IMPLEMENTACIÓN DE UN CONTROL Y GESTIÓN DE ACCESO IoT PARA LOS COLABORADORES DE MOVIVALLE S.A.S UTILIZANDO BIOMETRÍA Y RFID

ANDRES HERNANDEZ ARZUAGA

CARLOS EDUARDO PARRA POLO

UNIVERSIDAD POPULAR DEL CESAR

FACULTAD DE INGENIERÍA Y TECNOLÓGICAS

PROGRAMA DE INGENIERÍA ELECTRÓNICA

VALLEDUPAR - CESAR

2025

IMPLEMENTACIÓN DE UN CONTROL Y GESTIÓN DE ACCESO IOT PARA LOS COLABORADORES DE MOVIVALLE S.A.S UTILIZANDO BIOMETRÍA Y RFID

CLL 21 #7A - 80 BARRIO, LA GRANJA - VUP, CES.

ESTUDIANTES:

ANDRÉS HERNÁNDEZ ARZUAGA

CARLOS EDUARDO PARRA POLO

ahernandeza@unicesar.edu.co

ceparra@unicesar.edu.co

TRABAJO PRESENTADO COMO PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE INGENIERO ELECTRÓNICO

DIRECTOR:

Msc. CARLOS DÍAZ FERNANDEZ

LÍNEA DE INVESTIGACIÓN: ENERGÍA, AUTOMÁTICA E INSTRUMENTACIÓN

UNIVERSIDAD POPULAR DEL CESAR

FACULTAD DE INGENIERÍA Y TECNOLÓGICAS

INGENIERÍA ELECTRÓNICA

VALLEDUPAR - CESAR

2025

Nota de presentación

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Valledupar, Cesar. Día___ Mes___ Año___

CONTENIDO

Pág.

LISTA DE ANEXOS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

IoT: Internet de las Cosas

RFID: Identificación por Radiofrecuencia

TAG: Identificación automática de información contenida en etiquetas electrónicas

SETP: Sistema Estratégico de Transporte Público

SIVA: Sistema Integrado de transporte de Valledupar

RAEE: Registro y Apertura controlada al cuarto de reciclaje

NORMA BASC: Norma propuesta de gestión de control y seguridad en el Comercio Internacional en la gestión de la seguridad

NFC: Near Field Communication (Comunicación de campo cercano)

RESUMEN

El proyecto se realizó con el objetivo de Implementar un control y gestión de acceso IoT para los empleados y colaboradores de MOVIVALLE S.A.S, utilizando biometría y RFID, asimismo, se formularon los objetivos específicos, los cuales se busca: diseñar e implementar un sistema de identificación con biometría y RFID, Integrar dispositivos IoT para la gestión y monitoreo en tiempo real del sistema de control de acceso, implementando una plataforma basada en Python con la librería Tkinter como interfaz para la gestión de la información registrada en la nube; de esta manera se implementa una metodología en cascada estructurada, la cual aborda un problema central que afecta a 200 empleados de la empresa Movivalle S.A.S. Los resultados arrojados de la investigación, abordan diferentes aspectos que intervienen en el ensamblaje del Hardware, tales como el diseño e impresión de la PCB, el montaje de los componentes del circuito, seguido de la identificación del contenedor de estos, la presentación del contenedor, la disposición interna de los circuitos dentro del contenedor de circuitos, así mismo se realizó la interacción de funciones para envió de datos en tiempo real realizando la petición de datos del TAG; para concluir un sistema de control y gestión de acceso IoT para los empleados y colaboradores de MOVIVALLE S.A.S. ha permitido alcanzar los objetivos planteados, un sistema de control de acceso basado en biometría y RFID, cumpliendo con el objetivo de mejorar el control y la gestión de acceso en las instalaciones de la empresa. La integración de dispositivos IoT permitió el monitoreo en tiempo real del sistema, facilitando la toma de decisiones con respecto a los registros en las bases de datos, la creación de una base de datos centralizada para la gestión de acceso ha sido fundamental para almacenar la información.

Palabras claves: Biometría, dispositivos, datos, interacción, circuito, control.

ABSTRACT

The project was carried out with the objective of implementing IOT access control and management for the employees and collaborators of MOVIVALLE S.A.S using biometrics and RFID, with the specific objectives which propose to design and implement an identification system with biometrics and RFID, to integrate IoT devices for the management and real-time monitoring of the access control system, Implementing a platform based on Python with Tkinter library as an interface for the management of access control system information, through a methodology which addresses a central problem that affects 200 employees of the company Movivalle S.A.S., a structured cascade methodology. The results, in this chapter the different aspects involved in the assembly of the Hardware are taken, such as the desing and printing of the PCB, the assembly of the components on the circuit, followed by the identification of the container of these, as well as the presentation of the container, the internal arrangement of the circuits within the circuit container, as well as the interaction of functions to send data in real time by making the request for data from the TAG; to conclude an IoT access control and management system for the employees and collaborators of MOVIVALLE S.A.S. has made it possible to achieve the objectives set, access control system based on biometrics and RFID, fulfilling the objective of improving access control and management in the company's facilities, The integration of IoT devices allowed real-time monitoring of the system, facilitating decision-making regarding records in databases, The creation of a centralized database for access management has been essential in storing information.

Keywords: Biometrics, devices, data, interaction, circuit, control

INTRODUCCIÓN

A través de los tiempos, la tecnología ha sido el auge innovador qué ha trascendido en todas las comunidades, aportando beneficio y comodidades a cada uno de los habitantes del planeta, como también seguridad y confiabilidad en las actividades cotidianas ser humano. Es desde este concepto tecnología como esa herramienta implementada para mejorar las condiciones de los diferentes lugares, y que de una u otra manera brindan la seguridad directa.

Ventura (2015), ve la seguridad como la ausencia de riesgos y amenazas, que afectan la integridad del individuo, permitiendo obtener más seguridad ante esos lugares de riesgos y amenazas, presentes en cualquier punto. La Oficina de Seguridad del Internauta OSI define a la suplantación de identidad como la actividad maliciosa en la que un atacante se hace pasar por otra persona por motivos como: cometer fraudes, ciberacosar, sextorsión, entre otros (OSI, 2014).

Desde este concepto publicado por la OSI, plantean a su vez que los sistemas biometricos son herramientas que generan aportes a la sociedad, a partir de la suplementación entidad como una actividad maliciosa en la que un atacante se hace pasar por otra persona por motivos como: cometer un delito, en 3 fraude ciberacoso, sexforsión, entre otros. (OSI, 2014).

Los sistemas biométricos han generado aportes a la sociedad en general, ya que permite revisar la identificación inteligente de cada individuo mediante las características personales que estos poseen, rasgos faciales, dactilares y el iris, tecnología ha sido implementada desde años anteriores en diferentes empresas las cuales buscan registrar las entradas y salidas de sus empleados, instituciones para controlar el acceso hacia determinada área, entre otras funciones que permiten el control en las empresas.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

A pesar del auge de la revolución digital en todo el mundo, muchas empresas y organizaciones aún utilizan sistemas de gestión de acceso tradicionales, en los que se emplean un personal de vigilancia para esta tarea. Estos vigilantes solicitan credenciales de acceso a los colaboradores que desean ingresar a las instalaciones, debido a que en muchos casos, se realiza el llenado manual de planillas previamente impresas, donde se firma y se anota la hora de entrada y salida en cumplimiento del turno. (Díaz, A., 2022). Esto dificulta llevar un registro del control de las horas trabajadas por los colaboradores y el cumplimiento de los turnos según los horarios establecidos, lo que resulta especialmente problemático en empresas con empleados en turnos rotativos. (García M., 2020).

MOVIVALLE S.A.S. es una empresa que nace del legado de varias empresas que se dedicaban al transporte público colectivo en la ciudad de Valledupar (Buses del Valle, Transvupar y Transcacique), se le otorgó los permisos de operador de la flota de buses del SETP de Valledupar, (SIVA, 2023), mediante contrato de administración de flota suscrita con SIVA S.A.S el 1 de diciembre del 2022, se encarga desde de la operación, gestión y mantenimiento de la flota de buses de transporte público de la ciudad de Valledupar. Actualmente involucra en su operación alrededor de 200 operadores, quienes trabajan en turnos rotativos. Como se mencionó anteriormente, MOVIVALLE S.A.S. utiliza un sistema de control de acceso tradicional, lo que dificulta llevar un registro preciso del cumplimiento de las jornadas laborales y controlar quién accede a las instalaciones.

La gestión de personal es un proceso crítico en MOVIVALLE S.A.S, ya que el registro exacto de las horas trabajadas es esencial para calcular adecuadamente las remuneraciones y gestionar los turnos rotativos con franjas horarias específicas

y períodos de descanso entre servicios. Esto hace necesaria una actualización en el desarrollo de dicho proceso dentro de la gestión de la empresa. (Martínez, J. A., 2021).

En medio del auge tecnológico que se vive en la actualidad, se ha demostrado que la implementación de un sistema de control de acceso digital, basados en tecnologías como la biometría y el RFID, ofrece ventajas significativas en términos de seguridad, eficiencia y precisión en la gestión de la asistencia. Sin embargo, Movivalle S.A.S., al igual que muchas otras empresas, aún no ha adoptado estas soluciones tecnológicas, lo que limita su capacidad para optimizar sus procesos internos y mejorar la satisfacción de sus empleados.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo puede la implementación de un sistema de control de acceso basado en IoT, que integre tecnologías de biometría y RFID, mejorar la eficiencia y precisión en la gestión de la asistencia del personal en MOVIVALLE S.A.S., al mismo tiempo que garantiza el cumplimiento de las normativas laborales y contribuye a la satisfacción de los empleados?

2. JUSTIFICACIÓN

Con la llegada de la Cuarta Revolución Industrial, la tecnología se ha convertido en un aliado esencial que ha impactado significativamente la manera en que se gestionan los procesos en las entidades (Smith A. M., 2021). Esta transformación ha reducido la intervención humana y facilitado el análisis de datos gracias a su correcta cuantificación y digitalización, según la empresa TOTVS en su artículo sobre "Industria 4.0: el impacto en las empresas y la sociedad" (TOTVS, 2021).

Como las necesidades de cada empresa son particulares, y tras analizar la situación actual de MOVIVALLE S.A.S. y en reuniones con el personal operativo, se sugiere y recomienda la implementación de una solución tecnológica que optimice el registro de ingresos y egresos del personal. Para desarrollar esta solución, se instalará un módulo electrónico en el despacho que es donde se lleva el control de ingreso y egreso de la empresa, que registre el ingreso mediante una tarjeta RFID personal e intransferible o mediante huella dactilar para cada colaborador. Este sistema utilizará microcontroladores, fuentes de alimentación y sensores electrónicos integrados, que trabajarán en conjunto para subir la información a una base de datos en un servidor web propio, especialmente diseñado para esta tarea. (Zhang K., 2019).

Este sistema robusto permitirá controlar y registrar de manera precisa los datos de acceso, mejorando significativamente los resultados de un proceso que se realiza a diario. Un sistema de control de acceso eficiente no solo mejorará la seguridad de los activos y la integridad de los colaboradores, sino que también garantizará el cumplimiento normativo y optimizará la operación diaria de la empresa. Además, la automatización de los procesos de control de acceso y gestión del personal permitirá a MOVIVALLE S.A.S. reducir costos a largo plazo. Adicionalmente, se desarrollará una plataforma móvil Android para el monitoreo y gestión de datos en tiempo real (Rodríguez M. G. y. P. P. A., 2018).

La idea principal del proyecto, es mejorar la eficiencia operativa y aumentar la satisfacción de los colaboradores. La capacidad de monitorear y gestionar el acceso de manera precisa y en tiempo real, proporcionará datos valiosos para la toma de decisiones estratégicas y mejorará la respuesta ante incidentes. Desarrollar e implementar una solución de control de acceso adecuada y económica es una oportunidad no solo para resolver las necesidades inmediatas de MOVIVALLE S.A.S., sino también para establecer un modelo que otras empresas puedan implementar para mejorar su productividad mediante la innovación tecnológica y la mejora continua de los procesos (Fernández J. & L. M., 2019).

3. OBJETIVOS:

3.1 OBJETIVOS GENERALES:

Implementar un control y gestión de acceso IOT para los empleados y colaboradores de MOVIVALLE S.A.S utilizando biometría y RFID.

3.2 OBJETIVOS ESPECIFICOS:

- Diseñar e implementar un sistema de identificación con biometría y RFID
- Integrar dispositivos IoT para la gestión y monitoreo en tiempo real del sistema de control de acceso.
- Diseñar una base de datos centralizada IoT para la gestión de acceso.
- Implementar una plataforma móvil basada en Android para la gestión de la información del sistema de control de acceso.
- Elaborar un manual de usuario orientado a capacitar al personal en la utilización del aplicativo móvil, así como en el prototipo de gestión y monitoreo de acceso.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES INVESTIGATIVOS Y/O ESTADO DEL ARTE

A continuación, se presentan investigaciones, proyectos y artículos relacionados al tema presentado en la investigación, las cuales contribuyen a la información presentad para cumplir con el objetivo principal a cumplir. De esta manera, se explica de manera concisa la relación existente con nuestro proyecto de grado.

4.1.1 Antecedentes Históricos: La biometría tiene sus raíces en la antigüedad, pero como disciplina formal comenzó a desarrollarse a finales del siglo XIX. Uno de los pioneros en este campo fue Alphonse Bertillon, quien, en 1890, introdujo un sistema de identificación basado en la antropometría, que medía diversas dimensiones del cuerpo humano. Este método fue utilizado inicialmente por las fuerzas policiales para identificar criminales. (Bennett, C. J., & Groves, J., 2012).

El concepto biometría viene de las palabras *bio (vida) y metría (medida)*, trata sobre técnicas que miden e identifican las características físicas únicas de organismos vivos o patrones de su comportamiento, que permiten identificar los diferentes individuos, como por ejemplo las clásicas huellas digitales. El avance significativo en la biometría llegó con el trabajo de Francis Galton, quien en 1892 publicó *Fingerprints*, donde investigó las características únicas de las huellas dactilares. Galton demostró que las huellas eran únicas y no cambiaban a lo largo de la vida. Posteriormente, Edward Henry desarrolló un sistema de clasificación de huellas dactilares en 1901 que mejoró la eficacia del uso de esta técnica en el ámbito policial, adoptado por la Policía Metropolitana de Londres y muchas fuerzas policiales en todo el mundo.

A lo largo del siglo XX, la biometría se expandió para incluir otros rasgos, como el reconocimiento facial y el análisis del iris. Según Royer Jean-Marc (2007), la biometría implica medir características únicas del cuerpo humano para identificar individuos, eligiendo aquellas con alta variabilidad entre diferentes personas. Hoy en día, la tecnología biométrica es más accesible y económica, siendo el reconocimiento de huellas dactilares una de las técnicas más utilizadas a nivel mundial. (Osorio, J. A. C., Aguirre, F. A. M., & Escobar, J. A. M., 2010).

4.1.2 Antecedentes Investigativos: En los últimos años, el reconocimiento facial ha emergido como una de las tecnologías más innovadoras en el ámbito de la seguridad y vigilancia. Esta tecnología se ha convertido en un punto crucial en aplicaciones diversas, como en aeropuertos y empresas de telecomunicaciones, debido a la creciente necesidad de herramientas efectivas para garantizar la seguridad.

La investigación planteada por Carbonell Caballero, D. J. (2018), plantea la presentación de un diseño, el cual se sustenta en la necesidad de implementar un control de acceso biométrico que proporcione la agilidad y fiabilidad necesaria para el registro y apertura controlada al cuarto de reciclaje de los RAEE, con el fin de validar y administrar los ingresos al cuarto de reciclaje y mitigar el riesgo de intrusión y hurto, alineado a las exigencias de la norma BASC (Esta norma está destinada a ayudar a las organizaciones en el desarrollo de una propuesta de Gestión de Control y Seguridad en el Comercio Internacional en la gestión de la seguridad).

Para Torres-Londoño, C. I., Gallego-Giraldo, J. D., & Garay-Flórez, A. F., (2017) desarrollan el diseño para establecer un Sistema biométrico para control de acceso con doble validación. El sistema de control de acceso se implementó con el propósito de restringir el ingreso a diferentes áreas de una clínica, basado en las responsabilidades de cada miembro del personal. Este sistema incluye tecnología **RFID** para la apertura de puertas y el envío de tokens para confirmar identidades.

Es de esta manera que se desarrolló una aplicación informática que gestiona los accesos y genera una bitácora que registra la hora de ingreso y salida de cada colaborador.

Echavez, M., (2020) desarrolló un proyecto para establecer el Diseño e implementación de un sistema de biometría facial para el control de acceso en la universidad de Cartagena, enfocado para el reconocimiento facial, para el control de acceso a las instalaciones universitarias, mejorando la seguridad y eficiencia en la gestión de entradas. Se implemento tecnologías avanzadas para garantizar una identificación precisa y rápida, abordando las necesidades específicas de la comunidad académica.

Meneses, A. J., & García, C. G. (2016), realizaron un Diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital Francisco José de Caldas mediante el uso de torniquetes controlados por carnet con tecnología NFC y lector biométrico de huella dactilar, para el cual desarrollaron un sistema y protocolo para el control de acceso por medio de torniquetes y llevar a cabo su implementación junto a un sistema de autenticación por carnet personalizado NFC o huella dactilar para el ingreso de los funcionarios y la comunidad estudiantil a la sede de ingeniería permitiendo un mayor flujo de entrada y un nivel de seguridad mayor teniendo control a la hora de verificar el personal que ingresa. Asimismo, se eliminó la tarea de los guardas de seguridad de solicitar el carnet o recibo de pago para autorizar el ingreso.

4.2 BASES TEÓRICAS

En esta sección se desarrollan todas las consideraciones básicas que conforman la estructura teórica con el fin de brindar al lector el contexto necesario para contextualización del proyecto.

4.2.1 Sistema Biométrico: Innovatrics. (2021), define la biometría como un sistema de tecnología, basada en reconocimientos de huellas digitales, reconocimientos a través de óptica y en sistema de reconocimiento de voz, que se ha visto implementado en los últimos tiempos como medida de seguridad y a su vez como registro óptimo de personas, animales y objetos.

Según Valencia et al., (2014) actualmente, la mayoría de las técnicas de identificación de personas involucran parámetros inherentes al cuerpo del usuario y son clasificadas como sistemas biométricos de identificación. Los sistemas biométricos más empleados son el dactilar, facial y del iris. (Cedeño, J. R., & Párraga, C. L., 2017).

4.2.2 Reconocimiento Dactilar: Señala Borghello (2011), la identificación por huella dactilar es una de las biometrías más conocidas y publicitadas. Gracias a su unicidad y constancia en el tiempo las huellas dactilares han sido usadas para la identificación por más de un siglo, más recientemente volviéndose automatizada (ej. biométrica) debido a los avances en las capacidades de computación. La identificación por huellas dactilares es popular por su inherente comodidad de adquisición, las numerosas fuentes disponibles para recolección (diez dedos), y su establecido uso y recolección por parte del orden público e inmigración. (Cedeño, J. R., & Párraga, C. L., 2017).

4.2.3 Internet de las cosas (IOT): Internet de las cosas o IoT (Internet of Things), se refiere a la conexión de objetos tecnológicos o que sean electrónicos a Internet, este concepto se deriva del avance de la tecnología y a la necesidad de compartir y controlar las cosas que nos rodean. (Parra-Valencia, J., Guerrero, C., & Rico-Bautista, D., 2017).

4.2.4 RFID: La identificación por radiofrecuencia es una tecnología de captura e identificación automática de información contenida en etiquetas electrónicas (tags)

Cuando estas etiquetas entran en el área de cobertura de un lector RFID, éste envía una señal para que la etiqueta le transmita la información almacenada en su memoria. habitualmente un código de identificación. Una de las claves de esta tecnología es que la recuperación de la información contenida en la etiqueta se realiza sin necesidad de que exista contacto físico o visual (línea de vista) entre dispositivo lector y las etiquetas, aunque en muchos casos se exige una cierta proximidad de los elementos. (Huidobro, J., s/f).

5. HIPOTESIS

La implementación de un sistema de control de acceso basado en IoT, que integre tecnologías de biometría y RFID en Movivalle S.A.S., resultará en una reducción significativa de los errores en el registro de asistencia, mejorará la precisión en el cálculo de las horas trabajadas y facilitará el cumplimiento de las normativas laborales. Esta automatización integral de los procesos de control de acceso no solo optimizará la gestión del personal, sino que también aumentará la satisfacción de los empleados al proporcionar un entorno de trabajo más seguro y eficiente.

6. METODOLOGÍA

Este proyecto busca abordar un problema central que afecta a 200 empleados de la empresa Movivalle S.A.S. Para ello, se implementará una metodología en cascada estructurada en las siguientes fases:

✓ **Análisis del problema:** Investigación y análisis del problema, haciendo revisión de la literatura y casos a nivel local, nacional e internacional. Se recopilan y analizan soluciones aplicadas con éxito en contextos análogos.

✓ **Requisitos:** Diseño como solución al problema, de un diagrama de bloques que incluirá cada uno de los componentes necesarios para llevar a cabo la solución, este diagrama será de manera general sin referencias específicas de componentes. Se definirán los requisitos técnicos y funcionales incluyendo limitaciones y criterios de rendimiento para el proyecto.

✓ **Diseño:** Integración de cada uno de los componentes con referencias y que cumplan los requisitos planteados en el diagrama de bloques, entre ellos los límites absolutos máximos de cada uno de los componentes. Diseño de PCB y de layouts del aplicativo móvil Android, garantizando una interfaz intuitiva.

✓ **Implementación:** Ensamblaje de componentes y dispositivos según los diseños elaborados, realización de interconexión de todos los dispositivos para la comunicación bidireccional de cada uno de los módulos. Programación de microcontroladores y desarrollo de la interfaz del aplicativo móvil, integrando funcionalidades necesarias.

✓ **Verificación:** Ejecución y validación del funcionamiento del prototipo y ajustes finales, elaboración de un informe y manual de usuario para el dispositivo desarrollado, resultados obtenidos e impacto de la solución en la población objetivo.

7. CRONOGRAMA DE ACTIVIDADES

ITEM	ACTIVIDADES	MESES (SEMANAS) VIGENCIA - 2025															
		Enero				Febrero				Marzo				Abril			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Investigación																
2	Planificación y Planeación																
3	Implementación fisica																
4	Aplicativo WEB																
5	Pruebas finales																

FASE 1 - INVESTIGACIÓN:

- Desarrollar una investigación para obtener el estado del arte del eje temático principal, con el fin de establecer una base sólida para alcanzar el objetivo principal del proyecto. Duración: 30 días

FASE 2 - PLANIFICACIÓN Y PLANEACIÓN:

- Planificar y desarrollar diversos prototipos que cumplan con el objetivo del proyecto. A través de pruebas teóricas (no físicas), se eliminarán las opciones menos efectivas para identificar el prototipo ideal y más óptimo.
- Elaborar una tabla de costos detallada para facilitar la planificación de la posterior implementación del prototipo seleccionado. Duración: 60 días

FASE 3 – IMPLEMENTACIÓN FISICA

- Realizar la implementación física del proyecto, utilizando el prototipo más óptimo y viable, seleccionado mediante el análisis de la fase 2. Duración: 60 días

FASE 4 – APLICATIVO WEB

- Desarrollar un aplicativo que permita el control y monitoreo constante de las variables del sistema, asegurando una gestión eficiente y efectiva. Duración: 60 días

FASE 5 – PRUEBAS FINALES

- Llevar a cabo pruebas físicas finales del sistema, seguido de una evaluación integral y retroalimentación por parte del usuario, para asegurar el cumplimiento de los objetivos del proyecto. Duración: 60 días

8. PRESUPUESTO

RUBROS	FUENTES DE FINANCIACIÓN	
	RECURSOS PROPIOS	TOTAL
Personal	2.500.000	2.500.000
Equipos	1.000.000	1.000.000
Materiales	450.000	450.000
Viajes	0.00	0.00
Bibliografía	200.000	200.000
Software	200.000	200.000
Publicaciones	0.00	0.00
Servicios técnicos	0.00	0.00
Construcciones	0.00	0.00
Mantenimiento	150.000	150.000
Otros	0.00	0.00
Total	4.500.000	4.500.000

9. ALCANCE DEL PROYECTO

El proyecto contempla la implementación de un sistema tecnológico de control de acceso en MOVIVALLE S.A.S., que incluye el registro de ingresos y egresos del personal mediante RFID y huella dactilar. Se desarrollará una base de datos segura para gestionar estos registros y se creará una aplicación móvil para el monitoreo en tiempo real. Además, se busca mejorar la seguridad, optimizar procesos operativos y facilitar la toma de decisiones estratégicas. Finalmente, se evaluará el impacto en la satisfacción del personal y se establecerán mecanismos de retroalimentación para mejoras continuas.

10. DISEÑO Y ESPECIFICACIONES DEL PROTOTIPO

10.1 ETAPAS DEL PROTOTIPO

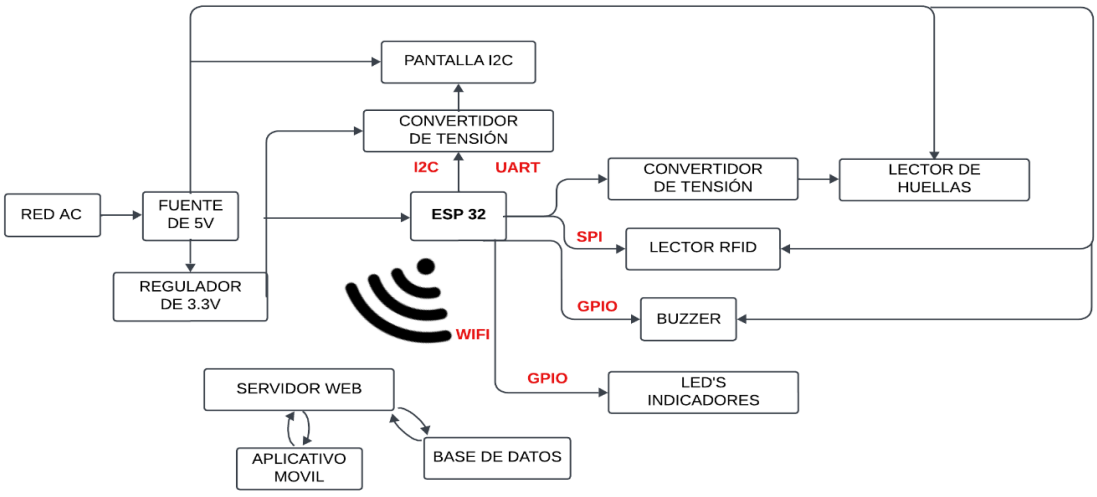
Para llevar a cabo el sistema propuesto, se optó por emplear un prototipo controlado por un microcontrolador con funcionalidades de conexión a redes inalámbricas, módulos con alimentación de tipo TTL o CMOS y una base de datos centralizada, el diagrama de bloques. (Ver figura 1).

En primer lugar, se tiene la etapa de instrumentación, en la cual, se implementaron los sensores necesarios para hacer funcionar el sistema. En la segunda etapa se estableció el control del prototipo, conformado por el microcontrolador, los indicadores sonoros y luminosos y la pantalla. Además, en la etapa de potencia, se establecieron las fuentes de alimentación y los reguladores.

Por último, se encuentra la etapa de comunicaciones, la cual consta de la base de datos y el servidor web, que permiten almacenar la información del sistema, junto con la interfaz local web.

Figura 1.

Diagrama de bloques del prototipo



Fuente: Autores

10.2 ELECCIÓN DE COMPONENTES ELECTRÓNICOS

En la presente sección se realizó un estudio sobre los sensores que se utilizaron, sus interfaces de comunicación y voltajes de alimentación.

10.2.1 Lector de tarjetas RFID. Para facilitar la interacción de los empleados con el sistema al momento de marcar horas de entrada y salidas, se optó por implementar un sistema que permita la identificación individual de cada uno, para esto se utiliza un sensor que detecte las mismas y que además cuente con las siguientes características técnicas, alimentación TTL o CMOS, protocolo de comunicación estándar, I2C, SPI, uart, entre otros, y por último que no requiera ningún sistema de acondicionamiento de señal.

10.2.2 Escogencia del lector de tarjetas RFID. Para la escogencia del lector se realizó un estudio de los componentes que pueden llegar a ser conseguidos en el mercado de tiendas electrónicas locales y nacionales, esto teniendo en cuenta las características anteriormente mencionadas.

Tabla 1.

Características de lectores de tarjetas RFID

Lector de tarjetas RFID	Voltaje de alimentación (voltios)	Corriente de consumo (mA)	Frecuencia (Hz)	Rango de medición (cm)	Costo
RC522	2.5V - 3.3V	13 mA – 26 mA	13.56 MHz	2 - 5 cm	$10.900
RDM6300	5V	50 mA	125 kHz	2 - 5 cm	$22.900
Em4100	1.5V	10 mA	100-150kHz	0 - 8 cm	$45.900

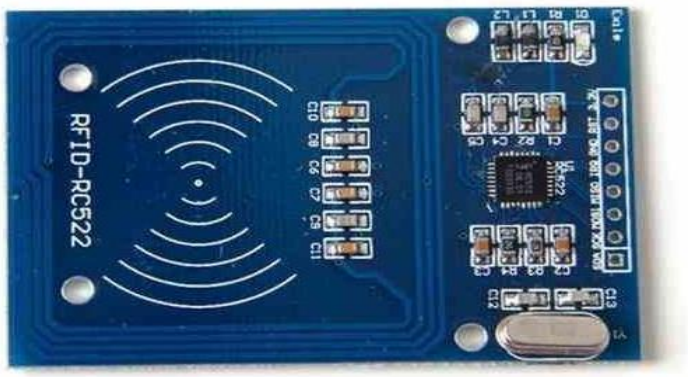
Fuente: los autores, extraído de cada Datasheet

Luego de realizar un análisis detallado de la tabla 1, se partió de cada una de las características y su costo, se escogió el lector RC522, el cual cuenta con una interfaz SPI, compatible con voltajes 3.3V, puede realizar mediciones hasta una distancia de 5cm, además, realizar una lectura rápida y precisa de tarjetas de

13.5Mhz, por otra parte, viene en un encapsulado tipo board y por lo tanto cuenta con todo lo necesario para hacer su función.

Figura 2.

Encapsulado de Lector rc522

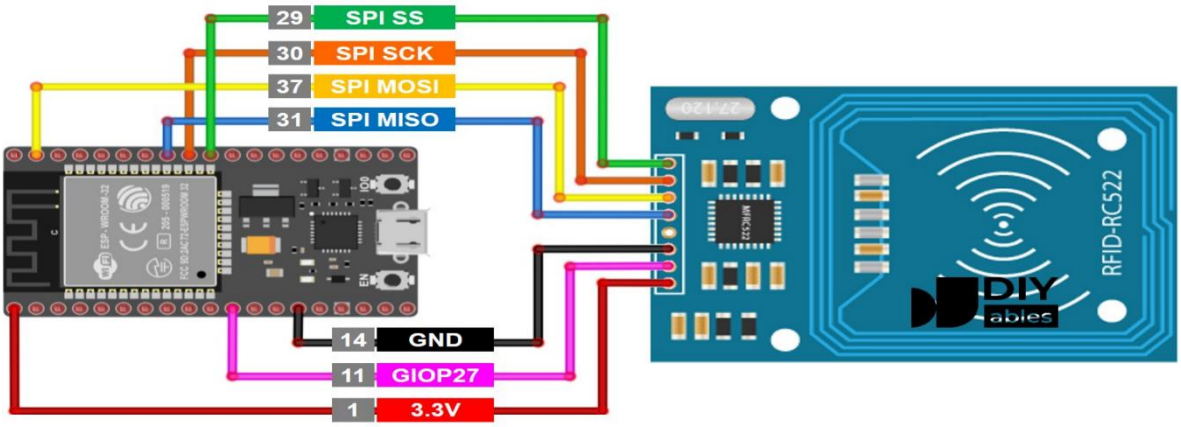


Fuente: SSDIELECT ELECTRONICA SAS

Lector de tarjetas RC522. El RC522 es un módulo RFID compacto y económico que permite leer y escribir datos en tarjetas y llaveros de 13.56 MHz. Ideal para proyectos de identificación y control de acceso, se comunica con microcontroladores como Arduino o ESP32-S3 mediante SPI, I2C o UART, siendo SPI el más usado. Su bajo consumo, la facilidad de uso y el alcance de lectura de 2-5 cm lo hacen perfecto para sistemas con aplicaciones prácticas de tecnología sin contacto.

Figura 1.

Diagrama de conexión sensor DHT22



Fuente: SSDIELECT ELECTRONICA SAS

Protocolo de comunicación SPI. El Bus SPI es un protocolo de comunicación síncrona utilizado para transferir datos entre un microcontrolador y otros dispositivos, como sensores, pantallas, memorias y periféricos. A diferencia de otros protocolos, el bus SPI utiliza múltiples líneas de comunicación, permitiendo una alta velocidad de transferencia y una flexibilidad excepcional.

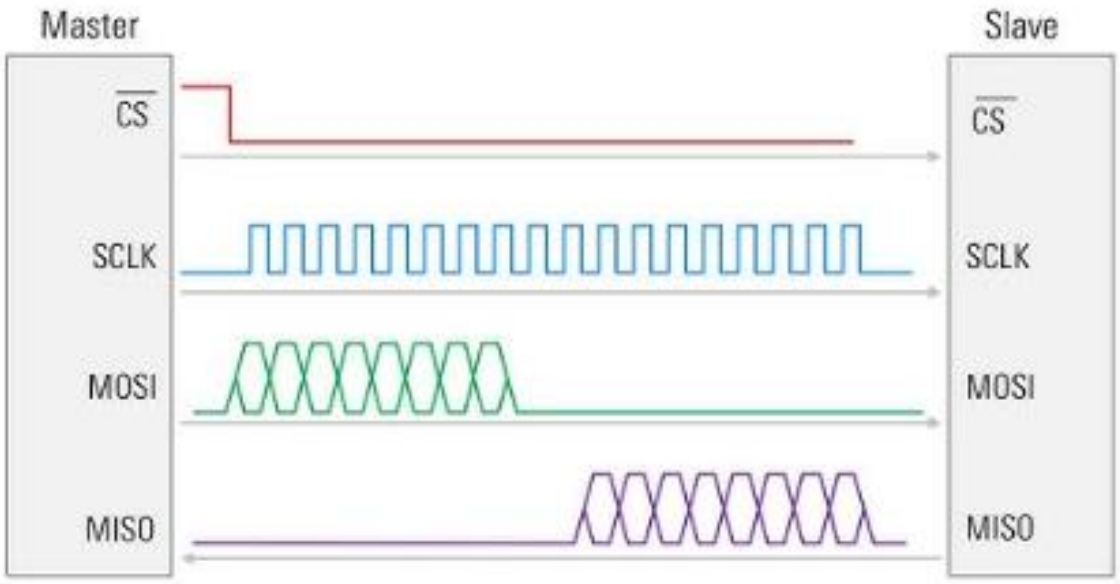
El puerto SPI es principalmente usado por su alta capacidad de transmitir datos. Por este motivo se encuentra en dispositivos que requieran gran cantidad de datos por segundo, como dispositivos de almacenamiento (memorias, SD) y pantallas.
El protocolo SPI (Serial Peripheral Interface) es un método de comunicación serial sincrónica entre un maestro y uno o más esclavos. En el diagrama, el maestro controla la comunicación usando las siguientes líneas:

- CS (Chip Select): Selecciona al esclavo al activarse (nivel bajo).
- SCLK (Serial Clock): Genera el reloj que sincroniza la transmisión de datos.
- MOSI (Master Out Slave In): Línea para enviar datos del maestro al esclavo.
- MISO (Master In Slave Out): Línea para enviar datos del esclavo al maestro.

En la figura 4, se puede ver como la comunicación comienza cuando el CS baja, y los datos se transmiten sincronizados con los pulsos de SCLK. MOSI transporta datos del maestro al esclavo, mientras que MISO hace lo opuesto, permitiendo una transferencia full-dúplex. La comunicación termina cuando CS vuelve a nivel alto. (Llamas L. (2025).

Figura 2.

Estructura de datos de protocolo SPI



Fuente: Llamas Luis (2025)

10.2.3 lector de huella dactilar. En caso de que el empleado no porte su tarjeta de identificación RFID, el sistema cuenta con un lector de huella dactilar el cual debía cumplir con las siguientes condiciones, algún tipo de comunicación estándar común en microcontroladores, voltajes de alimentación CMOS o TTL y sistema propio de acondicionamiento de señal.

Escogencia del lector de huella dactilar. Dicho lo anterior, se realizó una investigación en el mercado sobre las tiendas electrónicas, en la cual se consiguieron los 3 dispositivos que cuentan con las características que se pueden apreciar en la tabla 2.

Tabla 2.

Características de lector de huella

Lector de huella	Voltaje de alimentación (voltios)	Corriente de consumo (mA)	Protocolo	Capacidad de huellas	Costo
FMP1001	3.6V – 6V	100mA – 150mA	UART	162	$65.000
As608	3.3V – 5V	120mA	UART	172	$56.000
R307	4.2V – 6V	50mA	UART	1000	$150.000

Fuente: Autores, extraído de cada Datasheet

Una vez analizada la tabla 2, se escogió el sensor FMP1001, el cual es un sensor versátil que cuenta con alimentación de 3.3V, tiene comunicación de protocolo UART, su propio cable de alimentación y un encapsulado para realizar la medición.

Figura 3.

Encapsulado de sensor FM1001

Fuente: Llamas L. (2021)

FM1001. El FPM10A es un sensor biométrico de huellas dactilares ideal para proyectos en microcontroladores como Arduino. Este módulo cuenta con un procesador DSP de 32 bits que se encarga de registrar, leer y comparar huellas dactilares, con una capacidad de almacenamiento de hasta 162 huellas.

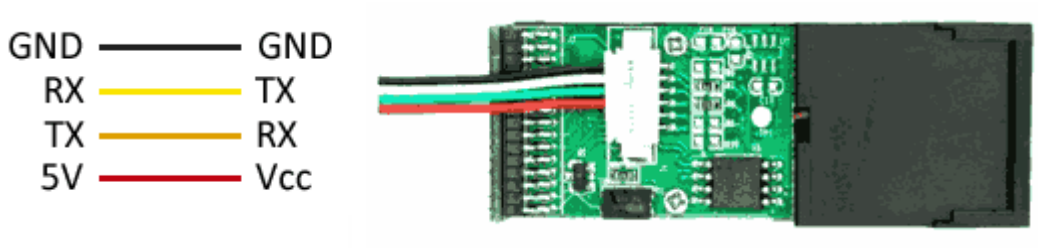
Destaca por su rapidez, con un tiempo de respuesta menor a 1 segundo, y su alta precisión, ofreciendo una tasa de falsos positivos inferior al 0.001% y de falsos negativos por debajo del 1%.

La comunicación se realiza mediante UART, compatible con velocidades de 9600 a 57600 baudios (configuración predeterminada en 57600), lo que facilita su integración en proyectos electrónicos. Opera con un rango de voltaje de 3.6V a 6.0V y tiene un consumo máximo de 150mA. (Llamas, L., 2021)

En la figura 6, se puede apreciar que para conectar el sensor al FM1001, se requiere de un puerto UART para realizar dicha comunicación, en este caso en específico el sensor permite comunicación a 3.3V.

Figura 4.

Conexión sensor FM1001



Fuente: Llamas, L. (2021)

10.3 ETAPA DE CONTROL

Esta etapa está compuesta de todo lo necesario para realizar control electrónico sobre el prototipo, entre ellos microcontrolador, pantalla, módulo de acondicionamiento de señal CMOS a TTL.

10.3.1 microcontrolador. Esta etapa consta de un microcontrolador el cual es el encargado de procesar las señales provenientes de los sensores, enviar las diferentes medidas vía microSD para su almacenamiento en base de datos, esto

debido a la falta de conectividad del prototipo, además también debe tener voltaje de alimentación CMOS o TTL, suficientes periféricos para controlar la electrónica requerida y por último suficiente capacidad de memoria RAM y ROM, para alojar los códigos correspondientes y variables.

Escogencia del microcontrolador. Existen en el mercado diferentes tipos de microcontrolador con prestaciones que se adecuan a la necesidad de los desarrolladores. En la Tabla 3 se muestran algunos con sus respectivas especificaciones**.**

Tabla 3.

Comparación de microcontroladores

Microcontrolador	Voltaje de alimentación (voltios)	Corriente de consumo (mA)	Puertos de entrada y salida	Módulo WI-FI integrado	Costo
ESP12F	3V – 3.6V	71mA – 500mA	16	SI	$12.400
ESP32	2.2V – 3.6V		34	Si	$37.800
ESP32-s3	3V - 3.6V	100mA – 140mA	45	SI	$56.000

Fuente: Autores, extraídos de los Datasheet.

Una vez analizada la tabla anterior, se empleó el microcontrolador ESP32 el cual es una evolución de la familia ESP32 diseñada por Espressif Systems, que ofrece mejoras específicas para aplicaciones que requieren procesamiento más potente y capacidades avanzadas de conectividad. A continuación, se detallan sus características principales:

- **Procesador:** El ESP32 cuenta con un procesador dual-core Xtensa LX que funciona a una frecuencia de hasta 240 MHz, proporcionando mayor rendimiento en comparación con versiones anteriores, Instrucciones SIMD (Single Instruction Multiple Data), que permiten procesar datos en paralelo,

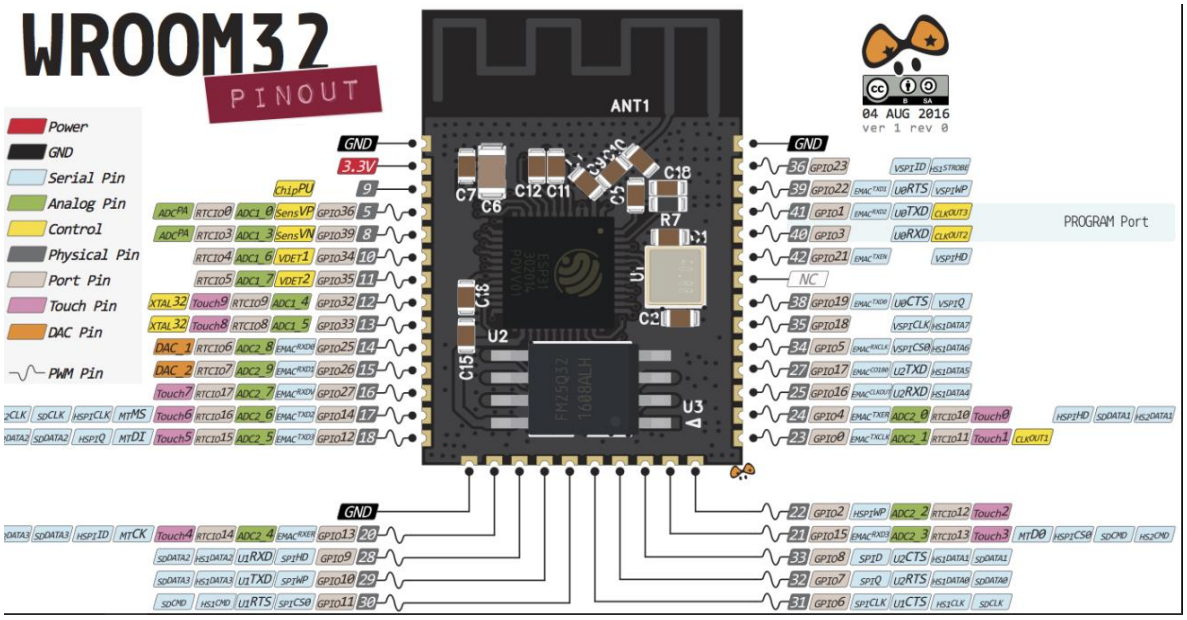
optimizando las operaciones que involucran procesamiento intensivo como la manipulación de imágenes o datos.

- **Memoria:** Posee 512 KB de SRAM y admite PSRAM externa (hasta 16 MB), lo que lo convierte en una opción ideal para aplicaciones que requieren mayor almacenamiento temporal de datos.
- **Conectividad:** Wi-Fi 802.11 b/g/n (2.4 GHz) integrado, ideal para conectividad inalámbrica en aplicaciones de IoT. Bluetooth 5.0 (BLE) con soporte para BLE Mesh, permitiendo la creación de redes de baja energía para dispositivos distribuidos.
- **Capacidades de IO:** Soporta una amplia gama de interfaces periféricas, incluyendo I2C, I2S, UART, SPI, ADC, DAC, PWM, RMT y más, lo que lo hace muy versátil para una amplia variedad de aplicaciones. Ofrece hasta 45 GPIOs, de los cuales muchos son configurables como entradas, salidas, y en algunos casos, como señales analógicas o digitales.

Consumo energético: El ESP32 está optimizado para bajo consumo de energía, con varios modos de ahorro que incluyen el modo de hibernación y el modo de suspensión profunda, lo que lo convierte en una excelente opción para dispositivos alimentados por batería o aplicaciones de IoT donde la eficiencia energética es primordial. ESP32, DEVKIT V1 DOIT, (s/f).

Figura 5.

ESP32 wroom

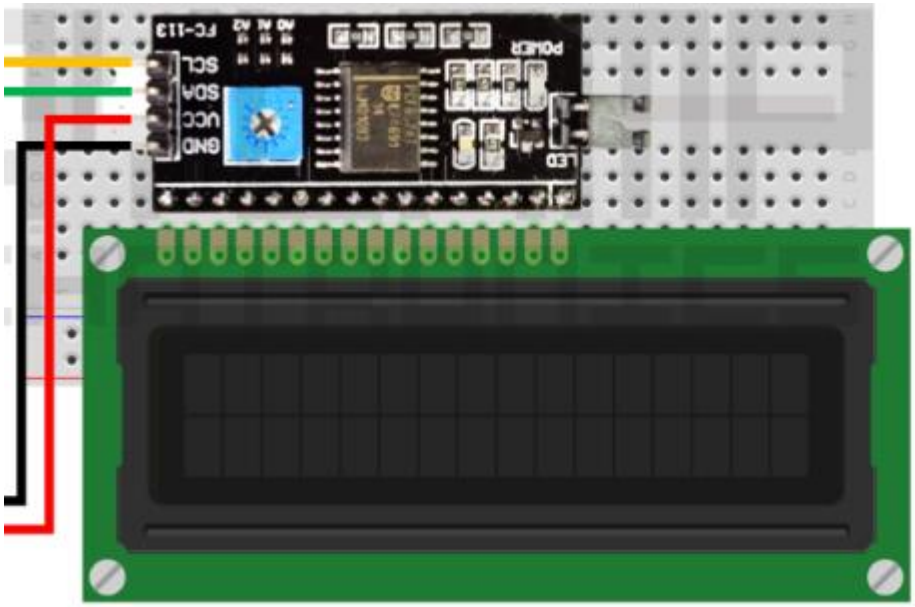


Fuente: ESP32, DEVKIT V1 DOIT, (s/f).

10.3.2 Lcd 16x2 I2C. La LCD es un periférico fundamental, ya que permite de manera local observar el comportamiento del prototipo y muestra el valor de los sensores y condición de las salidas en tiempo real de máximo 5 segundos. se optó por usar una LCD 16x2, junto con un módulo convertidor I2C, el cual disminuye de manera considerable el número de pines que se emplean para controlar la pantalla por parte del microcontrolador. Usando solo 2 pines SDA y SCL, para dicho propósito. El módulo adaptador LCD a I2C está basado en el controlador I2C PCF8574, el cual actúa como un expansor de entradas y salidas digitales controlado mediante el protocolo I2C. Este módulo se emplea específicamente para controlar pantallas LCD alfanuméricas, facilitando la comunicación entre el microcontrolador y el display. Además, al trabajar a un voltaje de 5V se debe utilizar un módulo de acondicionamiento de señal para convertir los 3.3V del microcontrolador a 5V, voltaje con el que trabaja la pantalla.

Figura 6.

Pantalla lcd 16x2 con modulo i2c



Fuente: Gutiérrez, A. A., Ceron M., Rodrigo, Magobel. (2022).

10.4 Etapa de potencia

Esta etapa se centra en las alimentaciones del prototipo y el cálculo de la potencia total requerida para el correcto funcionamiento del mismo.

10.4.1 Fuente de 5V. Es fundamental que la fuente de alimentación sea capaz de soportar toda la electrónica utilizada en el desarrollo del prototipo. Por ello, se calculó su capacidad de manera adecuada para garantizar el suministro de energía tanto al microcontrolador como a sus periféricos.

En la tabla 4 se presentan los componentes electrónicos del prototipo junto con una estimación de su consumo energético.

Tabla 4.

Cálculo de consumo de potencia del prototipo.

Elemento	Voltaje	Corriente	Potencia
ESP32	5V	500mA	2.5W
Pantalla lcd	5V	100mA	0.5W
Lector tarjetas RFID	3.3V	15mA	0.049w
Lector huella dactilar	3.3V	50mA	0.165W
Buzzer	3.3V	25mA	0.0825W

Se obtuvo al final un consumo de 3,5W aproximadamente. Se decidió emplear una fuente de 5V-2A, la cual cuenta con 10W máximo de potencia superando el consumo en más del doble y evitando cualquier inconveniente para abastecer todo el sistema.

Figura 7.

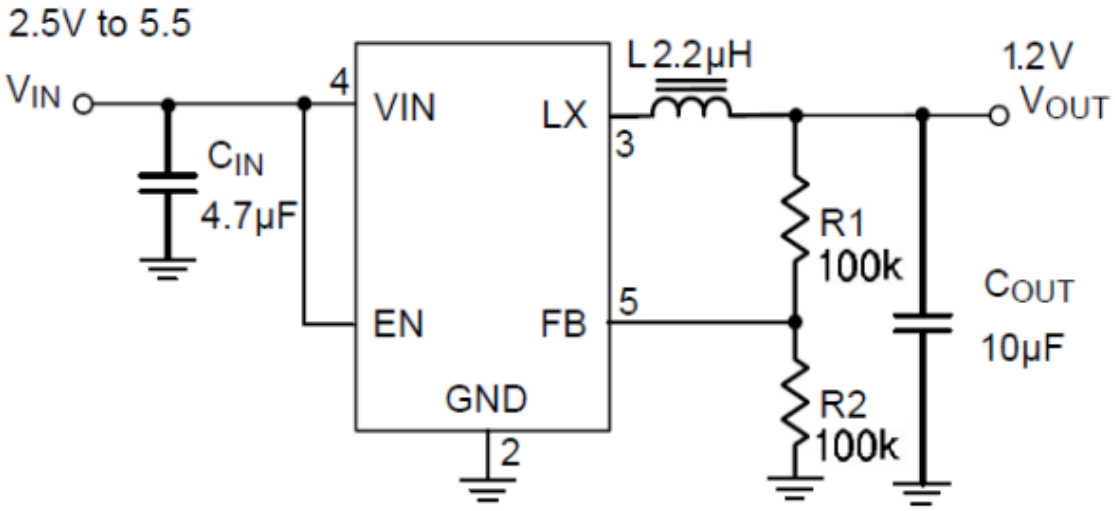
Fuente de 5V-2A DC

Fuente: SSDIELECT ELECTRONICA SAS (2025)

10.4.2 Reductor Buck 3.3V. Muchos de los dispositivos en este prototipo necesitan alimentarse con 3.3V DC debido a sus requisitos CMOS. Para lograr esta conversión desde 5V, se decidió utilizar un módulo reductor BUCK síncrono, conocido por su alta eficiencia en la transformación de voltajes en un rango de 6V a 1.2V. En este caso, se empleó el STI3408B, un convertidor que opera en modo PWM y cuenta con control de corriente y frecuencia constante. Este componente integra un interruptor principal y un rectificador sincrónico, eliminando la necesidad de un diodo Schottky externo y mejorando la eficiencia energética. Es especialmente adecuado para alimentar dispositivos portátiles que funcionan con baterías de ion de litio de una sola celda, ya que permite regular el voltaje de salida hasta niveles tan bajos como 0.6V. Además, su capacidad para operar al 100% del ciclo de trabajo lo convierte en una opción ideal para sistemas que requieren bajo dropout, ayudando a extender la vida útil de la batería. El STI3408B ofrece dos modos de operación, PWM y PFM, lo que garantiza una eficiencia óptima en diferentes niveles de carga.

Figura 8.

Esquema básico de reductor síncrono STI3408B



Fuente: SSDIELECT ELECTRONICA SAS (2025)

10.4.3 Etapa de Comunión. En esta etapa se tiene, todo lo relacionado con el envió de información hacia la nube por parte del prototipo.

10.4.4 Servidor web. El servidor web es el encargado de almacenar principalmente las bases de datos, el cual está ubicado en el URL XXXXXXXXXXXXX adquirido en el proveedor HOSTINGER, que se usó durante el desarrollo, las cuales son específicamente:

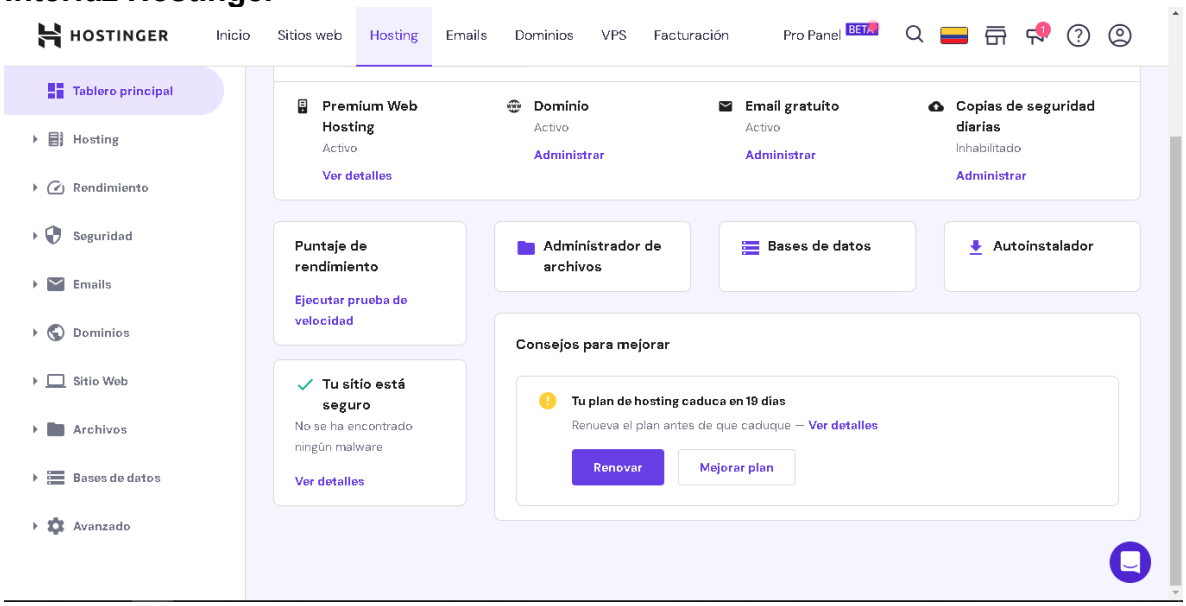
- Bases de datos de empleados
- Bases de datos de ingresos y salidas

Dicho servidor cuenta con un panel de gestión de alto nivel en el cual la programación puede quedar en segundo nivel, ya que se pueden hacer

configuraciones, creación y gestión de bases de datos sin usar el lenguaje principal SQL. (Boada, D., 2022)

Figura 9.

Interfaz Hostinger



Fuente: Boada, D., (2022)

En la tabla de la Figura 12, se tiene los datos que individualizan a cada uno de los empleados y adicionalmente un ID de identificación interno que se asigna a su huella dactilar y tarjeta RFID para con posterioridad poder reconocer sus ingresos y egreso.

Figura 10.

Base de datos empleados

	#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado	Comentarios	Extra
☐	1	**N**	int(11)			No	*Ninguna*		AUTO_INCREMENT
☐	2	**NOMBRE**	text	utf8mb4_unicode_ci		No	*Ninguna*		
☐	3	**DOC**	bigint(11)			No	*Ninguna*		
☐	4	**CARGO**	text	utf8mb4_unicode_ci		No	*Ninguna*		
☐	5	**ID**	text	utf8mb4_unicode_ci		No	*Ninguna*		

Fuente: Autores

En la tabla de la Figura 13, se tiene la estructura de la base de datos que se encarga de almacenar las entradas y salidas de los empleados usando el método timestamp, el cual con posterioridad se convierte a ticks para su comparación.

Figura 11.

Base de datos ingresos y egresos

	#	Nombre	Tipo	Cotejamiento	Atributos	Nulo	Predeterminado
☐	1	**N**	int(11)			No	*Ninguna*
☐	2	**Nombre**	text	utf8mb4_unicode_ci		No	*Ninguna*
☐	3	**Documento**	bigint(20)			No	*Ninguna*
☐	4	**Codigo**	bigint(20)			No	*Ninguna*
☐	5	**Fecha**	timestamp			No	*Ninguna*

Fuente: Autores

10.4.5 Comunicación PHP. El archivo PHP integrado en el proyecto lleva el nombre M0V1V@113.php En su contenido, se incluyen códigos que posibilitan la comunicación indirecta con la base de datos. En su encabezado, se establecen las condiciones iniciales necesarias para acceder a la base de datos y a las tablas que forman parte de la misma. En primer lugar, se dirige al hosting donde se encuentran alojados los archivos y las bases de datos, específicamente en www.electronicaunicesar.com.co. Para este acceso, se requiere usuario, contraseña y nombre de la base de datos, los cuales son generados durante la creación de la base de datos en el servidor web, como se muestra en la figura 12.

Figura 12.

Cabecera autenticación archivo PHP

```php
$host = "ingelectronicaunicesar.com.co";
    $host = "localhost";

$user = "u334793516_andres";
$pw = "+3Yn&u*cT";
$db = "u334793516_movivalle";
$conDB = new mysqli($host, $user, $pw, $db);
$conDB->set_charset("utf8");
```

Fuente: Autores

Posteriormente, se encuentra un switch que ofrece al usuario que consulta la base de datos varias opciones, como registrar un usuario, iniciar sesión, modificar un usuario o, de manera administrativa, ajustar parámetros dentro de la misma.
Una de las ventajas destacadas de los archivos PHP es su capacidad para ejecutar código con sintaxis SQL y realizar solicitudes a la base de datos. Además, gracias a las estructuras condicionales como If, for y while, estos archivos adquieren la potencia necesaria para llevar a cabo diversas tareas de manera efectiva.

10.5 MONTAJE DEL CIRCUITO

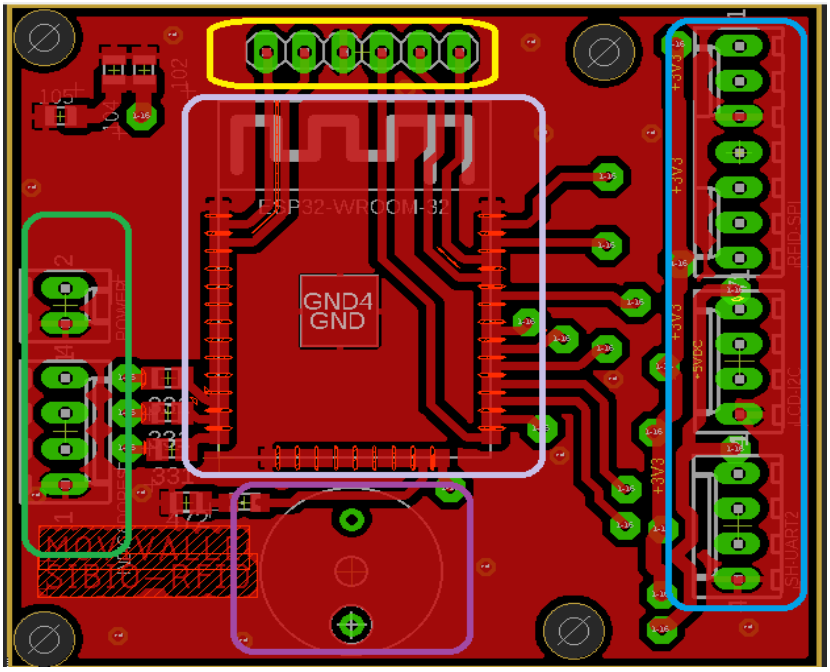
Para continuar con el desarrollo del proyecto, se procedió a montar los circuitos que posibilitan la conexión de cada una de las etapas mencionadas anteriormente. Con este objetivo, se planeó diseñar una tarjeta electrónica que integre todos los componentes y cumpla su rol dentro del prototipo. El diseño del circuito se realizó utilizando el software EAGLE (Easily Applicable Graphical Layout Editor), que proporciona las herramientas necesarias para este tipo de trabajo. El primer paso fue crear un esquema de conexión eléctrica que permita enlazar los componentes y lograr un dispositivo funcional. Se decidió utilizar un diseño de PCB de dos capas

para reducir el tamaño del conjunto y mejorar el aislamiento frente al ruido eléctrico que pueda surgir.

Para aprovechar mejor el espacio, los componentes se colocaron tanto en la capa superior como en la inferior de la PCB. En la figura 15 se observa la faz superior de la PCB en la cual se tiene en amarillo la regleta para conectar el loader para cargar el firmware, a la derecha en azul se tiene las salidas para los distintos periféricos, sensores y pantalla, en lila se tiene el microcontrolador ESP32 Wroom y del lado izquierdo una regleta en verde que tiene el conector de entrada de voltaje y una salida para conectar indicadores luminosos de ser necesarios, en la parte inferior en morado se tiene un buzzer circular.

Figura 13.

Vista superior de la PCB principal

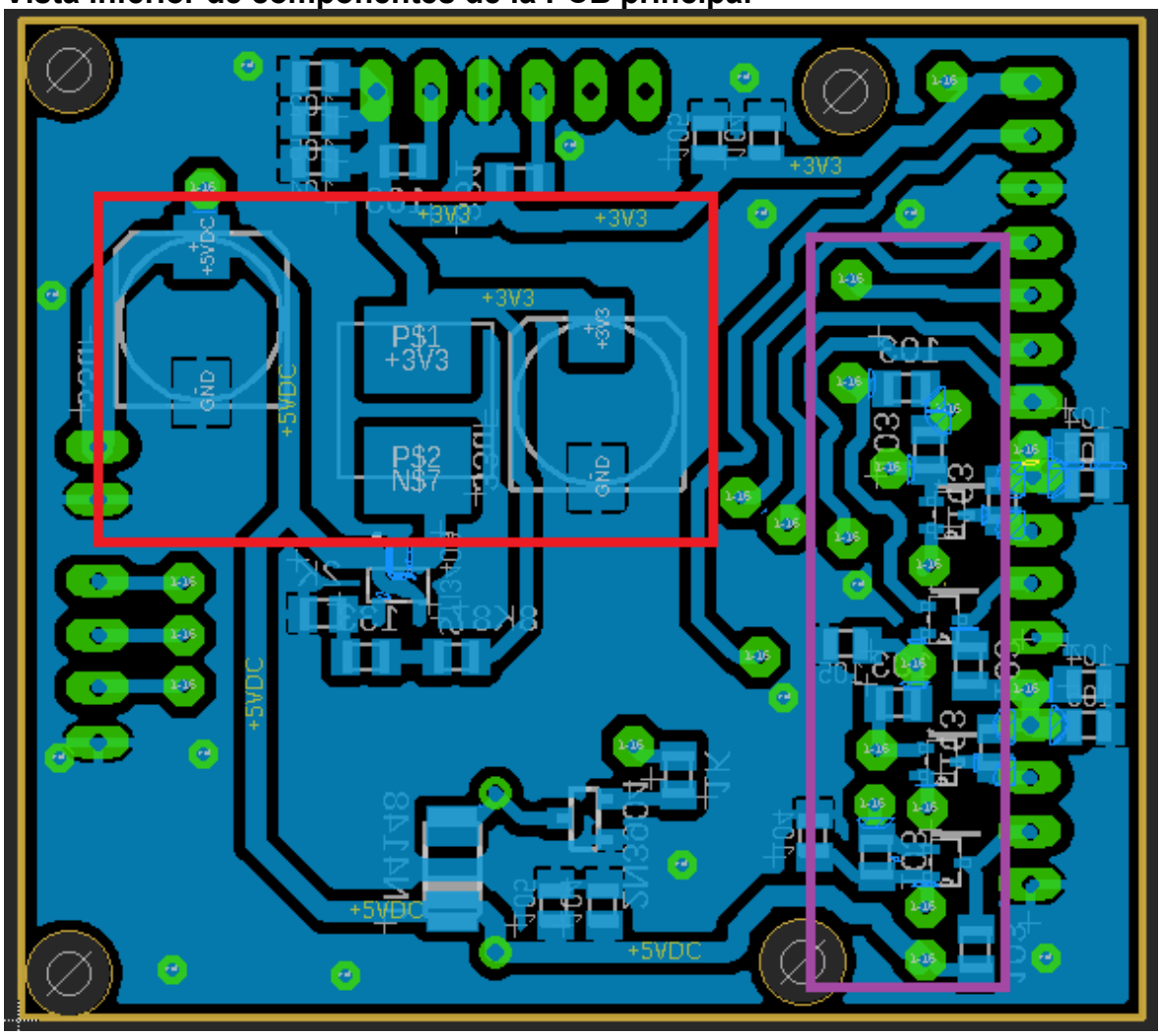


Fuente: Autores

En la figura16, se puede apreciar los componentes ubicados en la faz inferior de la PCB, en rojo se tiene el reductor síncrono que alimenta el microcontrolador, en azul el reductor síncrono que alimenta los sensores, y finalmente en morado se tiene los acondicionadores de señal.

Figura 14.

Vista inferior de componentes de la PCB principal



Fuente: Autores

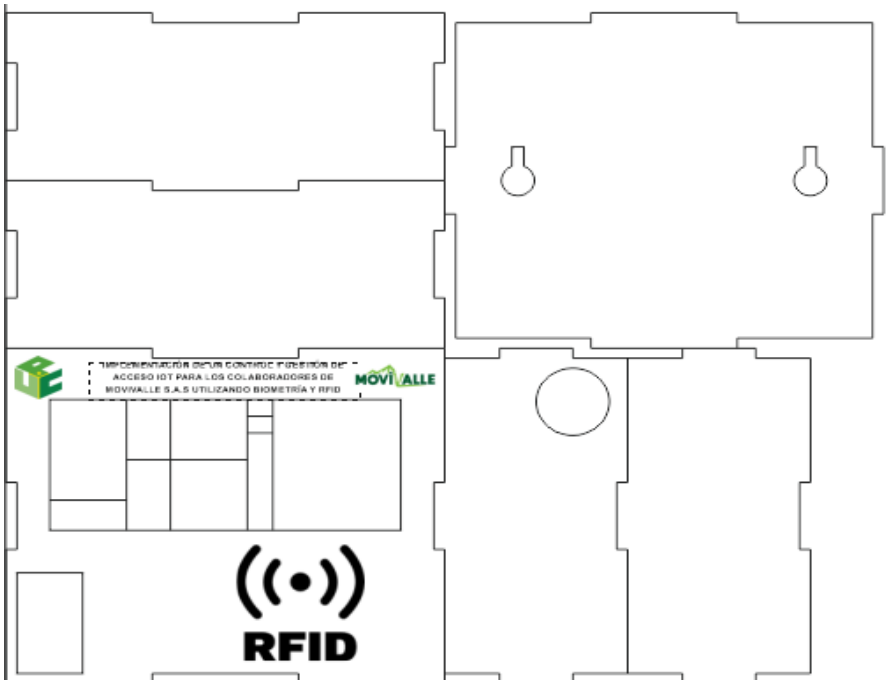
10.6 DISEÑO CONTENEDOR DE CIRCUITOS

Para el encapsulado contenedor de los circuitos se tuvo en cuenta que se cuenta con energía AC como entrada de alimentación, esto hizo obligatorio el uso de un material ignifugo para evitar la propagación de incendios en caso de fallas relacionadas con la electricidad, por esto se utilizo Polimetilmetacrilato, el cual es un material que se puede cortar en formas geométricas las cuales pueden ser armadas con posterioridad para formar un contenedor de circuitos. Para este caso en específico se hace uso de corelDRAW.

En la figura 17, se puede apreciar el diseño hecho en 2D el cual de manera posterior se transformó en una caja la cual encaja entre sí para evitar deformaciones en la misma, se tiene la ubicación de cada uno de los sensores y la pantalla, no se cuenta con interruptor para evitar que sea apagado por alguno de los operarios.

Figura 15.

Diseño de estructura en corelDRAW



Fuente: Autores

11. RESULTADOS DEL PROCESO DE MONTAJE

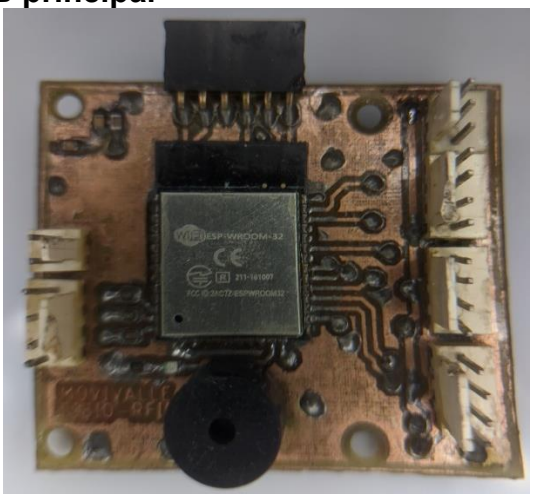
En este capítulo de abordaran los resultados obtenidos en el presente desarrollo para lograr a cabalidad de los objetivos planteados al inicio del mismo:

11.1 IMPLEMENTACIÓN DE HARDWARE

11.1.1 Montaje de circuito principal. Se utilizo una placa de baquela doble faz en fibra de vidrio para la realización del circuito principal, lo cual permite una mejor durabilidad y permite una posibilidad de mejor distribución de componentes en ambos lados de la misma.

En la figura 18, se puede apreciar la vista superior de la PCB principal, en la cual se aplica como se indicó en la sección anterior, el microcontrolador principal, la gran mayoría de componentes se conectaron a través de conectores tipo molex 2.54mm de distintos números de pines dependiendo de la finalidad de los mismos, entre estos tenemos 7 pines para el lector RFID, 4 pines para la pantalla 20x4 conectada vía I2C, 4 pines para el lector de huella dactilar conectado vía uart.

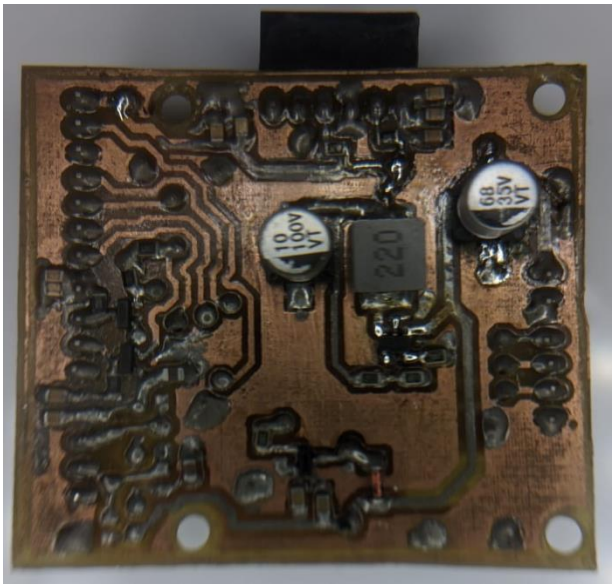
Figura 16.
Vista superior de PCB principal



Fuente: Autores

En la cara inferior, ver figura 19, se tiene la fuente de alimentación BUCK y sus componentes pasivos, también se tienen capacitores SMD y transistores mosfet SMD que permiten hacer convertidores de nivel de tensión para poder operar componentes que trabajan en distintos voltajes de 3.3V a 5V y viceversa.

Figura 17.
Vista inferior de PCB principal



Fuente: Autores

La PCB desarrollada permite la integración de hardware necesaria para la implementación de prototipo final, siendo compacta y con la potencia computacional necesaria para el control de los distintos periféricos con los que cuenta el prototipo.

11.1.2 Contenedor de circuitos. Como se planteó en el capítulo anterior, el contenedor de circuito fue diseñado en coreldraw e impreso en 2D para luego ser armado en una estructura encajable en forma de caja que cuenta con los compartimentos necesarios para el funcionamiento de cada uno de los periféricos

involucrados en el funcionamiento del prototipo, pantalla, lector de huella, lector RFID.

Una vez se tienen las caras en 2D para realizar el pegado de las mismas se procede utilizar Cloruro de metileno, el cual es un químico especial que permite fusionar placas de acrílico de manera fuerte para así poder armar una estructura resistente, ver figura 20.

Figura 18.

Vista frontal de encapsulado de circuitos

Fuente: Autores

En la figura 21, se puede apreciar la cara posterior de la estructura en la cual se tienen soportes para fijar con tornillos en el muro y así facilitar su instalación. Además de permitir intercambio de aire para evitar sobre calentamiento sobre todo de la fuente y el microcontrolador.

Figura 19.

Vista posterior del contenedor de circuitos

Fuente: Autores

En la figura 22, se puede apreciar cómo están puestos los circuitos en el interior de la caja contenedora de circuitos, se emplearon bases separadoras de pcb para las tarjetas de alimentación y de control, como se indicó anteriormente se usaron conectores molex, los cuales fueron usados con espadines para la conexión y adicionalmente se usó pegante tipo T-800, para evitar que el movimiento dañe las

conexiones eléctricas haciéndolas más duraderas, además se puede ver como se emplearon soportes en el mismo acrílico para soportar la pantalla, el lector RFID y el módulo lector de huella dactilar. Además del uso de termo encogible para proteger empalmes realizados en las conexiones.

Figura 20.

Disposición interna de circuitos dentro del contenedor de circuitos

Fuente: Autores

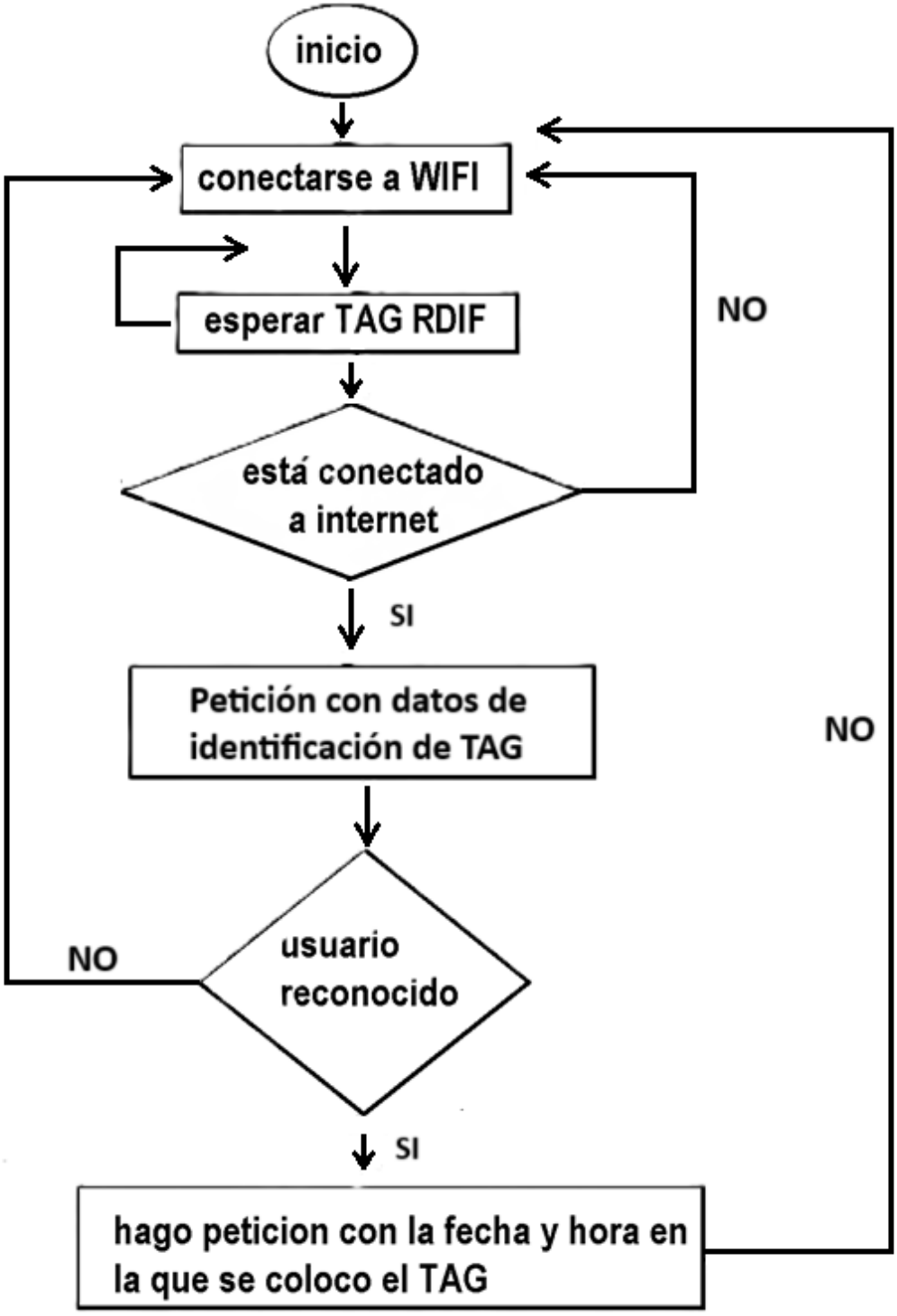
11.2 INTERACCIÓN DE FUNCIONES PARA ENVIÓ DE DATOS EN TIEMPO REAL

En esta sección, se mostrarán las funciones necesarias para subir datos en la nube, en primera medida se tiene que tener claridad que el dispositivo debe contar con conexión a una red wifi para que dichas funciones operen de manera correcta.

11.2.1 Función para el envío de datos RFID. Esta sección esta divida en 2 funciones principales, de la siguiente manera, ver figura 23. El método de funcionamiento es el siguiente, debido a limitantes de memoria del microcontrolador este no hace almacenamiento de datos de manera local, los datos de los usuarios están en la plataforma web, por esto, al colocar un TAG RFID, cerca del sensor este obtiene sus datos de identificación y estos son consultados en la plataforma web para ver si ese TAG corresponde a un usuario, obteniendo así, los datos de individuales de cada usuario, nombre, apellido, cargo, numero de documento. Con esos datos se procede a subir a la nube la fecha y hora en la que se colocó el TAG para informar su hora de entrada y salida. Teniendo claro esto, se debe tener en cuenta que se tendrá una base de datos de usuario y una base de datos de horarios de entrada y salida. Dicho control será realizado por el ESP32 y el archivo PHP, sin intervención alguna de la interfaz móvil.

Figura 21.

Algoritmo para él envió de datos en tiempo real



Fuente: Autores

Como se puede apreciar en la figura 24, la función realizar petición solicita los datos del TAG a la base de datos de usuarios, esto a través de una petición GET, de la cual se obtiene como respuesta una carga útil en forma de archivo JSON, el cual de ser valido contiene los datos del usuario propietario del TAG.

Figura 22.

Función de petición de datos del TAG

```
void realizarPeticion() {
  f_dato_si=0;
  if (WiFi.status() == WL_CONNECTED) { // Verifica que el WiFi esté conectado
    HTTPClient http;
    url = "https://ingelectronicaunicesar.com.co/MOVlV@ll3.php?act=Cl&CC="+String(ActualUID[0])+String(ActualUID[1])+
    Serial.println("");
    Serial.println(url);

    http.begin(url);                  // Inicia la conexión con la URL
    int httpResponseCode = http.GET(); // Realiza una petición GET

    if (httpResponseCode > 0) {
      Serial.print("Código de respuesta HTTP: ");
      Serial.println(httpResponseCode);

      if (httpResponseCode == HTTP_CODE_OK) {
        String payload = http.getString(); // Obtiene la respuesta en formato JSON
        Serial.println("Respuesta del servidor:");
        Serial.println(payload);

        // Procesar el archivo JSON
        StaticJsonDocument<512> doc; // Ajusta el tamaño si es necesario
        DeserializationError error = deserializeJson(doc, payload);

        if (error) {
          Serial.print("Error al analizar JSON: ");
          Serial.println(error.c_str());
          return;
```

Fuente: Autores

Se buscará en el archivo JSON, ver figura 25, en primera medida el documento, que es un número de identificación único y primario de la base de datos, con lo cual se podrá indicar quien fue quien coloco el TAG, adicionalmente se saludara al usuario en la pantalla con un Hola, su nombre y el número de identificación del TAG y por medio de una bandera se indicara si los datos del usuario fueron encontrados, esta bandera es llamada f_dato_si y se coloca en 1 si el usuario fue encontrado.

Figura 23.

Extracción de datos de archivo JSON

```
 // Acceder al primer elemento del arreglo
 JsonArray array = doc.as<JsonArray>();
 JsonObject obj = array[0]; // Primer elemento del arreglo

 // Extraer datos específicos
const char* nombre = obj["NOMBRE"];    // Cambia "nombre" por la clave del JSON
const char* documento = obj["DOC"];    // Cambia "nombre" por la clave del JSON
const char* ID1 = obj["ID"];

 // Verificar si 'nombre' tiene valor o está vacío
 if (nombre == nullptr || strlen(nombre) == 0) {
   Serial.println("La variable 'nombre' está vacía o no existe.");
 } else {
 // Mostrar los datos en el monitor serial
 Serial.print("Hola ");
 Serial.print(nombre);
 Serial.print(",Bienvenido");
 lcd.clear();
 lcd.print("Hola ");
 lcd.print(nombre);
 lcd.setCursor(0, 1);
 lcd.print("ID:");
 lcd.print(ID1);
 f_dato_si=1;
 N = nombre;
 Ced =documento;
 IDx =ID1;
 }
```

Fuente: Autores

Una vez se tienen los datos del usuario, se procede a realizar otra petición web a través de un GET, el cual usa la opción in_user del archivo PHP el cual tiene programada una función para marcar la hora de entrada o salida del usuario dependiendo del caso, en este caso solo se espera una respuesta afirmativa por parte del servidor y el módulo emite un sonido afirmativo si logra subir los datos a la nube, ver figura 26.

Figura 24.

Registro de hora de colocación del TAG

```
void enviar_datos() {
  if (WiFi.status() == WL_CONNECTED) { // Verifica que el WiFi esté conectado
    HTTPClient http;
    url = "https://ingelectronicaunicesar.com.co/MOVlV@ll3.php?act=in_user&NOMBRE="+String(N)+"&DOC="+String(Ced)+"&ID="+String(IDx);
    N = "";    // Cambia "nombre" por la clave del JSON
    Ced = "";    // Cambia "nombre" por la clave del JSON
    IDx="";
    Serial.println("");
    Serial.println(url);
    http.begin(url);                    // Inicia la conexión con la URL
    int httpResponseCode = http.GET(); // Realiza una petición GET

    if (httpResponseCode > 0) {
      Serial.print("Código de respuesta HTTP: ");
      Serial.println(httpResponseCode);

      if (httpResponseCode == HTTP_CODE_OK) {
        String payload = http.getString(); // Obtiene la respuesta en formato JSON
        Serial.println("Respuesta del servidor:");
        Serial.println(payload);
      }
    } else {
      Serial.print("Error en la solicitud HTTP: ");
      Serial.println(httpResponseCode);
    }

    http.end(); // Finaliza la conexión HTTP
  } else {
    Serial.println("WiFi desconectado.");
  }
}
```

Fuente: Autores

La primera función del Arduino utiliza el case C1, ver figura 27, en el cual debe dar un numero el cual corresponde a un documento de identificación del TAG RFID el cual busca en la base de datos en la Columba ID, de ser un usuario valido responde con un JSON con los archivos válidos.

Figura 25.

Función para solicitar datos de empleado

```
case 'C1':    // filtro dato para verificar contrase□a y usuario
  $Doc=  $_GET["CC"];
  $sql = "SELECT * FROM `Empleados` WHERE ID='$Doc';";

   $q =$conDB->query($sql); // ejecuto peticion
   $rows = array();
   while($r = mysqli_fetch_assoc($q)) // lee cada fila
   {
       $rows[] = $r;
   }
   print json_encode($rows); // envio datos devuelto
   break;
```

Fuente: Autores

Luego se emplea la función in_user, ver figura 28, la cual establece la hora en la que se colocó el TAG pero esta tiene una doble funciona, ya que en primera medida consulta si dicho ID RFID ya ha sido escrito en la base de datos en ese día, de no ser así, el usuario va entrando a su horario de trabajo y lo marca como hora de entrada, si existe una entrada antes de la actual, eso quiere decir que el usuario va saliendo de su puesto de trabajo, haciendo un mod para ver si la cantidad de resultados son pares o impares, para determinar si va entrando o saliendo. Esto se marca con una columna adicional que tiene la tabla de horarios en la cual se indica el estado de dicha ocasión en la que se colocó el TAG determinando entrada o salida.

Figura 26.

Función marcación de hora de entrada o salida

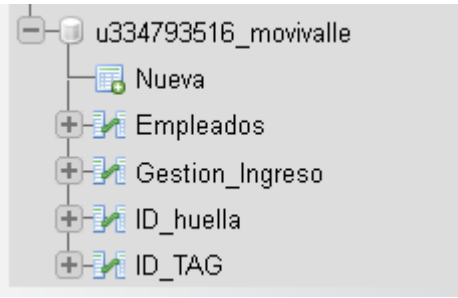
```
case 'in_user':
$Nombre = $_GET["NOMBRE"];
$Doc = $_GET["DOC"];
$ID = $_GET["ID"];

// Consulta para contar los registros del usuario en el día actual
$sqlCount = "SELECT COUNT(*) as total FROM `Gestion_Ingreso` WHERE `Codigo` = '$ID' AND DATE(`Fecha`) = CURDATE();";
$resultCount = $conDB->query($sqlCount);

if ($resultCount) {
 $row = $resultCount->fetch_assoc();
 $total = $row['total']; // Número de registros del día

 // Verificar si es entrada o salida
 if ($total % 2 == 0) {
     // Entrada
     $status = "Entrada";
 } else {
     // Salida
     $status = "Salida";
 }

 // Insertar el nuevo registro con la hora ajustada
 $sqlInsert = "INSERT INTO `Gestion_Ingreso` (`N`, `Nombre`, `Documento`, `Codigo`, `Fecha`, `Status`)
               VALUES (NULL, '$Nombre', '$Doc', '$ID', DATE_SUB(NOW(), INTERVAL 5 HOUR),'$status');";

 $resultInsert = $conDB->query($sqlInsert);

 // Preparar respuesta
 $rows = array();
 $rows['status'] = $status; // Indica si fue entrada o salida
 $rows['error_code'] = mysqli_errno($conDB); // Número de error
 $rows['error_message'] = mysqli_error($conDB); // Mensaje de error

 print json_encode($rows);
  } else {
```

Fuente: Autores

11.3 BASES DE DATOS CENTRALIZADAS

Las bases de datos están centralizadas en un servidor web propio obtenido para el almacenamiento de dichos datos y está compuesta de 4 tablas, las cuales son, ver figura 29.

Figura 27.
Bases de datos WEB



Fuente: Autores

Cada una de estas bases de datos tiene una función específica para el funcionamiento del prototipo, se tiene la tabla empleados la cual contiene datos de identificación únicos de cada usuario, la tabla gestión de ingreso permite almacenar e identificar las horas de entrada y salida de cada usuario, ID_huella permite que la interfaz sepa que se va agregar una nueva huella perteneciente a un nuevo usuario, de igual manera ID_TAG, ambas son bases de datos donde siempre se busca el ultimo valor y que este sin usar para ser empleado en la identificación de un nuevo usuario. Esto será explicado en detalle con posterioridad.

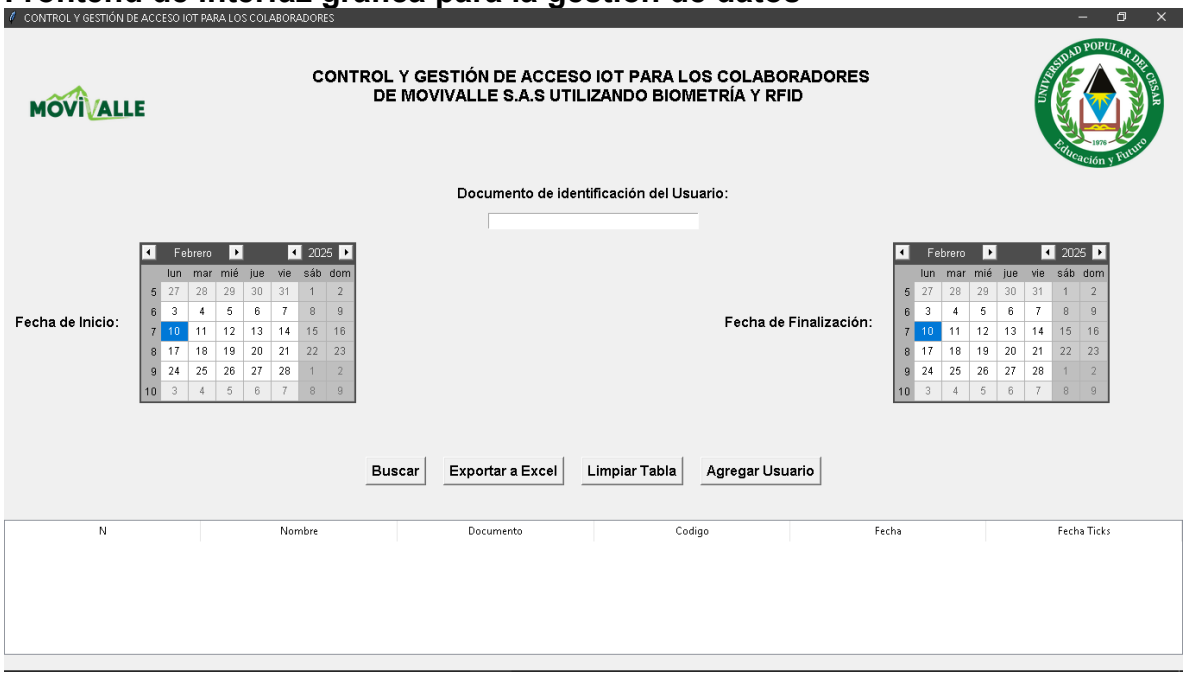
11.4 INTERFAZ PARA LA GESTIÓN DE LA INFORMACIÓN

Inicialmente se planteó un desarrollo móvil basado en Android, pero debido a peticiones realizadas por los encargados de Movivalle, se pidió modificar a una interfaz local que opere en Windows con conectividad a la red y que al igual que el Arduino tenga la capacidad de hacer peticiones web.

En la Figura 30, se puede apreciar la vista final de la interfaz gráfica creada para el desarrollo, la cual es diseñada en tkinter utilizando Python y como compilador visual studio code, en esta se tienen los logos de las entidades involucradas, el título del desarrollo, se cuenta con un entry el cual permite buscar el usuario por su documento o dejarlo vacío para buscar todos los usuarios. Se cuenta con 2 datapicker los cuales permiten delimitar las fechas de inicio y terminación de búsqueda, además se tienen varios botones de acción, entre ellos, buscar entre las fechas que ya se han seleccionado los resultados, esto llena la tabla que se en la parte inferior, adicionalmente se tiene el botón exportar el cual permite que la tabla sea enviada a un archivo en Excel con los resultados obtenidos, se tiene otro botón para vaciar la tabla, por último se tiene un botón que permite agregar usuarios.

Figura 28.

Frontend de interfaz gráfica para la gestión de datos



Fuente: Autores

Internamente para garantizar su funcionamiento, dentro del backend de la interfaz se realizan peticiones GET al servidor, para agregar nuevos usuarios o para consultar las horas de entrada en las fechas estipuladas en los datepicker.

11.4.1 Función para consultar horas de entrada y salida de usuarios. Dicha función, es denominada función buscar, ver figura 31, inicialmente lo que hace es tomar las fechas que están señaladas en los datepicker, teniendo en cuenta algunas condicionales, como que la fecha de finalización no puede ser mayor a la fecha de inicio, luego de esto se usa la función RALL_G1, dentro del archivo PHP, esta función responde con todo el listado los horarios marcados en la tabla GESTION_DE_INGRESO, en forma de archivo JSON el cual debe ser decodificado de manera posterior.

Figura 29.

Función buscar

```
def buscar():
    global busqueda_realizada
    try:
        # Obtener las fechas seleccionadas del calendario
        fecha_inicio = cal_inicio.get_date()
        fecha_fin = cal_fin.get_date()

        # Validar el rango de fechas
        fecha_inicio_dt = datetime.strptime(fecha_inicio.strip(), '%d/%m/%y')
        fecha_fin_dt = datetime.strptime(fecha_fin.strip(), '%d/%m/%y')
        if fecha_inicio_dt > fecha_fin_dt:
            messagebox.showerror("Error", "La fecha de inicio no puede ser mayor que la fecha de finalización.")
            return

        fecha_inicio_ticks = int(time.mktime(fecha_inicio_dt.timetuple()))
        fecha_fin_ticks = int(time.mktime(fecha_fin_dt.timetuple()))

        # Obtener el código del Entry
        codigo = entry_codigo.get().strip()

        # Realizar la petición GET a la URL
        url = "https://ingelectronicaunicesar.com.co/M0V1V@113.php?act=Rall_GI"
        response = requests.get(url)
        if response.status_code != 200:
            messagebox.showerror("Error", f"Error al obtener datos: {response.status_code}")
            return
```

Fuente: Autores

Una vez se tiene la respuesta del archivo JSON, Las fechas se convierten en ticks porque facilita su comparación y manipulación al representarlas como números en lugar de cadenas de texto, lo que permite operaciones matemáticas simples, y hace

que las búsquedas en bases de datos sean más rápidas y eficientes. Además, al eliminar la ambigüedad de formatos de fecha regionales, se evita la posibilidad de errores al comparar fechas en distintos formatos, garantizando precisión y coherencia en sistemas automatizados. Si entonces, se tienen fechas en la base de datos que a través de su tick sean menores a la fecha final y mayores a la fecha igual sin almacenadas en una variable matriz llamada registros filtrados, ver figura 32.

Figura 30.

Filtrado de fechas

```
data = response.json()

# Filtrar los registros dentro del rango de fechas
registros_filtrados = []
for registro in data:
    fecha_dt = datetime.strptime(registro["Fecha"], "%Y-%m-%d %H:%M:%S")
    fecha_ticks = int(time.mktime(fecha_dt.timetuple()))

    # Si entry_codigo está vacío, incluir todos los registros en el rango de fechas
    if fecha_inicio_ticks <= fecha_ticks <= fecha_fin_ticks:
        if not codigo or registro["Documento"] == codigo:
            registros_filtrados.append({
                "N": registro["N"],
                "Nombre": registro["Nombre"],
                "Documento": registro["Documento"],
                "Codigo": registro["Codigo"],
                "Fecha": registro["Fecha"],
                "Fecha Ticks": fecha_ticks
            })
```

Fuente: Autores

En la figura 33, se puede ver como se limpia la tabla y se procede a través de un for a insertar cada una de las filas con los datos filtrados, sino se tiene registros en las fechas seleccionadas se procede a informar al usuario con un mensaje emergente.

Figura 31.

Limpieza de tabla y escritura de datos

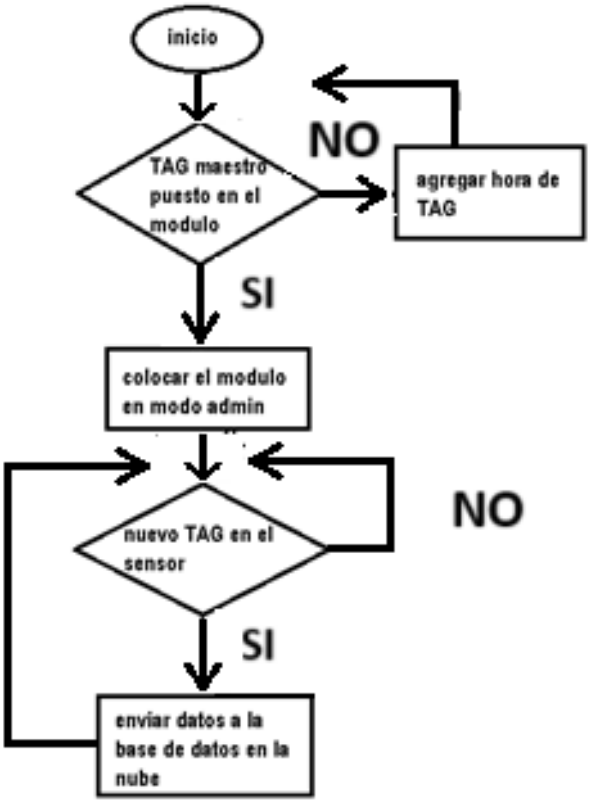
```
# Limpiar la tabla antes de cargar nuevos datos
for item in tabla.get_children():
    tabla.delete(item)

# Llenar la tabla con los registros filtrados
for registro in registros_filtrados:
    tabla.insert("", "end", values=(registro["N"], registro["Nombre"], registro["Documento"],
                                    registro["Codigo"], registro["Fecha"], registro["Fecha Ticks"]))

# Si no hay registros en el rango, mostrar mensaje
if not registros_filtrados:
    messagebox.showinfo("Información", "No se encontraron registros dentro del rango de fechas seleccionado.")

# Marcar la búsqueda como realizada
busqueda_realizada = True
```

Fuente: Autores

11.4.2 Función para agregar un nuevo usuario. Se debe tener claridad que, para agregar un nuevo usuario, no solo se requiere la interfaz sino también el dispositivo, el cual tendrá un TAG maestro el cual permitirá controlar si se va agregar un nuevo usuario o no, ya que se requiere el código del TAG y el ID de la huella almacenada. En la Figura 34, se tiene el algoritmo por el cual, al colocar la tarjeta administrador el microcontrolador, espera que se coloquen nuevas TAG para agregar un nuevo usuario, esto es mostrado en la pantalla y enviado a la nube a una base de datos especial marcando el valor STATUS con un cero, el cual solo será cambiado por la interfaz cuando dicho TAG sea guardado, lo mismo ocurre con una huella nueva agregada, existe su propia base de datos para informar del ID de huella que ha sido agregado.

Figura 32.

Algoritmo de como agregar nuevos usuarios



Fuente: Autores

Como se ve en la figura 35, cuando se recibe un nuevo TAG, se subirá al servidor usando la función add_ID, junto con el ID del mismo. Todo esto a través de una petición GET y esperando una respuesta afirmativa.

Figura 33.

Función para agregar un nuevo TAG a la nube

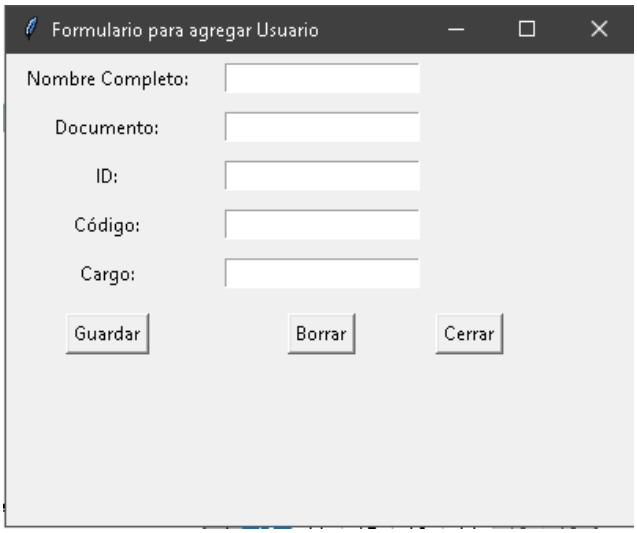
```
void agregar_TAG_nube(void){
  if (WiFi.status() == WL_CONNECTED) { // Verifica que el WiFi esté conectado
    HTTPClient http;
    url = "https://ingelectronicaunicesar.com.co/MOVlV@113.php?act=add_ID&ID="+String(ActualUID[0])+String(ActualUID[1])+String(ActualUID[2])+String(ActualUID[3])+"&status=0";
    Serial.println("");
    Serial.println(url);

    http.begin(url);                  // Inicia la conexión con la URL
    int httpResponseCode = http.GET(); // Realiza una petición GET

    if (httpResponseCode > 0) {
      Serial.print("Código de respuesta HTTP: ");
      Serial.println(httpResponseCode);

      if (httpResponseCode == HTTP_CODE_OK){
        String payload = http.getString(); // Obtiene la respuesta en formato JSON
        Serial.println("Respuesta del servidor:");
        Serial.println(payload);
      }
    } else {
      Serial.print("Error en la solicitud HTTP: ");
      Serial.println(httpResponseCode);
    }

    http.end(); // Finaliza la conexión HTTP
  } else {
    Serial.println("WiFi desconectado.");
  }
}
```

Fuente: Autores

La interfaz cuenta con un botón de agregar usuario, esto para poder adicionar trabajadores desde el más alto nivel, solo con apoyo de los sensores para obtener los datos biométricos y el TAG que se le asigne, esta sección abre un formulario que es visto en la figura 36.

Figura 34.

Formulario para agregar nuevos usuarios



Fuente: Autores

Como se indicó anteriormente, los datos de ID y código de huella son recibidas desde el servidor web a través del dispositivo, esto lo hace a través de peticiones web que son realizadas cada segundo, se va intentar mientras se tenga abierto el formulario descargar datos 200 veces, esto será reiniciado al cerrar y abrir nuevamente, como se mencionó al tocar el botón guardar, el estado de la columna STATUS a 1, solo va descargar datos mientas en esa columna se tenga un cero, al conseguir un cero, se ve como agrega el valor de ID descargado en el JSON en el entry código, se tiene una función igual para el TAG RFID nuevo.

Figura 35.

Función de búsqueda de datos ID y huella

```
def obtener_id_codigo(intentos=0):
    global max_intentos

    if intentos >= max_intentos:
        print("Se alcanzó el límite de intentos, deteniendo búsqueda de ID.")
        return

    url = "https://ingelectronicaunicesar.com.co/M0V1V@113.php?act=ultima_huella"
    try:
        response = requests.get(url)
        data = response.json()

        if isinstance(data, list) and len(data) > 0:
            data = data[0]  # Obtener el primer diccionario de la lista

        if isinstance(data, dict):
            if data.get("STATUS") == '0':
                entry_codigo.delete(0, 'end')
                entry_codigo.insert(0, data.get("ID", ""))

        else:
            print("La respuesta no es un diccionario.")
    except Exception as e:
        print(f"Error en la solicitud: {e}")
```

Fuente: Autores

Al presionar el botón guardar se utiliza la función *add,* la cual permite agregar usuarios en la base de datos de empleados, concatenando de manera sistemática los datos para crear de manera correcta los datos para la petición GET.

Figura 36.

Subir datos a base de datos empleados

```
base_url = "https://ingelectronicaunicesar.com.co/M0V1V@113.php"
params = {
    "act": "add",
    "NOMBRE": entry_nombre.get(),# &" "& entry_apellido.get(),
    "DOC": entry_documento.get(),
    "CARGO": entry_cargo.get(),
    "ID": entry_id.get(),
    "Huella_ID": entry_codigo.get()
}
url = f"{base_url}?{urllib.parse.urlencode(params)}"
print(url)
try:
    response = requests.get(url)
    if response.status_code != 200:
        messagebox.showerror("Error", f"Error al subir datos a la plataforma:
        return
except Exception as e:
    messagebox.showerror("Error", f"Excepción durante la solicitud: {e}")

max_intentos = 1
messagebox.showinfo("Éxito", "Datos guardados correctamente.")
```

Fuente: Autores

Figura 39.

Registros consultados en la base de datos

	A	B	C	D	E	F
1	CONTROL Y GESTIÓN DE ACCESO IOT PARA LOS COLABORADORES					
2	DE MOVIVALLE S.A.S UTILIZANDO BIOMETRÍA Y RFID					
3	Fechas: 20/1/25 a 27/1/25					
4						
5						
6						
7	**N**	**Nombre**	**Documento**	**Codigo**	**Fecha**	**Fecha Ticks**
8	40	juan	123456	12321	2025-01-24 09:26:18	1737728778
9	41	juan	123456	12321	2025-01-24 09:26:32	1737728792

Fuente: Autores

12. CONCLUSIONES

El proyecto de implementación de un sistema de control y gestión de acceso IoT para los empleados y colaboradores de MOVIVALLE S.A.S. permitió alcanzar los objetivos planteados, adaptándose a los cambios necesarios durante su desarrollo. A continuación, se presentan las conclusiones más relevantes:

Se logró implementar un sistema de control de acceso basado en biometría y RFID, cumpliendo con el objetivo de mejorar el control y la gestión de acceso en las instalaciones de la empresa MOVIVALLE S.A.S.

El prototipo de identificación con biometría y RFID demostró una gran robustez garantizando la autenticación precisa de los usuarios y reduciendo los riesgos de acceso no autorizado. La integración de dispositivos IoT permitió el monitoreo en tiempo real del sistema, facilitando la toma de decisiones con respecto a los registros en las bases de datos.

La creación de una base de datos centralizada para la gestión de acceso ha sido fundamental para almacenar la información. Esta base de datos permite el acceso rápido a los registros de entrada y salida, así como la generación de reportes y análisis de datos.

La decisión de cambiar el enfoque hacia una plataforma para sistemas de cómputo en lugar de una aplicación móvil resultó ser acertada. La interfaz desarrollada con Tkinter es intuitiva y se adapta mejor a las necesidades de los administradores, quienes suelen trabajar desde computadoras de escritorio y portátiles. Esta plataforma permite gestionar y monitorear el sistema de acceso de manera centralizada, brindando una experiencia de usuario más completa.

Se elaboró un manual de usuario detallado que facilita la capacitación del personal tanto en el uso del dispositivo como de la plataforma de gestión. Este manual garantiza que los administradores y colaboradores puedan utilizar el sistema teniendo en cuenta los requerimientos para su correcto funcionamiento, requisitos previos y mantenimiento.

REFERENCIAS BIBLIOGRÁFICAS

Bennett, C. J., & Groves, J. (2012). *Biometrics: A very short introduction*. Oxford University Press.

Boada, D. (2022). *¿Qué es un servidor web y cómo funciona?* Tutoriales Hostinger. https://www.hostinger.co/tutoriales/que-es-un-servidor-web

Borghello, C. 2011. Reconocimiento-de-huellas-dactilares. En línea. Formato HTML. Consultado el 22 de noviembre de 2015. Disponible en: http://blog.segu-info.com.ar/2011/05/reconocimiento-de-huellasdactilares.html

Carbonell Caballero, D. J. (2018) Propuesta de Diseño de un Control de Acceso Biométrico para el cuarto de Raee de la Empresa Securitas Colombia SA Sede Bogotá.

Cedeño, J. R., & Párraga, C. L. (2017). *Sistema biométrico de control de acceso para el laboratorio de cómputo de la Unidad Educativa Francisco González Álava*

Díaz, A. (2022). *La seguridad física evoluciona con la adopción de nuevas tecnologías, según un estudio de Genetec*. ESMARTCITY. https://www.esmartcity.es/2022/03/04/seguridad-fisica-evoluciona-con-adopcion-nuevas-tecnologias-segun-estudio-genetec

Echavez, M. (2020). *Diseño e implementación de un sistema de biometría facial para el control de acceso en la Universidad de Cartagena.* Universidad de Cartagena.

ESP32, DEVKIT V1 DOIT, (s/f). *ESP32 Pinout Reference: Which GPIO pins should you use?* Githubusercontent.com. Recuperado el 24 de febrero de 2025, de https://raw.githubusercontent.com/atomic14/esp32-pinouts/main/esp32.webp

Fernández J. & L. M. (2019) Sistema de control de acceso inteligente basado en IoT para la mejora de la seguridad y la eficiencia operativa en empresas de *Simposio Internacional de Aplicaciones Tecnológicas (SIAT)*, Quito, Ecuador.

García M., (2020). Sistemas de control de acceso: Tradicionales versus digitales," Revista de Tecnología y Seguridad, vol. 15, Nº 3, pp. 45-60.

Grupo Tecma Red S. L. (2022). La seguridad física evoluciona con la adopción de nuevas tecnologías, según un estudio de Genetec. ESMARTCITY. https://www.esmartcity.es/2022/03/04/seguridad-fisica-evoluciona-con-adopcion-nuevas-tecnologias-segun-estudio-genetec.

Gutiérrez, A. A., Ceron M., Rodrigo, Magobel. (2022). *Tutorial de Arduino y sensor ultrasónico HC-SR04*. Naylamp Mechatronics - Perú. https://naylampmechatronics.com/blog/10_tutorial-de-arduino-y-sensor-ultrasonico-hc-sr04.html

Huidobro, J. M. (s/f). La tecnología RFID. www.acta.es. Recuperado el 21 de septiembre de 2024, de https://www.acta.es/medios/articulos/ciencias_y_tecnologia/058037.pdf

Innovatrics. (2021). *sistema biométrico*. https://www.innovatrics.com/partner-program/. https://www.innovatrics.com/es/glosario/sistema-biometrico/

Llamas, L. (2021), Lector de huellas dactilares con Arduino y sensor FPM10A. Luis Llamas. https://www.luisllamas.es/lector-de-huellas-dactilares-con-arduino-y-sensor-fpm10a/

Llamas, L. (2021a). *Sensor FM1001*. Luisllamas.es. https://www.luisllamas.es/wp-content/uploads/2021/04/arduino-lector-huellas-dactilares-esquema.png

Martínez, J. A. (2021) «La importancia del registro de horas trabajadas en la gestión de personal: Un enfoque práctico,» *Revista de Administración y Recursos Humanos,* vol. 2, nº 10, pp. 34-45.

Meneses, A. J., & García, C. G. (2016) Diseño e Implementación de un Prototipo para el Control de Acceso en la Sede de Ingeniería de la Universidad Distrital Francisco José de Caldas Mediante el Uso de Torniquetes Controlados por Carnet con Tecnología NFC y Lector Biométrico de Huella Dactilar.

OSI (Oficina de Seguridad del Internauta). (2014). En línea. Formato HTML. Disponible en https://www.osi.es/es/actualidad/blog/2014/05/14/como-denunciar-unasuplantacion-de-identidad-en-internet

Osorio, J. A. C., Aguirre, F. A. M., & Escobar, J. A. M. (2010). Sistemas de seguridad basados en biometría. Scientia et technica, 17(46), 98-102.

Parra-Valencia, J., Guerrero, C., & Rico-Bautista, D. (2017). IOT: una aproximación desde ciudad inteligente a universidad inteligente. Revista Ingenio, 13(1), 142–153. https://doi.org/10.22463/2011642X.2128

Rodríguez M. G. y. P. P. A., (2018) Diseño e implementación de un sistema de control de acceso mediante RFID y biometría en entornos empresariales, de *Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, Bogotá, Colombia.

SIVA (2023), «sistema integrado de transporte Valledupar,» [En línea]. Available: https://siva.gov.co/.

Smith A. M., (2021) Impacto de la Cuarta Revolución Industrial en la gestión de procesos empresariales, *Revista Internacional de Tecnología y Gestión,* vol. 15, Nº 1, pp. 45-58.

Torres-Londoño, C. I., Gallego-Giraldo, J. D., & Garay-Flórez, A. F. (2017). *Sistema biométrico para control de acceso con doble validación Biometric system for access control with double validation*. Utp.ac.pa. https://revistas.utp.ac.pa/index.php/memoutp/article/view/1474/2120

TOTVS, (2021) Industria 4.0: el impacto en las empresas y la sociedad. Available: https://www.totvs.com/industria-4-0-impacto-en-las-empresas-y-la-sociedad.

Valencia, J; Cruz, J; Caicedo, L; Chamorro, C. 2014. Extracción de características del iris como mecanismo de identificación biométrica. CO. Revista Virtual Universidad Católica del Norte. Núm. 42. p 185.

Ventura, J. (2015). Introducción al concepto de seguridad. . En línea. Formato HTML. Consultado el 21 de noviembre de 2015. Disponible en 40 http://elordenmundial.com/seguridad/introduccion-al-concepto-deseguridad/

Zhang K., (2019) Design of an Intelligent Access Control System Based on RFID and Fingerprint Identification, *IEEE International Conference on Electronics and Information Engineering (ICEIE)*, Xi'an, China.

ANEXOS

ANEXO 1. EVIDENCIA FOTOGRÁFICA DE LA IMPLEMENTACIÓN DEL PROTOTIPO

Foto 1. Prototipo instalado

Foto 2. Punto de Acceso a la empresa

Foto 3. Empleado utilizando el dispositivo

Foto 4. Tarjetas contramarcadas con el código