar un mejor control administrativo del acceso, como fecha de registro, fecha de activación, fecha de desactivación, responsable del cambio y observaciones del usuario. Estos campos facilitarían el seguimiento de las credenciales y permitirían tener mayor trazabilidad sobre el uso del sistema.

En cuanto a la conectividad, se recomienda evaluar en una etapa posterior el uso de la comunicación mediante tarjeta SIM integrada en la LilyGO A7670 ESP32. Aunque las pruebas de consulta a la base de datos se realizaron mediante Wi-Fi, la conectividad celular permitiría proyectar el sistema hacia una operación más independiente de redes locales, especialmente si el módulo contenedor se

instala en un lugar donde no exista una conexión Wi-Fi estable.

También se recomienda implementar mecanismos de respaldo para la validación de accesos en caso de pérdida temporal de conexión a internet. Una alternativa sería almacenar localmente una lista limitada de credenciales autorizadas que permita mantener el funcionamiento básico del sistema mientras se restablece la comunicación con la base de datos externa.

Para aumentar la seguridad del sistema, se recomienda revisar la protección lógica de la consulta a la base de datos, evitando que los enlaces, credenciales o rutas de acceso queden expuestos dentro del código de forma insegura. En una implementación definitiva, este aspecto debe considerarse para proteger la información de usuarios y reducir el riesgo de modificaciones no autorizadas.

Se recomienda ampliar el plan de pruebas incorporando más repeticiones por cada escenario evaluado, diferentes credenciales RFID y tiempos de operación más prolongados. Esto permitiría obtener mayor evidencia sobre la estabilidad del sistema, la repetibilidad de la respuesta, la duración de la alarma, el comportamiento del relé y la activación de la cerradura en ciclos sucesivos.

Finalmente, se recomienda que el diseño energético propuesto sea revisado y ajustado por personal competente antes de una implementación física en el módulo contenedor. Aunque el proyecto plantea una base técnica para la alimentación del sistema, la instalación real debe considerar protecciones eléctricas, calibre de conductores, ubicación de equipos, normatividad aplicable y condiciones ambientales del lugar de instalación.

Capítulo 10

# Anexos

# Anexo 1 – Manual de usuario del sistema de acceso

El presente manual describe el procedimiento básico para operar el sistema electrónico de control de acceso desarrollado para el módulo contenedor. Su propósito es orientar al usuario o responsable del sistema en el encendido, uso de credenciales RFID, interpretación de señales, administración básica de accesos desde Google Sheets y apagado seguro del prototipo.

El sistema permite controlar el acceso mediante tarjetas o llaveros RFID, los cuales son leídos por el módulo RC522 y validados por la tarjeta LilyGO A7670 ESP32. La autorización de ingreso depende de la información registrada en una base de datos en Google Sheets, donde se define si una credencial está activa y si cuenta con permiso para acceder al contenedor.

## Componentes principales del sistema

El sistema de acceso está conformado por una tarjeta LilyGO A7670 ESP32, un lector RFID RC522, tarjetas o llaveros RFID, un relé, una cerradura electrónica de 12 V, LED rojos, un buzzer, un transformador de 12 V y una base de datos de usuarios alojada en Google Sheets. Estos elementos trabajan en conjunto para identificar credenciales, validar permisos, activar la cerradura y generar señales de advertencia cuando el acceso no es autorizado.

La ESP32 actúa como unidad de control del sistema. Esta tarjeta recibe el identificador leído por el módulo RFID, consulta la base de datos de usuarios y determina si debe permitir o negar el acceso. Cuando la credencial es válida y está activa, la ESP32 activa el relé, el cual permite alimentar la cerradura electrónica mediante el transformador de 12 V.

## Encendido del sistema

Antes de encender el sistema, se debe verificar que las conexiones principales estén correctamente instaladas. Se debe revisar que la tarjeta ESP32 esté conectada a su fuente de alimentación, que el módulo RFID esté conectado, que el relé esté vinculado a la salida de control, que la cerradura esté alimentada mediante el transformador de 12 V y que los elementos de señalización se encuentren conectados.

Una vez revisado el montaje, se energiza la tarjeta de control y posteriormente la fuente o transformador encargado de alimentar la cerradura electrónica. Al iniciar, el sistema debe permanecer en estado de espera, sin activar el relé, la cerradura, el LED rojo ni el buzzer.

Si el sistema está conectado al computador durante las pruebas, el monitor serial puede utilizarse para verificar el estado inicial del prototipo, la conexión Wi-Fi, la lectura de credenciales y

las respuestas generadas por la lógica de control.

### Uso de tarjetas RFID

Para solicitar acceso, el usuario debe aproximar su tarjeta o llavero RFID al lector RC522. El sistema lee el identificador de la credencial y lo compara con los registros disponibles en la base de datos de Google Sheets.

Si la credencial se encuentra registrada, activa y con permiso de acceso al contenedor, el sistema autoriza el ingreso. En este caso, la ESP32 activa el relé durante un tiempo definido, permitiendo que la cerradura electrónica reciba alimentación de 12 V y habilite la apertura del acceso.

Si la credencial se encuentra registrada, pero su campo *ACTIVO* está configurado como "NO", el sistema reconoce la llave como existente, pero no permite el ingreso. En este caso, la cerradura permanece bloqueada y se activa la señalización de rechazo correspondiente.

Si la credencial no aparece registrada en la base de datos, el sistema la clasifica como una llave no registrada. Ante esta condición, el acceso permanece bloqueado y el sistema genera una señal de advertencia mediante los elementos de señalización.

### Estados del sistema

La operación del prototipo se puede interpretar a partir de los estados principales mostrados en la Tabla 10.2. Estos estados permiten reconocer la respuesta del sistema ante una credencial autorizada, no autorizada o no registrada.

Cuadro 10.1: Estados principales del sistema de acceso

| **Estado del sistema** | **Condición que lo genera** | **Respuesta del prototipo** |
|---|---|---|
| Espera | Sistema energizado y sin lectura de credencial. | Cerradura bloqueada, relé desactivado y sin alarma activa. |
| Acceso autorizado | Credencial registrada con campo *ACTIVO* en "SI" y permiso válido. | Se activa el relé y la cerradura recibe alimentación durante el tiempo definido. |

| **Estado del sistema** | **Condición que lo genera** | **Respuesta del prototipo** |
|---|---|---|
| Acceso denegado | Credencial registrada con campo *ACTIVO* en "NO". | La cerradura permanece bloqueada y se activa una señal breve de rechazo. |
| Llave no registrada | Identificador RFID no encontrado en Google Sheets. | El acceso permanece bloqueado y se genera señalización de advertencia. |
| Intentos fallidos | Lecturas consecutivas de credenciales no autorizadas o no registradas. | El sistema incrementa el contador de intentos fallidos. |
| Alarma temporal | Se alcanzan tres intentos fallidos consecutivos. | El LED rojo y el buzzer se activan de forma repetida durante un tiempo determinado. |
| Retorno al inicio | Finaliza una autorización, rechazo o alarma. | El sistema desactiva las salidas y vuelve al estado de espera. |

### Administración de usuarios en Google Sheets

La base de datos de usuarios se administra desde una hoja de cálculo en Google Sheets. Esta hoja contiene los campos *uid*, *USUARIO*, *ACTIVO* y *PERMISO*. El campo *uid* corresponde al identificador RFID de la tarjeta o llavero; el campo *USUARIO* permite asociar la credencial a una persona; el campo *ACTIVO* define si la llave puede ser utilizada; y el campo *PERMISO* indica el tipo de acceso asignado.

Para agregar un nuevo usuario, se debe registrar una nueva fila en la hoja de cálculo con el identificador RFID correspondiente, el nombre o referencia del usuario, el estado de autorización y el permiso asignado. Si el campo *ACTIVO* se configura como "SI", el sistema permitirá el acceso cuando se presente esa credencial.

Para retirar temporalmente el acceso de un usuario, no es necesario eliminar la fila de la base de datos. Basta con cambiar el campo *ACTIVO* de 'SI" a 'NO". De esta forma, la llave seguirá registrada, pero el sistema no permitirá la apertura de la cerradura.

Para eliminar completamente una credencial del sistema, se puede retirar la fila correspondiente de la hoja de cálculo. En este caso, cuando la tarjeta sea presentada al lector RFID, el sistema no encontrará el identificador en la base de datos y la clasificará como llave no registrada.

### Operación básica

Para operar el sistema, primero se debe verificar que el prototipo esté energizado y conectado a la red Wi-Fi definida para la consulta de la base de datos. Luego, el usuario debe aproximar su tarjeta o llavero RFID al lector. El sistema consultará la información registrada en Google Sheets y ejecutará la respuesta correspondiente según el estado de la credencial.

Si el acceso es autorizado, la cerradura se activará durante el tiempo configurado y posteriormente volverá a su condición de bloqueo. Si el acceso es rechazado, el sistema no activará el relé y generará una señal de advertencia. Después de cada evento, el prototipo debe retornar al estado de espera para recibir una nueva lectura RFID.

### Solución de problemas

Si el lector RFID no reconoce una tarjeta, se recomienda verificar la conexión del módulo RC522, revisar la alimentación del sistema y confirmar que la credencial esté ubicada correctamente sobre el área de lectura. También se puede utilizar el monitor serial para comprobar si el identificador RFID está siendo leído por la ESP32.

Si una tarjeta autorizada no permite el acceso, se debe revisar la base de datos en Google Sheets. Es necesario confirmar que el identificador RFID esté registrado correctamente, que el campo *ACTIVO* se encuentre en "SI" y que el permiso asignado corresponda al acceso del contenedor.

Si la cerradura no se activa después de una autorización válida, se debe revisar el estado del relé, la conexión del transformador de 12 V y el cableado de la cerradura. También se debe comprobar que la ESP32 esté enviando la señal lógica de activación hacia el relé durante el tiempo definido en la programación.

Si el LED rojo o el buzzer no se activan ante un acceso denegado o una alarma, se deben revisar las conexiones de estos elementos, la polaridad del LED, la resistencia asociada y el pin asignado en el código. También se puede verificar mediante el monitor serial si el sistema está entrando correctamente al estado de rechazo o alarma.

Si el sistema no consulta la base de datos, se debe revisar la conexión Wi-Fi, el enlace utilizado para acceder a Google Sheets y la disponibilidad de internet. En caso de pérdida de conexión, el sistema puede no actualizar correctamente los permisos hasta que se restablezca la comunicación con la hoja de cálculo.

### Apagado del sistema

Para apagar el sistema, se recomienda desconectar primero la alimentación de la cerradura o transformador de 12 V y posteriormente la alimentación de la tarjeta de control. Esto permite retirar la energía de la etapa de potencia antes de apagar la lógica de control del prototipo.

Después del apagado, se debe verificar que el relé, la cerradura, el LED rojo y el buzzer queden desactivados. También se recomienda evitar la manipulación del cableado mientras el sistema se encuentre energizado, especialmente en la etapa asociada al transformador y a la cerradura electrónica.

# Anexo 2 – Mantenimiento del sistema

El mantenimiento del sistema tiene como propósito conservar el funcionamiento adecuado del prototipo de control de acceso, evitando fallas por desconexiones, errores en la base de datos, problemas de alimentación o deterioro de los componentes electrónicos. Estas actividades deben realizarse de forma preventiva y, en caso de falla, como apoyo para identificar el origen del problema.

## Revisión física del montaje

Se recomienda revisar periódicamente el estado físico de la tarjeta LilyGO A7670 ESP32, el módulo RFID RC522, el relé, la cerradura electrónica, el buzzer, los LED y el transformador de 12 V. Durante esta revisión se debe verificar que los componentes se encuentren firmes, sin cables sueltos, contactos flojos o signos visibles de daño.

También se debe comprobar que el lector RFID se mantenga ubicado en una posición adecuada para permitir la lectura correcta de las tarjetas o llaveros. En caso de instalar el sistema dentro del módulo contenedor, los componentes deben protegerse mediante cajas, soportes o compartimientos que eviten golpes, humedad o manipulación no autorizada.

## Revisión eléctrica

La revisión eléctrica debe centrarse en comprobar que la etapa de control y la etapa de potencia se mantengan separadas. La ESP32 no debe alimentar directamente la cerradura electrónica, ya que esta requiere 12 V y una corriente mayor a la que puede entregar el microcontrolador. Por esta razón, se debe verificar que la cerradura reciba energía desde el transformador y que su activación se realice mediante el relé.

También se recomienda revisar que el transformador entregue el voltaje adecuado, que el relé conmute correctamente y que los elementos de señalización respondan cuando el sistema lo indique. Si el buzzer o los LED no se activan, se deben revisar sus conexiones, polaridad, resistencia asociada y pines asignados en el código.

## Revisión de la base de datos

La base de datos en Google Sheets debe mantenerse actualizada y organizada. Se debe revisar que cada usuario tenga registrado correctamente su *uid*, nombre o referencia, estado de activación y permiso de acceso. Un error en alguno de estos campos puede impedir que una tarjeta autorizada sea aceptada o puede generar una respuesta incorrecta del sistema.

Para retirar el acceso de un usuario, se recomienda cambiar el campo *ACTIVO* a "NO" en lugar de eliminar inmediatamente el registro. Esto permite conservar trazabilidad sobre la llave registrada y facilita una posible reactivación futura. Si se desea eliminar completamente una credencial, se debe retirar su fila de la hoja de cálculo.

### Revisión de conectividad

Debido a que el sistema consulta la base de datos mediante Wi-Fi, se debe comprobar que la red utilizada esté disponible y que la ESP32 pueda conectarse correctamente. Si el sistema no reconoce cambios realizados en Google Sheets, se recomienda revisar la conexión a internet, el enlace de consulta y la disponibilidad de la hoja de cálculo.

Durante las pruebas o mantenimiento, el monitor serial puede utilizarse como herramienta de diagnóstico. Este permite observar si la ESP32 está leyendo la tarjeta RFID, consultando la base de datos, reconociendo el estado de la credencial y ejecutando la respuesta correspondiente.

### Fallas comunes

Si una tarjeta no es reconocida, se debe revisar primero que el módulo RFID esté conectado correctamente y que la credencial se acerque a la zona de lectura. También se debe verificar en el monitor serial si el *uid* está siendo leído por el sistema.

Si una tarjeta registrada no permite el acceso, se debe revisar que el *uid* coincida exactamente con el registrado en Google Sheets, que el campo *ACTIVO* esté configurado como "SI" y que el permiso asignado corresponda al acceso del contenedor.

Si la cerradura no se activa aunque el acceso sea autorizado, se debe revisar el relé, el transformador de 12 V y las conexiones de la cerradura. También se debe comprobar que la ESP32 esté enviando correctamente la señal de activación al relé.

Si el sistema activa la alarma sin razón aparente, se recomienda revisar el conteo de intentos fallidos, las tarjetas utilizadas durante la prueba y los mensajes generados en el monitor serial. Esto permite identificar si la alarma se generó por credenciales no autorizadas, llaves no registradas o errores en la base de datos.

### Frecuencia recomendada de mantenimiento

La revisión física y eléctrica del sistema puede realizarse de forma mensual o cada vez que se detecte una falla de operación. La revisión de la base de datos debe realizarse cada vez que

se agregue, retire o modifique un usuario. En caso de una instalación definitiva en el módulo contenedor, se recomienda realizar una revisión general antes de iniciar cada jornada prolongada de uso.

# Anexo 3 – Código fuente del prototipo

El código fuente del prototipo fue desarrollado en Arduino IDE para la tarjeta LilyGO A7670 ESP32, integrando la lectura de credenciales RFID mediante el módulo RC522, la conexión a una red Wi-Fi, la consulta de permisos en Google Sheets y la activación de las salidas asociadas al relé, cerradura electrónica, LED rojo y buzzer.

Por seguridad, en este anexo no se presentan las credenciales reales de conexión, como nombre de red, contraseña, identificador del script o token de acceso. Estos datos deben mantenerse protegidos y reemplazarse por valores genéricos o variables de configuración cuando el código sea documentado o compartido.

El programa se estructuró en bloques funcionales, con el fin de separar la configuración de comunicaciones, la lectura RFID, la consulta a la base de datos, el análisis de respuesta y la activación de salidas. Esta organización facilitó la depuración del sistema y permitió validar cada función dentro de la lógica general de control de acceso.

Cuadro 10.2: Estructura general del código fuente del prototipo

| **Bloque del código** | **Función dentro del sistema** |
|---|---|
| Librerías | Incluye las librerías necesarias para conexión Wi-Fi, solicitudes HTTP, comunicación segura, SPI y lectura del módulo RFID RC522. |
| Configuración Wi-Fi | Define los parámetros de conexión a la red utilizada para consultar la base de datos externa. |
| Configuración de Google Apps Script | Define la ruta de consulta hacia Google Sheets mediante un script publicado como servicio web. |
| Asignación de pines | Establece los pines utilizados para el módulo RFID, el relé y la salida de señalización asociada al LED rojo y buzzer. |
| Estados de acceso | Define las posibles respuestas del sistema: acceso autorizado, acceso sin permiso, llave no registrada y error de consulta. |
| Conexión Wi-Fi | Permite conectar la ESP32 a la red y reintentar la conexión en caso de pérdida de comunicación. |
| Consulta a Google Sheets | Envía el identificador RFID leído y recibe la respuesta asociada al estado de autorización de la credencial. |
| Lectura RFID | Obtiene el identificador único de la tarjeta o llavero RFID presentado ante el lector RC522. |

| Bloque del código | Función dentro del sistema |
|---|---|
| Control de salidas | Activa o desactiva el relé, la cerradura, el LED rojo y el buzzer según la condición evaluada. |
| Lógica principal | Evalúa la credencial leída, consulta la base de datos y ejecuta la respuesta correspondiente del sistema. |

La lógica de validación se basó en la respuesta obtenida desde Google Sheets. Si la base de datos retornaba una condición de acceso autorizado, el sistema activaba el relé durante un tiempo definido para alimentar la cerradura electrónica. Si la credencial estaba registrada pero sin permiso, el sistema mantenía la cerradura bloqueada y generaba una señal breve de rechazo. Si la llave no estaba registrada, el sistema incrementaba el contador de intentos no registrados y, al alcanzar tres intentos consecutivos, activaba una alarma temporal mediante el LED rojo y el buzzer.

De forma general, el código permitió integrar la consulta remota de permisos con la actuación física del sistema de acceso. Esto hizo posible modificar, agregar o retirar permisos desde Google Sheets sin reprogramar la ESP32, manteniendo la lógica de control vinculada a una base de datos externa y editable.

El código completo del prototipo se conserva como archivo fuente del proyecto en formato compatible con Arduino IDE. Para su uso en una implementación futura, se recomienda proteger las credenciales de red, el identificador del script y el token de consulta, evitando dejarlos visibles dentro de versiones públicas del documento o repositorios compartidos.

# Anexo 4 – Base de datos en Google Sheets

La base de datos del sistema de control de acceso fue organizada en Google Sheets, con el propósito de administrar las credenciales RFID utilizadas por los usuarios del módulo contenedor. Esta hoja permite registrar cada llave, asociarla a un usuario, definir si se encuentra activa y establecer el permiso correspondiente para el ingreso.

La hoja utilizada se denominó *Accesos* y se estructuró mediante cuatro campos principales: *uid*, *usuario*, *activo* y *permiso*. El campo *uid* corresponde al identificador leído por el módulo RFID RC522; el campo *usuario* permite asociar la llave con una persona; el campo *activo* indica si la credencial tiene autorización vigente; y el campo *permiso* define el tipo de acceso asignado.

Cuadro 10.3: Ejemplo de estructura de la base de datos en Google Sheets

| **uid** | **USUARIO** | **ACTIVO** | **PERMISO** |
|---|---|---|---|
| 7E1BFA05 | Sergio | NO | CONTENEDOR |
| EC60F105 | Juan | SI | CONTENEDOR |

La tabla anterior muestra la estructura básica utilizada en Google Sheets para la administración de accesos. La columna *uid* almacena el identificador leído por el módulo RFID; la columna *USUARIO* permite asociar la credencial con una persona; la columna *ACTIVO* define si la llave tiene autorización vigente; y la columna *PERMISO* indica el acceso asignado dentro del sistema.

Para conectar la ESP32 con la hoja de cálculo se utilizó un código en Google Apps Script publicado como servicio web. Este script recibe el identificador RFID enviado por la ESP32, consulta la hoja de Google Sheets y retorna una respuesta en texto que puede ser interpretada por el microcontrolador.

El código de Apps Script valida inicialmente un token de seguridad y normaliza el identificador RFID recibido, convirtiéndolo a mayúsculas y eliminando caracteres no válidos. Luego compara el *uid* recibido con los registros existentes en la hoja *Accesos*.

Si el identificador RFID se encuentra registrado y el campo *activo* indica una condición válida, como *SI*, *TRUE*, *1* o *ACTIVO*, el script retorna una respuesta de acceso autorizado. En este caso, la ESP32 interpreta la respuesta y activa el relé para permitir la apertura de la cerradura electrónica.

Si el identificador RFID está registrado, pero el campo *activo* no permite el ingreso, el script retorna una respuesta de acceso denegado. En esta condición, la ESP32 mantiene la cerradura bloqueada y activa la señalización correspondiente mediante el LED rojo y el buzzer.

Cuando el identificador RFID no existe en la hoja de cálculo, el script retorna una respuesta de

llave no registrada. Esta condición permite que el sistema diferencie entre una credencial registrada sin permiso y una llave completamente desconocida dentro de la base de datos.

Por seguridad, los datos reales asociados al identificador de la hoja de cálculo y al token de consulta no se presentan dentro del documento. Estos valores deben mantenerse protegidos para evitar accesos no autorizados o modificaciones indebidas sobre la base de datos.

El uso de Google Sheets permitió que los permisos de acceso pudieran modificarse de forma externa, sin reprogramar la ESP32. De esta manera, el administrador del sistema puede agregar usuarios, activar o desactivar credenciales y retirar accesos directamente desde la hoja de cálculo.

# Anexo 4 – Registro audiovisual de las pruebas del prototipo

Como complemento de los resultados presentados en el documento, se dispone de una carpeta de Google Drive que contiene los registros audiovisuales de las pruebas realizadas al prototipo. El material se encuentra organizado en dos grupos: pruebas funcionales y pruebas con usuarios potenciales.

En la carpeta de pruebas funcionales se incluyen los videos correspondientes a la verificación de los componentes y funciones del sistema, como la lectura de llaves RFID, la validación de permisos, la activación de la cerradura electrónica, el funcionamiento de los indicadores LED y del buzzer, y la respuesta ante llaves autorizadas, llaves registradas sin autorización y llaves no registradas.

En la carpeta de pruebas con usuarios potenciales se presentan los registros audiovisuales de las actividades desarrolladas con los propietarios de los dos emprendimientos de alimentos seleccionados. En estos videos se evidencia la explicación inicial del sistema, la interacción de los participantes con el prototipo y la ejecución de la secuencia de operación establecida.

Los registros audiovisuales pueden consultarse mediante el siguiente enlaces:

**Videos de las pruebas**

# Bibliografía


[1] Departamento Administrativo de Planeación, "Plan de desarrollo estratégico comuna cuatro 2004–2008," Alcaldía de Santiago de Cali, Tech. Rep., 2003. [Online]. Available: https://www.cali.gov.co/publico2/documentos/planeacion/planterritorial/com04.pdf

[2] Universidad Icesi and Departamento Administrativo de Planeación Municipal, "Caracterización socioeconómica de la comuna 4," Universidad Icesi, Tech. Rep., 2007. [Online]. Available: http://hdl.handle.net/10906/65164

[3] A. de Santiago de Cali, "Diagnóstico socioeconómico de la comuna 4 en cali," Alcaldía de Santiago de Cali, Tech. Rep., 2022. [Online]. Available: https://www.cali.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=75261

[4] Ministerio de Minas y Energía, "Reglamento técnico de instalaciones eléctricas - RETIE," https://www.minenergia.gov.co/es/misional/energia-electrica-2/reglamentos-tecnicos/reglamento-t%C3%A9cnico-de-instalaciones-el%C3%A9ctricas-retie/, 2024, resolución 40117 de 2024.

[5] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), "Norma técnica colombiana ntc 2050: Código eléctrico colombiano," Bogotá, D.C., 2020, adoptada por el Ministerio de Minas y Energía mediante Resolución 40117 de 2024.

[6] Institute of Electrical and Electronics Engineers (IEEE), "Ieee taxonomy," IEEE, Tech. Rep., 2022. [Online]. Available: https://apmc-mwe.org/apmc2022/pdf/IEEE_Taxonomy.pdf

[7] P. Marwedel, *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*, 4th ed. Springer, 2021. [Online]. Available: https://doi.org/10.1007/978-3-030-60910-8

[8] International Organization for Standardization, "Iso/iec 14443-4: Identification cards – contactless integrated circuit cards – proximity cards – part 4: Transmission protocol," ISO Online Browsing Platform, 2018. [Online]. Available: https://www.iso.org/standard/73599.html

[9] International Renewable Energy Agency, "Off-grid renewable energy solutions: Empowering communities and transforming lives," IRENA, Tech. Rep., 2019. [Online]. Available: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Jan/IRENA_Off-grid_RE_Access_2019.pdf

[10] ——, "Renewable energy for remote communities," IRENA, Tech. Rep., 2023. [Online]. Available: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2023/Nov/IRENA_Remote_Communities_2023.pdf

[11] International Renewable Energy Agency, International Energy Agency, World Bank, World Health Organization, United Nations Statistics Division, and United Nations Department of Economic and Social Affairs, "Tracking sdg 7: The energy progress report 2022," IRENA, Tech. Rep., 2022. [Online]. Available: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2022/Jun/SDG7_Tracking_Progress_2022.pdf

[12] M. Soeiro and A. Dias, "Renewable energy community projects: Motivations, drivers and barriers," *Energy Research & Social Science*, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484720315122

[13] A. Pérez, M. Gómez, and J. Ramírez, "Energías renovables como herramienta de inclusión: una propuesta en poblaciones vulnerables," *ResearchGate*, 2020. [Online]. Available: https://www.researchgate.net/publication/347500225_Energias_renovables_como_herramienta_de_inclusion_una_propuesta_en_poblaciones_vulnerables

[14] International Renewable Energy Agency, "Understanding the socio-economics of renewable energy deployment," IRENA, Tech. Rep., 2017. [Online]. Available: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2017/Nov/IRENA_Understanding_Socio_Economics_2017.pdf

[15] S. K. Jha and P. Mishra, "Solar photovoltaic technology as a tool for sustainable development and poverty reduction," *Renewable and Sustainable Energy Reviews*, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214629621003054

[16] United Nations, "Goal 7: Affordable and clean energy," United Nations Sustainable Development, n.d. [Online]. Available: https://www.un.org/sustainabledevelopment/es/energy/

[17] ——, "Goal 9: Industry, innovation and infrastructure," United Nations Sustainable Development, n.d. [Online]. Available: https://www.un.org/sustainabledevelopment/infrastructure-industrialization/

[18] ——, "Goal 10: Reduced inequalities," United Nations Sustainable Development, n.d. [Online]. Available: https://www.un.org/sustainabledevelopment/inequality/

[19] J. Álvarez and L. Ramírez, "Uso de contenedores modulares como espacios educativos temporales en contextos urbanos vulnerables," *Revista de Arquitectura y Urbanismo*, 2018. [Online]. Available: https://revistas.unal.edu.co/index.php/bitacora/article/view/67789

[20] S. Mandelli, J. Barbieri, R. Mereu, and E. Colombo, "Off-grid systems for rural electrification in developing countries: Definitions, classification and a comprehensive literature review," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1621–1646, 2016. [Online]. Available: https://doi.org/10.1016/j.rser.2015.12.338

[21] International Renewable Energy Agency, "Renewable energy and jobs – annual review 2022," IRENA, Tech. Rep., 2022. [Online]. Available: https://www.irena.org/Publications/2022/Sep/Renewable-Energy-and-Jobs-Annual-Review-2022

[22] Energy Sector Management Assistance Program (ESMAP), "Mini grids for half a billion people: Market outlook and handbook for decision makers," World Bank Group, Tech. Rep., 2020. [Online]. Available: https://www.worldbank.org/en/topic/energy/publication/mini-grids-for-half-a-billion-people

[23] S. Bielecki, "Microgrids as a tool for energy self-sufficiency," *Sensors*, vol. 25, no. 21, p. 6707, 2025.

[24] International Electrotechnical Commission, *IEC 60364-7-712:2017 Low-voltage electrical installations – Part 7-712: Requirements for special installations or locations – Solar photovoltaic (PV) power supply systems*, International Electrotechnical Commission Std., 2017.

[25] M. Laidi, B. Abbad, M. Berdja, and M. Chikh, "Performance of a photovoltaic solar container under mediterranean and arid climate conditions," *Energy Procedia*, vol. 18, pp. 423–432, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1876610212009332?utm

[26] L. K. Frimpong, "Do access control features reduce perceived risk of property victimisation? insights from residential neighbourhoods in sekondi-takoradi, ghana," *SN Social Sciences*, vol. 1, no. 3, p. 70, 2021. [Online]. Available: https://link.springer.com/article/10.1007/s43545-021-00075-z

[27] A. L. Imoize and O. B. Alabi, "Implementation of a user-friendly radio frequency identification and password-enabled security access system," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 13, no. 2, pp. 23–30, 2021. [Online]. Available: https://jtec.utem.edu.my/jtec/article/view/5966

[28] D. Palma, J. E. Agudo, H. Sánchez, and M. M. Macías, "An internet of things example: Classrooms access control over near field communication," *Sensors*, vol. 14, no. 4, pp. 6998–7012, 2014. [Online]. Available: https://www.mdpi.com/1424-8220/14/4/6998

[29] H. R. Abdulshaheed, H. H. Abbas, I. Al Barazanchi, and W. Hashim, "Control and alert mechanism of rfid door access control system using iot," *3C Tecnología. Glosas de innovación aplicadas a la pyme*, pp. 269–285, 2022. [Online]. Available: https://3ciencias.com/articulos/articulo/control-and-alert-mechanism-of-rfid-door-access-control-system-using-iot/

[30] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: Defining gamification," in *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*. New York, NY, USA: Association for Computing Machinery, 2011, pp. 9–15.

[31] LilyGO, "LilyGo A7670X ESP32 Version," https://github.com/Xinyuan-LilyGO/LilyGo-Modem-Series/blob/main/docs/en/esp32/a7670-esp32/README.MD, 2026, consultado el 25 de junio de 2026.

[32] NXP Semiconductors, *MFRC522 Standard Performance MIFARE and NTAG Frontend Datasheet*, NXP Semiconductors, 2016, consultado el 25 de junio de 2026. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf

[33] Cables y Más Bucaramanga, "Cerradura Electrónica 12v," 2026, consultado el 25 de junio de 2026. [Online]. Available: https://www.cymbucaramanga.com/producto/cerradura-electronica-12v/