Sistema de Control y Acceso de Prestamos de Equipos para Laboratorios de Ingeniería

Nicolás David Olmos Castilla

Julián Camilo García Aponte

Universitaria Agustiniana - Uniagustiniana

Facultad de Ingeniería

Ingeniería de Telecomunicaciones

Bogotá D.C.

2026

Sistema de Control y Acceso de Prestamos de Equipos para Laboratorios de Ingeniería

Nicolás David Olmos Castilla

Julián Camilo García Aponte

Tutor:

Edgar Fabián Rodríguez Veloza

Trabajo para optar al título de Ingeniero de Telecomunicaciones

Universitaria Agustiniana - Uniagustiniana

Facultad de Ingeniería

Ingeniería de Telecomunicaciones

Bogotá D.C.

2026

Tabla de Contenido

Resumen (Abstract) 8
Abstract (resumen) 9
Problema 10
Pregunta Problema 11
Justificación 12
Objetivos 13
Objetivo General 13
Objetivos Específicos 13
Marco Referencial 14
Antecedentes 14
Marco Teórico 18
Tecnología Rfid 18
El transpondedor (Etiqueta o tag) 19
Tipos de transpondedor 20
Transpondedor pasivo 20
Transpondedor activo 21
El interrogador (lector) 22
Antenas 22
Frecuencias de operación 22
Alta Frecuencia - 13.56 MHz 23
Automatización 24
Base de datos 25
Importancia de la base de datos 25
Diseño de base de datos 25
Etapa del diseño conceptual 26
Etapa del diseño lógico 27
Primera forma normal (1FN): 27
Segunda forma normal (2FN): 28
Tercera forma normal (3FN): 28
Control de Acceso 28
Marco Legal 28

Diseño metodológico 29
Metodología de desarrollo: modelo tipo v 29
Análisis de necesidades 30
Necesidades identificadas 30
Objetivos del sistema 30
Especificación de funciones 31
Características funcionales 31
Características de desempeño 31
Diseño arquitectónico 32
Diagrama del sistema 32
Selección de componentes 33
Selección de Software 34
Cronograma 35
Presupuesto 36
Desarrollo del proyecto 38
Objetivo 1 38
Objetivo 2 43
Diseño de la base de datos 43
Implementación del sistema de registro 45
Registro de usuarios 45
Gestión de permisos 46
Registro de accesos 47
Desarrollo del dashboard 48
Integración con el sistema de alertas 51
Objetivo 3 53
Prueba de actualización en tiempo real de la información mostrada en la plataforma. 56
Conclusiones 57
Alcances 59
Limitaciones 60
Recomendaciones 61
Referencias 62

Lista de Figuras

Figura 1 19
Figura 2 20
Figura 3 21
Figura 4 23
Figura 5 26
Figura 6 32
Figura 7 38
Figura 8 39
Figura 9 40
Figura 10 41
Figura 11 42
Figura 12 44
Figura 13 44
Figura 14 45
Figura 15 46
Figura 16 47
Figura 17 48
Figura 18 49
Figura 19 49
Figura 20 50
Figura 21 52
Figura 22 53
Figura 23 55

Lista de Tablas

Tabla 1 28
Tabla 2 33
Tabla 3 35
Tabla 4 36
Tabla 5 37
Tabla 6 37

Anexos

Anexo A 65
Anexo B 69
Anexo C 71
Anexo D 75
Anexo E 77

Resumen (Abstract)

La gestión manual de préstamo de equipos en los laboratorios de ingeniería representa un cuello de botella, la cual suele derivar en tiempos de espera prolongados con una disponibilidad limitada de los recursos. Este documento propone la transición de una gestión de laboratorios basada en procesos manuales hacia un sistema automatizado mediante tecnologías de identificación por radiofrecuencia (RFID). El objetivo principal es desarrollar un prototipo de sistema de control y registro para un laboratorio de ingeniería, capaz de automatizar el préstamo de equipos y agilizar su proceso de entrega.

La metodología empleada sigue el modelo de desarrollo en V, lo que permite una integración estructurada entre las fases de diseño y las etapas de verificación y validación del sistema. Como resultado, el prototipo integra la identificación automática de usuarios y equipos, el registro histórico de movimientos en tiempo real y la generación de alertas ante irregularidades. La implementación de este sistema no solo optimiza la eficiencia operativa del laboratorio, sino que reduce la carga administrativa y mejora la experiencia académica de los estudiantes al garantizar un control más riguroso y dinámico de los activos tecnológicos.

Palabras Clave: RFID (identificación por radiofrecuencia), Control de Acceso, Automatización, Base de datos.

Abstract (resumen)

Manual management of equipment loans in engineering laboratorios creates a bottleneck, which often results in long wait times and limited availability of resources. This document proposes the transition from manual laboratory management to an automated system using radio-frequency identification (RFID) technology. The main objective is to develop a prototype control and tracking system for an engineering laboratory, capable of automating equipment loans and streamlining the delivery process.

The methodology employed follows the V-model of development, which allows for structured integration between the design phases and the system verification and validation stages. As a result, the prototype integrates automatic identification of users and equipment, real-time tracking of movements, and the generation of alerts in case of irregularities. The implementation of this system not only optimizes the laboratory's operational efficiency but also reduces the administrative burden and improves the academic experience of students by ensuring more rigorous and dynamic control of technological assets.

Keywords: RFID (radio-frequency identification), Access Control, Automation, Database.

Problema

Los laboratorios cumplen un papel fundamental en los procesos de aprendizaje, ya que permiten a los estudiantes aplicar los conocimientos teóricos en entornos prácticos. Sin embargo, los accesos suelen presentar dificultades por normativas de uso del espacio, si bien buscan garantizar la seguridad y el control de los equipos, terminan ralentizando el uso de los elementos, una disponibilidad inmediata, la reducción de tiempo destinado a las prácticas y menor interés de uso por trámite que conlleva. Entre los principales inconvenientes se encuentran la necesidad de supervisión constante por parte de los laboratoristas, los trámites para el préstamo de equipos y la falta de un sistema ágil que garantice el acceso controlado de los estudiantes. Estas dificultades pueden generar retrasos en las actividades académicas, pérdida de los equipos, desorden en los registros de uso, e incluso desmotivación en los estudiantes al enfrentarse a procesos arduos para realizar sus prácticas. En este contexto, surge la necesidad de implementar mecanismos de monitoreo y automatización que permitan optimizar el control de acceso y el uso de los recursos en los laboratorios de ingeniería.

Una alternativa a este problema consiste en desarrollar un sistema de identificación mediante un carnet RFID (Identificación por radiofrecuencia), donde cada estudiante pueda desbloquear el aula y acceder a los dispositivos de manera rápida, segura y controlada. Así mismo llevar un registro de uso, daños y determinar las futuras renovaciones del laboratorio. Este tipo de solución facilita la gestión por parte de los laboratoristas, de hecho, también reduciría la dependencia de protocolos manuales, garantizando mayor eficiencia, aprovechamiento del espacio y generando mayor disponibilidad del laboratorio hacia el estudiante.

Pregunta Problema

¿Cómo automatizar el acceso y la gestión de equipos en los laboratorios de ingeniería para reducir la complejidad de los prestamos actuales y optimizar el uso de los equipos por parte de los estudiantes?

Justificación

Las prácticas en los laboratorios de ingeniería son importantes para fortalecer el aprendizaje. En estos espacios se les permite experimentar y aplicar parte de sus conocimientos de forma física. Sin embargo, los procesos para el uso de los equipos presentan limitaciones las cuales entorpecen la eficiencia y disponibilidad de los equipos del laboratorio.

Esta situación se repite en laboratorios de ingeniería de varias universidades, pues como señalan los autores:

> Esta dependencia genera una limitación importante en cuanto a la disponibilidad de los recursos, ya que el encargado no puede estar permanentemente en el día y mucho menos en horarios no hábiles. Como resultado, los estudiantes enfrentan dificultades para acceder a los dispositivos y materiales en horarios extendidos, lo que puede retrasar el progreso de sus proyectos y limitar su capacidad de trabajo autónomo. (Pérez y Villarroel, 2025, p.14).

Frente a este contexto, es necesario implementar una solución que permita agilizar los procesos para el uso de los recursos. La automatización del acceso mediante tecnología rfid brinda una alternativa eficiente y facilita los instrumentos a los estudiantes, además se reduce la carga operativa sobre el personal del laboratorio y se mejora significativamente la organización interna. Adicionalmente, un sistema de monitoreo permite recopilar información en tiempo real sobre acceso, uso de dispositivos y gestión del inventario, donde se garantiza que los recursos sean utilizados de forma responsable y eficiente.

En consecuencia, la implementación de esta herramienta aporta beneficios para los estudiantes como para administradores, incrementando la disponibilidad de equipos, mejorando la experiencia de uso y potenciando la calidad de los procesos académicos.

Objetivos

Objetivo General

Desarrollar un prototipo de sistema de acceso, control y registro para un laboratorio de telecomunicaciones, con la capacidad de automatizar el préstamo de equipos y agilizar su proceso de entrega.

Objetivos Específicos

1. Diseñar un prototipo de acceso y control que permita la automatización de préstamos y devolución de equipos.

2. Implementar un sistema de registro que almacene y gestione la información de los usuarios y del inventario de equipos.

3. Probar y validar el prototipo para evaluar su funcionalidad, eficiencia y facilidad de uso.

Marco Referencial

Antecedentes

Casquete y Cedeño (2024). Investigación realizada en Ecuador, titulada **"*Implementación de un sistema de control de accesos mediante módulos biométricos y tarjeta rfid de los laboratorios de la Carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnología de la Uleam*"**, en este proyecto se propone desarrollar e implementar un sistema de control de acceso basado en módulos biométricos y tarjetas RFID para los laboratorios de la carrera de "Agroindustria" en la "Facultad de Ciencias de la Vida y Tecnologías". De acuerdo con los requerimientos, el sistema de control de acceso implementado en la facultad ha tenido resultados positivos, tanto en términos de seguridad como de eficiencia. Al integrar tecnologías biométricas (como el reconocimiento de huellas dactilares o iris) junto con tarjetas RFID (Identificación por radiofrecuencia), como resultado el sistema ha logrado superar las limitaciones de los métodos tradicionales de control de acceso. Este enfoque avanzado proporciona una autenticación más precisa y segura, minimizando el riesgo de accesos no autorizados.

De esta manera, Pérez y Villarroel (2025). Estudio efectuado en Colombia, titulado **"*Autolab: Automatización de la entrega de dispositivos electrónicos en el laboratorio de electrónica mediante rfid*"** El propósito de esta investigación es, diseñar e implementar un sistema para automatizar el proceso de préstamo de equipos en el laboratorio de electrónica de la Pontificia Universidad Javeriana de Cali, mediante técnicas de automatización para la entrega, registro y monitoreo de equipos, así como la gestión del suministro eléctrico en los puestos de trabajo. Como resultado, el proyecto AutoLab optimizó la gestión automatizada de equipos en el

laboratorio de electrónica y telecomunicaciones, reduciendo el tiempo promedio de interacción a menos de un tercio del método manual, de igual manera también fomenta una cultura de responsabilidad entre los estudiantes, quienes ahora tienen un mayor control sobre el acceso y la gestión de los equipos.

Siguiendo por la misma línea, Vega (2022). Investigación desplegada en Ecuador, que lleva el título ***"Implementación de un sistema integral de seguridad mediante tecnología rfid en el laboratorio de cómputo número catorce en la Facultad de Ciencias Técnicas de la Carrera Tecnología de la Información de la Universidad Estatal del Sur de Manabí*****",** con el fin de implementar un sistema integral de seguridad mediante tecnología rfid en el laboratorio de TI número catorce de la carrera de tecnología de la información de la universidad estatal del sur de Manabí. Tras el análisis del laboratorio de cómputo número catorce, se determinó que la implementación de la tecnología rfid fortalece la seguridad de los equipos. Se realizaron los análisis de requerimientos, configuraciones y registros de usuarios sin inconvenientes, logrando que el sistema de control de acceso funcionara correctamente. Finalmente, la instalación y pruebas del sistema se ejecutaron con éxito, quedando plenamente operativo.

Por su parte, Quintana (2022). Estudio practicado en España, con el nombre de **"*Un módulo de detección rfid para tareas de manipulación robótica*",** se formula como objetivo diseñar e implementar un sistema de localización y trazabilidad de objetos basado en tecnología rfid, mediante el uso de antenas distribuidas en un entorno controlado, que permita identificar la posición aproximada de un objeto, almacenar información descriptiva en su tag y ponerla a disposición de un robot manipulador para optimizar los procesos de manipulación. El desarrollo de este proyecto ha permitido que sea posible la localización de un producto en un área

determinada. Además, se ha pudo desarrollar un programa que sea capaz de guardar coordenadas del producto en la memoria interna de un tag, así mismo como, la mesa de trabajo en la que se encuentra dicho producto.

Se igual forma, Gutiérrez (2024). Estudio llevado a cabo en Colombia, titulado **"*Prototipo de sistema de control de acceso utilizando tecnología rfid*",** se plantea Desarrollar un prototipo funcional de un sistema de automatización con tecnología RFID para la empresa HBM Technologies SAS que automatice el control de asistencia de estudiantes y/o visitantes para un colegio campestre. A partir de lo anterior, se alcanzó la adquisición de los datos de asistencia de los estudiantes a los que iba dirigido. Proporcionando información de ingreso del estudiante, intentos no autorizados, estados del sistema y reporte de errores.

Asimismo, Duque, Clavijo, et al. (2023). Estudio implementado en Colombia, llamado ***"Sistema de control de acceso utilizando tecnologías rfid",*** en esta propuesta se pretende desarrollar un sistema de control de acceso utilizando tecnologías RFID para Tecno academia y Tecno parque nodo Cúcuta, regional Norte de Santander. Con esta finalidad el sistema esté compuesto por tres roles de autorización, el primario (administrador) accede a historial de ingresos y salidas de las personas, los secundarios (usuarios) solo registran idas y entradas registrando un control detallado del sistema.

Finalmente, Sánchez (2022). Análisis hecho en Honduras, bajo el nombre de **"Diseño y simulación de un sistema de seguridad electrónico utilizando arduino uno para una puerta automática corrediza en el laboratorio de electrónica de ceutec"**, se busca Diseñar y simular un sistema de seguridad electrónico mediante el uso de Arduino uno y diferentes elementos electrónicos, para su uso en una puerta automática corrediza para restringir y optimizar el acceso

al laboratorio de electrónica en CEUTEC. La implementación permitió demostrar que el sistema ofrece seguridad mediante contraseña, número limitado de intentos, modo de bloqueo y control con sensor RFID. Conjuntamente, se evaluó su rentabilidad y consumo eléctrico, obteniendo un sistema de bajo gasto energético y con un nivel de seguridad confiable.

En los inventarios, Lino (2022). Investigación materializada en Ecuador, con el título ***"Sistema web para el control de inventarios y prestamos de equipos de laboratorio de suelos de la carrera de ingeniería civil de la universidad estatal del sur de Manabí",*** se trata de desarrollar un sistema web para el control de inventarios y prestamos de equipos del laboratorio de suelos de la carrera de Ingeniería Civil de la Universidad Estatal del sur de Manabí. La implementación permitió demostrar que un sistema web logra un mayor control de inventario de los materiales, llevando registro de los materiales que entran y salen a la hora de realizar prácticas, logrando automatizar procesos.

Como cierre, Rodríguez (2024). Investigación llevada a cabo en México, titulada ***"Diseño de un módulo de monitoreo para un laboratorio remoto mediante dispositivos IoT",*** el proyecto busca el diseño e implementación de un Sistema de Monitoreo para un Laboratorio Remoto empleando dispositivos IoT, que permita supervisar y controlar mediante una plataforma web, el control del monitoreo en tiempo real. Se refleja que el sistema puede controlar de forma remota una cámara desplazable en el laboratorio, brindando control total, fortaleciendo la manipulación remota de los equipos y supervisión en tiempo real.

En primer lugar, la búsqueda y hallazgos presentados evidencian que la tecnología rfid es la más favorable de implementar para el control de acceso al laboratorio de telecomunicaciones. Además de ser de bajo costo, y con otras aplicaciones como sensor de ubicación.

Marco Teórico

Comprender el propósito del sistema al fundamentar los conceptos que sustentan el desarrollo de un prototipo de acceso, control y registro para laboratorios de ingeniería.

Este proyecto busca simplificar protocolos manuales mediante tecnologías, donde se abordan las bases teóricas relacionadas con la tecnología rfid, automatización de procesos, las bases de datos y sistemas de control de acceso. Estos componentes son fundamentales para el desarrollo de un sistema seguro y de fácil uso, capaz de gestionar la información en tiempo real para mejorar la administración e inventario en los laboratorios.

Tecnología Rfid

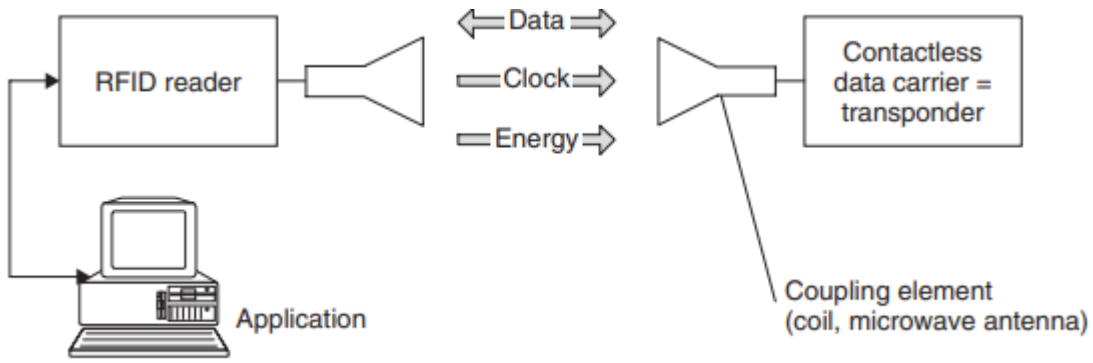
La tecnología rfid (Identificación por radiofrecuencia) es un sistema que utiliza campos electromagnéticos para identificar de forma automática tarjetas con información y objetos. Según Finkenzeller (2010), los sistemas RFID se relacionan directamente con las tarjetas inteligentes, pero a diferencia de estas últimas, la alimentación eléctrica del dispositivo portador de datos y el intercambio de datos entre este y el lector se realizan sin utilizar contactos galvánicos, sino campos magnéticos o electromagnéticos.

Un sistema RFID está compuesto invariablemente por dos componentes principales: "el transpondedor (etiqueta), que se localiza en el objeto a ser identificado, y el interrogador o lector,

que, dependiendo del diseño y la tecnología utilizada, puede ser un dispositivo de lectura o de lectura/escritura" (Finkenzeller, 2010, p. 6).

Figura 1

Componentes principales de un sistema rfid.



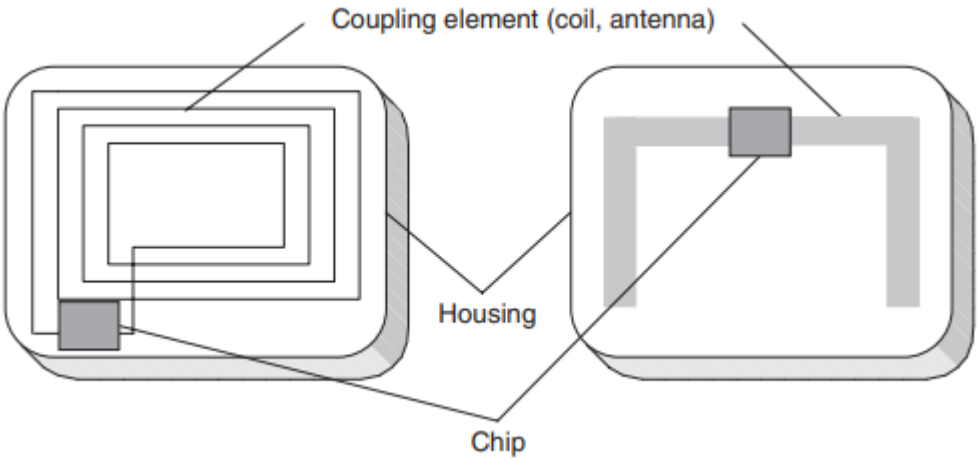
*Nota***:** recuperado de *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication (p.8),* K. Finkenzeller et al, 2010.

El transpondedor (Etiqueta o tag)

La etiqueta representa “el dispositivo portador de datos real en un sistema rfid y normalmente consta de un elemento de acoplamiento (antena) y un microchip electrónico” (Finkenzeller, 2010, p. 9).

Figura 2

Diseño de un transpondedor.



Nota: recuperado de *"RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication (p.8),* K. Finkenzeller et al, 2010.

Tipos de transpondedor

Hay dos categorías principales:

Transpondedor pasivo

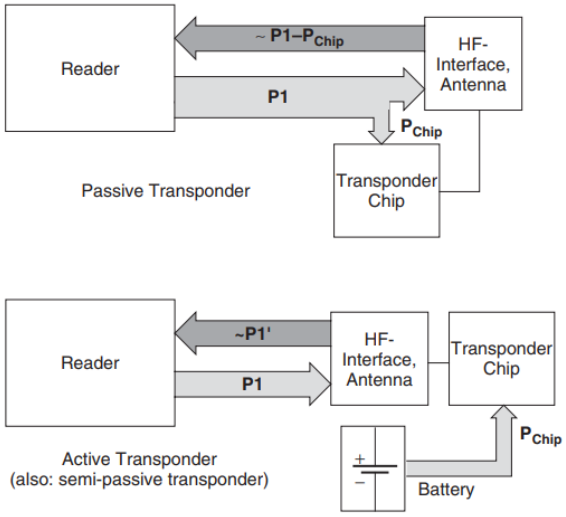
Los transpondedores pasivos no tienen ninguna fuente de alimentación. A través de la antena del transpondedor, el campo magnético o electromagnético del lector proporciona toda la energía necesaria para el funcionamiento del transpondedor. Esto significa que la energía emitida por el lector se utiliza para la transmisión de datos tanto desde el lector al transpondedor como de vuelta al lector. Si el transpondedor se encuentra fuera del alcance del lector, no tiene suministro de energía y, por lo tanto, no podrá enviar señales (Finkenzeller, 2010, p. 22).

Transpondedor activo

Los transpondedores activos tienen su propio suministro de energía. En este caso, la fuente de alimentación se utiliza para proporcionar voltaje al chip. Por lo tanto, el campo magnético o electromagnético recibido por el lector ya no es necesario para la alimentación eléctrica del chip. Eso significa que el campo puede ser mucho más débil que el campo necesario para el funcionamiento de un transpondedor pasivo (Finkenzeller, 2010, p. 22).

Figura 3

Comparación de modelo transpondedor activo y pasivo.



Nota: recuperado *de RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication (p.23),* K. Finkenzeller et al, 2010.

El interrogador (lector)

El lector es responsable de suministrar un campo electromagnético suficiente para activar la etiqueta y comunicarse con ellos. En consonancia Finkenzeller (2010), "un lector típicamente contiene un módulo de radiofrecuencia (transmisor y receptor), una unidad de control y un elemento de acoplamiento al transponder".

Antenas

Las antenas son parte esencial del sistema rfid. El diseño, y tamaño de las antenas dependen directamente de la frecuencia de operación del sistema, principalmente en el lector. Usualmente consisten en bobinas de alambre enrolladas en marcos rectangulares o circulares, diseñadas para generar campos magnéticos. Finkenzeller (2010) describe que "el lector genera un campo electromagnético de alta frecuencia que penetra el área transversal de la bobina y el área circundante".

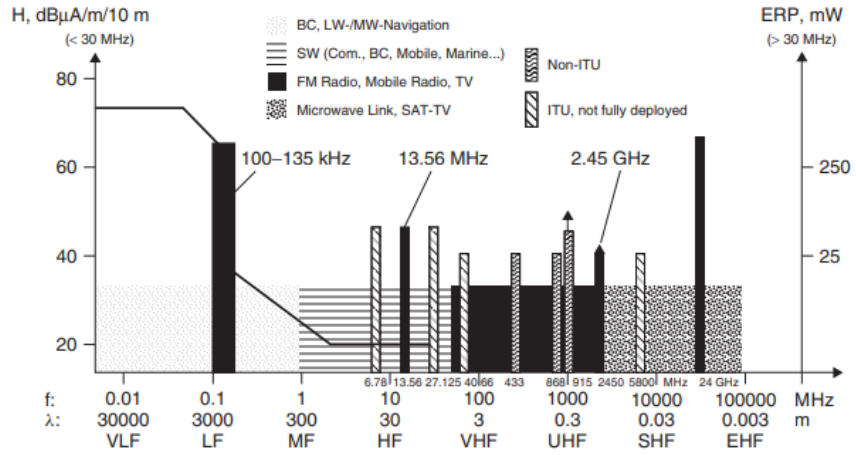
Frecuencias de operación

Dado que los sistemas rfid generan y emiten ondas electromagnéticas, están clasificados legalmente como sistemas de radio. El funcionamiento de otros servicios de radio no debe verse interrumpido ni perjudicado en ningún caso por el funcionamiento de los sistemas rfid.

Hay dos frecuencias de tipo ism (industrial, científico y médico), destinadas internacionalmente para aplicaciones no comerciales, para este caso de los sistemas rfid. Los rangos de frecuencias más usados son los de alta frecuencia (HF) 13.56 MHz y microondas 2.45GHz.

Figura 4

Rangos de frecuencia disponibles para los sistemas rfid.



Nota: recuperado de *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication,* K. Finkenzeller et al, 2010.

Alta Frecuencia - 13.56 MHz

Representa la banda más utilizada a nivel mundial para aplicaciones de tarjetas inteligentes sin contacto y sistemas de rango medio, la longitud de onda es de aproximadamente 22.1 metros, manteniendo al sistema en el campo cercano para distancias típicas de operación, donde el acoplamiento entre lector y transponedor sigue siendo de forma inductivo (magnético), aunque comienzan a aparecer componentes de radiación electromagnética.

Esta frecuencia proporciona un rango de lectura medio (de 10 cm a 1 metro), velocidades de transferencia de datos moderadas a altas (hasta 848 kbit/s), bajo consumo energético y la antena de transpondedor compactas (típicamente de 3 a 10 vueltas) (Finkenzeller, 2010, p. 243-256).

Sus aplicaciones incluyen sistemas de pago sin contacto (nfc), pasaportes electrónicos, control de acceso a edificios y áreas seguras, gestión de préstamos en bibliotecas, proporcionando una solución más versátil en el espectro de radiofrecuencia para identificación automática (Finkenzeller, 2010, p. 260-263).

Automatización

De acuerdo a lo establecido en la Encyclopaedia Britannica (s.f.), La automatización se ha convertido en algo indispensable dentro de los procesos industriales. Este término acuñado alrededor de 1946 por un ingeniero de Ford Motor Co., utilizado para describir una amplia variedad de sistemas en los que se sustituye significativamente la acción mecánica, eléctrica o computarizada por el esfuerzo y la inteligencia humana. En términos generales, la automatización se define como una tecnología capaz ejecutar un proceso mediante comandos programados combinados con control automático de retroalimentación para garantizar la correcta ejecución de las instrucciones. El sistema resultante es capaz de operar sin intervención humana.

Por otro lado, tenemos la automatización industrial, según Neobotik. (2021). "***¿Qué tipos de automatización industrial hay?***" habla de introducir equipos o software industrial que se encargue de realizar aquellas tareas repetitivas o más peligrosas para los trabajadores. El objetivo final es aumentar la productividad y reducir el porcentaje de error dentro de una cadena de trabajo.

Base de datos

Como afirma Marqués (2012), una base de datos es un conjunto de datos almacenados en memoria externa que están organizados mediante una estructura de datos. Cada base de datos ha sido diseñada para satisfacer los requisitos de información de una empresa u otro tipo de organización, como, por ejemplo, una universidad o un hospital.

Una base de datos se puede percibir como un gran almacén de datos que se define y se crea una sola vez, y que se utiliza al mismo tiempo por distintos usuarios.

Importancia de la base de datos

La importancia radica en su capacidad de recopilar, almacenar y gestionar información de manera rápida, estructurada y eficiente. Por otra parte, Marqués (2012), los sistemas de base de datos son fundamentales por varias razones como: control sobre la redundancia de datos, consistencia de datos, compartición de datos e integridad de datos.

Diseño de base de datos

Mendoza y López (2018). "***Bases de datos****",* el diseño de una base de datos no es un proceso sencillo. Habitualmente, la complejidad de la información y la cantidad de requisitos de los sistemas de información hacen que sea complicado; por este motivo, cuando se diseñan bases de datos es interesante aplicar la vieja estrategia de dividir para vencer. Por lo tanto, conviene descomponer el proceso del diseño en varias etapas; en cada una se obtiene un resultado intermedio que sirve de punto de partida de la etapa siguiente, y en la última etapa se obtiene el resultado deseado.

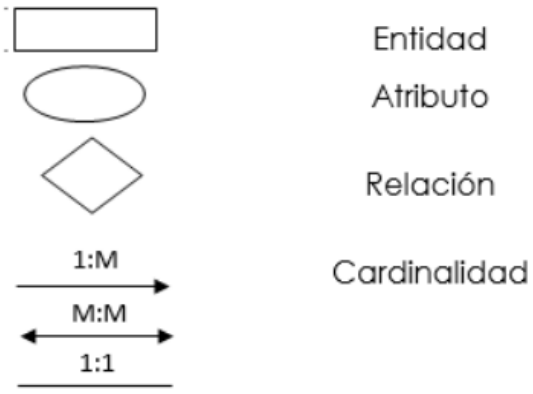
Etapa del diseño conceptual

Se realiza una estructuración con la información de la futura base de datos independiente de la tecnología que se empleará. No se tiene en cuenta todavía qué tipo de base de datos se utilizará (relacional, orientada a objetos, jerárquica); tampoco se tiene en cuenta con qué SGBD (sistema de gestión de base de datos) ni con qué lenguaje concreto se implementará la base de datos. El resultado de esta etapa es un modelo de flujo de información de alto nivel, uno de los más empleados es el modelo entidad relación (ER) y se obtiene luego de entrevistas, visitas y una investigación adecuada del sistema de información (Mendoza y López, 2018).

El diagrama de entidad relación utiliza formas para representar entidades, atributos y relaciones, reflejados en la figura 5.

Figura 5

Modelo relacional de base de datos.



Nota: recuperado de *Bases de datos*, A. Mendoza y R. López, 2018

Etapa del diseño lógico

En esta etapa se parte del resultado del diseño conceptual, que se transforma al tipo de base de datos a utilizar. Más concretamente, es preciso que se ajuste al modelo del SGBD (Estructura lógica utilizada por un Sistema Gestor de Bases de Datos para organizar y almacenar datos) con el que se desea implementar la base de datos. Por ejemplo, si se trata de un SGBD relacional, esta etapa obtendrá un conjunto de relaciones donde las entidades se transforman a tablas normalizadas con sus atributos, claves primarias y claves foráneas. El proceso de normalización que se aplica en esta etapa consiste en una serie de reglas que deben cumplir las tablas y relaciones obtenidas tras el paso del modelo entidad relación al modelo relacional, para entonces ser un modelo lógico. Las bases de datos relacionales se normalizan básicamente para: evitar la redundancia de los datos, evitar problemas de actualización de los datos en las tablas, proteger la integridad de los datos (Mendoza y López, 2018).

Existen varios niveles de normalización de base de datos, en este caso aplicaremos las tres primeras formas normales que se describen a continuación:

Primera forma normal (1FN):

Se eliminan todos los campos o atributos repetidos

Se asegura la atomicidad de los campos, en caso de existir atomicidad, se evalúa la creación de una nueva tabla

Cada tabla debe tener una llave primaria

Se asegura una dependencia funcional respecto a la llave primaria.

Segunda forma normal (2FN):

Debe cumplir la primera forma normal

No deben existir dependencias parciales: todos los campos no llaves deben depender solo de la llave primaria

Tercera forma normal (3FN):

Debe cumplir con la segunda forma normal

No deben existir dependencias transitivas: ningún campo debe depender de un campo no llave

Control de Acceso

Conforme a la unión internacional de telecomunicaciones (2021), procedimiento utilizado para determinar si se debe conceder a una entidad acceso a recursos, instalaciones, servicios o informaciones, sobre la base de normas preestablecidas, y la autoridad o los derechos específicos asociados a la parte solicitante.

Marco Legal

Tabla 1

Normativa colombiana de tratamiento de datos y uso de rfid.

LEY	ARTÍCULO	DESCRIPCIÓN	RELEVANCIA
Ley 1581 de 2012	Art. 3	Datos personales, datos sensibles, tratamiento, responsable.	Los registros de acceso son datos personales.
	Art. 4	Principios de tratamiento: legalidad, finalidad, libertad, seguridad.	Usar datos rfid solo para propósito de control de acceso, con protección adecuada.

LEY	ARTÍCULO	DESCRIPCIÓN	RELEVANCIA
	Art. 17	Deberes del responsable: seguridad, confidencialidad, actualización.	Las Instituciones deben proteger bases de datos con controles técnicos y administrativos.
Ley 1273 de 2009	Art. 269F	Violación de datos personales, acceso o uso sin autorización.	Cualquier ataque o filtración de la BD constituye delito informático.
	Art. 269G	Suplantación informática.	Clonación o uso indebido de tarjetas rfid es un delito tipificado.
Decreto 1377 de 2013	Art. 5	Autorización previa e informada del titular.	Los estudiantes deben aceptar el tratamiento de sus datos rfid.
	Art. 12	Medidas de seguridad para bases de datos.	Debe implementarse cifrado, control de roles y protección del servidor.

Nota: Marco normativo aplicable al sistema. Fuente: autoridad propia con base en la Ley 1581 de 2012, Ley 1273 de 2009 y Decreto 1377 de 2013.

Diseño metodológico

En este apartado se define el enfoque metodológico orientado al desarrollo de un prototipo de un sistema para el control de acceso mediante rfid a un laboratorio de ingeniería.

Metodología de desarrollo: modelo tipo v

El desarrollo del prototipo se hace bajo el modelo en V. El método en V se presenta como un modelo estructurado que relaciona cada fase del desarrollo con su correspondiente fase de validación y verificación, permitiendo un control riguroso de la calidad y cumplimiento de objetivos a lo largo del ciclo de vida del proyecto (Pressman, 2014).

Análisis de necesidades

La finalidad del sistema de control de acceso mediante rfid para el préstamo de equipos de un laboratorio de ingeniería será identificar, registrar, almacenar y gestionar tanto el ingreso como el préstamo de equipos. De forma que garantice la disponibilidad de la información en una base de datos y el sistema genere alertas predefinidas oportunas hacia un laboratorista, cuando se detecten eventos irregulares y accesos no autorizados.

Necesidades identificadas

- Automatización del proceso de identificación del estudiante al momento de acceder a un laboratorio.
- Registro en tiempo real de todos los eventos de acceso.
- Capacidad de notificación inmediata ante irregularidades de seguridad relevantes.
- Generación de reportes de asistencia y daños de equipos.

Objetivos del sistema

Los objetivos del sistema se basan en suplir las necesidades identificadas, tales como:

- Reducir el tiempo de acceso al laboratorio y los equipos.
- Eliminar la necesidad de supervisión humana continua para el préstamo de equipos.
- Mejorar la capacidad de respuesta ante incidentes de seguridad mediante alertas automáticas.

Especificación de funciones

Se establece de forma detallada las condiciones de operación, rangos de operación, protocolos de comunicación y respuestas del sistema ante diferentes casos de uso.

Características funcionales

- Hará la captura e identificación de tarjetas rfid mediante lectores ubicados en cajón de acceso.
- Validara las credenciales de acceso en una base de datos de usuarios autorizados en tiempo real.
- Registrará cada intento de acceso con información de tipo: número de referencia de la tarjeta, fecha, hora, puerta de acceso y resultado de la validación (autorizado/denegado).
- Almacenara de manera continua los registros de acceso en una base de datos.
- Generará alertas automáticas ante situaciones como: accesos fuera de horario autorizado, equipos sin retorno al laboratorio después del tiempo.
- Enviara notificaciones a personal administrativo mediante bot de telegram.
- Proporcionará una interfaz de administración para la gestión de usuarios y credenciales de acceso.

Características de desempeño

- Validara una credencial y activara la apertura de una cerradura de acceso en un tiempo máximo de 5 segundos.
- La distancia de lectura del transpondedor debe ser como mínima de 3 cm y máxima de 5 cm.

- Los datos de usuarios y registros deberán almacenarse de forma rápida, segura y eficiente.
- La interfaz administrativa deberá ser intuitiva y fácil de acceder.
- El prototipo debe ser de bajo costo y fácil implementación.

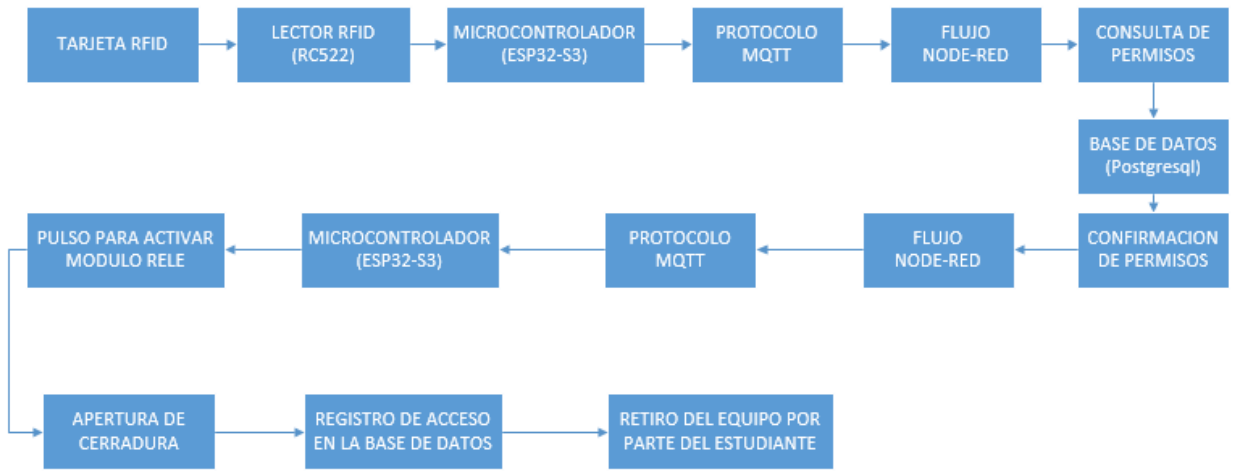
Diseño arquitectónico

Se define la arquitectura general del sistema, eligiendo los componentes, sus conexiones e interrelaciones y software a utilizar. Por consiguiente, la arquitectura se divide en tres fases.

Diagrama del sistema

Figura 6

Diagrama de bloques de operación del sistema.



Nota: Diagrama de bloques paso a paso de operación del sistema. Fuente: autoridad propia (2026).

Selección de componentes

Tabla 2

Listado de componentes.

COMPONENTE	REFERENCIA	JUSTIFICACIÓN
LECTOR RFID	RC522	Bajo costo, amplia documentación, fácil integración con microcontroladores.
	PN532	Compatible con NFC (para uso de celulares), cifrado mejorado, soporta más protocolos.
MICROCONTROLADOR	ESP32	Wifi integrado, mayor velocidad de procesamiento, ideal para sistemas de acceso con conexión a red.
	Raspberry Pi (Pi 3B, Pi Zero 2 W)	Corre linux, base de datos local, integración de servidor web, software de control.
	Arduino Uno	Estable, fácil de programar, soporte directo con RC522 Y PN532.
TECLADO MATRICIAL	Touch Ttp229 4x4	Respuesta táctil rápida, mayor durabilidad, cero desgaste
	Membrana Matricial 4x3	Integración sencilla con Arduino/ESP32, adhesivo a superficies
	Profesional 3x4 Formato PCB	Resistencia, duradero y profesional, fijación por tornillos
CERRADURA	Pendiente	
FUENTE DE ALIMENTACIÓN	Fuente DC 12V/2–5A	Entrega el voltaje y la corriente suficiente para alimentar de forma estable el sistema.

Nota: Tabla de análisis de distintos componentes. Fuente: autoridad propia con apoyo de inteligencia artificial (2026).

Selección de Software

Tabla 2

Listado de software.

COMPONENTE	REFERENCIA	JUSTIFICACIÓN
BASE DE DATOS	MY SQL	fácil de integrar con ESP32, PHP, Python para logeos de acceso.
	SQLITE	Base de datos ligera que no necesita servidor; ideal para sistemas locales.
SERVICIO SMTP	Gmail SMTP	Wifi integrado, mayor velocidad de procesamiento, ideal para sistemas de acceso con conexión a red.
	Bot Telegram	Útil si no se quiere depender de servicios externos.
PANEL DE ADMINISTRACION	Node-Red	Un solo archivo JSON, ideal para sistemas pequeños.

Nota: Tabla de análisis de distintos softwares. Fuente: autoridad propia con apoyo de inteligencia artificial (2026).

Cronograma

Tabla 3

Cronograma de actividades.

Actividad	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14
Análisis del proyecto	X													
Diseño del sistema	X													
Compra de componentes		X												
Conexión de hardware			X											
Programación ESP32				X	X									
Integración RFID						X								
Configuración MQTT						X								
Desarrollo Node-RED							X	X	X	X	X			
Pruebas del sistema											X	X		
Ajustes finales													X	X

Nota: Cronograma del trabajo de grado. Fuente: autoridad propia (2026).

Presupuesto

Tabla 4

Costos fijos

Materia prima	Cantidad	V/unitario	V/total
ESP32-S3	1	$45.000	$45.000
RFID RC522	2	$10.000	$10.000
Tarjetas RFID	2	$1.500	$3.000
Módulo relé 4 canales	1	$20.000	$20.000
Cerraduras electromagnéticas	4	$30.000	$120.000
Fuente 12V	1	$25.000	$25.000
Pantalla LCD 20x4 I2C	1	$35.000	$35.000
LM2596 Step-down	2	$6.000	$12.000
Lector/Escritor RFID	1	$50.000	$50.000
Condensador (100uF)	2	$100	$200
Diodos (1N4007)	4	$200	$800
Borneras	6	$400	$2.400
Cables	2M	$2.000	$4.000
TOTAL:		$225.200	$324.400

Nota: Presupuesto del proyecto. Fuente: autoridad propia (2026).

Tabla 5

Mano de obra

Mano de obra	Cantidad	V/unitario	V/total
Programación ESP32	1	$100.000	$100.000
Integración RFID + MQTT	1	$90.000	$90.000
Diseño en Node-RED	1	$600.000	$600.000
Montaje electrónico	1	$100.000	$100.000
Pruebas y depuración	1	$300.000	$300.000
TOTAL:		$1.190.000	$1.190.000

Nota: Presupuesto de mano de obra del proyecto. Fuente: autoridad propia (2026).

Tabla 6

Costos totales

Concepto Valor	Valor
Costos fijos	$324.400
Mano de Obra	$1.190.000
Total general	$1.514.400

Nota: Valor total. Fuente: autoridad propia (2026).

Desarrollo del proyecto

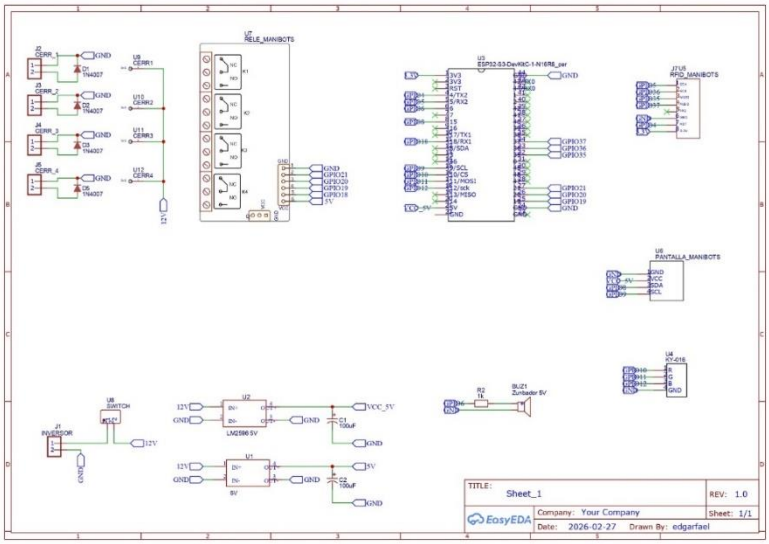
Objetivo 1

Diseñar un prototipo de acceso y control que permita la automatización de préstamos y devolución de equipos:

Para cumplir este objetivo, se diseñó un prototipo basado en el uso del microcontrolador ESP32 como unidad principal de procesamiento, debido a su capacidad de conectividad inalámbrica y compatibilidad.

Figura 7

Esquemático automatización préstamo de equipos.



Nota. Desarrollo de esquemático en easyeda. Fuente: autoridad propia (2026).

El diseño esquemático del sistema electrónico se realizó mediante el software EasyEDA, una herramienta de diseño asistido que permite representar de manera gráfica la interconexión de los componentes que conforman el prototipo. En esta etapa se definieron las conexiones eléctricas entre el microcontrolador, los sensores, el módulo de comunicación y los dispositivos

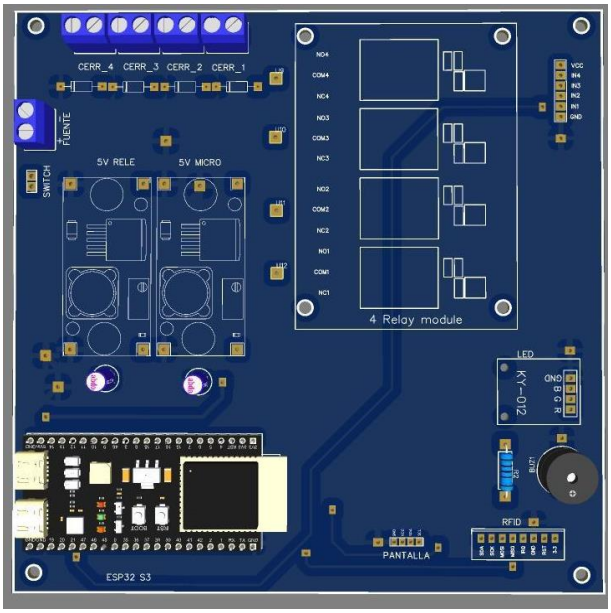
de control, con el propósito de verificar el correcto funcionamiento del circuito antes de la fabricación física de la tarjeta o del montaje del prototipo.

El esquemático constituye una fase fundamental dentro del desarrollo del proyecto, ya que permite identificar la distribución de señales, alimentación eléctrica y comunicación entre los diferentes módulos del sistema, reduciendo errores durante la implementación y facilitando posteriores procesos de prueba, mantenimiento y documentación técnica.

Una vez definidos los implementos necesarios en el sistema de registro, se realizó el diseño del circuito impreso (PCB) en donde fue posible organizar las conexiones eléctricas entre el microcontrolador y los demás elementos del sistema, optimizando el espacio disponible y garantizando una mejor integración del prototipo

Figura 8

Diseño 3d elaborado en el programa easyeda.



Nota: Modelo 3d de la placa. Fuente: autoridad propia (2026).

El sistema incorpora un lector RFID encargado de identificar a cada usuario mediante tarjetas previamente registradas en la base de datos del sistema. Cuando el usuario acerca la tarjeta al lector, el sistema valida la información y determina si el préstamo de los elementos puede realizarse.

Figura 9

Modulo rc522 y tarjeta rfid.



Nota: módulo rc522. Fuente: autoridad propia (2026).

Además, se integró un mecanismo de apertura con cerraduras electromagnéticas para permitir el acceso controlado al compartimiento donde se encuentran almacenados los equipos. De esta manera, el prototipo reduce la intervención manual del administrador y mejora el control sobre la entrega de los dispositivos.

Figura 10

Placa pcb con componentes soldados y cerraduras tipo celenoide conectada.



Nota: Conexiones y prueba de cerradura. Fuente: autoridad propia (2026).

Para complementar el desarrollo visual del proyecto, se elaboró un render en 3D del armario utilizando la plataforma SketchUp. Esta herramienta permite representar digitalmente la estructura física del prototipo antes de su construcción, facilitando la visualización del diseño general, la distribución de los compartimientos y la ubicación de los componentes electrónicos dentro del sistema. Mediante el modelado en tres dimensiones fue posible analizar aspectos relacionados con el tamaño, la proporción y la funcionalidad de la cajonera, lo que contribuyó a realizar ajustes previos en el diseño y mejorar la presentación del proyecto desde una perspectiva técnica y estética.

Figura 11

Render de armario realizado en sketchup.



Nota: Diseño del armario. Fuente: autoridad propia (2026).

Como resultado, el desarrollo del diseño electrónico, la incorporación del sistema de identificación por radiofrecuencia y la implementación del mecanismo de apertura automatizada permitieron materializar un prototipo orientado al control inteligente de préstamos y devoluciones de equipos. La integración de estos elementos en una única estructura funcional contribuyó a mejorar la administración de los recursos disponibles, optimizar los tiempos de operación y fortalecer la seguridad durante el proceso de acceso. Además, la validación previa del diseño mediante herramientas de simulación y modelado permitió garantizar una adecuada correspondencia entre la parte electrónica y la estructura física del sistema.

Objetivo 2

Implementar un sistema de registro que almacene y gestione la información de los usuarios, préstamo de equipos y permisos.

La comunicación entre el hardware y la plataforma de gestión se realizó mediante el protocolo MQTT, el cual permite el envío de datos en tiempo real entre el microcontrolador y el servidor local. Para la visualización y administración de la información se utilizó Node-RED, donde se diseñó una interfaz que permite:

- Registrar usuarios.
- Asociar tarjetas RFID a cada usuario.
- Consultar historial de préstamos.
- Conceder los permisos al usuario.

El sistema almacena automáticamente cada transacción realizada, permitiendo llevar un control detallado de la utilización de los implementos por parte del usuario.

Diseño de la base de datos

Para almacenar la información, se diseñó una base de datos relacional utilizando postgresql la cual permite una gestión estructurada y segura de los datos. Además, el soporte nativo de postgresql ofrece un gran portafolio de funciones incorporadas para extraer, editar y construir estructuras json directamente en sql.

El modelo de datos se compone principalmente de:

- **Tabla de usuarios (users)**

  Almacena la información básica de cada usuario, incluyendo su identificador único (UID), nombre y código de acceso.

Figura 12

Tabla de datos de usuarios, información de usuarios.

	id [PK] integer	uid character varying (50)	username character varying (100)	code character varying (10)	created_at timestamp without time zone	updated_at timestamp without time zone
1	19	00194360	camilo	12345678	2026-04-26 23:01:34.080004	2026-04-26 23:01:34.080004

Nota: Tabla de registro de usuarios. Fuente: autoridad propia (2026).

- **Tabla de permisos (permissions)**

  Permite asociar a cada usuario los permisos correspondientes para el acceso a diferentes cerraduras o recursos del sistema.

Figura 13

Tabla de datos, asignación de permisos de cerraduras.

	id [PK] integer	uid character varying (50)	lock1 boolean	lock2 boolean	lock3 boolean	lock4 boolean	updated_at timestamp without time zone
1	25	00194360	false	false	false	true	2026-04-27 18:28:59.927714

Nota: Tabla de permisos de usuarios. Fuente: autoridad propia (2026).

- **Tabla de registros de acceso (access_logs)**

  Almacena el historial de eventos de acceso, incluyendo el uid, nombre del usuario, estado del acceso (permitido o denegado), y las cerraduras activadas.

Figura 14

Tabla de datos, historial de eventos.

	id [PK] integer	uid character varying (50)	username character varying (100)	status character varying (20)	locks_opened text	timestamp timestamp without time zone
1	28	00194360	Camilo	granted	Cerradura 1, Cerr...	2026-04-26 14:58:01.003998
2	29	00194360	Camilo	denied	Sin permisos	2026-04-26 14:58:27.29547
3	30	43D84106	No registrado	denied	Sin registro	2026-04-26 14:58:53.120047
4	31	00194360	Camilo	granted	Cerradura 1, Cerr...	2026-04-26 14:59:16.073522

Nota: Tabla de historial de accesos. Fuente: autoridad propia (2026).

Se establecieron relaciones entre las tablas mediante claves foráneas, asegurando la integridad referencial. En particular, la tabla de permisos se relaciona con la tabla de usuarios a través del campo uid, permitiendo eliminar automáticamente los permisos asociados en caso de eliminación de un usuario.

Este diseño permite garantizar la trazabilidad de los eventos y una adecuada gestión del inventario y los accesos.

Implementación del sistema de registro

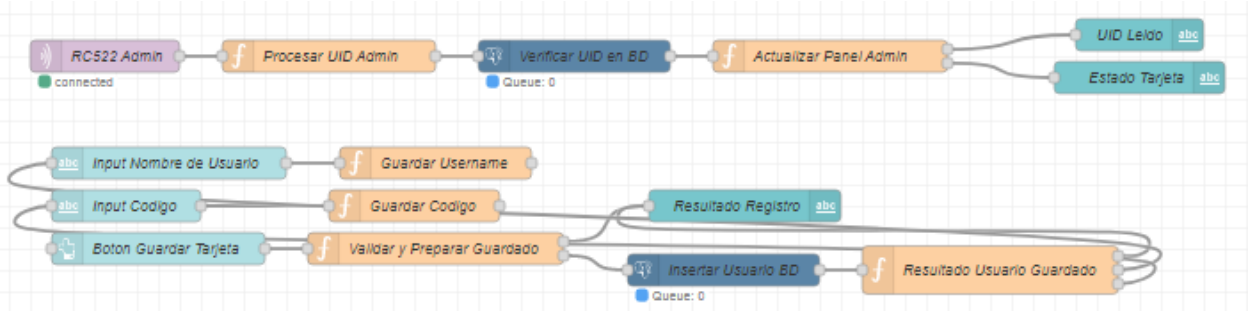
Registro de usuarios

El registro se hace por medio de tarjetas rfid grabadas previamente por el administrador del laboratorioa usuarios y/o estudiantes nuevos, de las cuales se obtiene un identificador único (uid). Este uid es procesado y utilizado como clave principal para el almacenamiento de la información del usuario.

A través del flow desarrollado en Node-RED, el administrador puede ingresar el nombre y un código asociado al usuario. Posteriormente, esta información se almacenada en la base de datos por medio de consultas sql parametrizadas, garantizando la integridad de los datos y evitando duplicidades.

Figura 15

Flujo del registro de usuario en node-red.



Nota: Nodo de registro. Fuente: autoridad propia (2026).

Gestión de permisos

El flujo permite asignar permisos específicos a cada usuario, los cuales determinan el acceso a diferentes cerraduras donde están los equipos del laboratorio.

Mediante la interfaz gráfica (dashboard), el administrador puede habilitar o deshabilitar el acceso a cada cerradura utilizando controles tipo interruptor. Estos permisos son almacenados en la base de datos y pueden ser modificados en cualquier momento.

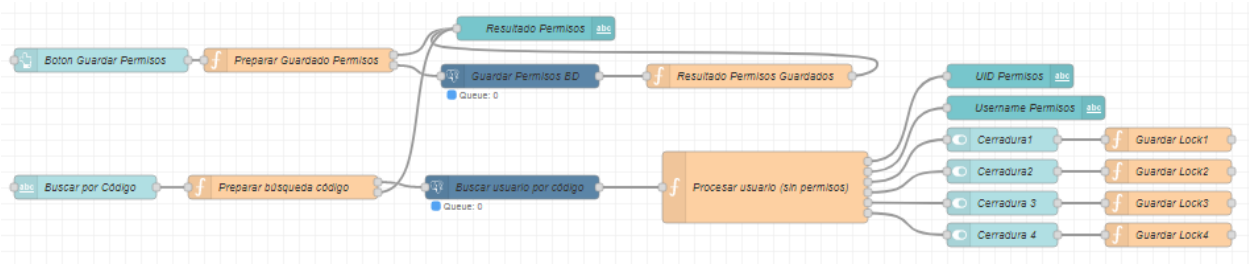
La gestión de permisos en el sistema se implementa mediante el uso de variables booleanas, las cuales permiten ver el estado de acceso a cada una de las cerraduras controladas.

En la base de datos, estos permisos se almacenan en la tabla permisos, donde los campo (lock1, lock2, lock3, lock4) corresponde a una cerradura y puede tomar valores de tipo booleano

(true o false). Un valor true indica que el usuario tiene permiso para activar la cerradura correspondiente, mientras que un valor false indica que el acceso está restringido.

Figura 16

Flujo de los permisos de usuario en node-red.



Nota: Nodo de permisos. Fuente: autoridad propia (2026).

Registro de accesos

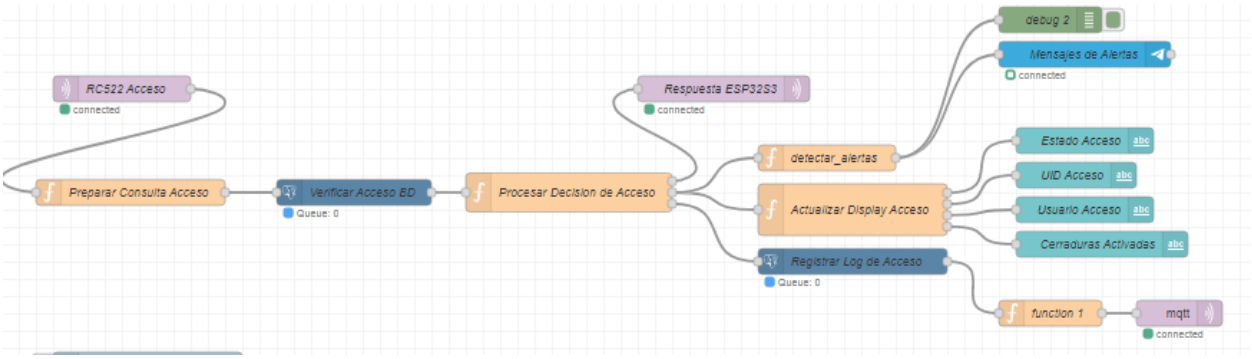
Cada vez que un usuario y/o estudiante intente acceder a los equipos de laboratorio, se realiza una validación del uid en la base de datos. Si el usuario está registrado y tiene permisos activos, el acceso es concebido y de lo contrario, se deniega.

Cada evento es registrado en la tabla de historial (access_logs), incluyendo información relevante como el usuario, el estado del acceso y las cerraduras activadas.

Este registro permite mantener un control detallado de todas las interacciones con el sistema rfid, facilitando auditorías de ingresos, seguridad para su análisis posterior.

Figura 17

Flujo del acceso de usuario en node-red.



Nota: Nodo de acceso. Fuente: autoridad propia (2026).

Desarrollo del dashboard

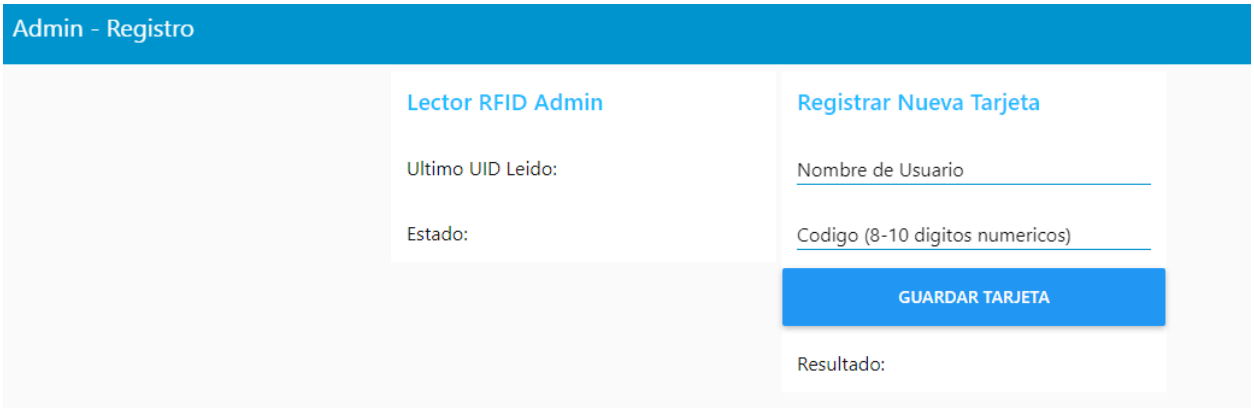
El dashboard se divide en diferentes secciones:

- **Panel de registro**: permite la creación y actualización de usuarios.
- **Panel de permisos**: facilita la asignación y modificación de accesos.
- **Panel de historial**: muestra en tiempo real los registros de acceso almacenados en la base de datos.
- **Panel de estado**: indica si un acceso fue permitido o denegado.

La interfaz fue diseñada para ser intuitiva y facilitar la administración del sistema sin requerir conocimientos avanzados por parte del laboratorista o administrador.

Figura 18

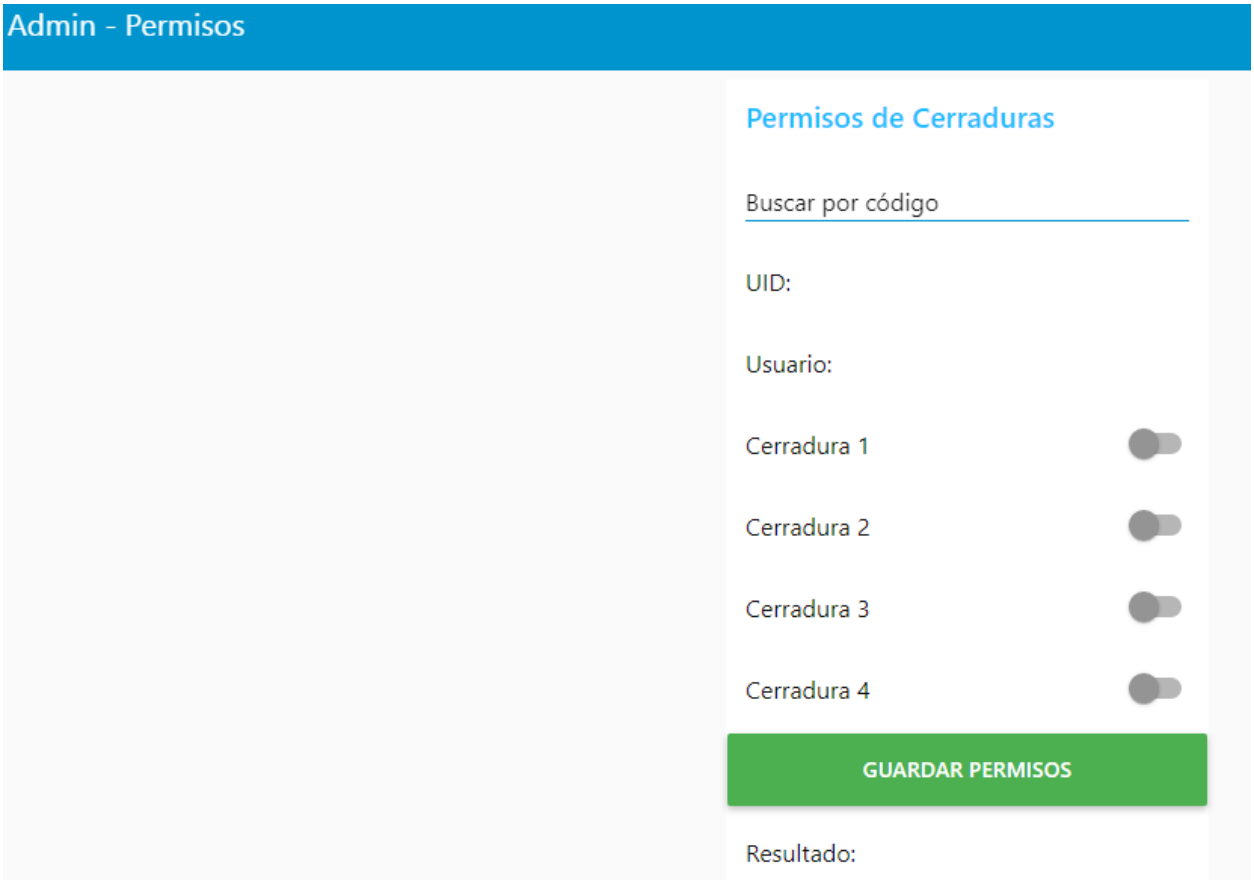
Panel de registro.



Nota: Interfaz gráfica del panel de registro. Fuente: autoridad propia (2026).

Figura 19

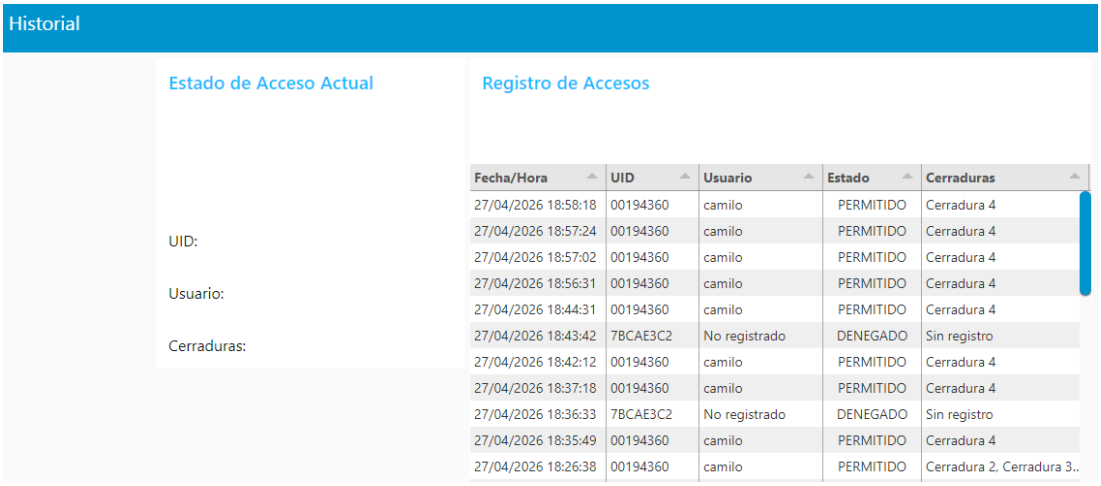
Panel de permisos.



Nota: Interfaz de selección de cerraduras. Fuente: autoridad propia (2026).

Figura 20

Panel de historial y estado de acceso.



Nota: Interfaz de revisión de historial. Fuente: autoridad propia (2026).

Integración con el sistema de alertas

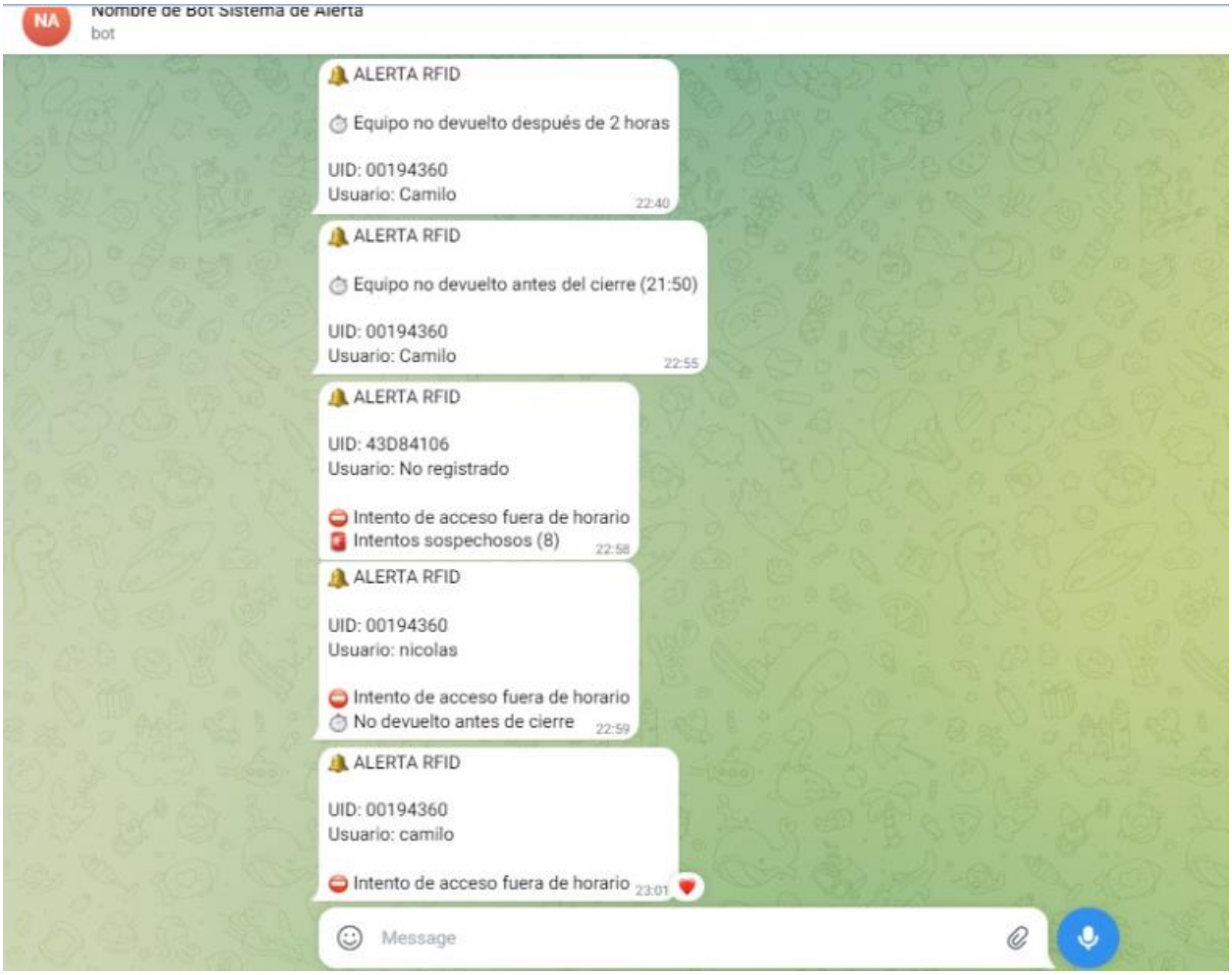
Para la seguridad del sistema, se implementó un módulo de alertas utilizando un bot de Telegram, el cual permite notificar al administrador en tiempo real sobre eventos críticos.

- Accesos fuera del horario permitido.
- Equipos no devueltos dentro del tiempo establecido.
- Intentos de acceso repetidos considerados sospechosos.

Estas alertas son generadas a partir de los eventos de acceso y enviadas automáticamente al laboratorista y/o administrador mediante el bot de Telegram, permitiendo una respuesta oportuna ante posibles incidentes.

Figura 21

Mensajes de alerta para el laboratorista usando un bot de telegram.



Nota: Captura de bot de telegram. Fuente: autoridad propia (2026).

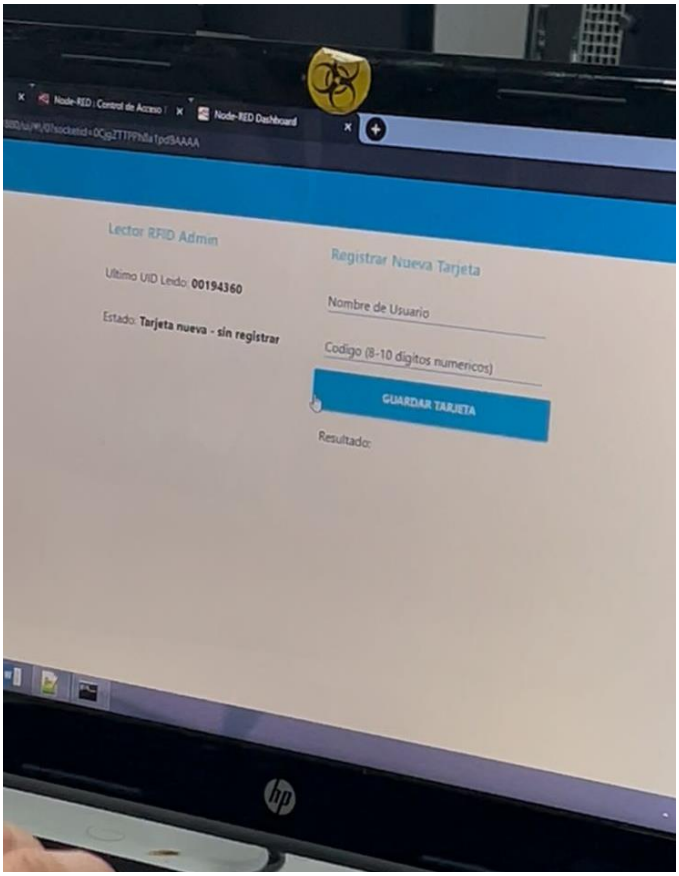
Objetivo 3

Probar y validar el prototipo para evaluar su funcionalidad, eficiencia y facilidad de uso.

La validación del prototipo se realizó mediante pruebas en un entorno controlado para verificar el correcto funcionamiento de sus componentes, donde la validación del registro correcto de nuevos usuarios en la interfaz desarrollada en node-red.

Figura 22

Reconocimiento de un uid sin registrar.



Nota: Testeo de interfaz gráfica. Fuente: autoridad propia (2026).

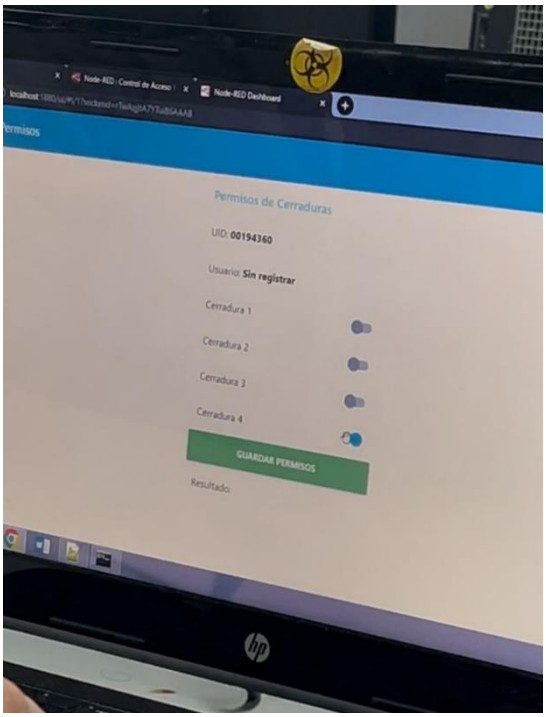
Para verificar el correcto funcionamiento del proceso de registro de usuarios, se realizaron pruebas sobre la interfaz administrativa implementada en node-red, destinada a la asociación de nuevas tarjetas rfid con la información correspondiente de cada usuario. Durante esta prueba, el sistema detectó automáticamente el uid de una tarjeta acercada al lector, mostrando en pantalla el último código leído junto con el estado de la tarjeta, indicando si esta se encontraba registrada o disponible para su vinculación dentro del sistema.

Posteriormente, mediante el formulario de registro, se ingresaron los datos requeridos del usuario, como el nombre y su número de cedula, los cuales fueron asociados al uid detectado. Una vez completados los campos solicitados, se ejecutó la acción de almacenamiento a través del botón de registro, permitiendo que la información fuera enviada al sistema para su procesamiento y posterior almacenamiento en la base de datos. La respuesta mostrada en la interfaz permitió confirmar que el procedimiento se realizó de manera satisfactoria, garantizando que cada tarjeta quedara vinculada de forma única a un usuario autorizado.

Esta validación permitió comprobar que la plataforma desarrollada puede gestionar correctamente el registro inicial de usuarios, facilitando la administración del sistema de acceso y asegurando la integridad de la información almacenada para futuras operaciones de préstamo y devolución de equipos.

Figura 23

Asignacion de permisos de cerraduras.



Nota: Testeo de asignación de permisos. Fuente: autoridad propia (2026).

Con el fin de verificar el funcionamiento del sistema de autorización, se realizó la evaluación del módulo encargado de la asignación de permisos para el acceso a los equipos almacenados dentro del prototipo. A través de la interfaz desarrollada en node-red, el sistema mostró el identificador único de la tarjeta rfid detectada y permitió visualizar el estado del usuario asociado antes de definir los permisos correspondientes.

Dentro de esta interfaz se habilitó una sección destinada a la configuración individual de cada cerradura, donde fue posible seleccionar de manera independiente cuáles compartimientos podían ser habilitados para una tarjeta específica. Mediante interruptores de activación, el administrador pudo establecer qué equipos estarían disponibles para cada usuario según los

permisos asignados. Consecutivamente, al ejecutar la opción de almacenamiento, la información fue registrada en el sistema para ser utilizada durante futuras validaciones de acceso.

La prueba permitió comprobar que el sistema puede gestionar de forma correcta la concesión de permisos personalizados, garantizando que cada usuario únicamente tenga acceso a los compartimientos previamente autorizados. De esta manera, se confirmó que el proceso de control implementado fortalece la seguridad del prototipo y mejora la administración de los equipos dentro del laboratorio.

Prueba de actualización en tiempo real de la información mostrada en la plataforma.

Durante la fase de validación se observó que el sistema logró transmitir la información correctamente entre el hardware y la plataforma de administración, permitiendo un control más organizado del inventario y una interacción sencilla para el usuario encargado.

Los resultados obtenidos demostraron que el prototipo presenta un funcionamiento estable, una respuesta adecuada en la comunicación de datos y una interfaz comprensible para la gestión de usuarios y equipos.

Conclusiones

El resultado de la operatividad del prototipo evidencia que el objetivo general fue alcanzado, porque el sistema puesto a prueba permitió supervisar en tiempo real el acceso y registro de los dispositivos de laboratorio mejorando los tiempos de entrega.

Se diseñó un prototipo de acceso y control de registro, orientado a la automatización del préstamo de equipos, permitiendo agilizar procesos que anteriormente se realizaban de manera manual. Este prototipo integra tecnologías rfid, microcontroladores con la capacidad de consultar bases de datos para verificar permisos y emitir decisiones a otros circuitos para garantizar o denegar el acceso. Asimismo, la integración de software (dashboard) practico para el monitoreo permitió optimizar la supervisión del sistema y mejorar la administración de los equipos del laboratorio. Las pruebas realizadas en tiempo real con usuarios reales evidenciaron un funcionamiento estable, logrando reducir los tiempos asociados al préstamo de equipos y las pruebas de acceso no autorizado demostraron la capacidad del prototipo para responder ante intentos forzados sin permisos. Gracias a este prototipo, se redujeron tiempos de espera, se minimizan errores humanos. Además, el prototipo demostró ser una alternativa eficiente y adaptable para entornos académicos o también empresariales donde se requiera un control seguro y automatizado a recursos físicos.

Se implementó un dashboard programado y ejecutado en node-red que cumple como centro de monitoreo y administrativo. Por consecuente, se integra a postgresql para apoyar el sistema de almacenamiento de datos. La integración de ambos sistemas permitió organizar mejor la información relacionada con uid de las tarjetas rfid, identificación e ingreso de nuevos usuarios, concebir o denegar permisos, horarios de ingreso y actualizaciones de registros,

garantizando una administración más organizada. Las pruebas realizadas evidenciaron un adecuado desempeño del sistema, destacándose por sus buenos tiempos de respuesta para realizar consultas y la confiabilidad en el manejo de la información, garantizando un acceso rápido y seguro.

Las pruebas realizadas al prototipo permitieron evaluar y comprobar el correcto funcionamiento del sistema en diferentes escenarios de uso, verificando la precisión en el registro de acceso a los equipos, como la estabilidad de la comunicación entre los dispositivos implementados. Durante el proceso de evaluación se verifica el correcto funcionamiento de los mecanismos de lectura rfid, autenticación de usuarios, apertura de cerraduras solenoides, registro automático de préstamos, así como el envío de alertas a través de telegram y que la integración entre los diferentes módulos del sistema no afectara los tiempos de respuestas generando cuello de botella, lo que contribuyó a fortalecer el desempeño general del proyecto.

El sistema fue sometido a diferentes pruebas de acceso no autorizado como los diferentes uid de tarjetas rfid, tarjetas tipo nfc, tags, número de intentos en el menor tiempo con la justificación de saturar el sistema para confirmar el correcto funcionamiento de los mecanismos de restricción y validación de permisos, fortaleciendo la seguridad en el acceso a los equipos de laboratorio. Por otra parte, las pruebas prácticas realizadas con personas externas al prototipo permitieron validar la facilidad de uso del dashboard administrativo y la navegación intuitiva de la plataforma, favoreciendo la interacción de los usuarios con el sistema de gestión y control. Finalmente, se identificaron mejoras relacionadas con la dependencia de la red y el desarrollo futuro de una pcb con relés independientes para cada cerradura, con el fin de garantizar una mejor escalabilidad, robustez y protección de picos de voltaje en el prototipo.

Alcances

El sistema es un control de acceso automatizado mediante rfid, que permite la identificación y registro automático de los estudiantes que toman prestados equipos del laboratorio. Para ello, cada intento de acceso es validado en tiempo real en una base de datos (postgresql), la cual determina si la tarjeta cuenta con la autorización para permitir o denegar el ingreso. Adicionalmente, el sistema tiene un registro histórico de todos los accesos, incluyendo ingresos autorizados, accesos denegados e intentos repetitivos. Este historial garantiza la trazabilidad de los préstamos de equipos del laboratorio, facilitando procesos de consulta y auditoría cuando sean requeridos.

En cuanto a la seguridad, el sistema incorpora un chat bot en telegram para la generación de alertas automáticas que notifica al administrador ante la detección de accesos no autorizados, retardo en devolución de equipos y otros eventos. Estas notificaciones permiten una respuesta oportuna frente a situaciones que puedan comprometer la seguridad del laboratorio y los equipos que lo conforman.

Finalmente, se incluye la implementación de una interfaz de administrador, diseñada como el puente de interacción entre el sistema y quienes lo gestionan. A través de esta interfaz, el administrador podrá consultar el historial de accesos, conceder permisos y visualizar en tiempo real las alertas generadas por el sistema, sin necesidad de conocimientos técnicos avanzados.

Limitaciones

La seguridad del prototipo es básica, suficiente para el contexto académico al que está destinado. No obstante, es importante señalar que no se implementarán mecanismos de seguridad como cifrado extremo a extremo o autenticación multifactor. Estas características, quedan fuera del alcance del presente proyecto, dado que su implementación excedería los recursos y el tiempo disponibles para el desarrollo del prototipo. En cuanto al sistema de alertas, el prototipo generará únicamente notificaciones de carácter urgente y no se contempla el desarrollo de dashboards avanzados para el monitoreo y visualización de datos.

El prototipo tiene una dependencia directa de la infraestructura de conectividad del laboratorio, a través de una red wifi o lan. Esta condición implica que cualquier interrupción en la red podría afectar la validación en tiempo real de los carnets y el registro oportuno de los eventos de acceso.

El sistema está centrado en mayor parte al control de acceso a los equipos del laboratorio, limitándose al tipo de registro ya mencionado y no se desarrollará un sistema completo de gestión de préstamos de equipos que incluya disponibilidad o reservas, con el propósito de ser visualizados en el dashboard. En caso de que alguna funcionalidad básica en este sentido resulte necesaria para el prototipo, podrá incorporarse de manera sencilla y sin la necesidad de modificar todo el sistema.

Recomendaciones

Se recomienda que por parte de la institución de educación un número telefónico oficial asignado exclusivamente al laboratorio, el cual debe ser utilizado para el bot de telegram a través del cual el sistema envía las alertas automáticas. El uso de un número oficial garantiza la continuidad del servicio de notificaciones, evitando interrupciones derivadas del cambio de número personal del administrador, cambios de turno de personal o de la pérdida de acceso a la cuenta vinculada.

Se sugiere establecer una contraseña de acceso a la interfaz web de node-red, dado que la plataforma no requiere autenticación para ingresar desde la dirección ip local, sin esta medida, cualquier persona que se encuentre dentro de la red del laboratorio podría modificar los flujos del sistema o alterar su configuración. La contraseña puede configurarse editando el archivo settings.js ubicado en el directorio de datos de node-red y habilitando el parámetro adminauth.

En cuanto al diseño del circuito electrónico y la pcb, se aconseja utilizar un módulo de relé independiente por cada cerradura controlada, en lugar de emplear un módulo de cuatro relés en una sola placa como se realizó en el prototipo expuesto. Esta decisión obedece a fallos durante las pruebas del sistema, debido a que los picos de voltaje inverso generados al activar una cerradura pueden dañar el módulo completo, dejando inoperativas todas las salidas simultáneamente. Sin embargo, al usar relés individuales y ante un eventual fallo eléctrico afectaría únicamente el canal comprometido, preservando el funcionamiento del resto del sistema.

Referencias

Casquete Rodríguez, J. P., & Cedeño López, J. E. (2024). *Implementación de un sistema de control de accesos mediante módulos biométricos y tarjeta RFID de los laboratorios de la Carrera de Agroindustria de la Facultad de Ciencias de la Vida y Tecnología de la Uleam* [Tesis de pregrado, Universidad Laica Eloy Alfaro de Manabí]. https://repositorio.uleam.edu.ec/handle/123456789/7171

Castro Vega, L. A., & Pin García, L. J. (2023). *Implementación de un sistema integral de seguridad mediante tecnología RFID en el laboratorio de cómputo número catorce en la Facultad de Ciencias Técnicas de la carrera Tecnología de la Información de la Universidad Estatal del Sur de Manabí* [Tesis de pregrado, Universidad Estatal del Sur de Manabí]. http://repositorio.unesum.edu.ec/handle/53000/4752

Duque-Suárez, M. C., Clavijo-Pérez, C. M., Molina-Granados, J. E., & Duque-Suárez, O. M. (2023). Sistema de control de acceso utilizando tecnologías RFID. *Revista TEINNOVA, 7*(1), 23–31. https://doi.org/10.23850/25007211.5479

Finkenzeller, K. (2010). *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, third edition* [Manual de RFID: fundamentos y aplicaciones en tarjetas inteligentes sin contacto, identificación por radiofrecuencia y comunicación de campo cercano, tercera edición]. Wiley.

Gutiérrez Díaz, E. R. (2024). *Prototipo de sistema de control de acceso utilizando tecnología RFID* [Tesis de pregrado, Universidad Distrital Francisco José de Caldas]. http://hdl.handle.net/11349/41732

Mendoza, A., & López, R. (2018). *Bases de datos*. Universidad de Chile. https://repositorio.uchile.cl/bitstream/handle/2250/151632/Bases-de-datos.pdf?sequence=1&isAllowed=y

Pressman, R. S. (2014). *Ingeniería de software: Un enfoque práctico (7a ed.)*. McGraw-Hill.

Peñafiel, K. A. (2023). *Sistema web para el control de inventarios y préstamos de equipos del laboratorio de suelos de la carrera de Ingeniería Civil de la Universidad Estatal del Sur de Manabí* [Tesis de pregrado, Universidad Estatal del Sur de Manabí]. http://repositorio.unesum.edu.ec/handle/53000/4769

Pérez Jaramillo, M. A. (2025). *AUTOLAB: Automatización de la entrega de dispositivos electrónicos en el laboratorio de electrónica mediante RFID* [Tesis de pregrado, Pontificia Universidad Javeriana Cali]. http://hdl.handle.net/11522/4436

Quintana Tukasaki, D. F. (2022). *Un módulo de detección RFID para tareas de manipulación robótica* [Trabajo final de máster oficial, Universidad Politécnica de Catalunya]. https://hdl.handle.net/2117/367823

Rodríguez Gordillo, A. M. (2024). *Diseño de un módulo de monitoreo para un laboratorio remoto mediante dispositivos IoT* [Tesis de licenciatura, Universidad Autónoma del Estado de Morelos (UAEM)]. http://riaa.uaem.mx/handle/20.500.12055/4620

Sánchez Castro, R. D. (2025). *Diseño y simulación de un sistema de seguridad electrónico utilizando Arduino Uno para una puerta automática corrediza en el laboratorio de electrónica de CEUTEC* [Trabajo de grado, Centro Universitario Tecnológico (CEUTEC)]. https://repositorio.unitec.edu//handle/123456789/13515

Anexos

Anexo A

Manual de Instalación

Este manual es el procedimiento de instalación de los programas necesarios para el correcto funcionamiento del prototipo de préstamo de equipos del laboratorio. Los programas que deben instalarse son los siguientes:

- Node.js v22.x lts — Entorno de javascript, necesario para instalar node-red.
- node-red v4.1.x — Plataforma para visualizar él dashboard.
- Postgresql v17.x — Base de datos.
- Eclipse Mosquitto v2.0.x — Broker mqtt para comunicación entre dispositivos.

Instalación de Node.js

1. Abrir el navegador web e ingresar a la dirección oficial: https://nodejs.org
2. En la página de inicio, seleccionar la opción "LTS". Al momento de redacción de este manual, la versión recomendada es Node.js 22.x.
3. Descargar el instalador para windows (.msi) correspondiente a la arquitectura del equipo (64 bits en la mayoría de los casos).
4. Ejecutar el archivo descargado con doble clic. El instalador requiere permisos de administrador.
5. Seguir las instrucciones del asistente de instalación, aceptando los términos de licencia y dejando las opciones predeterminadas.

Instalación de Node-red

1. Abrir cmd como administrador (clic derecho sobre el ícono y seleccione 'Ejecutar como administrador').
2. Ejecutar el siguiente comando para instalar node-red de forma global:

   npm install -g --unsafe-perm node-red
3. Esperar a que finalice la instalación. Este proceso puede tardar varios minutos dependiendo de la conexión a internet.
4. Una vez instalado, iniciar node-red ejecutando el siguiente comando en cmd: node-red
5. Abrir el navegador web e ingresar a la siguiente dirección:

   http://localhost:1880
6. Si se despliega la interfaz gráfica de node-red, la instalación ha sido completada exitosamente.

Instalación de Nodos para el Correcto Funcionamiento de Node-red

Para el correcto funcionamiento del sistema de control de acceso, es necesario instalar los siguientes nodos una vez que node-red esté en ejecución:

- node-red-dashboard — Proporciona los elementos visuales del panel de administración.
- node-red-contrib-postgresql — Permite la conexión y ejecución de consultas sobre la base de datos Postgresql.
- node-red-node-ui-table — Agrega la tabla al dashboard para visualizar el historial de accesos.
- node-red-contrib-telegrambot — Permite el envío de notificaciones y alertas automáticas a través de telegram.

Intalacion desde la interfaz grafica de node-red

1. En la esquina superior derecha, hacer clic en el ícono de menú (≡) y seleccionar 'Manage palette'.
2. En la ventana que se abre, seleccionar la pestaña 'Install'.
3. En el campo de búsqueda, escribir el nombre del nodo a instalar (por ejemplo: node-red-dashboard) y presionar Enter.
4. Localizar el nodo correspondiente en los resultados y hacer clic en el botón 'Install'.
5. Confirmar la instalación en el cuadro de diálogo que aparece y esperar a que finalice el proceso.
6. Repetir los pasos 1 al 4 para cada uno de los nodos listados anteriormente.

Instalación de Postgresql

1. Ingresar al sitio oficial de descarga: https://www.postgresql.org/download
2. Hacer clic en el enlace "Download the installer".
3. Seleccionar la versión 17.x y la arquitectura Windows x86-64, luego descargar el instalador.
4. Ejecutar el archivo descargado con permisos de administrador y seguir el asistente de instalación.
5. Durante la instalación, se solicitará definir una contraseña para el usuario administrador 'postgres'. Anotar esta contraseña, ya que será necesaria para la configuración posterior del sistema.

6. Seleccionar el puerto de conexión y valor predeterminado (5432), se recomienda dejarlo sin cambios.
7. Completar la instalación y al finalizar.
8. Verificar la instalación abriendo el programa pgAdmin 4 con simbología de un elefante azul (instalado junto con Postgre sql) o ejecutando en cmd: psql -U postgres.

Instalación de Eclipse Mosquitto

1. Ingresar al sitio oficial: https://mosquitto.org/download/
2. En la sección Windows, descargar el instalador correspondiente a 64 bits (mosquitto-2.x.x-install-windows-x64.exe).
3. Ejecutar el instalador con permisos de administrador.
4. En el asistente de instalación, asegurarse de marcar la opción 'Service' para que Mosquitto se instale como servicio de windows e inicie automáticamente, con el fin de evitar estando iniciando cada vez que se apaga él computador.
5. Dejar la ruta de instalación predeterminada (C:\Program Files\mosquitto) y continuar.
6. Al finalizar, abrir el cmd como administrador y ejecutar: net start mosquitto, para iniciarlo.
7. Para verificar que el broker está activo, abrir otra ventana de cmd y ejecutar: mosquitto -v.

Terminadas todas las instalaciones, reinicie el computador con el fin de guardar correctamente los cambios y programas instalados.

Anexo B

Manual de Usuario Administrador

Acceso a la interfaz de administración

1. Abrir el navegador web (Google Chrome, Microsoft Edge o Firefox).
2. Ingresar la dirección del panel de administración: `http://localhost:1880/dashboard`
3. Una vez dentro, el panel mostrará las opciones principales: registro de usuarios, asignación de permisos e historial de accesos.

Registro de usuarios nuevos

1. Acerque la tarjeta al lector rc522, en el panel de registro se refleja la información de la tarjeta, sea nueva o de un estudiante ya registrado.
2. Para estudiantes nuevos, al lado derecho se encuentra dos espacios para ingresar el nombre del estudiante, su código y en la parte inferior el botón de guardar. Asegúrese que se muestre en pantalla el mensaje de “guardado”.
3. Nuevamente acerque la tarjeta para verificar que el uid esté relacionado con la información que acaba de guardar del estudiante.

Asignación de permisos de cerraduras

1. Diríjase al segundo apartado del lado izquierdo y haga clic en la opción “Admin-permisos”.
2. En el apartado UID, escriba el código del estudiante con el fin de que aparezca en pantalla el nombre del portador de esa tarjeta, sino se encuentra registrado no se muestra información alguna en pantalla.
3. Abajo hay cuatro botones que representan cada cerradura, según los equipos que necesite el estudiante, seleccioné y guarde los permisos con el botón ubicado en la parte inferior.
4. Siempre revise que se muestre el mensaje de “Permisos guardado que especifica cada cerradura”.

Consulta historial de acceso

1. Diríjase al tercer apartado del lado izquierdo y haga clic en la opción “Historial”.
2. Se visualiza la tabla del historial de accesos y en la parte izquierda el último intento de acceso.

Anexo C

Código en Arduino para el Esp32-S3 de Acceso

```
// Librerias
#include <SPI.h>
#include <MFRC522.h>
#include <WiFi.h>
#include <PubSubClient.h>
#include <ArduinoJson.h>
// Pines RC522
#define RC522_SS_PIN   5
#define RC522_RST_PIN  4
#define SCK_PIN  36
#define MOSI_PIN 35
#define MISO_PIN 37
// PINES RELAY (4 canales - activo en LOW)
#define RELAY_1  21
#define RELAY_2  20
#define RELAY_3  19
#define RELAY_4  18
#define TIEMPO_CERRADURA 3000

//Configuracion de red
const char* WIFI_SSID     = "ssid";
const char* WIFI_PASSWORD = "12345678";
const char* MQTT_SERVER   = "192.168.....";  // IP servidor Mqtt
const int   MQTT_PORT     = 1883;
const char* MQTT_CLIENT_ID = "esp32-acceso";
// Topicos MQTT
const char* TOPIC_PUBLISH  = "rfid/access/uid";
const char* TOPIC_SUBSCRIBE = "rfid/access/response";

// OBJETOS
MFRC522 rfid(RC522_SS_PIN, RC522_RST_PIN);
WiFiClient wifiClient;
PubSubClient mqtt(wifiClient);
// VARIABLES
unsigned long tiempoUltimaLectura = 0;
const unsigned long DELAY_LECTURA = 2000;
bool relayActivo = false;
unsigned long tiempoActivacionRelay = 0;
int relaysActivos[4] = {0, 0, 0, 0};

//  BLOQUE WIFI
void conectarWiFi() {
  Serial.print("Conectando a WiFi: ");
  Serial.println(WIFI_SSID);
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  int intentos = 0;
  while (WiFi.status() != WL_CONNECTED && intentos < 30) {
    delay(500);
    Serial.print(".");
    intentos++;
  }
```

```
  }
  if (WiFi.status() == WL_CONNECTED) {
    Serial.println("WiFi conectado");
    Serial.print("IP: ");
    Serial.println(WiFi.localIP());
  } else {
    Serial.println("Error WiFi - reiniciando...");
    ESP.restart();
  }
}

// BLOQUE DE DESICION DE PERMISOS
void callbackMQTT(char* topic, byte* payload, unsigned int length) {
  String mensaje = "";
  for (unsigned int i = 0; i < length; i++) {
    mensaje += (char)payload[i];
  }
  Serial.println("-----------------------------");
  Serial.print("Mensaje recibido: ");
  Serial.println(mensaje);
  StaticJsonDocument<512> doc;
  DeserializationError error = deserializeJson(doc, mensaje);
 if (error) {
  Serial.print("Error JSON: ");
  Serial.println(error.c_str());
  return;
}
if (!doc.containsKey("uid") || !doc.containsKey("status")) {
  Serial.println("JSON incompleto (falta uid o status)");
  return;
}
const char* uid    = doc["uid"];
const char* status = doc["status"];
JsonArray locks    = doc["locks"] | JsonArray();
  Serial.print("UID: ");
  Serial.println(uid);
  Serial.print("Estado: ");
  Serial.println(status);
  memset(relaysActivos, 0, sizeof(relaysActivos));
  if (strcmp(status, "granted") == 0) {
    Serial.println("ACCESO PERMITIDO");
    for (JsonVariant lock : locks) {
      int numCerradura = lock.as<int>();

      Serial.print(" Abriendo cerradura ");
      Serial.println(numCerradura);

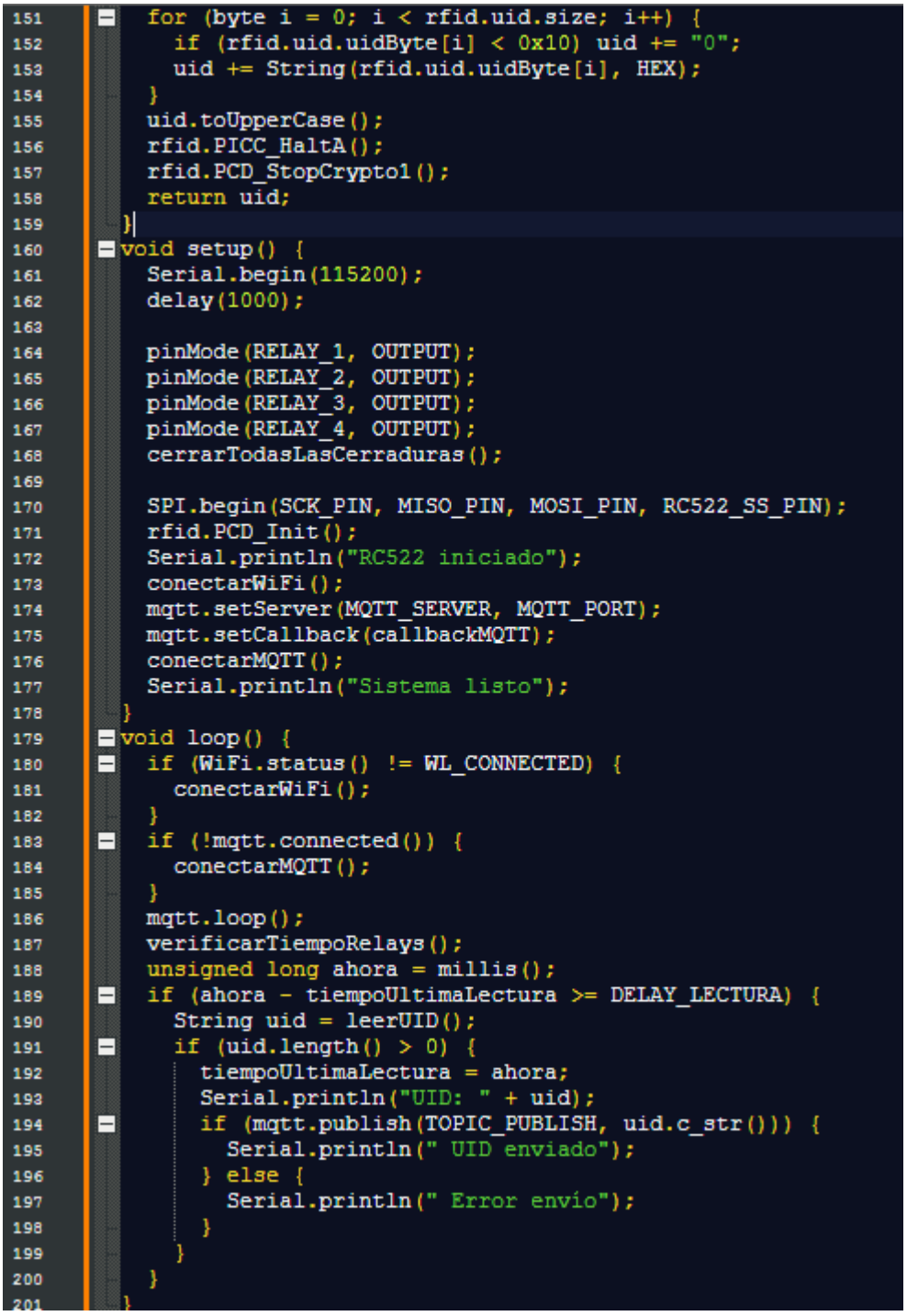
      switch (numCerradura) {
        case 1: digitalWrite(RELAY_1, LOW); relaysActivos[0] = 1; break;
        case 2: digitalWrite(RELAY_2, LOW); relaysActivos[1] = 1; break;
        case 3: digitalWrite(RELAY_3, LOW); relaysActivos[2] = 1; break;
```

```
            case 3: digitalWrite(RELAY_3, LOW); relaysActivos[2] = 1; break;
            case 4: digitalWrite(RELAY_4, LOW); relaysActivos[3] = 1; break;
          }
        }
        relayActivo = true;
        tiempoActivacionRelay = millis();
      } else {
        Serial.println(" ACCESO DENEGADO");
        cerrarTodasLasCerraduras();
      }
    }

    //BLOQUE RELAYS
    void cerrarTodasLasCerraduras() {
      digitalWrite(RELAY_1, HIGH);
      digitalWrite(RELAY_2, HIGH);
      digitalWrite(RELAY_3, HIGH);
      digitalWrite(RELAY_4, HIGH);
      relayActivo = false;
      memset(relaysActivos, 0, sizeof(relaysActivos));
      Serial.println(" Todas las cerraduras cerradas");
    }
    void verificarTiempoRelays() {
      if (relayActivo && (millis() - tiempoActivacionRelay >= TIEMPO_CERRADURA)) {
        cerrarTodasLasCerraduras();
        Serial.println(" Tiempo agotado - cerraduras cerradas");
      }
    }

    // BLOQUE DE CONEXION MQTT
    void conectarMQTT() {
      while (!mqtt.connected()) {
        Serial.print("Conectando a MQTT...");
        if (mqtt.connect(MQTT_CLIENT_ID)) {
          Serial.println("MQTT conectado");
          mqtt.subscribe(TOPIC_SUBSCRIBE);
          Serial.println("Suscrito");
        } else {
          Serial.print("Error MQTT rc=");
          Serial.println(mqtt.state());
          delay(3000);
        }
      }
    }

    // BLOQUE RFID
    String leerUID() {
      if (!rfid.PICC_IsNewCardPresent()) return "";
      if (!rfid.PICC_ReadCardSerial()) return "";
      String uid = "";
      for (byte i = 0; i < rfid.uid.size; i++) {
```



```
  for (byte i = 0; i < rfid.uid.size; i++) {
    if (rfid.uid.uidByte[i] < 0x10) uid += "0";
    uid += String(rfid.uid.uidByte[i], HEX);
  }
  uid.toUpperCase();
  rfid.PICC_HaltA();
  rfid.PCD_StopCrypto1();
  return uid;
}
void setup() {
  Serial.begin(115200);
  delay(1000);

  pinMode(RELAY_1, OUTPUT);
  pinMode(RELAY_2, OUTPUT);
  pinMode(RELAY_3, OUTPUT);
  pinMode(RELAY_4, OUTPUT);
  cerrarTodasLasCerraduras();

  SPI.begin(SCK_PIN, MISO_PIN, MOSI_PIN, RC522_SS_PIN);
  rfid.PCD_Init();
  Serial.println("RC522 iniciado");
  conectarWiFi();
  mqtt.setServer(MQTT_SERVER, MQTT_PORT);
  mqtt.setCallback(callbackMQTT);
  conectarMQTT();
  Serial.println("Sistema listo");
}
void loop() {
  if (WiFi.status() != WL_CONNECTED) {
    conectarWiFi();
  }
  if (!mqtt.connected()) {
    conectarMQTT();
  }
  mqtt.loop();
  verificarTiempoRelays();
  unsigned long ahora = millis();
  if (ahora - tiempoUltimaLectura >= DELAY_LECTURA) {
    String uid = leerUID();
    if (uid.length() > 0) {
      tiempoUltimaLectura = ahora;
      Serial.println("UID: " + uid);
      if (mqtt.publish(TOPIC_PUBLISH, uid.c_str())) {
        Serial.println(" UID enviado");
      } else {
        Serial.println(" Error envío");
      }
    }
  }
}
```

Nota: autoridad propia (2026).

Anexo D

Codigo en Arduino para el Esp32 del Administrador

```
//Librerias
#include <SPI.h>
#include <MFRC522.h>
#include <WiFi.h>
#include <PubSubClient.h>
// Pines RC522  a ESP32
#define SS_PIN  5
#define RST_PIN 21
#define SCK_PIN  18
#define MOSI_PIN 23
#define MISO_PIN 19
//CONFIGURACIÓN DE RED
const char* WIFI_SSID     = "ssid";
const char* WIFI_PASSWORD = "12345678";
const char* MQTT_SERVER   = "192.168.....";  // IP servidor Mqtt
const int   MQTT_PORT     = 1883;
const char* MQTT_TOPIC    = "rfid/admin/uid";
const char* MQTT_CLIENT   = "esp32_admin_rfid";


//Objetos
MFRC522 mfrc522(SS_PIN, RST_PIN);
WiFiClient espClient;
PubSubClient mqttClient(espClient);

String ultimo_uid = "";
unsigned long ultimo_tiempo = 0;
const unsigned long DEBOUNCE_MS = 2000; // Tiempo de lecturas del mismo UID

void setup() {
  Serial.begin(115200);
  SPI.begin(SCK_PIN, MISO_PIN, MOSI_PIN, SS_PIN);
  mfrc522.PCD_Init();
  Serial.println("Iniciando módulo RFID Administrador...");
  // Conexion WiFi
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  Serial.print("Conectando WiFi");
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("\nWiFi conectado. IP: " + WiFi.localIP().toString());
  // Conexion MQTT
  mqttClient.setServer(MQTT_SERVER, MQTT_PORT);
  conectarMQTT();
  Serial.println("Listo. Acerque una tarjeta RFID...");
}

void loop() {
  if (!mqttClient.connected()) {
    conectarMQTT();
```

```
  if (!mqttClient.connected()) {
    conectarMQTT();
  }
  mqttClient.loop();
  if (!mfrc522.PICC_IsNewCardPresent() || !mfrc522.PICC_ReadCardSerial()) {
    delay(50);
    return;
  }
  // Construir string del UID
  String uid = "";
  for (byte i = 0; i < mfrc522.uid.size; i++) {
    if (mfrc522.uid.uidByte[i] < 0x10) uid += "0";
    uid += String(mfrc522.uid.uidByte[i], HEX);
    if (i < mfrc522.uid.size - 1) uid += ":";
  }
  uid.toUpperCase();
  // Evitar múltiples publicaciones del mismo UID
  unsigned long ahora = millis();
  if (uid == ultimo_uid && (ahora - ultimo_tiempo) < DEBOUNCE_MS) {
    mfrc522.PICC_HaltA();
    return;
  }
  ultimo_uid = uid;
  ultimo_tiempo = ahora;
  Serial.println("UID leído: " + uid);
  // Publicar por via MQTT
  if (mqttClient.publish(MQTT_TOPIC, uid.c_str())) {
    Serial.println("UID publicado en MQTT: " + String(MQTT_TOPIC));
  } else {
    Serial.println("Error al publicar MQTT");
  }
  mfrc522.PICC_HaltA();
  mfrc522.PCD_StopCrypto1();
}

void conectarMQTT() {
  int intentos = 0;
  while (!mqttClient.connected() && intentos < 5) {
    Serial.print("Conectando a MQTT...");
    if (mqttClient.connect(MQTT_CLIENT)) {
      Serial.println(" conectado");
    } else {
      Serial.println(" fallo, rc=" + String(mqttClient.state()));
      delay(2000);
    }
    intentos++;
  }
}
```

Nota: autoridad propia (2026).

Anexo E

Codigo en Postgresql paraa la Base de Datos

```sql
-- Tabla de usuarios
CREATE TABLE IF NOT EXISTS users (
    id       SERIAL PRIMARY KEY,
    uid      VARCHAR(50) UNIQUE NOT NULL,
    username VARCHAR(100) NOT NULL,
    code     VARCHAR(10)  NOT NULL,
    created_at TIMESTAMP DEFAULT NOW(),
    updated_at TIMESTAMP DEFAULT NOW()
);

-- Tabla de permisos
CREATE TABLE IF NOT EXISTS permissions (
    id         SERIAL PRIMARY KEY,
    uid        VARCHAR(50) UNIQUE NOT NULL REFERENCES users(uid) ON DELETE CASCADE,
    lock1      BOOLEAN DEFAULT FALSE,
    lock2      BOOLEAN DEFAULT FALSE,
    lock3      BOOLEAN DEFAULT FALSE,
    lock4      BOOLEAN DEFAULT FALSE,
    updated_at TIMESTAMP DEFAULT NOW()
);

-- Tabla de historial de accesos
CREATE TABLE IF NOT EXISTS access_logs (
    id           SERIAL PRIMARY KEY,
    uid          VARCHAR(50),
    username     VARCHAR(100),
    status       VARCHAR(20),    -- 'granted' o 'denied'
    locks_opened TEXT,
    timestamp    TIMESTAMP DEFAULT NOW()
);
```

Nota: autoridad propia (2026).