UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE ELECTRICIDAD

PROPUESTA TECNOLÓGICA

IMPLEMENTACIÓN DE UN SISTEMA DOMÓTICO DE SEGURIDAD Y CONTROL MEDIANTE IOT APLICADO A UN LABORATORIO

Proyecto de Titulación presentado previo a la obtención del Título de Ingeniero Eléctrico

Autores:

Moreno Chuqui Washington Rafael

Serna Moreno Dilan Javier

Tutor Académico:

Ing. Corrales Bastidas Byron Paúl MSc

LATACUNGA – ECUADOR

2023

DECLARACIÓN DE AUTORÍA

Nosotros **Moreno Chuqui Washington Rafael**, con cedula de ciudadanía N° **060579849-5** y **Serna Moreno Dilan Javier**, con cedula de ciudadanía N° **050443959-7,** estudiantes de la carrera de Ingeniería en Electricidad declaramos ser autores de la presente propuesta tecnológica: **"Implementación de un sistema domótico de seguridad y control mediante IoT aplicado a un laboratorio"**, siendo el Ing. Corrales Bastidas Byron Paul, tutor del presente trabajo; y exime expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales se posibles reclamos o acciones legales.

Además, certificamos que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de nuestra exclusiva responsabilidad.

Latacunga, Agosto 2023

Moreno Chuqui Washington Rafael
C.C. 060579849-5

Serna Moreno Dilan Javier
C.C. 050443959-7

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de tutor de la siguiente propuesta tecnológica sobre el título: **"Desarrollo de un sistema de seguridad y control mediante IOT"** de los ponentes: **Moreno Chuqui Washington Rafael** y **Serna Moreno Dilan Javier**, de la Carrera de Ingeniería en Electricidad, considero que dicho informe cumple con los requerimientos metodológicos y aporte científico técnico suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de Ciencia de la Ingeniería y Aplicada de la Universidad Técnica de Cotopaxi digne, para su correspondiente estudio y calificación.

Latacunga, Agosto 2023

Ing. Corrales Bastidas Byron Paul MSc.

CC: 050234776-8

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN.

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la **Facultad de Ciencias de la Ingeniería y Aplicadas**; por cuanto, los postulantes: Moreno Chuqui Washington Rafael, con cédula de ciudadanía N° 060579849-5 y Serna Moreno Dilan Javier, con cédula de ciudadanía N° 050443959-7 con el título de Proyecto de titulación:

"Desarrollo de un sistema de seguridad y control mediante IOT", han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, Agosto 2023

Primer Lector

Ing. Castillo Fiallos Jessica Nataly MSc.

CC: 0604590216

Segundo Lector

Ing. Vásquez Teneda Franklin Hernán MSc.

CC: 171043449-7

Tercer Lector

Ing. Salazar Achig Edgar Roberto MSc.

CC: 050284761-9

AVAL DE IMPLEMENTACIÓN

En calidad de Técnico de laboratorio de la facultad de Ciencias de la Ingeniería y Aplicadas certifico que mediante el proyecto tecnológico "**Desarrollo de un sistema de seguridad y control mediante IOT**" de los señores **Moreno Chuqui Washington Rafael**, y **Serna Moreno Dilan Javier**, realizan la implementación del sistema de seguridad y control mediante IOT.

Latacunga, agosto 2023

Ing. Diego Paul Corrales Vargas.

CC: 0504375502

DEDICATORIA

Con un profundo sentido de gratitud, dedico este trabajo a mis amados padres, cuyo apoyo desde mis primeros pasos hasta este momento ha sido la base sólida que me impulsa a superar obstáculos y a seguir adelante. Sus enseñanzas, paciencia y amor incondicional han sido la chispa que encendió mi pasión por el aprendizaje y el crecimiento personal.

A mi familia, que ha estado siempre a mi lado, quiero expresar mi agradecimiento por su constante presencia y cuidado. Su apoyo y aliento han sido el viento bajo mis alas, permitiéndome explorar nuevas ideas y desafíos con confianza.

A mis amigos, quienes han sido parte activa de esta historia, les dedico un reconocimiento especial. Vuestra compañía, risas y respaldo han iluminado los momentos de dificultad y han compartido los logros con entusiasmo. Vuestras palabras alentadoras y amistad sincera son un regalo preciado que atesoro profundamente.

Cada página de este trabajo lleva implícito el reflejo de sus valiosas contribuciones y el impacto positivo que han tenido en mi vida. Esta dedicatoria es un modesto tributo a la influencia transformadora que han tenido en mi camino. Sin su apoyo y amor, este logro no sería posible. Desde lo más profundo de mi corazón, gracias por estar a mi lado y ser parte de este viaje.

Washington Moreno

Dedicado a todos aquellos que creen en el poder del conocimiento, la perseverancia y el esfuerzo. A mis seres queridos, amigos y mentores, cuyo apoyo incondicional ha sido mi fuente de inspiración a lo largo de este camino. Que esta tesis sea un tributo a la búsqueda constante de la excelencia y al deseo incansable de aprender y crecer. Con gratitud y humildad, les dedico este logro.

Dilan Serna

AGRADECIMIENTO

Quiero expresar mi sincero agradecimiento a mis padres, familiares y amigos por su inquebrantable apoyo a lo largo de esta travesía académica. Sus palabras de aliento, su confianza y su constante respaldo han sido pilares fundamentales en la realización de esta tesis. Cada uno de ustedes ha contribuido de manera directa o indirecta, y estoy profundamente agradecido por su presencia en este emocionante viaje de investigación. Su apoyo ha sido inestimable y ha marcado una diferencia significativa en mi logro académico.

Washington Moreno

Agradezco profundamente a mis padres por su constante apoyo y guía a lo largo de mi infancia y juventud. Mi gratitud también se extiende a mis compañeros de clase en el colegio, quienes han sido testigos y soportado con paciencia mis weas. Sin embargo, mi mayor reconocimiento va dirigido hacia mis compañeros y amigos que han sido parte esencial de mi experiencia universitaria. Su presencia a lo largo de este camino me ha brindado acompañamiento, valiosas enseñanzas y aliento para transformarme en la persona que soy hoy.

Dilan Serna

ÍNDICE GENERAL

DECLARACIÓN DE AUTORÍA i
AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN ii
APROBACIÓN DEL TRIBUNAL DE TITULACIÓN. iii
DEDICATORIA iv
AGRADECIMIENTO vi
ÍNDICE GENERAL viii
ÍNDICE DE FIGURAS xiii
ÍNDICE DE TABLAS xvi
RESUMEN xviii
ABSTRACT xix
AVAL DE TRADUCCIÓN xx
1. INFORMACIÓN GENERAL 1
2. INTRODUCCIÓN 2
2.1. EL PROBLEMA 2
2.1.1. Situación Problémica 2
2.1.2. Formulación del Problema 3
2.2. OBJETO Y CAMPO DE ACCIÓN 3
2.3. BENEFICIARIOS 3
2.4. JUSTIFICACIÓN 3
2.5. OBJETIVOS 4
2.5.1. Objetivo General 4
2.5.2. Objetivos Específicos 4
2.6. SISTEMA DE TAREAS 5
3. FUNDAMENTACIÓN TEÓRICA 6
3.1. ANTECEDENTES 6
3.2. MARCO REFERENCIAL 9

3.2.1. Sistemas de control de acceso 9
3.2.1.1. Sistemas biométricos 9
3.2.1.1.1. Reconocimiento facial 10
3.2.1.2. Sistemas basados en tarjetas magnéticas 10
3.2.1.2.1. Tarjetas magnéticas RFID 10
3.2.2. Sistema Domótico 11
3.2.2.1. Estructura de un sistema domótico 12
3.2.2.1.1. Controladores 12
3.2.2.1.2. Sensores 12
3.2.2.1.3. Actuadores 12
3.2.2.1.4. Interfaces 13
3.2.3. Internet de las cosas (IoT) 13
3.2.3.1. Telegram como medio IoT 14
3.2.3.1.1. Bots 14
3.2.3.1.2. Botfather 14
3.2.4. Microcontroladores 15
3.2.4.1. NodeMCU 15
3.2.4.2. ESP32 16
3.2.4.3. ESP32CAM 17
3.2.5. Entorno de desarrollo de Arduino IDE 18
3.2.5.1. Interfaz y editor de código 18
3.2.5.2. Compilación y verificación de errores 18
3.2.5.3. Carga y ejecución de programas 19
3.2.5.4. Bibliotecas de Arduino 19
3.2.5.5. Monitor serial 19
3.2.5.6. Compatibilidad con diversas placas 19
4. METODOLOGÍA Y MATERIALES 20

4.1. DESCRIPCIÓN DEL PROYECTO 20
4.1.1. Situación actual del laboratorio 20
4.1.2. Descripción del sistema 21
4.2. DISEÑO DEL SISTEMA 22
4.2.1. Definición de requerimientos 22
4.2.2. Selección de los microcontroladores 23
4.2.2.1. Microcontrolador para sistema de reconocimiento facial y cámara de entrada 23
4.2.2.2. Microcontrolador para el sistema de Identificación por radio frecuencia (RFID) 24
4.2.2.3. Microcontrolador para el control de luminarias y tomacorrientes mediante IoT 25
4.2.2.4. Elección de sensor de intrusión en ventanas 27
4.2.2.5. Selección de la Bocina de Alarma 28
4.2.2.5.1. Selección de módulo de cámara 29
4.2.2.5.2. Selección de luminarias adecuadas 29
4.2.2.5.3. Elección de sensor de movimiento 29
4.2.2.5.4. Elección del sensor para detectar incendios 30
4.2.2.5.5. Elección de lector RFID 31
4.2.2.5.6. Selección del relé 31
4.2.2.5.7. Selección de la Cerraduras Eléctricas 32
4.2.2.6. Ubicación de los elementos del sistema completo 33
4.2.2.6.1. Ubicación de camas de video vigilancia 33
4.2.2.6.2. Ubicación de las luminarias 35
4.2.2.6.3. Ubicación de las bocinas de alarmas 36
4.2.2.6.4. Ubicación de los sensores de intrusión en ventanas 36
4.2.2.6.5. Ubicación de los sensores de humo 36
4.2.3. Programación 38
4.2.3.1. Funcionamiento de la programación del sistema de reconocimiento facial 38
4.2.3.2. Funcionamiento de la programación del sistema RFID 42

4.2.3.3. Funcionamiento de la programación de la cámara de fotografía de registro.....44
4.2.3.4. Funcionamiento de la programación del control mediante IoT.....45
4.2.3.4.1. Funcionamiento del sistema de control por medio de IoT 47
4.2.4. Diagramas de funcionamiento.....48
4.2.4.1. Flujograma del reconocimiento facial 49
4.2.4.2. Flujograma del sistema RFID.....50
4.2.4.3. Flujograma del sistema de fotografía de registro 51
4.2.4.4. Flujograma del sistema de control IoT 53
4.2.4.4.1. Flujograma del control manual del sistema de control IoT 53
4.2.4.4.2. Flujograma del control automático del sistema de control IoT 53
4.2.4.4.3. Flujograma del control remoto del sistema de control IoT 54
4.2.5. Funcionamiento 55
4.2.5.1. Comandos del sistema de fotografía de registro.....56
4.2.5.2. Comandos para el sistema de control IoT 56
4.2.5.3. Comandos reconocimiento facial 57
4.2.6. Diseño de placas electrónicas.....58
4.2.6.1. Diseño de la PCB del sistema cámara de fotografía de registro.....58
4.2.6.2. Diseño de la PCB del sistema de control de acceso al laboratorio.....59
4.2.6.3. Diseño de la PCB del sistema de control IoT.....61
4.2.7. Diseño 3D.....62
4.2.7.1. Diseño 3D del sistema de fotografía de registro.....62
4.2.7.2. Diseño 3D del sistema de control de acceso (Portero electrónico) 62
4.2.7.3. Diseño 3D de la botonera 63
4.2.8. Dimensionamiento sistema de respaldo de energía.....63
4.2.8.1. Dimensionamiento del UPS para el diseño del sistema 63
4.2.8.2. Dimensionamiento del UPS para la implementación.....66
4.3. DIAGRAMA DE CONEXIÓN GENERAL DEL SISTEMA DESARROLLADO 67

4.4. IMPLEMENTACIÓN DEL SISTEMA EN EL LABORATORIO DE MANUFACTURA ADITIVA Y SUSTRACTIVA DE LA FACULTAD DE CIYA 68
4.4.1. Adecuación del sistema eléctrico 68
4.4.2. Ubicación de los elementos 69
4.4.2.1. Ubicación del sistema de control de acceso 70
4.4.2.2. Ubicación del sistema de fotografía de registro 71
4.4.2.3. Ubicación del sistema control IoT 72
4.4.2.4. Ubicación del sistema de respaldo de energía 72
4.4.3. Conexión del sistema respaldo de energía 74
4.4.4. Diagramas del sistema implementado 74
5. ANÁLISIS DE RESULTADOS 75
5.1. PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA 75
5.1.1. Conectividad Wi-Fi 75
5.1.2. Pruebas del sistema de control IoT 75
5.1.3. Pruebas de envió de fotografías 77
5.1.4. Pruebas del reconocimiento facial y RFID 80
5.1.5. Prueba de autonomía del sistema 81
5.2. COSTO DEL PROYECTO 82
5.2.1. Costos del diseño 82
5.2.2. Costos de implementación 83
5.3. COMBATIVA CON OTROS SISTEMAS COMERCIALES 84
6. CONCLUSIONES Y RECOMENDACIONES 85
6.1. CONCLUSIONES 85
6.2. RECOMENDACIONES 85
7. REFERENCIAS 86

ÍNDICE DE FIGURAS

Figura 1. BotFather y Telegram. 15

Figura 2. Microcontroladores de la familia ESP. 15

Figura 3. Pines de conexión NodeMCU con ESP8266. 16

Figura 4. Distribución de pines de la ESP32. 17

Figura 5. Distribución de pines ESP32 CAM. 18

Figura 6. Entorno de desarrollo de Arduino. 19

Figura 7. Plano antiguo del Laboratorio. 20

Figura 8. Área de cobertura de las cámaras. 35

Figura 9. Ubicación de los sensores de humo. 37

Figura 10. Selección de la placa AI Thinker ESP32-CAM. 38

Figura 11. Librerías utilizadas para el sistema de reconocimiento facial. 39

Figura 12. Datos de la red Wifi. 39

Figura 13. Inicialización del WbsocketsServer. 39

Figura 14. Página web CyberChef para desencriptar el código hexadecimal. 41

Figura 15. Interfaz de la ESP32-CAM por defecto. 41

Figura 16. Interfaz modificada. 42

Figura 17. Selección de la placa Generic ESP8266 Module. 42

Figura 18. Librerías utilizadas para el sistema RFID. 43

Figura 19. Ingreso de UID de nuevos usuarios. 44

Figura 20. Selección de la placa AI Thinker ESP32-CAM. 44

Figura 21. Librerías utilizadas en la cámara de fotografía de registro. 44

Figura 22. Datos de la red Wifi y Token de Telegram. 45

Figura 23. Libreas del del sistema de control IoT. 46

Figura 24. Función Ticker de las luminarias. 46

Figura 25. Función de teclado CTBot. 46

Figura 26. Interfaz del teclado en Telegram. 47

Figura 27. Diagrama de control por Telegram. 47

Figura 28. Retroalimentación del sistema de control IoT. 48

Figura 29. Flujograma del sistema de reconocimiento facial. 49

Figura 30. Flujograma del sistema RFID. 50

Figura 31. Flujograma del sistema de fotografía de registro con Telegram. 51

Figura 32. Flujograma del sistema de fotografía de registro con el sensor PIR. 52

Figura 33. Flujograma del control manual del sistema de control IoT. 53

Figura 34. Flujograma del control automático del sistema de control IoT. 54

Figura 35. Flujograma del control remoto del sistema de control IoT. 55

Figura 36. Comandos mostrados al enviar el comando "/config". 56

Figura 37. Comando "opciones" del sistema IoT. 57

Figura 38. Interfaz del reconocimiento facial 58

Figura 39. PCB del sistema de fotografía de registro 59

Figura 40. Esquemático del sistema de fotografía de registro 59

Figura 41. PCB del sistema de control de acceso. 60

Figura 42. Esquemático sistema de control de acceso. 60

Figura 43. PCB del sistema de control IoT. 61

Figura 44. Esquemático del sistema de control IoT. 61

Figura 45. Diseño 3D del sistema de fotografía de registro. 62

Figura 46. Diseño 3D del sistema de control de acceso (Portero electrónico). 63

Figura 47. Diseño 3D de la Botonera. 63

Figura 48. UPS CDP ON LINE UPO22-10AX. 65

Figura 49. Datos de las baterías del UPS. 65

Figura 50. Diagrama de conexión general del sistema. 68

Figura 51. Estado inicial del Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA. 69

Figura 52. Estado actual del Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA. 69

Figura 53. Altura para colocación del portero. 70

Figura 54. Ubicación del portero. 71

Figura 55. Ubicación del control IoT. 72

Figura 56. Ubicación del sistema de respaldo de energía. 73

Figura 57. Diagrama de conexión del sistema de respaldo de energía. 74

Figura 58. Plano actual del Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA. 74

Figura 59. Nomenclatura del sistema implementado. 75

Figura 60. Comando “opciones” de Telegram. 76

Figura 61. Porcentaje de la tasa de éxito del sistema de control IoT. 77

Figura 62. Activación del sensor PIR de la cámara. 78

Figura 63. Prueba de acceso del laboratorio con el sensor PIR. 78

Figura 64. Pedido de fotografía de la cámara. 78

Figura 65. Porcentaje de tasa de éxito del sistema de control de acceso. 80

ÍNDICE DE TABLAS

Tabla 1 Norma ISO 14443 partes 1 al 4. 11

Tabla 2 Especificaciones del ESP8266. 16

Tabla 3 Características técnicas de modulo ESP32-CAM. 17

Tabla 4 Comparativa de módulos de cámaras con microcontroladores. 24

Tabla 5 Comparativa de microcontroladores para el sistema RFID. 25

Tabla 6 Comparativa de microcontroladores para el sistema de control IoT. 26

Tabla 7 Comparativa de los sensores SW-18010P y el SW-420. 27

Tabla 8 Tabla 8 28

Tabla 9 Módulos de cámaras compatibles con la ESP32-CAM. 29

Tabla 10 Tabla Comparativa de Sensores de Movimiento. 30

Tabla 11 Comparativa sensores de detección de incendios. 30

Tabla 12 Comparativa de lector RFID. 31

Tabla 13 Comparativa de Tipos de Relés y sus Especificaciones Técnicas. 32

Tabla 14 Cerraduras Eléctricas y sus Especificaciones Técnicas. 32

Tabla 15 Comandos del sistema de fotografía de registro. 56

Tabla 16 Funciones del teclado del sistema IoT en Telegram. 57

Tabla 17 Acciones de los botones de la interfaz del reconocimiento facial 58

Tabla 18 Dimensionamiento del UPS para el diseño del sistema. 64

Tabla 19 Autonomía del UPS con el consumo total. 65

Tabla 20 Autonomía del UPS sin impresoras 3D y laptops. 66

Tabla 21 Tenciones de alimentación de los distintos sistemas. 66

Tabla 22 Consumo energético de los distintos sistemas. 66

Tabla 23 Tiempo de conexión Wifi de los módulos. 75

Tabla 24 Pruebas del sistema de control IoT. 76

Tabla 25 Porcentaje de tasa de éxito del sistema de control IoT. 76

Tabla 26 Tiempo de acción del sistema de control IoT. 77

Tabla 27 Pruebas de toma de fotografías.....79

Tabla 28 Porcentaje de tasa de éxito en la toma de fotografías.....79

Tabla 29 Promedio del tiempo de acción en la toma de fotografías.....79

Tabla 30 Pruebas del sistema de control de acceso. 80

Tabla 31 Porcentaje de tasa de éxito del sistema de control de acceso. 80

Tabla 32 Promedio del tiempo de acción del reconocimiento facial.....81

Tabla 33 Prueba de autonomía del sistema.....81

Tabla 34 Costos estimados del diseño completo 82

Tabla 35 Costos del sistema de control de acceso y tomacorrientes. 83

Tabla 36 Comparación con sistemas comerciales. 84

RESUMEN

Tema: "IMPLEMENTACIÓN DE UN SISTEMA DOMÓTICO DE SEGURIDAD Y CONTROL MEDIANTE IOT APLICADO A UN LABORATORIO"

Autores:

Moreno Chuqui Washington Rafael

Serna Moreno Dilan Javier

El presente proyecto se centra en el desarrollo de un sistema seguro de control de acceso basado en Internet de las cosas (IoT) con el objetivo de mejorar el funcionamiento del Laboratorio de Manufactura Aditiva y Sustractiva. La concepción de este sistema se focaliza en dos componentes fundamentales: el control de acceso e IoT al laboratorio. Uno de los pilares esenciales se relaciona con el control de acceso de las personas al laboratorio. Con este fin, se ha planteado la implementación de un sistema que posibilite el acceso mediante reconocimiento facial, lectura de tarjetas o llaveros RFID, así como a través de IoT por medio de la plataforma Telegram. Además, se busca mantener un registro visual de las personas que ingresan al laboratorio. Por otro lado, se destaca la importancia del control lumínico, el cual se traduce en la capacidad de encender y apagar automáticamente las luces. Esta función resulta especialmente útil para prevenir el desperdicio de energía, así como para el control de tomacorrientes, ya que se conectan impresoras 3D que continúan consumiendo energía incluso cuando no están en uso. Para determinar la configuración del sistema, se lleva a cabo un análisis de diversos microcontroladores que podrían ser considerados. Además, se aplican criterios de dimensionamiento a cada uno de los aspectos clave del sistema. La evaluación global del sistema arroja resultados con un índice de éxito superior al 95% en cada uno de los aspectos evaluados. Además de su desempeño actual, el sistema posee la capacidad de ser mejorado y actualizado, ya que se emplean microcontroladores programables.

Palabras Clave: Control de Acceso, microcontroladores, ESP, WiFi, IoT, Telegram, sistema.

ABSTRACT

Topic: "IMPLEMENTATION OF A HOME AUTOMATION SECURITY AND CONTROL SYSTEM THROUGH IOT APPLIED TO A LABORATORY"

Authors:

Moreno Chuqui Washington Rafael

Serna Moreno Dilan Javier

This project focuses on the development of a secure access control system based on the Internet of Things (IoT) with the objective of improving the operation of the Additive and Subtractive Manufacturing Laboratory. The conception of this system focuses on two fundamental components: access management to the laboratory and control through IoT. One of the essential pillars is related to the management of people entering the laboratory. To this end, the implementation of a system that enables access through facial recognition, card reading or RFID key fobs, as well as through IoT via the Telegram platform, has been proposed. In addition, the aim is to keep a visual record of the people who enter the laboratory. On the other hand, it highlights the importance of light control, which translates into the ability to automatically turn lights on and off. This function is especially useful for preventing energy waste, as well as for controlling power outlets, since 3D printers are connected that continue to consume energy even when they are not in use. To determine the system configuration, an analysis of various microcontrollers that could be considered is carried out. In addition, sizing criteria are applied to each of the key aspects of the system. The overall evaluation of the system yields results with a success rate of over 90% in each of the aspects evaluated. In addition to its current performance, the system has the capacity to be improved and upgraded, since programmable microcontrollers are used.

Keywords: Access Control, microcontrollers, ESP, WiFi, IoT, Telegram, system.

UNIVERSIDAD TÉCNICA DE COTOPAXI

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que:

La traducción del resumen al idioma Inglés del proyecto de investigación cuyo título versa: **"DESARROLLO DE UN SISTEMA DE SEGURIDAD Y CONTROL MEDIANTE IOT"** presentado por: **Moreno Chuqui Washington Rafael y Serna Moreno Dilan Javier** egresados de la Carrera de Ingeniería en Electricidad perteneciente a la **Facultad de Ciencias de la Ingeniería y Aplicadas,** lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del presente aval para los fines académicos legales.

Latacunga, agosto del 2023

Atentamente,

Firmado electrónicamente por:
BLANCA GLADYS SANCHEZ AVILA

CENTRO DE IDIOMAS

Mgs. Blanca Gladys Sánchez Avila
DOCENTE CENTRO DE IDIOMAS-UTC
CI: 2100275375

1. INFORMACIÓN GENERAL

Título: Implementación de un sistema domótico de seguridad y control mediante IoT aplicado a un laboratorio.

Fecha de inicio: Abril del 2023

Fecha de finalización: Agosto del 2023

Lugar de ejecución: Universidad Técnica de Cotopaxi

Facultad que auspicia: Facultad de Ciencias de la Ingeniería y Aplicadas (CIYA)

Carrera que auspicia: Carrera de Electricidad

Proyecto Macro Asociado: Aplicación de tecnologías electrónicas y comunicación para la seguridad barrial

Equipo de Trabajo: Moreno Chuqui Washington Rafael

Serna Moreno Dilan Javier

Grupo de Investigación:

Tutor de Titulación: Ing. Corrales Bastidas Byron Paul M.Sc.

Área de Conocimiento: 07 Ingeniería, Industria y Construcción / 071 Ingeniería y Profesiones Afines / 0713 Electricidad y Energía.

Línea de investigación: Procesos de industriales

Sublineas de investigación de la Carrera:

Sublínea 1: Control y optimización en el uso de la energía del sector industrial, comercial y residencial.

Sublínea 2: Inteligencia artificial y modelación de sistemas.

2. INTRODUCCIÓN

2.1. EL PROBLEMA

2.1.1. Situación Problémica

A nivel mundial, en diversos países se han enfrentado crisis de seguridad. Este fenómeno ha resultado en un aumento de los índices delictivos, con la particularidad de que estos actos delictivos han trascendido sus zonas de origen, extendiéndose hacia lugares menos poblados como la ciudad de Latacunga [1]. Los efectos de esta problemática también han repercutido en la Universidad Técnica de Cotopaxi, donde se han registrado múltiples incidentes de hurto.

Para hacer frente a esta situación, los laboratorios cuentan con medidas de seguridad como la instalación de cerraduras y candados en las puertas, con el propósito de prevenir la entrada de personas que carezcan de la debida autorización. Sin embargo, esta solución ha generado una serie de inconvenientes para el personal docente que requiere acceso regular a estos espacios, como los laboratorios. En estos casos, los docentes se ven obligados a solicitar al encargado correspondiente que les permita el ingreso, lo que implica una espera hasta que dicha persona pueda atender la solicitud.

Otro aspecto que demanda atención es el sistema de iluminación, que en varias ocasiones queda encendido de manera prolongada, lo que resulta en un consumo de energía innecesario. Dado que los laboratorios cuentan con cerraduras y candados, las luminarias permanecen encendidas hasta que el encargado realice la apertura, apague las luminarias y luego cierre la puerta.

Adicionalmente, la falta de una adecuada seguridad se hace evidente al constatar que, al término de una clase, las puertas quedan abiertas hasta el regreso del encargado, lo que incrementa el riesgo de ingresos no autorizados y sustracción de elementos. Este problema ha ocasionado pérdidas de equipos que son necesarios para la prestación del servicio a los estudiantes.

Dentro de este contexto, resulta esencial resaltar que el Laboratorio de Manufactura Aditiva y Sustractiva, ubicado en la Facultad de CIYA, estará equipado con impresoras 3D. Estas máquinas, pese a su inactividad, siguen consumiendo energía, lo cual presenta un aspecto a considerar. Adicionalmente, el laboratorio está dotado de sistemas de iluminación tanto internos como externos, cuyo encendido está restringido al interior. Actualmente, el laboratorio opera con un sistema de cierre convencional que depende de la acción del encargado para su apertura y cierre. Esta disposición complica la tarea de apagar las luces en caso de que queden encendidas y dificulta la desconexión de las impresoras 3D cuando no están en uso.

2.1.2. Formulación del Problema

La ausencia de un sistema que permita controlar de forma segura el acceso al Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA, junto con la necesidad de evitar el desperdicio de energía en las luminarias cuando no es necesario y el consumo continuo de corriente por parte de las impresoras 3D.

2.2. OBJETO Y CAMPO DE ACCIÓN

Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA.

El campo de acción para el proyecto (Código UNESCO):330000 Ciencias Tecnológicas / 3304 Tecnología de los Ordenadores / 3304.12 Dispositivos de Control

2.3. BENEFICIARIOS

Beneficiarios directos: Facultad de CIYA.

Beneficiarios indirectos: Estudiantes, docentes de la Facultad de CIYA, Comunidad Científica.

2.4. JUSTIFICACIÓN

En la Facultad de CIYA de la Universidad Técnica de Cotopaxi, se tiene planificado poner en funcionamiento del laboratorio de Manufactura Aditiva y Sustractiva. En la actualidad, se dispone del espacio destinado a la implementación de dicho laboratorio, el cual contara con impresoras 3D. El propósito fundamental de este laboratorio es mejorar el diseño y la creación de modelos 3D desarrollados por docentes y estudiantes de la institución, con el objetivo central de brindar beneficios a la comunidad. Además de reducir de manera significativa los plazos y los gastos relacionados con los procedimientos de fabricación.

Considerando lo mencionado previamente, se aporta con el primer paso hacia la mejora de la seguridad en el acceso al laboratorio. Esto se logra a través de la implementación de un sistema de control de acceso, diseñado para ser más rápido en comparación a depender de un encargado para abrir la puerta.

El propósito fundamental del sistema propuesto es controlar el acceso de docentes, estudiantes e invitados al laboratorio. Esto se lleva a cabo mediante la combinación de tecnologías como el reconocimiento facial, identificación por radiofrecuencia (RFID) y un sistema remoto mediante IoT. Además, se supervisa la entrada de las personas al laboratorio empleando una cámara equipada con un sensor infrarrojo pasivo (PIR) para detectar cuando la persona haya ingresado,

estos datos fotográficos se transmiten a través de una red de Internet de las Cosas (IoT) hacia un dispositivo móvil.

Adicionalmente, se busca automatizar la iluminación y controlar los tomacorrientes dentro del laboratorio, utilizando Internet de las Cosas (IoT). Esto con el fin de evitar el consumo de energía, en situaciones donde las luces queden encendidas sin motivo o las impresoras 3D permanezcan encendidas sin estar en proceso de impresión.

Con el fin de alcanzar este objetivo, se utilizará un entorno de programación, en conjunto con microcontroladores dotados de conectividad a internet. Estos microcontroladores desempeñarán un papel fundamental como el corazón del sistema, albergando las instrucciones de programación.

Asimismo, se incorporarán actuadores y sensores que servirán para el accionamiento y toma de mediciones del Laboratorio. Finalmente, se utilizará la plataforma de Telegram para desempeñar el papel de interfaz IoT de todo el sistema.

2.5. OBJETIVOS

2.5.1. Objetivo General

Desarrollar un sistema integral de control de acceso, iluminación y tomacorrientes en el Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA, mediante IoT.

2.5.2. Objetivos Específicos

- Revisar el estado del arte de sistemas de control de acceso, iluminación y tomacorrientes en espacios.
- Diseñar un sistema de control de acceso, iluminación y tomacorrientes con IoT.
- Implementar el sistema en el Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA.
- Evaluar el correcto funcionamiento del sistema en el control de acceso, luminarias y control de tomacorrientes.

2.6. SISTEMA DE TAREAS

Objetivos específicos	Actividades (tareas)	Resultados Esperados	Técnicas, Medios e Instrumentos
Revisar el estado del arte de sistemas de control de acceso, iluminación y tomacorrientes en espacios.	Recopilación de información sobre los diversos sistemas de control de acceso iluminación y tomacorrientes en espacios.	Un conjunto de sistemas de acceso a espacios que abarquen tecnologías como IoT, métodos biométricos y sistemas de tarjetas electromagnéticas, entre otros.	Bibliografía relacionada a la los sistemas de control de acceso. Artículos científicos. Catálogos. Tesis.
Diseñar un sistema de control de acceso, iluminación y tomacorrientes con IoT.	Establecer la selección de sensores, microcontroladores, actuadores y plataformas que se emplearán. Crear el código de programación específico para cada microcontrolador.	Listado de microcontroladores adecuados para el control de acceso. Creación de programación individualizada para los microcontroladores elegidos.	Lista de sensores y Actuadores adecuados. Software de programación. Datasheets.
Implementar el sistema en el Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA.	Implementación del sistema integral del de control de acceso iluminación y tomacorrientes.	Elaboración de diagramas de interconexión del sistema.	Módulos ESP. AutoCAD. Normativas.
Evaluar el correcto funcionamiento del sistema en el control de acceso, luminarias y control de tomacorrientes.	Ejecutar un conjunto de pruebas de operatividad en cada uno de los sistemas.	Tasas de éxito y de falla de los sistemas.	Observación Directa.

3. FUNDAMENTACIÓN TEÓRICA

Este capítulo introduce los conceptos fundamentales del proyecto, abordando temas clave como los diversos sistemas de control de acceso, el Internet de las cosas (IoT), los microcontroladores y el entorno de programación, entre otros.

3.1. ANTECEDENTES

A lo largo de los siglos, los seres humanos anhelaron asegurar sus propiedades regulando el acceso, en busca de seguridad y tranquilidad. En épocas pasadas, las ciudades levantaban murallas y portones con guardias para supervisar las entradas de personas. De manera semejante, castillos y residencias importantes contaban con personal para vigilar y gestionar el acceso. Con el transcurso del tiempo, se ha observado cómo la gestión de accesos ha evolucionado hacia sistemas avanzados. Lo que comenzó como asistencia para determinar quién entraba, se ha transformado en control, permitiendo no solo identificar a los visitantes, sino también limitar la entrada a áreas específicas y prevenir intrusiones no autorizadas [2].

En el año 2005, Massimo Banzi, entonces estudiante del Instituto IVRAE, dio origen a Arduino. Su impulso primordial radicaba en la creación de una herramienta didáctica para los estudiantes de informática y electrónica. Más allá de su capacidad para fomentar la realización económica de proyectos escolares, Banzi también ansiaba contribuir a la solidez financiera de su institución al comercializar placas Arduino dentro del campus. En síntesis, este proyecto nació con la finalidad de atender las necesidades educativas de los estudiantes y respaldar la sostenibilidad financiera de la escuela [3].

En 2013, Zynnia Vargas [4] desarrolló un sistema de control de acceso y monitoreo mediante la tecnología RFID, como respuesta a la necesidad de fortalecer la seguridad de los equipos en el laboratorio de Telemática de la Universidad Politécnica Salesiana. El diseño abarcó un Sistema de Control de Acceso al Laboratorio que posibilitó una supervisión constante de los equipos y reguló la entrada exclusiva del personal con autorización. El sistema se basó en la utilización del módulo inalámbrico de Identificación por Radiofrecuencia (RFID), cuya finalidad radica en la identificación, gestión y control del personal docente y de mantenimiento habilitado. El monitoreo se llevó a cabo a través de LabVIEW.

En el año 2018, F. Paredes llevó a cabo el desarrollo de un sistema domótico inteligente con adaptabilidad a diversos tipos de edificios. Este sistema hace uso de sensores y actuadores para el control y la adquisición de datos. Se basa en plataformas de desarrollo distribuidas como los

controladores de lógica (NodeMCU), una plataforma de desarrollo central (Raspberry Pi 3) que actúa como servidor, y un sistema de seguridad destinado al control de acceso [5].

La viabilidad de este sistema domótico quedó demostrada a través de la implementación exitosa de un prototipo. El autor concluyó que este sistema posee la capacidad no solo de igualar, sino también de superar a los controladores industriales y domóticos disponibles en el mercado global. Asimismo, se destacó su aplicabilidad en contextos industriales, personales, así como en proyectos gubernamentales o relacionados con entidades de responsabilidad social [5].

En el año 2020, Hema N y Juli Yadav llevaron a cabo el desarrollo de un innovador prototipo orientado a mejorar la seguridad en las entradas. Este prototipo se basa en la utilización de un sensor de infrarrojos que tiene la capacidad de detectar cualquier movimiento en la puerta principal. Una vez que se detecta el movimiento, se activa una cámara que captura una imagen, la cual es posteriormente enviada al propietario a través de la plataforma de mensajería Telegram.

La funcionalidad clave de este sistema radica en la identificación del visitante. Si la imagen del visitante se encuentra registrada en la base de datos, la puerta se abrirá automáticamente para permitir el acceso. Sin embargo, en caso de que el visitante no esté registrado, el propietario recibirá la imagen del intruso, lo que le permitirá tomar una decisión informada sobre si autorizar o denegar la entrada.

Una característica distintiva de este sistema es su elección de utilizar la plataforma de Telegram para las notificaciones. Este enfoque presenta múltiples ventajas, entre ellas, la facilidad de uso para la generación de mayor edad, ya que no es necesario disponer de una cuenta de correo electrónico para utilizar las notificaciones de Telegram. De esta manera, el sistema propuesto no solo brinda mayor seguridad a las entradas, sino que también se adapta a las necesidades y preferencias de diversos usuarios [6].

En el año 2020, Rukmana y Darmalaksana llevaron a cabo la concepción de un innovador sistema de control inteligente para el hogar basado en el chat de Telegram. Este sistema automático de control, desarrollado en el marco de su investigación, hace uso del microcontrolador ESP32. El ESP32 es un dispositivo dotado de tecnología Wi-Fi y Bluetooth de 2,4 GHz, y su kit de desarrollo se encuentra disponible en el mercado a un precio accesible.

Dentro del sistema, se emplea un sensor LDR para gestionar la iluminación de forma automática, encendiéndola o apagándola según las condiciones lumínicas. Asimismo, se emplea el sensor DHT11 para medir la temperatura y humedad ambiente, además de regular el

funcionamiento de un ventilador. Las conclusiones extraídas de este trabajo revelan la viabilidad y utilidad de la implementación del microcontrolador ESP32 en este contexto. El sistema de control inteligente diseñado demuestra su capacidad para regular diversos aspectos del hogar de manera automática y eficiente, aportando comodidad y optimización a la vida cotidiana de los usuarios [7].

En 2021, Lascano Endara y colaboradores desarrollaron un sistema de identificación y reconocimiento facial que utiliza inteligencia artificial a través de una plataforma web y dispositivos móviles. Este sistema emplea el módulo WI-FI ESP32-CAM para capturar imágenes y coordenadas de personas, mientras que el procesamiento se realiza en un servidor local utilizando la librería face-api y una red neuronal previamente entrenada. La implementación se integra en gafas espía ergonómicas con un sistema háptico que alerta al usuario sobre la detección de una persona y su ubicación en el campo de visión de las gafas. El sistema presenta una alta precisión en el reconocimiento facial, alcanzando un porcentaje de acierto de 94,94% cuando la persona está frente a la cámara. Sin embargo, esta precisión disminuye a medida que el ángulo de visión se desvía, llegando a 84,38% a 67,94% cuando el rostro se encuentra en un ángulo de ±45°. El rendimiento se deteriora significativamente cuando la persona está de perfil, con un rango de acierto de tan solo 8,72% a 3,05%. Cabe destacar que el sistema está diseñado para operar en tiempo real, pero la limitación de la cámara utilizada restringe la tasa de captura a 1 imagen por segundo, afectando su capacidad de respuesta. El algoritmo de reconocimiento se ejecuta en un servidor local conectado al módulo ESP32-CAM, el cual envía las imágenes procesadas a los diversos sistemas implementados [8].

En 2022, Juan David Tapia López implementó un sistema de seguridad integral compuesto por diversos componentes interconectados. Este sistema abarca un subsistema de control de acceso, un sistema de videovigilancia mediante cámaras y un subsistema de gestión de usuarios. Además, se incorpora un subsistema dedicado a la autenticación de usuarios y la conexión a una base de datos alojada en la nube con enlace directo a Google.

El sistema de control de acceso utiliza la plataforma Firebase para la captura de datos, y aunque es eficiente, la función de envío de notificaciones puede generar retrasos en la apertura de la puerta. En relación a las cámaras de vigilancia, pueden surgir conflictos en la transmisión y procesamiento de video cuando se ejecutan acciones en un solo módulo ESP32. No obstante, la gestión del sistema de seguridad a través de la aplicación móvil se destaca por su eficiencia [9].

En el mismo año, J. Tapia finalizó la implementación de un completo sistema de seguridad compuesto por diversos subsistemas, entre ellos control de acceso, videovigilancia mediante cámaras, gestión y autenticación de usuarios. El objetivo era brindar a los estudiantes una herramienta que les permitiera explorar la domótica y su aplicación práctica a través de un banco de pruebas, utilizando un módulo ESP-32 con conexión WIFI y controlado mediante el asistente virtual ALEXA de Amazon.

El autor concluye que, si bien la seguridad del sistema es ya muy elevada, existe margen para mejoras adicionales. Además, se destaca la posibilidad de expandir el sistema hacia la automatización, con dispositivos de bajo costo y materiales fácilmente disponibles, lo que permitiría su escalabilidad hacia un sistema domótico más completo y asequible [10].

3.2. MARCO REFERENCIAL

3.2.1. Sistemas de control de acceso

Un sistema de control de acceso es una solución electrónica diseñada de manera eficiente para registrar y supervisar el ingreso del personal a una empresa o institución, y actualmente, es una tecnología altamente demandada en el mercado. Diversos métodos están disponibles, como tarjetas, botones de control remoto y sistemas biométricos, entre otros [11].

3.2.1.1. Sistemas biométricos

Un equipo biométrico permite medir, codificar, comparar, almacenar, transmitir y reconocer con precisión características únicas de una persona. Basada en la singularidad científica de rasgos individuales, la tecnología biométrica ofrece una forma segura de identificar a personas sin depender de métodos susceptibles de fraude. Utilizando atributos como huellas dactilares, rasgos vocales, geometría de la mano, patrones de venas y retina, iris, rasgos faciales y firma, se verifica la identidad digitalmente comparando con datos almacenados. Esto requiere un software avanzado con reconocimiento de formas, inteligencia artificial, algoritmos matemáticos y aprendizaje automático, mientras que la criptografía se emplea para cifrar datos biométricos almacenados o transmitidos.

Un sistema biométrico, en su conjunto, comprende tanto componentes físicos como tecnológicos esenciales para llevar a cabo el proceso de reconocimiento. Dentro de la categoría de hardware, los elementos clave incluyen principalmente los sensores, dispositivos encargados de capturar la característica específica requerida. Una vez que el sensor ha obtenido la información necesaria, es crucial llevar a cabo los procedimientos de acondicionamiento adecuados, para lo cual se emplean diversos enfoques dependiendo del tipo de sistema

biométrico en uso. Por consiguiente, se han identificado y definido los tipos primordiales de sistemas biométricos:

- Identificación de huellas dactilares.
- Reconocimiento facial.
- Identificación de iris/retina.
- Geometría de dedos y manos.
- Verificación vocal.
- Reconocimiento de firmas.

La evolución de los sistemas biométricos ha sido motivada por la creciente necesidad de seguridad en la actualidad. A pesar de que algunos de estos sistemas son altamente confiables, es importante señalar que ningún sistema es completamente infalible. Estos sistemas también presentan vulnerabilidades y la posibilidad de ser burlados [12].

3.2.1.1.1. Reconocimiento facial

Un sistema de reconocimiento facial es una aplicación informática que identifica automáticamente a una persona en una imagen digital al comparar características faciales específicas en la imagen con una base de datos facial. Aunque su desarrollo se remonta a los años 60, los métodos actuales utilizan cámaras para capturar y analizar imágenes faciales, identificando puntos clave como la distancia entre los ojos o la anchura de la nariz. La adquisición de la imagen, alineación y generación de una plantilla facial única son pasos esenciales en este proceso. Los sistemas modernos emplean imágenes tridimensionales para mayor precisión y utilizan algoritmos matemáticos para medir distancias entre puntos en la superficie del rostro, lo que permite reconocer caras en diferentes orientaciones y condiciones de iluminación y expresiones faciales [12].

3.2.1.2. Sistemas basados en tarjetas magnéticas

Estas tarjetas emplean uno o múltiples métodos de identificación únicos o especiales, como banda magnética, identificación por radiofrecuencia, raspadura, entre otros. Estos dispositivos se aplican en una amplia gama de contextos, desde sistemas de identificación hasta programas de integridad, abarcando diversas aplicaciones [13].

3.2.1.2.1. Tarjetas magnéticas RFID

Estas tarjetas comparten similitudes de estructura y funcionalidad con las tarjetas inteligentes de contacto, pero se diferencian en que ya no requieren contacto físico, empleando una interfaz

inductiva para la transferencia de información entre el lector y la tarjeta a través de antenas, siguiendo protocolos definidos en el estándar ISO 14443.

Estas tarjetas permiten lecturas más rápidas al evitar la inserción en el lector, eliminando problemas de deterioro en los contactos o residuos. Su energía proviene de una batería junto al chip o a través de un hilo metálico que induce una corriente eléctrica. Entre las ventajas se encuentran: capacidad segura de almacenamiento y procesamiento con el microprocesador, uso universal gracias a estándares internacionales, larga vida útil y capacidad para múltiples aplicaciones y políticas de seguridad en una tarjeta. Sin embargo, sus desventajas incluyen el costo unitario y gestión elevada, la necesidad de instalar lectores en dispositivos y ambigüedades legales en torno a la privacidad del usuario [13].

Cada tipo de tarjeta inteligente se adhiere a los estándares ISO que detallan sus características. Las tarjetas inteligentes sin contacto, reguladas por la norma ISO 14443 partes 1 al 4, se muestran en la Tabla 1 y se dividen en:

Tabla 1 Norma ISO 14443 partes 1 al 4.

ISO 14443	
ISO 14443-1	que define atributos físicos.
ISO 14443-2	que establece la frecuencia de operación y potencia de transmisión.
ISO 14443-3	que rige la comunicación inicial y anticolisión.
ISO 14443-4	que define protocolos de transmisión.

Los lectores, que acceden a la información en estas tarjetas, se pueden conectar a una computadora a través de diferentes puertos, integrarse en dispositivos específicos como cajeros automáticos o ser portátiles con recursos integrados.

3.2.2. Sistema Domótico

Un sistema domótico se fundamenta en la automatización de una amplia gama de procesos y funciones esenciales en un hogar. Su propósito central es brindar servicios que mejorar el confort, bienestar y seguridad de los residentes, además de enfocarse en la gestión de la energía. Este logro se alcanza al establecer comunicación, supervisar y regular diversas variables tanto en espacios interiores como exteriores de una vivienda, creando así entornos inteligentes y habitables [14], [15].

La domótica abarca una variedad de niveles y enfoques, que van desde la manipulación remota de interruptores simples hasta la integración de dispositivos de red que controlan la totalidad de

un edificio. En el mercado, se encuentran sistemas domóticos capaces de llevar a cabo una serie de tareas, como encender y apagar dispositivos, programar funcionalidades, ajustar la luminosidad, y detectar y regular variables físicas como la luminosidad, gases y temperatura, entre otras posibilidades [14].

La domótica está experimentando una revolución impulsada por el Internet de las Cosas (IoT), un concepto que se centra en la interconexión de diversos dispositivos a través de internet para la compartición, monitorización y control remoto de datos desde distintas ubicaciones [14].

3.2.2.1. Estructura de un sistema domótico

La estructura de un sistema domótico comprende dispositivos con conexiones y configuraciones específicas, en consonancia con la arquitectura y necesidades del sistema. Estos elementos pueden clasificarse en cuatro categorías: controladores, sensores, actuadores e interfaces [15].

3.2.2.1.1. Controladores

Estos componentes asumen el papel central al actuar como el núcleo de toma de decisiones. Su responsabilidad consiste en interpretar la información proporcionada por los sensores distribuidos en el hogar y utilizarla para ejecutar acciones en los diversos actuadores. Mediante la programación, los usuarios pueden definir y personalizar operaciones para los dispositivos que conforman la red doméstica [15].

3.2.2.1.2. Sensores

Un sensor es un dispositivo diseñado para medir una magnitud física en su entorno, convirtiéndola en una señal eléctrica proporcional que ofrece información sobre el estado de una variable específica. Dicha variable puede ser evaluada mediante distintos circuitos para tomar decisiones conforme a su estado [16].

En el ámbito de la domótica, se emplean sensores analógicos y digitales. Por ejemplo, los sensores analógicos se utilizan para captar la variación de la iluminación a través de perillas, mientras que los sensores digitales pueden tener dos estados (uno o cero lógicos). Un ejemplo claro de sensores digitales son aquellos utilizados para detectar la presencia [15].

3.2.2.1.3. Actuadores

Un actuador se define como un dispositivo encargado de ejecutar una acción específica para modificar una variable dentro del entorno en el que está instalado, siguiendo las instrucciones

proporcionadas por un controlador. En el ámbito de la domótica, existen múltiples tipos de actuadores, como reles, electroválvulas, sirenas y motores, entre otros [17].

Los actuadores se clasifican según su principio de funcionamiento, abarcando categorías como eléctricos, electrónicos, electromecánicos, piezoeléctricos, neumáticos e hidráulicos. Estas variantes desempeñan roles diversos, desde ajustar la temperatura de calefacción o aire acondicionado en una vivienda hasta cortar el suministro de gas o agua, controlar la iluminación, entre otros usos [14].

3.2.2.1.4. Interfaces

Las interfaces representan los canales a través de los cuales los usuarios interactúan con el sistema domótico, emitiendo comandos y supervisando el estado de los dispositivos. Estos componentes abarcan una variedad de elementos como pantallas, teclados, dispositivos móviles e incluso la conectividad a Internet. Una instalación domótica completa debe incluir interfaces que permitan a los usuarios ajustar parámetros, configurar la instalación y recibir información de manera clara y accesible [14].

A través de estas interfaces, se generan comandos para encender, apagar la iluminación, crear escenas adaptadas a distintas situaciones y controlar los tomacorrientes, entre otras funciones. Estas interfaces de control pueden ubicarse tanto en el interior del hogar como conectarse con el exterior a través de Internet o mensajes móviles, proporcionando una flexibilidad esencial al sistema [14].

3.2.3. Internet de las cosas (IoT)

El Internet de las cosas (IoT) es una red interconectada de objetos físicos a través de internet, permitiendo interacciones mediante sistemas embebidos, comunicación en red, cómputo en la nube y aplicaciones. Facilita la comunicación, acceso a datos e interacciones entre objetos y usuarios humanos, creando entornos más conectados e inteligentes. IoT abarca objetos, procesos y estructuras que pueden comunicar estados, responder a eventos e incluso actuar autónomamente, impulsando la convergencia de tecnologías inalámbricas, redes de datos, dispositivos inteligentes y sistemas MEMS [18].

Es un pilar de la Industria 4.0, una revolución basada en la digitalización que transformará la sociedad y la economía, impulsada por la coordinación de información para la predicción, planificación, producción, control y modificación en tiempo real, generando mayor valor en los ciclos de vida de los productos y mejorando eficiencia, calidad e innovación. La Industria 4.0

requiere conocimiento profundo en diversos campos y traerá cambios radicales en la producción y relaciones sociales, transformando la vida humana y generando oportunidades inesperadas en la economía y el desarrollo [18].

3.2.3.1. Telegram como medio IoT

Telegram, fundada en 2013 por los hermanos Dúrov, es una aplicación de mensajería en tiempo real con una amplia base de usuarios que supera los 400 millones globalmente. Proporciona una plataforma versátil para administrar dispositivos IoT a través de bots, posibilitando órdenes y comunicación fluida entre dispositivos y la nube, incluso entre los propios dispositivos. Esto la convierte en una herramienta eficaz en ambientes IoT, junto con características únicas como mensajes automáticos y chats secretos encriptados [19].

La incorporación de técnicas de mensajería instantánea y bots en Telegram posibilita la gestión remota de dispositivos IoT, permitiendo controlarlos desde cualquier lugar, lo que resulta especialmente ventajoso en aplicaciones como la supervisión de espacios inteligentes y sistemas de vigilancia [19].

3.2.3.1.1. Bots

Los bots de Telegram son aplicaciones de terceros integradas en la plataforma de mensajería que funcionan como si fueran personas reales con las que interactúas. No es necesario instalarlos, ya que se ejecutan directamente en la app y son compatibles con diferentes sistemas operativos. Su interfaz es puramente textual, y los controlas mediante mensajes que contienen comandos específicos. Estos bots son automatizados y ofrecen respuestas predefinidas según los comandos que reciben. Pueden variar en complejidad, desde los más básicos que muestran información hasta los más especializados que realizan tareas específicas [6].

3.2.3.1.2. Botfather

Su función principal es permitir a los usuarios controlar otros bots existentes y, aún más interesante, la posibilidad de crear sus propios bots personalizados. Reconocido y respaldado por los desarrolladores de Telegram, BotFather Figura 1, es considerado como una de las herramientas más accesibles y sencillas para aquellos que deseen crear su propio bot en la plataforma [20]. Esta función abre un mundo de posibilidades para la comunidad de usuarios ya que permite desarrollar bots que se adapten a sus necesidades y preferencias específicas.

Figura 1. BotFather y Telegram.

3.2.4. Microcontroladores

Un microcontrolador es un circuito integrado con capacidad de programación que puede llevar a cabo instrucciones almacenadas en su memoria. Está conformado por diversos bloques funcionales diseñados para realizar tareas específicas, como unidad central de procesamiento, memoria y periféricos de entrada/salida.

Su función principal radica en procesar información de entrada y generar salidas correspondientes, convirtiéndolo en un componente esencial para la creación de sistemas o procesos automatizados.

Los microcontroladores Figura 2 se aplican en una amplia gama de usos, incluyendo sistemas de vigilancia gracias a su bajo consumo energético y características técnicas.

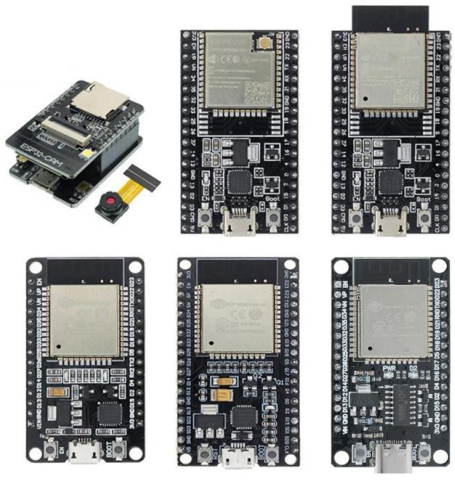


Figura 2. Microcontroladores de la familia ESP [3].

3.2.4.1. NodeMCU

El NodeMCU es una plataforma de desarrollo de código abierto diseñada para programar un microcontrolador, o MCU (Microcontroller Unit). Esta placa comparte similitudes con las

conocidas placas Arduino, lo que facilita su programación utilizando el mismo entorno, como el IDE de Arduino, y es compatible con las librerías de dicho entorno.

Una de las ventajas más destacadas del NodeMCU es, que viene equipado con un módulo WiFi integrado, lo que amplía sus capacidades de conectividad. En la Tabla 2 se detallan las especificaciones de la placa de desarrollo.

Tabla 2 Especificaciones del ESP8266.

VOLTAJE	**3.3 V**
CONSUMO DE CORRIENTE	10 µA – 170 mA
WI-FI	802.11 b/g/n
MEMORIA FLASH	16 MB máx. (512 k normal)
PROCESADOR	Tensilica L106 32 bit
VELOCIDAD DEL PROCESADOR	80 – 160 MHz
GPIOS	17

Una ventaja importante del NodeMCU es su tamaño compacto en comparación con otras placas similares. Esta característica permite la creación de circuitos finales más pequeños y simplifica el proceso de instalación [20]. El NodeMCU ofrece un total de 30 pines de conexión, distribuidos en dos filas de 15 como se muestra en la Figura 3.

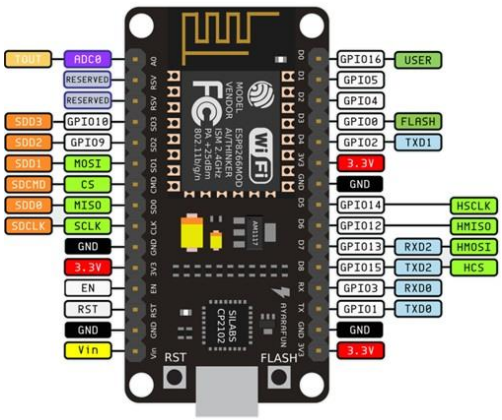


Figura 3. Pines de conexión NodeMCU con ESP8266 [20].

3.2.4.2. ESP32

El ESP32, es un microcontrolador de alto rendimiento perteneciente a la familia de módulos ESP de Espressif Systems, ha ganado amplia popularidad en los campos de la electrónica y el Internet de las cosas (IoT) gracias a su potencia y versatilidad. Impulsado por un procesador dual-core Tensilica Xtensa LX6 de 32 bits, el ESP32 ofrece un rendimiento excepcional [21].

Una característica destacada del ESP32 es su versatilidad en cuanto a la programación. Compatible con el entorno de desarrollo Arduino, facilita la creación e implementación de

proyectos dentro de este ecosistema [21]. Además, ofrece la opción de programación a través del entorno de desarrollo Espressif IDF (ESP-IDF), brindando un mayor nivel de control y flexibilidad para proyectos más avanzados. La distribución de pines y la apariencia del ESP32 se pueden apreciar en la Figura 4.

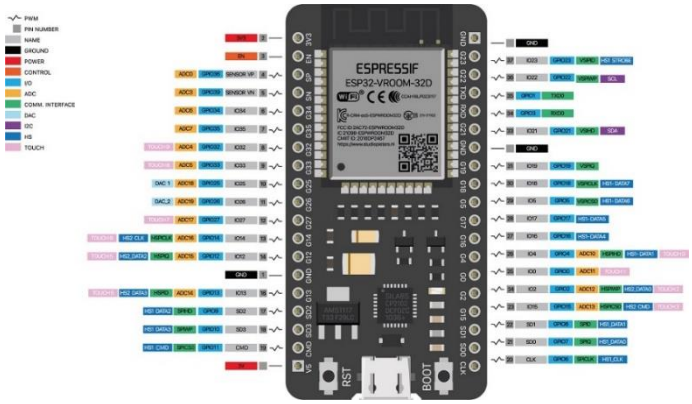


Figura 4. Distribución de pines de la ESP32 [21].

3.2.4.3. ESP32CAM

La ESP32-CAM representa una placa de desarrollo construida alrededor del chip ESP32, integrando una cámara a color OV2640 de 2 MP. Esta placa es sumamente útil en proyectos que demandan transmisión inalámbrica de datos, captura de imágenes o incluso transmisión de video. Una de las ventajas más destacadas radica en su diseño compacto, lo que la convierte en una elección idónea para su implementación en dispositivos portátiles, robots y aplicaciones de bajo consumo, como sistemas de seguridad y domótica [21]. En la Tabla 3 se muestran las características técnicas primordiales de la ESP32-CAM.

Tabla 3 Características técnicas de modulo ESP32-CAM.

CARACTERÍSTICA	DESCRIPCIÓN
MICROCONTROLADOR	ESP32 (dual-core 32-bit MCU)
VELOCIDAD DE RELOJ	Hasta 240 MHz
MEMORIA	520 KB SRAM + 4 MB de memoria flash
CONECTIVIDAD WI-FI	802.11 b/g/n (2.4 GHz)
CÁMARA	Sensor OV2640 (2 megapíxeles) con soporte para JPEG y RAW
RANURA PARA TARJETA MICROSD	Admite tarjetas microSD de hasta 4 GB
INTERFAZ USB	Micro USB para programación y alimentación
PINES DE E/S	9 pines GPIO, ADC de 12 bits, UART, I2C, SPI, etc.
SALIDA DE VIDEO	NTSC/PAL
CONSUMO DE ENERGÍA	Aproximadamente 70 mA durante la operación normal
DIMENSIONES	27 mm x 40 mm
VOLTAJE DE FUNCIONAMIENTO	5V (se puede alimentar mediante el puerto micro USB o pines de E/S)

El ESP32-CAM se usa ampliamente en varias aplicaciones de IoT, como dispositivos inteligentes domésticos, control inalámbrico industrial, monitoreo inalámbrico, identificación inalámbrica QR, señales de sistemas de posicionamiento inalámbricos y otras aplicaciones de IoT [21]. En la Figura 5 se muestra la ESP32CAM asi como la distribución de los puertos que posee el módulo.

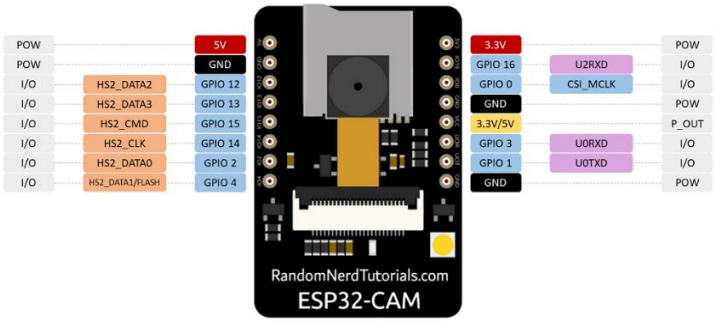


Figura 5. Distribución de pines ESP32 CAM [21].

3.2.5. Entorno de desarrollo de Arduino IDE

Arduino IDE (Integrated Development Environment) es un entorno de desarrollo integrado diseñado para la programación y desarrollo de proyectos utilizando placas Arduino y microcontroladores compatibles. Proporciona a los usuarios una interfaz gráfica intuitiva que simplifica la tarea de escribir, compilar y cargar programas en las placas Arduino [3].

3.2.5.1. Interfaz y editor de código

Arduino IDE (Entorno de Desarrollo Integrado de Arduino) es una plataforma esencial en el mundo de la electrónica y la programación. Su interfaz intuitiva proporciona un entorno de trabajo cómodo para desarrollar proyectos con placas Arduino y microcontroladores compatibles. Uno de los componentes centrales es su editor de código, diseñado para simplificar la escritura, edición y organización del código fuente. Este editor resalta la sintaxis del lenguaje de programación C/C++, facilitando la corrección y detección de errores [3].

3.2.5.2. Compilación y verificación de errores

Arduino IDE ofrece la función de compilación que verifica el código para identificar posibles errores de programación antes de la carga en la placa como se muestra en la Figura 6. Esta característica es crucial para asegurarse de que el código esté libre de errores y funcione como se espera. Los errores, si los hay, se muestran en la ventana de mensajes, lo que ayuda a los programadores a identificar y solucionar problemas antes de continuar [20].

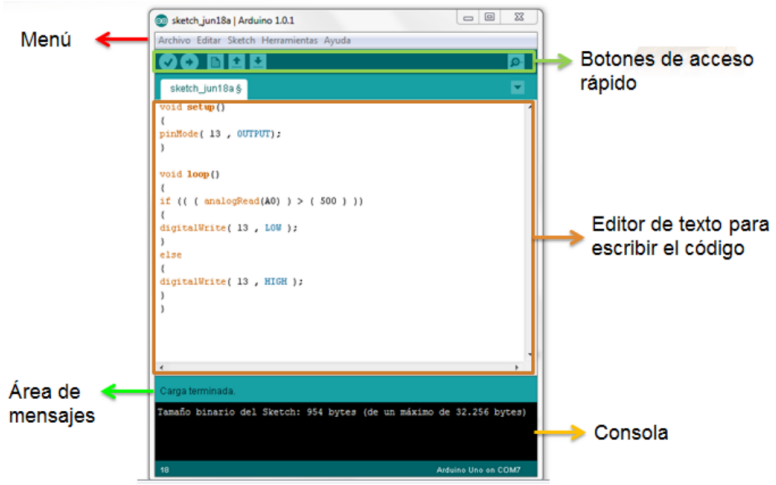


Figura 6. Entorno de desarrollo de Arduino [20].

3.2.5.3. Carga y ejecución de programas

Una vez que el código ha sido escrito y compilado correctamente, Arduino IDE permite cargar el programa en la placa Arduino a través de un cable USB. Esta función de carga transfiere el programa compilado desde la computadora a la placa, permitiendo que el dispositivo electrónico ejecute las instrucciones definidas en el código [3].

3.2.5.4. Bibliotecas de Arduino

Una de las ventajas clave de Arduino IDE es su extensa colección de bibliotecas de Arduino. Estas bibliotecas contienen conjuntos de funciones y rutinas predefinidas que abordan diversas tareas y funcionalidades comunes. Al incorporar estas bibliotecas en su código, los programadores pueden ahorrar tiempo y esfuerzo al aprovechar soluciones ya establecidas para problemas comunes [20].

3.2.5.5. Monitor serial

Arduino IDE incluye un monitor serial que permite la comunicación en tiempo real entre la placa Arduino y la computadora. Este monitor serial es una herramienta valiosa para la depuración y el seguimiento, ya que muestra la salida generada por el programa y permite a los usuarios interactuar con la placa mediante comandos y respuestas en tiempo real [3].

3.2.5.6. Compatibilidad con diversas placas

Arduino IDE es compatible con una amplia gama de placas Arduino y microcontroladores compatibles de otros fabricantes como los módulos ESP. Esto proporciona a los usuarios opciones flexibles para elegir la placa que mejor se adapte a sus necesidades y objetivos de

proyecto [20]. La capacidad de trabajar con diferentes placas amplía las posibilidades de desarrollo y experimentación.

4. METODOLOGÍA Y MATERIALES

En este capítulo, se abordan las técnicas y métodos empleados. En la Sección 4.2 se detalla el diseño del sistema, mientras que en la Sección 4.4 se presenta la implementación junto con los criterios que guiaron dicho proceso.

4.1. DESCRIPCIÓN DEL PROYECTO

4.1.1. Situación actual del laboratorio

En la actualidad, el laboratorio emplea un sistema convencional de cerradura con llave para el acceso. Asimismo, cuando un docente necesita entrar al laboratorio, depende de la presencia del encargado para autorizar su entrada en persona. La iluminación sigue un procedimiento convencional, requiriendo activación manual a través de interruptores, lo que implica que, si se olvida apagar la luz, esta permanecerá encendida hasta que se atienda. Además, cabe destacar la ausencia de tomas de corriente en las instalaciones como se muestra en el plano de la Figura 7, los detalles de los planos se pueden encontrar en el ANEXO K.

Figura 7. Plano antiguo del Laboratorio.

4.1.2. Descripción del sistema

El objetivo de este proyecto es iniciar la mejora del Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA, a través de la implementación de un sistema de control de accesos, así como la integración de soluciones para la automatización de luminarias y tomacorrientes.

El propósito del sistema de control de accesos es proporcionar una forma más rápida de ingresar al laboratorio, haciendo que ya no sea necesario un encargado que tenga la llave para abrir y cerrar la puerta, el control de acceso permite tres métodos para poder acceder al laboratorio, el primero es mediante el uso de tarjetas electromagnéticas RFID que solo requieren acercarlas al sensor y así abrir la puerta.

El segundo se basa en el reconocimiento facial de los individuos previamente registrados, permitiendo que puedan acceder al acercarse a una cámara ubicada fuera del laboratorio. Tanto este sistema como el lector de tarjetas RFID se encuentran en una unidad única, similar a un portero eléctrico, ubicada en el exterior del laboratorio.

El tercer y último método para el control de acceso es utilizar la plataforma de Telegram como interfaz gráfica y medio IoT para poder realizar la apertura de la puerta de manera remota en caso de ser necesario.

También se busca implementar una cámara dentro del laboratorio de tal manera que cuando una persona ingrese esta envíen una foto de la persona a un grupo de Telegram, esta cámara estará ubicada frente a la puerta.

Así mismo se busca automatizar el encendido y apagado de las luces en el laboratorio, de tal manera que cuando ingrese una persona las luces se enciendan automáticamente y de igual manera cuando no haya personas en el laboratorio las luces se apaguen después de un cierto tiempo de espera, además de poder controlar las luces de manera remota utilizando Telegram.

Otro aspecto a tener en cuenta es la gestión de los enchufes a los que se conectarán las impresoras 3D. El propósito es habilitar el control de la conexión y desconexión de la alimentación de estas impresoras a través de IoT. Esto permitirá que los usuarios puedan apagarlas de forma remota si no se encuentran en el laboratorio en ese momento.

Además, se plantea el diseño de un sistema de seguridad más robusto, abordando una gama más amplia de aspectos. Esto incluye la seguridad ante posibles intrusiones mediante la detección de rupturas en las ventanas del laboratorio, gracias a sensores diseñados para identificar este

tipo de eventos. También se contempla en el diseño un sistema de videovigilancia que abarque todo el laboratorio, junto con sensores contra incendios. Este conjunto de medidas se complementará con un sistema de alarma y control través de IoT.

Es esencial destacar que el diseño presentado sienta los cimientos para implementaciones futuras, ya que este proyecto de tesis se concentra en establecer inicialmente el sistema de control de acceso al laboratorio como su primer paso.

4.2. DISEÑO DEL SISTEMA

4.2.1. Definición de requerimientos

En el laboratorio actual, se han identificado algunas áreas críticas en términos de seguridad que requieren atención. Estas áreas representan vulnerabilidades que deben ser abordadas para garantizar la integridad de los activos y la protección del entorno. Para abordar estas preocupaciones, es esencial diseñar un sistema de seguridad y control integral que cubra los siguientes aspectos:

- **Sensores de intrusión en ventanas:** Reconociendo la presencia de ventanales que pueden ser un punto débil, se plantea instalar sensores de vibración o de rotura en las ventanas. Esto permitirá detectar cualquier intento de ingreso no autorizado y alertar al sistema de seguridad.
- **Detección de incendios:** Detectores de humo, para detectar incendios y activar alarmas de incendio.
- **Sistema de alarma:** Un sistema de alarma conectado a los sensores de intrusión en ventanas y puertas es crucial. En caso de un intento de robo, este sistema alertará al personal de seguridad o a las autoridades pertinentes, garantizando una respuesta rápida.
- **Cámaras de seguridad:** Colocar cámaras de vigilancia estratégicamente en zonas vulnerables, como los ventanales y las entradas, fortalece la vigilancia y disuade posibles intrusos. Estas cámaras no solo actúan como disuasivo, sino que también proporcionan evidencia en caso de incidentes.
- **Iluminación adecuada:** La instalación de iluminación interior y exterior adecuada es esencial para disuadir a los intrusos y mejorar la visibilidad en áreas vulnerables durante la noche, minimizando así los riesgos de actividades ilícitas.
- **Control de acceso:** Implementar un sistema de control de acceso es fundamental para limitar el ingreso al laboratorio solo a personal autorizado. Pueden emplearse tarjetas

de acceso, sistemas biométricos etc. para asegurar que solo quienes tienen permiso puedan entrar.

- **Integración de sistemas:** Coordinación y automatización de los diversos componentes que componen el sistema.

Además de estos aspectos de seguridad, también se propone la implementación de un sistema de UPS (Sistema de Alimentación Ininterrumpida) para garantizar la continuidad del sistema en caso de cortes de energía. También, se plantea la posibilidad de controlar las luminarias y los tomacorrientes a través de Telegram como una solución de IoT, permitiendo un control remoto.

Es fundamental reconocer que la seguridad es una prioridad en capas y que la combinación de estos aspectos proporcionará un sistema de seguridad y control completo y robusto. Además, se debe realizar una revisión y adaptación periódica de estas medidas para garantizar una seguridad constante y eficaz en el laboratorio.

4.2.2. Selección de los microcontroladores

4.2.2.1. Microcontrolador para sistema de reconocimiento facial y cámara de entrada

El microcontrolador requerido debe incluir una cámara con una resolución adecuada para capturar imágenes, además de garantizar estabilidad y conectividad a internet. También es crucial que sea capaz de realizar reconocimiento facial y que ofrezca flexibilidad en la utilización de diverso lenguaje de programación para adaptarse a diversas necesidades.

Para la selección del microcontrolador destinado al proyecto de control de acceso, se inicia mediante una revisión de diversas alternativas de microcontroladores y cámaras disponibles. Los resultados de esta evaluación se encuentran detallados en la Tabla 4 que presenta varios sistemas de cámaras que cumplen con la resolución mínima requerida por la norma ISO/IEC 19794-5. Esta norma establece que la resolución facial mínima aceptable es de 250 píxeles de ancho por 250 píxeles de alto [8].

Al analizar en detalle las características de cada opción, se observa que tanto la tarjeta Raspberry Pi como la tarjeta ESP32-CAM cumplen con los requisitos establecidos y además comparten similitudes, lo que las convierte en posibles candidatas para el proyecto. No obstante, es importante considerar otros factores cruciales además de los mencionados previamente, como las dimensiones del dispositivo y la tasa de cuadros por segundo de las cámaras.

Tabla 4 Comparativa de módulos de cámaras con microcontroladores.

CARACTERÍSTICAS	MODULO DE CAMARA ARDUINO CMOS VGA OV7670	CAMARA PARA RASPBERRY	ESP32-CAM
RESOLUCION DEL SENSOR	640 x 480	2592 x 1944	1600 x 1200
VOLTAJE DE ENTRADA	3.3 VDC	5 VDC	5 VDC
FLASH	No	No	Si
CONECTIVIDAD	No	No	Wifi y bluetooth
INTERFAZ DE CONTROL	SCCB (compatible con I2C)	CSI-2	UART, SPI, I2C, PWM
TEMPERATURA DE OPERACIÓN	-30 a 70 °C	-20 a 60°C	-20° a 85°C
ÁNGULO DE VISIÓN	25°	54°	65°
MÁXIMA FRECUENCIA DE IMAGEN	30 FPS	30 FPS	15 y 60 FPS
SOPORTA VIDEO	Si	Si	Si
FORMATOS DE SALIDA (8 BITS)	YUV/YCbCr 4:2:2, RGB565/555, GRB 4:2:2, Raw RGB	JPEG, BMP, GRAYSCALE	JPEG (OV2640) BMP GRAYSCALE
PRECIO	$25	$65	$16

Tras una evaluación, se optó por la adopción de la ESP32-CAM debido a su conectividad wifi, tamaño compacto idóneo para espacios reducidos, resolución de cámara adecuada para la captura de datos biométricos y una amplia gama de interfaces de control, superando a las alternativas disponibles en este aspecto.

En contraste, la opción de emplear la cámara de Raspberry Pi demandaría una placa adicional para su control, incrementando la complejidad y ocupando mayor espacio. Del mismo modo, el módulo de cámara de Arduino presenta una resolución notablemente baja y requiere la presencia de un Arduino para su funcionamiento, considerando que estos dispositivos típicamente carecen de conectividad WiFi.

4.2.2.2. Microcontrolador para el sistema de Identificación por radio frecuencia (RFID)

El microcontrolador debe incorporar dos aspectos esenciales: conectividad a internet y un procesador de rendimiento moderado, ambos constituyen factores importantes. Con el fin de abordar estas necesidades en la Tabla 5 se llevó a cabo una comparativa de microcontroladores donde se incluyen los datos técnicos.

Tabla 5 Comparativa de microcontroladores para el sistema RFID.

CARACTERÍSTICAS	RASPBERRY PI ZERO W	ESP32	ESP8266
PROGRAMACIÓN	Python, C/C++	Arduino IDE, ESP-IDF	Arduino IDE, LUA
PROCESADOR	ARM1176JZF-S	Tensilica Xtensa LX6	Tensilica Xtensa L106
Nº BITS	32	32	32
Nº NÚCLEOS	1	2	1
VELOCIDAD CPU	1 GHz	160 MHz - 240 MHz	80 MHz
MEMORIA	Micro SD, RAM	Flash, SRAM	Flash, SRAM
CAPACIDAD RAM	512 MB	520 KB - 8 MB	80 KB - 160 KB
ALIMENTACIÓN	5 V	3.3 - 5 V	3.3 - 5 V
CONSUMO	Aprox. 150 mA	80 mA - 260 mA	20 mA - 170 mA
WIFI	802.11 b/g/n	802.11 b/g/n (2.4 GHz)	802.11 b/g/n
BLUETOOTH	Bluetooth 4.1 LE	Bluetooth 4.2 (ESP32-S2)	No Bluetooth
PINES E/S	40	36	17 - 22 (GPIO)
SALIDAS PWM	2	16	6
ADC (Nº/ PUERTOS/ BITS)	1 / 16 / 10	2 / 18 / 12	01/10/2010
DAC (Nº/ PUERTOS/ BITS)	01/02/2008	01/02/2008	No DAC
UART	1	3 (4 con conversor)	1
I2C	1	2	1
TAMAÑO	65 x 30 mm	54 x 26 mm	25.5 x 16 mm
TEMPERATURA TRABAJO	Max 85 oC	-40 oC - +85 oC	-40 oC - +85 oC
PRECIOS	32.5	12	7

El ESP8266 satisface los requisitos esenciales de conectividad a Internet y un procesador de rendimiento moderado, además de tener un tamaño más compacto en comparación con otros microcontroladores. Su incorporación en un sistema RFID asegura una comunicación sin problemas, un control confiable y una simplificación en el desarrollo, aprovechando al máximo sus destacadas características.

4.2.2.3. Microcontrolador para el control de luminarias y tomacorrientes mediante IoT

Con el propósito de satisfacer las necesidades en el control de luminarias y tomacorrientes, se busca un microcontrolador programable que no solo proporcione acceso a la red de internet, sino que también se integre de manera fluida con sensores y actuadores. En esta línea, es fundamental que cumpla con los siguientes criterios esenciales:

- **Versatilidad en la programación:** El microcontrolador que seleccionemos debe ofrecer una versatilidad en la programación que permita una adaptación y modificación

sencilla del funcionamiento, en concordancia con los requisitos específicos de cada situación.

- **Conectividad a internet:** Es necesario que el microcontrolador elegido proporcione una conectividad a internet, lo que resulta fundamental para habilitar la funcionalidad en el contexto del Internet de las Cosas (IoT).
- **Integración con sensores y actuadores:** Uno de los aspectos cruciales es que el microcontrolador seleccionado cuente con numerosas entradas y salidas, facilitando así la integración sin complicaciones de diversos sensores y actuadores. Además, debe ser compatible con una variedad de interfaces de comunicación, tales como SPI, I2C, entre otras.

En la Tabla 6 se comparan distintos microcontroladores programables que consideran el primer criterio.

Tabla 6 Comparativa de microcontroladores para el sistema de control IoT.

CARACTERÍSTICAS	ARDUINO YUN	RASPBERRY PI ZERO W	ESP32
POGRAMACION	Arduino IDE, Python	Python, C/C++	Arduino IDE, ESP-IDF, Micropython
PROCESADOR	ATmega32u4	ARM1176JZF-S	Tensilica Xtensa X36
Nº BITS	8	64	32
Nº NÚCLEOS	1	1	2
VELOCIDAD CPU	400 MHz	1 GHz	160 MHz-240 MHz
MEMORIA	EEPROM 1 KB	Micro SD	Flash
SRAM	2,5 KB + 32 KB (Flash)	512 MB	512 KB
ALIMENTACIÓN	5 V	5 V	3.3 V- 5 V
FRECUENCIA RELOJ	16 MHz	19,2 MHz	40 MHz
CONSUMO	Desconocido	350 mA	80 mA-225 mA
WIFI	802.11b/g/n	802.11 b/g/n 2.4GHz	802.11 b/g/n 2,4 ~ 2,5 GHz
BLUETOOTH	no	V4.1 LE	v4.2 BR/EDR
PINES E/S	20	26	36
SALIDAS PWM	8	2	16
ADC (Nº/ PUERTOS/ BITS)	1 / 12/ 10	1/ 16/ 10	2 / 18 / 12
DAC (Nº/ PUERTOS/ BITS)	1/ 7/ 8	1/ 2/ 8	1/ 2/ 8
UART	-	1	4
I2C	1	2	2
I2S	-	1	2
SPI	1	2	4
TAMAÑO	68.6 x 53.3 mm	65 x 30 mm	54 x 26 mm
TEMPERATURA TRABAJO	–5 oC - +45 oC	Max 85 oC	-40 oC - +85 oC
PRECIO	58.8	32.5	12

Al analizar los criterios establecidos, se concluye que el microcontrolador que satisface estos requisitos es el ESP32. Este microcontrolador presenta ventajas, tales como su capacidad de programación en diversos lenguajes, una mayor conectividad a internet en comparación con alternativas, un mayor número de entradas y salidas disponibles, así como una amplia gama de pines de comunicación para protocolos como SPI, I2C y UART. Además, su tamaño más reducido en comparación con otros microcontroladores lo convierte en una opción favorable en diversos aspectos.

4.2.2.4. Elección de sensor de intrusión en ventanas

Uno de los aspectos cruciales del sistema de seguridad es la selección adecuada de sensores para detectar eventos específicos, como la ruptura de ventanas. En este contexto, se han considero dos opciones de sensores: el SW-18010P y el SW-420. A continuación, en la Tabla 7 se presenta una comparativa detallada de las características técnicas de ambos sensores.

Tabla 7 Comparativa de los sensores SW-18010P y el SW-420.

CARACTERÍSTICA TÉCNICA	SENSOR SW-18010P	SENSOR SW-420
VOLTAJE DE OPERACIÓN	3.3V - 5V	3.3V - 5V
CORRIENTE DE OPERACIÓN	10mA - 20mA	10mA - 20mA
PRINCIPIO DE DETECCIÓN	Sensor de choque mecánico	Sensor de vibración piezoeléctrico
SENSIBILIDAD	Sensible a golpes fuertes o cambios bruscos de aceleración	Sensible a vibraciones, no tan sensible a choques
SALIDA	Digital (alta/baja)	Digital (alta/baja)
NIVEL DE SALIDA	Alto al detectar golpe/vibración, bajo en reposo	Alto al detectar vibración, bajo en reposo
AJUSTE DE SENSIBILIDAD	Posible ajuste mecánico	No suele tener ajuste de sensibilidad
DIMENSIONES	Compactas	Compactas
APLICACIONES COMUNES	Detección de impactos, seguridad de ventanas, detección de movimiento brusco	Detección de vibraciones en dispositivos, sistemas de alarma, electrónica en movimiento
CONDICIONES AMBIENTALES	Sensible a vibraciones ambientales, posibles falsos positivos	Puede ser afectado por vibraciones constantes
COSTO ESTIMADO	Variable, generalmente económico	Variable, generalmente económico

Basándonos en las características técnicas y en el propósito específico de detectar la ruptura de ventanas, se ha considerado que el sensor SW-18010P es la elección más adecuada. Esto se debe a su capacidad para detectar golpes o impactos fuertes, lo cual es una característica clave durante una ruptura de ventana. El SW-18010P está diseñado para reaccionar ante cambios bruscos de aceleración, como los que se producen en un evento de ruptura. Además, su capacidad para ajustar la sensibilidad mecánicamente podría permitir adaptarlo a diferentes condiciones y necesidades.

Si bien el sensor SW-420 también puede ser efectivo en ciertos escenarios de detección de vibraciones, su sensibilidad resultar insuficiente para capturar impactos significativos, como los que ocurren al romper una ventana. El SW-420 está más orientado a la detección de vibraciones continuas o repentinas en aplicaciones como maquinaria o sistemas de alarma en movimiento.

4.2.2.5. Selección de la Bocina de Alarma

Los aspectos a tener en cuenta al elegir una alarma que cumpla con la norma NFPA 72 son los siguientes:

- **Niveles de Sonido:** Verifica que la alarma tenga niveles de sonido adecuados y ajustables según las necesidades del entorno. Puede ser útil si la alarma tiene diferentes configuraciones de volumen.
- **Inteligibilidad del Sonido:** Asegúrate de que la alarma emita un sonido claro y distintivo que pueda ser entendido fácilmente en situaciones de emergencia.
- **Ubicación y Distribución:** Considera la capacidad de la alarma para ser ubicada y distribuida de manera efectiva en el edificio, de acuerdo con las pautas de la NFPA 72.
- **Señalización Visual:** Evalúa si la alarma también incluye señalización visual, como luces intermitentes, para alertar a personas con discapacidades auditivas.
- **Fuente de Energía y Respaldo:** Asegúrate de que la alarma tenga una fuente de energía confiable y sistemas de respaldo en caso de cortes de energía.
- **Facilidad de Instalación y Mantenimiento:** Considera la facilidad de instalación y mantenimiento de la alarma, incluyendo la accesibilidad para realizar pruebas y mantener el sistema.
- **Compatibilidad y Integración:** Si es necesario, verifica si la alarma es compatible con otros sistemas de seguridad y si puede integrarse con sistemas de monitoreo o notificación.

A continuación, en la Tabla 8 se muestra la comparativa de varias alarmas existentes.

Tabla 8 Tabla 8

MARCA/MODELO	CUMPLIMIENTO NFPA 72	NIVELES DE SONIDO (DB)	SEÑALIZACIÓN VISUAL	COMPATIBILIDAD
ALARMA ZLK	Sí	80-100	Sí	Integración con Sistemas XYZ
SAFEGUARD	Sí	75-95	Sí	Compatible con Sistemas Domóticos
SOUNDALERT	Sí	85-110	No	Integración con Plataforma PQR

Dado que el sistema desarrollado funcionaba con microcontroladores programables, se optó por seleccionar la alarma Safeguard debido a su compatibilidad con la plataforma en desarrollada.

4.2.2.5.1. Selección de módulo de cámara

En el apartado de microcontroladores se ha elegido la ESP32-CAM, teniendo en cuenta esto para el diseño del sistema de cámaras y videovigilancia, se ha llevado a cabo una evaluación de varias opciones de módulos de cámaras compatibles con la ESP32-CAM entre las opciones consideradas, se destaca especialmente el modelo OV2640 debido a su equilibrio entre resolución y calidad de imagen. Con una resolución de 2 MP y una apertura focal de f/2.8, la OV2640 ofrece una combinación versátil que satisface las necesidades tanto de claridad visual como de capacidad de captura de detalles en la Tabla 9 se muestran los sensores considerados.

Tabla 9 Módulos de cámaras compatibles con la ESP32-CAM.

MODELO DE CÁMARA	RESOLUCIÓN	APERTURA FOCAL	CARACTERÍSTICAS NOTABLES
OV2640	2 MP	f/2.8	Asequible, buena calidad de imagen, ampliamente compatible.
OV7670	VGA (640x480)	-	Económica, adecuada para aplicaciones básicas.
OV5640	5 MP	f/2.8	Alta resolución, buena calidad de imagen.
OV7725	VGA (640x480)	f/2.0	Mejor rendimiento, pero baja resolución.
MT9D111	2 MP	-	Ajustes de exposición y configuración personalizable.

Es importante mencionar que, aunque la OV2640 ha sido elegida como la opción principal para este sistema, gracias a la versatilidad que la ESP32-CAM tiene, brinda la posibilidad de intercambiar la cámara por otros modelos según las necesidades específicas del proyecto.

4.2.2.5.2. Selección de luminarias adecuadas

En relación a las luminarias propuestas, se consideran aquellas con una temperatura de color neutra o fría de 4000K - 5000K, y una potencia de 35W.

4.2.2.5.3. Elección de sensor de movimiento

En este caso, se han evaluado cuatro opciones de sensores de movimiento: Sensor PIR (HC-SR501), Sensor ultrasónico (HC-SR04), Sensor de microondas (RCWL-0516), Sensor infrarrojo activo (QRE1113). A continuación, en la Tabla 10 se presenta una comparativa de las características técnicas de los sensores:

Tabla 10 Tabla Comparativa de Sensores de Movimiento.

CARACTERÍSTICA	SENSOR PIR (HC-SR501)	SENSOR ULTRASÓNICO (HC-SR04)	SENSOR DE MICROONDAS (RCWL-0516)	SENSOR INFRARROJO ACTIVO (QRE1113)
PRINCIPIO DE DETECCIÓN	Infrarrojo Pasivo	Ultrasonido	Microondas	Infrarrojo Activo
ALCANCE MÁXIMO	3-7 metros	2-400 cm	Hasta 7 metros	1-4 cm
SENSIBILIDAD AJUSTABLE	Sí	No	Sí	Sí
DETECCIÓN DE MOVIMIENTO	Sí	Sí	Sí	Sí
DETECCIÓN DE DISTANCIA	No	Sí	Sí	No
INMUNIDAD A MASCOTAS	Posible	No	No	Alta
VOLTAJE DE OPERACIÓN	4.5-20V	5V	4-28V	3.3-5V
CONSUMO DE CORRIENTE	<50 mA	<15 mA	~2.8 mA	<20 mA
TIEMPO DE RETARDO	Ajustable	200-3800 ms	Ajustable	-
APLICACIONES COMUNES	Seguridad doméstica, Iluminación automática	Estacionamientos, alarma de intrusos	Automatización industrial, control de tráfico	Fotografía, detección de objetos

La elección del sensor de infrarrojo pasivo (PIR) se justifica por su bajo consumo energético y detección pasiva de cambios térmicos, lo que lo hace altamente efectivo en ambientes controlados como laboratorios u oficinas, minimizando falsas alarmas causadas por movimientos de plantas o iluminación. Su facilidad de implementación lo convierten en una opción versátil para aplicaciones de seguridad, iluminación automática y alarmas. La capacidad de ajustar la sensibilidad y el tiempo de retardo lo adapta a necesidades específicas, mientras que su capacidad para detectar presencia humana o animal lo hace ideal para su aplicación en el presente proyecto.

4.2.2.5.4. Elección del sensor para detectar incendios

Al considerar la elección del sensor más adecuado para la detección de incendios, es esencial evaluar cuidadosamente las características técnicas de los sensores disponibles. En la Tabla 11 se analizarán las opciones de los sensores MQ-2, MQ-7 y MQ-8, teniendo en cuenta su rendimiento en términos de detección de incendios.

Tabla 11 Comparativa sensores de detección de incendios.

CARACTERÍSTICA	SENSOR MQ-2	SENSOR MQ-7	SENSOR MQ-8
			
DETECTA GASES	Gas inflamable, humo, LPG, GLP	Monóxido de Carbono (CO)	Hidrógeno (H2), Gas inflamable
TENSIÓN DE OPERACIÓN (V)	5V	5V	5V
SENSIBILIDAD AJUSTABLE	Sí	No	Sí
SALIDA ANALÓGICA	Sí	Sí	Sí

SALIDA DIGITAL	Sí	No	No
TIEMPO DE RESPUESTA (SEG)	**<10**	**60**	<10
RANGO DE DETECCIÓN (%)	300-10,000 ppm	10-500 ppm	100-1,000 ppm
PRECISIÓN	Variable	Buena	Buena
RANGO DE TEMPERATURA (°C)	-10 a 50	-10 a 50	-10 a 50
RANGO DE HUMEDAD (%)	33147	33147	33147
USO PRINCIPAL	Detección de gas inflamable, humo y otros gases	Detección de monóxido de carbono	Detección de hidrógeno y gas inflamable

El Sensor MQ-2 se seleccionó por ser la opción más completa y adaptable para la detección de incendios debido a su capacidad para identificar múltiples gases inflamables y humo.

4.2.2.5.5. Elección de lector RFID

En la Tabla 12 se muestra la comparativa de los diferentes lectores RFID que existen el mercado.

Tabla 12 Comparativa de lector RFID.

Característica	Lector RFID RC522	Lector RFID PN532	Lector RFID RDM6300	Lector RFID RDM8800
Frecuencia	13.56MHZ	13.56MHZ	125KHZ	125KHZ
Protocolos Soportados	ISO 14443A/B, MIFARE	ISO 14443A/B, MIFARE	EM4100	EM4100, EM4200
Interfaces	SPI	I2C, SPI	UART	UART
Alcance de Lectura	HASTA 3 CM	HASTA 7 CM	HASTA 10 CM	HASTA 10 CM
Alimentación	3.3V	3.3V	5V	5V

La selección del Lector RFID RC522 13.56MHz se justifica por su versatilidad y amplia compatibilidad con protocolos estándar, como ISO 14443A/B y MIFARE, que son comunes en aplicaciones de seguridad, control de acceso y automatización. Su capacidad de comunicación a través de la interfaz SPI lo hace adecuado para integración en una variedad de sistemas, y su alcance de lectura de hasta 3 cm es apropiado para aplicaciones de corto alcance.

4.2.2.5.6. Selección del relé

En la Tabla 13 se muestra la comparación entre diferentes tipos de relés, incluyendo relés mecánicos y de estado sólido.

Tabla 13 Comparativa de Tipos de Relés y sus Especificaciones Técnicas.

CARACTERÍSTICA	RELÉ DE ESTADO SÓLIDO	MÓDULO RELÉ
TIPO	Estado Sólido	Mecánico
CONTACTOS	Sin partes móviles	Móviles
TIEMPO DE CONMUTACIÓN	Menor	Mayor
VIDA ÚTIL	Mayor	Limitada
RUIDO ELECTROMAGNÉTICO	Bajo	Bajo
CORRIENTE DE ACCIONAMIENTO	Baja a alta	Baja a alta
APLICACIONES COMUNES	Control de cargas en alta frecuencia, aplicaciones donde se requiere una vida útil prolongada	Control de dispositivos eléctricos, automatización industrial

La elección del módulo relé se debió a que, a pesar de sus desventajas, satisface los requisitos de la instalación. Además, si se anticipa un uso intensivo del actuador, en ese contexto, la alternativa más adecuada sería optar por el relé de estado sólido.

4.2.2.5.7. Selección de la Cerraduras Eléctricas

En la siguiente Tabla 14 se presenta una comparación entre distintos modelos de cerraduras eléctricas, con sus características.

Tabla 14 Cerraduras Eléctricas y sus Especificaciones Técnicas.

CARACTERÍSTICA	CERRADURA ELÉCTRICA A	CERRADURA ELÉCTRICA B	CERRADURA ELÉCTRICA C	CERRADURA ELÉCTRICA ZKTECO AL-180
TIPO	Tipo A	Tipo B	Tipo C	Tipo D
VOLTAJE DE OPERACIÓN	12V	24V	12V	12V
CORRIENTE DE OPERACIÓN	800 mA	500 mA	600 mA	400 mA
MATERIAL	Acero inoxidable	Aleación de aluminio	Acero inoxidable	Aleación de zinc
MODO DE DESBLOQUEO	Tarjeta RFID, Contraseña	Contraseña, Llave	Tarjeta RFID, Contraseña	Tarjeta RFID, Contraseña
GRADO DE PROTECCIÓN	IP65	IP54	IP67	IP65
APLICACIONES COMUNES	Acceso a puertas de entrada, control de acceso	Acceso a oficinas, almacenes	Puertas exteriores, ambientes húmedos	Control de acceso, puertas de entrada
VENTAJAS	Alta protección IP, opciones de desbloqueo seguras	Versatilidad de modos de desbloqueo, material resistente	Resistente a condiciones ambientales adversas	Amplia compatibilidad con sistemas de control de acceso

La Cerradura Eléctrica ZKTeco AL-180 se seleccionó debido a su combinación de características deseables, que incluyen un voltaje de operación estándar de 12V, una corriente de operación de 400 mA y un material duradero de aleación de zinc. Además, su grado de

protección IP65 la hace adecuada tanto para uso en interiores como en exteriores, mientras que su amplia compatibilidad con sistemas de control de acceso asegura una integración sencilla en diversas aplicaciones.

4.2.2.6. Ubicación de los elementos del sistema completo

4.2.2.6.1. Ubicación de camas de video vigilancia

La colocación estratégica de cámaras de videovigilancia es fundamental para garantizar una cobertura efectiva y una vigilancia integral en un área determinada. A continuación, se presentan criterios y normas para la ubicación las cámaras de video vigilancia, considerando aspectos de seguridad, visibilidad y cumplimiento normativo:

- **Distribución Equitativa:** Se debe planificar la distribución de las cámaras de manera equitativa para cubrir todos los puntos críticos y áreas de interés. Esto incluye entradas, salidas, pasillos, áreas de almacenamiento y zonas con mayor afluencia de personas.
- **Ángulo de Visión:** Cada cámara debe estar colocada de manera que su ángulo de visión cubra el área deseada sin obstrucciones. Asegúrate de ajustar la inclinación y rotación para capturar imágenes claras y sin puntos ciegos.
- **Altura de Montaje:** Las cámaras deben colocarse a una altura que permita capturar rostros y detalles de manera efectiva. En exteriores, una altura de alrededor de 3 a 4 metros es común, mientras que, en interiores, alrededor de 2 a 3 metros suele ser adecuado.
- **Evitar Reflejos y Deslumbramiento:** Coloca las cámaras de manera que no se enfrenten directamente a fuentes de luz intensa, lo que podría generar reflejos y deslumbramientos que afecten la calidad de la imagen.
- **Cámaras Visibles y Disuasorias**: Algunas cámaras pueden colocarse de manera visible para actuar como elemento disuasorio. Esto puede ayudar a prevenir conductas indeseadas y mejorar la percepción de seguridad.
- **Protección y Resguardo:** Si las cámaras se instalan en exteriores, es importante que estén protegidas contra condiciones climáticas adversas, como lluvia, polvo y exposición directa al sol. Utiliza carcasas protectoras para asegurar su durabilidad.

- **Revisión y Ajuste:** Una vez instaladas las cámaras, realiza revisiones periódicas para asegurarte de que mantienen una funcionalidad óptima. Si es necesario, realiza ajustes en su ubicación o ángulo de visión para optimizar su desempeño.

Con base en las consideraciones previas, se ha diseñado un plan para la ubicación de un total de 10 cámaras de vigilancia, con el propósito de cubrir de manera integral y estratégica todo el espacio del laboratorio. La disposición y orientación de estas cámaras han sido planificadas meticulosamente para optimizar la seguridad y la supervisión:

- **Cámaras en las Esquinas:** deberá haber 4 cámaras en las esquinas del laboratorio, una en cada esquina. Esta disposición permitirá una cobertura completa del espacio, minimizando los puntos ciegos y brindando una vigilancia eficaz desde diferentes ángulos.
- **Cámara hacia el Área de Impresoras 3D:** Una cámara deberá estar dirigida hacia el área de impresoras 3D. Esta cámara capturará imágenes detalladas de esta sección clave, brindando control visual sobre las operaciones y los posibles eventos que ocurran en este espacio.
- **Cámara hacia el Área de Estudiantes:** Otra cámara deberá estará enfocada hacia el área de estudiantes. Esto permitirá supervisar y asegurar un ambiente propicio para el estudio y el trabajo en equipo, contribuyendo al bienestar de los usuarios.
- **Cámaras Frontal y Trasera:** Dos cámaras se deberán estar colocadas en la parte frontal y trasera del laboratorio. Estas cámaras proporcionarán una vista amplia y estratégica de los accesos principales, reforzando la seguridad en los puntos de entrada y salida.
- **Cámaras Exteriores:** Para el área exterior, se ubicará una cámara en la entrada y otra en la parte trasera del laboratorio. La cámara de la entrada permitirá supervisar las llegadas y salidas, mientras que la cámara trasera contribuirá a la seguridad de la parte trasera del edificio. Se garantizará que la cámara trasera cuente con una protección adecuada contra la lluvia para mantener su funcionamiento eficiente.

En la Figura 8 se muestra el área de cobertura en color tomate de las 10 cámaras de vigilancia.

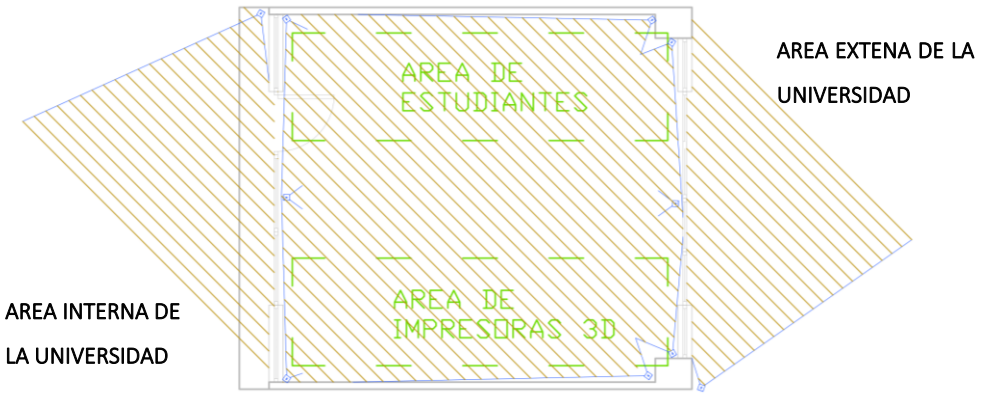


Figura 8. Área de cobertura de las cámaras.

4.2.2.6.2. Ubicación de las luminarias

La ubicación adecuada de luminarias en un laboratorio es esencial para garantizar una iluminación que fomente la seguridad, la productividad y el bienestar de los ocupantes. Al considerar la distribución de las luminarias, es importante tener en cuenta tanto criterios técnicos como normas de iluminación como Norma IESNA (Illuminating Engineering Society of North America). En este caso, se presenta la ubicación de 10 luminarias en el interior del laboratorio y 4 luminarias en el exterior para mejorar la iluminación en la parte frontal y trasera del edificio como se muestra a continuación.

- **Área de Impresoras 3D:** Se propone la ubicación de 3 luminarias en esta sección para garantizar una iluminación uniforme y suficiente durante las operaciones de impresión.
- **Área de Estudiantes:** Otros 3 dispositivos luminosos en el área de estudiantes para proporcionar una iluminación adecuada para las actividades de estudio y trabajo en equipo.
- **Zona Central:** En el centro del laboratorio, se propone 4 luminarias adicionales. Dos de ellas estarán ubicadas en la parte frontal y las otras dos en la parte trasera.

En cuanto a las luminarias en el exterior del Laboratorio se propone las siguientes:

- **Iluminación Frontal:** Dos luminarias para la parte frontal, en la entrada principal.
- **Iluminación Trasera:** Dado que la parte trasera carece de techo y es plana, considera la ubicación de dos luminarias empotradas en la pared. Estas luminarias pueden arrojar luz hacia abajo para iluminar el área y disuadir posibles intrusiones.

4.2.2.6.3. Ubicación de las bocinas de alarmas

A continuación, se presenta las ubicaciones planteadas de las bocinas:

- **Bocina de Alarma Exterior (Esquina Superior Izquierda - Parte Frontal):** La bocina exterior fue ubicada en la esquina superior izquierda de la parte frontal del laboratorio, en el exterior.
- **Bocina de Alarma Exterior (Esquina Superior Derecha - Parte Trasera):** La segunda bocina de alarma exterior se planteó en la esquina superior derecha de la parte trasera del laboratorio.
- **Bocina de Alarma Interior (Mitad Superior de la Pared Izquierda - Interior):** Para la bocina de alarma interior, esta se planteó su colocación en la mitad del laboratorio.

4.2.2.6.4. Ubicación de los sensores de intrusión en ventanas

Estos sensores desempeñan un papel crucial en la detección temprana de intentos de intrusión, contribuyendo a la seguridad integral del laboratorio. A continuación, se detalla la distribución planificada de estos sensores, de acuerdo con las normativas pertinentes:

Ubicación Individual por Ventana: Se plantea la ubicación un sensor de intrusión en cada ventana del laboratorio. Esta disposición permitirá una detección precisa y localizada en caso de cualquier intento de ruptura o acceso no autorizado a través de las ventanas. Los sensores estarán programados para activarse al detectar vibraciones o impactos característicos de un intento de romper el vidrio.

- **Parte Trasera del Laboratorio (7 Sensores):** En la parte trasera del laboratorio, se ubicarán 7 sensores de intrusión en las ventanas correspondientes. Esta distribución asegurará una cobertura completa y efectiva de las áreas vulnerables en la parte trasera del edificio.
- **Parte Delantera del Laboratorio (15 Sensores):** En la parte delantera del laboratorio, se plantean 15 sensores de intrusión en las ventanas. Esta cantidad mayor de sensores se justifica por la mayor exposición y visibilidad de la parte frontal del laboratorio.

4.2.2.6.5. Ubicación de los sensores de humo

La ubicación de los sensores de humo en un laboratorio debe seguir ciertas pautas de seguridad para garantizar la detección efectiva de incendios, tomando eso en consideración se da uso de la norma NFPA (Asociación Nacional de Protección contra Incendios). Dado que mencionas

que las zonas de estudiantes y de impresoras 3D están en las zonas más altas y que el laboratorio tiene dimensiones de 6.5 x 7.6 metros, tomando en consideración la norma se aplican los criterios:

1. **Altura y Detección Ascendente:** Las zonas de estudiantes y de impresoras 3D se encuentran en las áreas más altas del laboratorio, lo que aumenta la probabilidad de que el humo se eleve hacia estas áreas en caso de incendio. Colocar los sensores cerca del techo en estas zonas maximiza la capacidad de detectar humo ascendente y proporciona una alerta temprana en caso de emergencia.
2. **Detección en Zonas de Riesgo Potencial:** Se considera ubicar sensores de humo en la zona de estudiantes y de impresoras 3D, ya que estas áreas podrían presentar riesgos potenciales debido a las actividades de formación, el uso de equipos de alta temperatura y la posible presencia de sustancias inflamables.
3. **Distancia a Paredes y Esquinas:** Los sensores de humo se coloquen a una distancia mínima de 30 centímetros de las paredes y esquinas, de acuerdo con las regulaciones de seguridad. En este caso se ubican a 50 centímetros de la pared, para cada sensor.
4. **Distribución Equitativa:** Para asegurar una detección uniforme en todo el laboratorio, se planea distribuir los sensores de humo en la zona de estudiantes y de impresoras 3D, cubriendo áreas donde las personas trabajan y actividades que podrían generar calor o sustancias peligrosas.
5. **Ausencia de Riesgos Potenciales:** Dado que no se identifican riesgos significativos en relación con la contaminación y la ventilación en el laboratorio, no se considera necesario ubicar sensores de humo en estas ubicaciones.

Los sensores de humo en las zonas de estudiantes y de impresoras 3D en el laboratorio se basa en la altura de las zonas, la detección en áreas de riesgo potencial, la distancia a paredes y esquinas, la interconexión, la distribución equitativa y el tamaño moderado del laboratorio como se muestra en el la Figura 9.

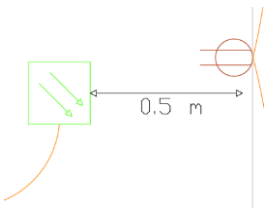


Figura 9. Ubicación de los sensores de humo.

4.2.3. Programación

4.2.3.1. Funcionamiento de la programación del sistema de reconocimiento facial

En el desarrollo del código del sistema de reconocimiento facial, se emplea el entorno IDE de Arduino, diseñado para programar y desarrollar proyectos con microcontroladores. Este entorno ofrece una interfaz específica que facilita la programación en un lenguaje sencillo como C++, además de proporcionar herramientas para cargar el código en el microcontrolador y supervisar su funcionamiento en tiempo real durante la conexión.

Para que el IDE de Arduino pueda detectar y trabajar con la placa ESP32-CAM, que previamente ha sido seleccionada, es necesaria la instalación de los componentes específicos a través de un proceso detallado en el ANEXO C, al momento de instalar la versión de la placa se recomienda usar la versión 1.0.5 ya que en esta versión funciona mejor el reconocimiento facial. Una vez completada esta instalación, se procede a escoger la placa "AI Thinker ESP32-CAM" en Herramientas – Placa – ESP32 como se muestra en la Figura 10.

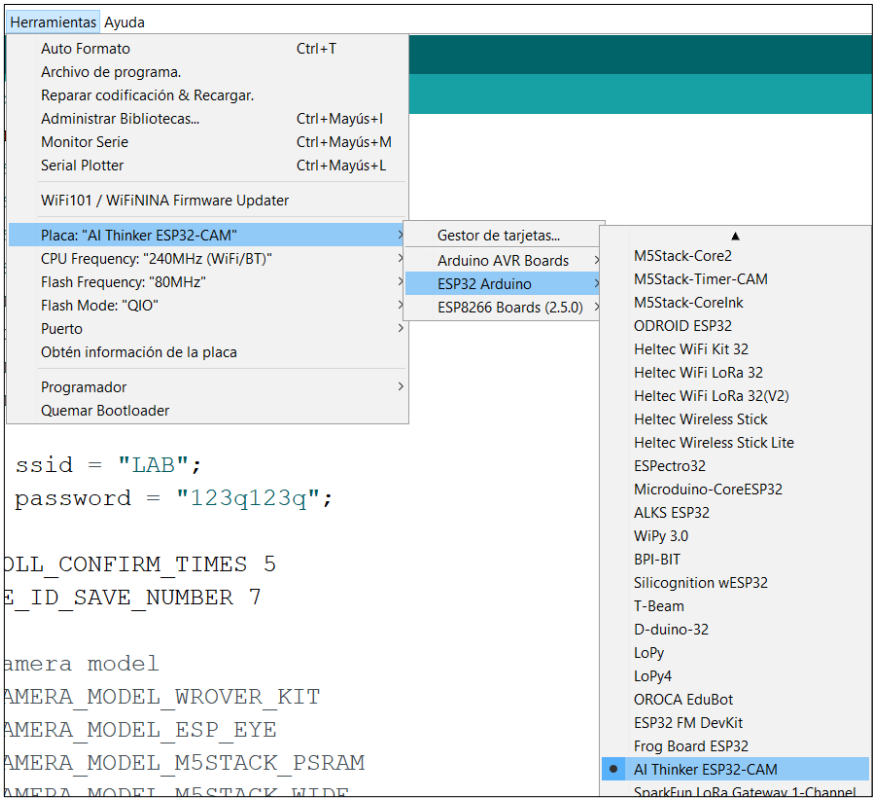


Figura 10. Selección de la placa AI Thinker ESP32-CAM.

Para lograr una detección y reconocimiento facial exitoso, resulta imperativo incorporar las bibliotecas señaladas en la Figura 11. Estas bibliotecas desempeñan un papel crucial al asegurar el rendimiento del sistema.

```
#include <ArduinoWebsockets.h>
#include "esp_http_server.h"
#include "esp_timer.h"
#include "esp_camera.h"
#include "camera_index.h"
#include "Arduino.h"
#include "fd_forward.h"
#include "fr_forward.h"
#include "fr_flash.h"
```

Figura 11. Librerías utilizadas para el sistema de reconocimiento facial.

Para incorporar las librerías mencionadas en el entorno de desarrollo de Arduino, es necesario utilizar la opción "Herramientas" y luego seleccionar "Administrador de Bibliotecas", conforme se explica detalladamente en el ANEXO D. Además, en el ANEXO E se ofrece una breve descripción de cada una de estas librerías.

La configuración de la conexión a la red Wi-Fi es un paso esencial. Para lograrlo, se requiere introducir tanto el nombre de usuario como la contraseña correspondiente de la red Wi-Fi en el código del programa. Específicamente, esta información se ajusta en la sección que hace referencia a "ssid", donde se ingresa el nombre de la red deseada. De manera similar, en el campo "password" se proporciona la contraseña pertinente, tal como se ilustra de manera gráfica en la Figura 12. Este proceso garantiza una conexión efectiva del dispositivo a la red y permite un acceso adecuado a los servicios en línea.

```
const char* ssid = "LAB";
const char* password = "123q123q";
```

Figura 12. Datos de la red Wifi.

La Figura 13, ilustra el proceso de inicialización del objeto WebsocketsServer, que asume una función crucial en la administración de las conexiones WebSockets. Este término describe un protocolo de comunicación que permite interacciones bidireccionales y en tiempo real entre un servidor y un cliente mediante una conexión continua. En el ámbito de la programación, esta tecnología se utiliza para recibir datos en tiempo real, derivados de los comandos emitidos desde el servidor web, y llevar a cabo su ejecución por medio del dispositivo ESP32-CAM.

```
using namespace websockets;
WebsocketsServer socket_server;
```

Figura 13. Inicialización del WbsocketsServer.

La placa ESP32-CAM ofrece la capacidad de llevar a cabo el reconocimiento facial, permitiendo la creación de un código que pueda enviar señales a través de sus pines de salida,

estableciendo así un sistema de control de acceso. Para lograr esto, es necesario comprender algunos aspectos del código y definir variables y objetos globales clave.

En la función `void app_facenet_main()`, que actúa como el punto de entrada principal del programa, se realizan las configuraciones iniciales necesarias para el reconocimiento facial y la gestión de identidades. La línea `face_id_name_init(&st_face_list, FACE_ID_SAVE_NUMBER, ENROLL_CONFIRM_TIMES);` inicializa la estructura `st_face_list`, que está relacionada con el almacenamiento y la administración de identidades, configurando parámetros como `FACE_ID_SAVE_NUMBER` y `ENROLL_CONFIRM_TIMES`, que definen la cantidad de identidades almacenables y las muestras necesarias para el registro. También se reserva memoria para una matriz llamada `aligned_face` en la línea `aligned_face = dl_matrix3du_alloc(1, FACE_WIDTH, FACE_HEIGHT, 3);`, destinada a almacenar datos de rostros detectados.

La función `read_face_id_from_flash_with_name(&st_face_list);` se encarga de leer las identidades previamente registradas desde el almacenamiento, como la memoria flash. Además, la función `do_enrollment()` se encarga del proceso de registro de nuevas identidades faciales. Las funciones `send_face_list()` y `delete_all_faces()` están diseñadas para enviar la lista de identidades faciales y eliminarlas, respectivamente, a través de conexiones WebSockets hacia un cliente o página web, brindando funcionalidades esenciales para la gestión del sistema de control de acceso.

La ESP32-CAM proporciona una página web que se puede ajustar con ciertos conocimientos de HTML y CSS, otorgando la posibilidad de personalizar la interfaz web de acuerdo a las preferencias del usuario. La sección correspondiente de código está encriptada en formato hexadecimal, y para desencriptarla, se utiliza la herramienta CyberChef, que se ilustra en la Figura 14.

Con esta herramienta, es posible recuperar el código original, lo que permite llevar a cabo las modificaciones necesarias. Una vez finalizado este proceso, el código alterado se vuelve a convertir a formato hexadecimal para luego integrarlo en la programación. Los detalles de este procedimiento se encuentran minuciosamente explicados en el ANEXO F.

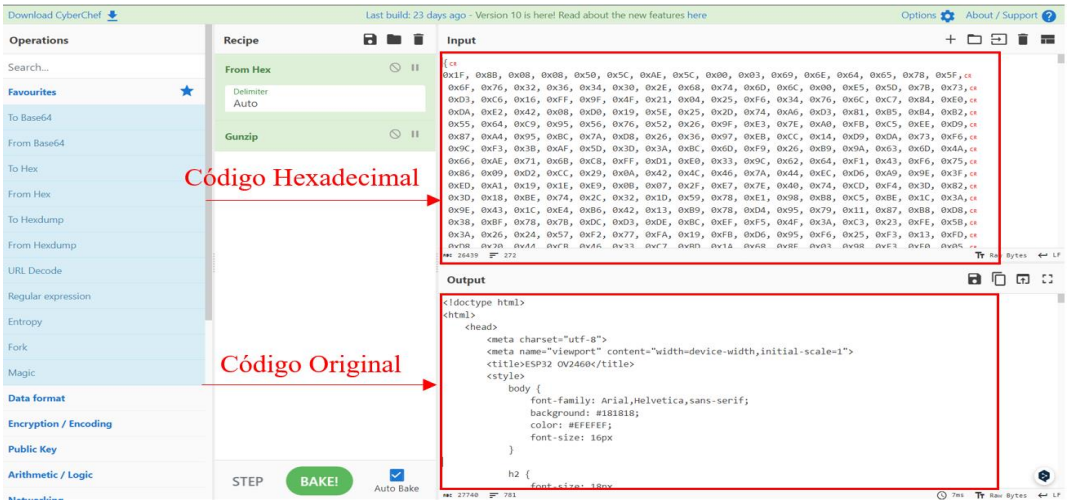


Figura 14. Página web CyberChef para desencriptar el código hexadecimal.

La Figura 15, presenta la interfaz web predeterminada suministrada por la ESP32-CAM, que abarca diversas configuraciones y funciones relacionadas con la cámara. No obstante, muchas de estas opciones resultan superfluas para el funcionamiento del sistema de portero. Por consiguiente, se ha llevado a cabo una selección y ajuste focalizado únicamente en las funcionalidades esenciales, como se puede apreciar en la Figura 16.

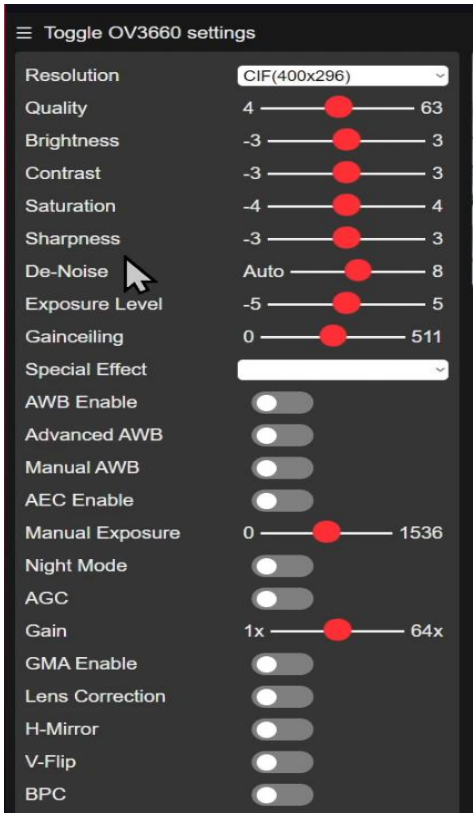


Figura 15. Interfaz de la ESP32-CAM por defecto.

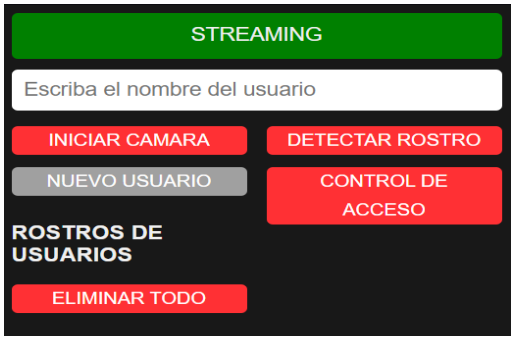


Figura 16. Interfaz modificada.

Este cambio fue llevado a cabo por dos razones fundamentales. La primera, con el propósito de simplificar la experiencia del usuario en el manejo, y la segunda, con el objetivo de mejorar el rendimiento de la cámara. Al eliminar configuraciones de imagen adicionales, se logra reducir la carga de procesamiento.

4.2.3.2. Funcionamiento de la programación del sistema RFID

Para iniciar la programación del sistema RFID, es necesario comenzar por la instalación de la placa de control ESP8266. El procedimiento detallado para llevar a cabo esta instalación se encuentra explicado en el ANEXO C. Luego, se debe seleccionar la placa "Generic ESP8266 Module" que se ubica en la opción Herramientas - Placa - ESP8266 Boards, como se muestra en la Figura 17.

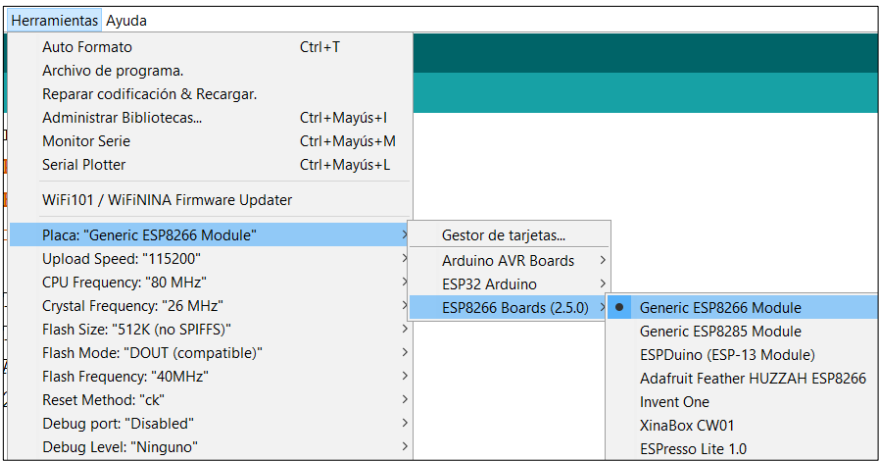


Figura 17. Selección de la placa Generic ESP8266 Module.

El siguiente paso consiste en agregar las bibliotecas requeridas, las cuales se encuentran detalladas en la Figura 18. El procedimiento para instalar estas bibliotecas se encuentra detallado en el ANEXO D, mientras que la descripción de cada una de ellas se proporciona en el ANEXO E.

```
#include <Arduino.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Ticker.h>
```

Figura 18. Librerías utilizadas para el sistema RFID.

Al implementar las librerías necesarias, el primer paso conlleva establecer las configuraciones y variables esenciales para el funcionamiento efectivo del sistema RFID. Se asigna el pin PUERTA como una salida, el cual se utilizará para controlar la apertura y cierre de la puerta. Además, se define la variable TIME_APERTURA_PUERTA que determina el tiempo en segundos durante el cual la puerta permanecerá abierta después de activarse.

Para rastrear el estado de la puerta (abierto o cerrado), se inicializa la variable PUERTA_ESTADO. En la función setup(), se inician las configuraciones iniciales necesarias para el funcionamiento del programa. Se establece la comunicación serial a 115200 baudios para la interacción con la consola o monitor serial. Se configura el pin PUERTA como salida y se establece en un estado alto (puerta cerrada) como estado inicial.

Los buses SPI y el módulo RC522 (RFID) se inicializan para su operación, y se imprime un mensaje para señalar el inicio del sistema de control de acceso. En cuanto a la función loop(), representa el núcleo en constante actividad del programa. Durante su ejecución, se verifica la proximidad de nuevas tarjetas RFID mediante mfrc522.PICC_IsNewCardPresent(). Si se detecta una tarjeta válida, se lee su UID y se compara con los UID de usuarios autorizados. Si concuerda con algún UID permitido, se imprime "Acceso concedido" y se llama a Apertura_Puerta() para abrir la puerta. En caso contrario, si el UID no coincide con usuarios autorizados, se imprime "Acceso denegado" y la puerta permanece cerrada.

Después de procesar la tarjeta, la lectura se finaliza mediante mfrc522.PICC_HaltA(). Paralelamente, la función compareArray() se emplea para comparar dos arrays de bytes y determinar si son idénticos. Esta función asegura que los UID extraídos de las tarjetas RFID coincidan con los UID almacenados de los usuarios autorizados, garantizando un acceso controlado al sistema. Una sección a resaltar del código se refiere a la incorporación de nuevos usuarios al sistema para que este pueda reconocer las tarjetas de proximidad. Este proceso se realiza en la porción de código mostrada en la Figura 19. Aquí se inserta el UID único de cada usuario para que el sistema pueda contrastarlo cuando se pase la tarjeta por el sensor. Los detalles de cómo agregar nuevos usuarios se encuentra explicado en el ANEXO I.

```
byte ActualUID[4]; //almacenará el código del Tag leído
byte Usuario1[4]= {0x45, 0x7D, 0x08,     } ; //código del usuario 1
byte Usuario2[4]= {0xCC, 0xD7, 0x3A,     } ; //código del usuario 2
byte Usuario3[4]= {0x99, 0x29, 0x22,     } ; //código del usuario 3
```

Figura 19. Ingreso de UID de nuevos usuarios.

4.2.3.3. Funcionamiento de la programación de la cámara de fotografía de registro

Siguiendo la metodología establecida, es necesario elegir la placa que se empleará. En este contexto, se opta por la placa "AI Tinker ESP32-CAM", como se ilustra en la Figura 20. Es fundamental referirse a la guía de instalación de la placa en el ANEXO C para un procedimiento adecuado.

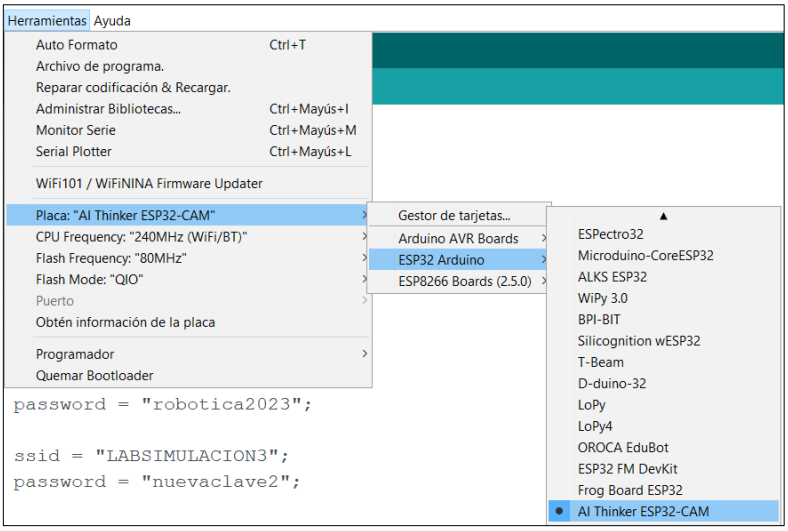


Figura 20. Selección de la placa AI Thinker ESP32-CAM.

Las bibliotecas empleadas en el programa están listadas en la Figura 21, e incluyen aquellas que facilitan la comunicación con la plataforma Telegram a través de comandos, como se detalla en el ANEXO E.

```
#include <Arduino.h>
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include "soc/soc.h"
#include "soc/rtc_cntl_reg.h"
#include "esp_camera.h"
#include <UniversalTelegramBot.h>
#include <ArduinoJson.h>
```

Figura 21. Librerías utilizadas en la cámara de fotografía de registro.

La cámara establece su comunicación a través de Telegram, que sirve como la plataforma de IoT empleada en este caso. Para lograr esta conexión, es esencial contar con acceso a internet. Se debe proporcionar el nombre de usuario y contraseña en la sección correspondiente del

código (ssid y password) para que la cámara pueda acceder a la red Figura 22. Además, para que la cámara se comunique con Telegram, es crucial introducir el "token", un código alfanumérico necesario para que el bot utilice la API de Bot de Telegram. Este token se obtiene al crear el bot en Telegram y el proceso se detalla en el ANEXO B.

```
const char* ssid = "usuario";
const char* password = "contraseña";
const String token = "token proporcionado por telegram";
String CHAT_ID = "ID del token";
```

Figura 22. Datos de la red Wifi y Token de Telegram.

Dentro del código las funciones `configInitCamera()` y `setup()` son responsables de la configuración inicial de la cámara y el entorno WiFi, respectivamente. La función `handleNewMessages()` gestiona los mensajes recién recibidos a través de Telegram y ejecuta acciones específicas basadas en el contenido del mensaje. Por otro lado, la función `sendPhotoTelegram()` se encarga de capturar una imagen mediante la cámara y enviarla a través de Telegram. Dentro del ciclo principal (`loop()`), se verifica el estado del sensor PIR y la necesidad de enviar una fotografía a través de Telegram. Si se detecta movimiento o se activa manualmente, se toma una imagen y se envía. Asimismo, se controla el tiempo para revisar y gestionar nuevos mensajes provenientes de Telegram.

4.2.3.4. Funcionamiento de la programación del control mediante IoT

La programación tiene como fin controlar tres partes fundamentales mostradas a continuación:

- **Control manual:** El control manual permite operar los sistemas principales, como la iluminación y la apertura de la puerta desde el interior del Laboratorio.
- **Control mediante IoT:** Se establece un sistema basado en el Internet de las cosas (IoT) para controlar los mismos elementos. Esto permitirá a los usuarios encender y apagar los dispositivos de manera remota a través de una plataforma conectada a la red.
- **Control automatizado:** El sistema estará equipado con sensores capaces de detectar la presencia o ausencia de personal en el laboratorio. De esta forma, si se deja la iluminación encendida y no hay nadie presente, el sistema se encargará automáticamente de apagarla para evitar el desperdicio innecesario de energía.

En la Figura 23 se presentan las librerías que se utilizarán en este sistema. Para obtener más detalles sobre el funcionamiento e instalación de cada una de ellas, se puede consultar el ANEXO D y ANEXO E. En dichos Anexos, se proporciona una descripción completa de cada

librería, así como las instrucciones paso a paso para su correcta implementación y configuración en el sistema.

```
#include <WiFi.h>
#include <Ticker.h>
#include "CTBot.h"
```

Figura 23. Libreas del del sistema de control IoT.

En la primera parte cabe destacar la importación de bibliotecas las cuales son:

- **WiFi.h:** se utiliza para establecer la conectividad.
- **Ticker.h:** sirve para la programación de tareas periódicas que haciendo referencia al sistema de apagado automático de las luminarias y senos de los botones manuales.
- **CTBot.h:** para la integración con Telegram como demuestra para el control mediante IoT además de funcionar para él diseño de un teclado en Telegram.

En la Figura 24 se muestra la declaración de funciones Ticker, esta función sirve para repetir periódicamente una acción sin que esta se encuentre en el bucle principal void loop().

```
PIR_IN_TcK.attach(0.15, Encendido_Lum_PIR_IN);
PIR_IN_TIME_TcK.attach(T_LUCES_IN, TIME_Lum_PIR_IN);
PIR_IN_TIME_TcK.detach();
```

Figura 24. Función Ticker de las luminarias.

La librería Ticker se emplea para la gestión de dos componentes fundamentales:

- **Pulsadores:** Se realiza un muestreo periódico de los pulsadores para detectar si han sido activados.
- **Luminarias:** Se registra el tiempo durante el cual las luces permanecen encendidas. Si transcurrido un periodo determinado las luminarias aún están encendidas y el sensor de presencia no detecta actividad en el laboratorio, se procede a apagarlas de manera automática.

La Figura 25 ilustra la sección donde se crea el teclado para la interfaz de Telegram.

```
miTeclado.addButton("luces ON", "LON", CTBotKeyboardButtonQuery);
miTeclado.addButton("luces OFF", "LOFF", CTBotKeyboardButtonQuery);
miTeclado.addRow();
```

Figura 25. Función de teclado CTBot.

El teclado en la Figura 26 desempeña diversas funciones clave, las cuales se detallan a continuación:

- **"Abrir la puerta":** Permite la apertura de la puerta mediante Telegram.
- **"Luces ON/OFF":** Facilita el control de encendido y apagado de las luces interiores del laboratorio.
- **"Luces afuera ON/OFF":** Posibilita el control de encendido y apagado de las luces exteriores del laboratorio.
- **"T1 ON/OF":** Proporciona la capacidad de encender o apagar el suministro eléctrico en los tomacorrientes, abarcando desde el tomacorriente 1 al 4.
- **"Infórmate":** Ofrece acceso al manual de usuario detallado del sistema para brindar información completa sobre su operación y características.

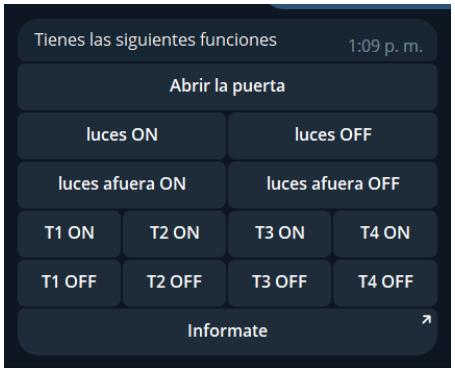


Figura 26. Interfaz del teclado en Telegram.

4.2.3.4.1. Funcionamiento del sistema de control por medio de IoT

El control vía Telegram mediante IoT de tomacorrientes, luminarias y la apertura de puerta posibilita a los usuarios encender o apagar estos dispositivos en un entorno físico, utilizando la plataforma de mensajería Telegram y aprovechando el concepto de Internet de las Cosas (IoT). Para llevar a cabo estas acciones, se emplea un método de control de lazo abierto como se muestra en la Figura 27.

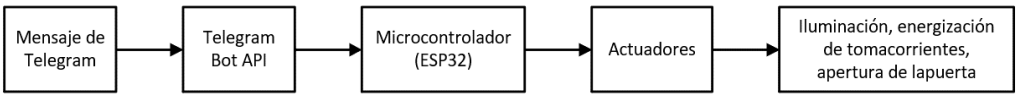


Figura 27. Diagrama de control por Telegram.

En este sistema, los tomacorrientes, luminarias y puerta cuentan con actuadores que se conectan a la placa PCB, la cual incorpora un módulo ESP32. Este módulo se conecta a Internet a través

de WiFi y se vincula con la API de Bots de Telegram, lo que posibilita la interacción mediante mensajes entre el bot y el usuario.

El dispositivo puede recibir comandos enviados desde la aplicación Telegram y ejecutar las acciones correspondientes, como activar o desactivar los tomacorrientes, controlar la iluminación o abrir la puerta. Estas interacciones se realizan a través de mensajes de texto o pulsando los botones de la interfaz, que el usuario envía por medio de Telegram. Además, se muestra un mensaje en la parte superior de Telegram para indicar si la acción se completó exitosamente.

A pesar de que el control de lazo abierto implica que el sistema no reciba retroalimentación directa, la confirmación de que la acción se ha llevado a cabo correctamente se exhibe en la parte superior de Telegram. El usuario envía comandos a través de Telegram y, a su vez, recibe una notificación de confirmación una vez que se ha ejecutado la acción.

Por ejemplo, si el usuario emite un comando para encender las luminarias, el bot de Telegram a través de IoT transmitirá la señal a la placa ESP32, que ejecutará la acción de encendido según el comando recibido. Tras completar la acción, la placa ESP32 enviará una confirmación de que las luces han sido encendidas. Similarmente, si el usuario envía un comando para abrir la puerta, el sistema responderá al comando y enviará una verificación de que la puerta ha sido abierta, como se visualiza en la Figura 28.

Figura 28. Retroalimentación del sistema de control IoT.

4.2.4. Diagramas de funcionamiento

En esta sección se proporcionan los diagramas de flujo correspondientes a la sección de programación, ofreciendo una presentación más intuitiva y fácil de entender. Esta sección se divide en tres partes: el funcionamiento del reconocimiento facial, el funcionamiento del sistema RFID y el funcionamiento de la cámara de registro fotográfico.

4.2.4.1. Flujograma del reconocimiento facial

Para una mejor comprensión visual del funcionamiento del código, se presenta el diagrama de flujo del proceso de reconocimiento facial en la Figura 29.

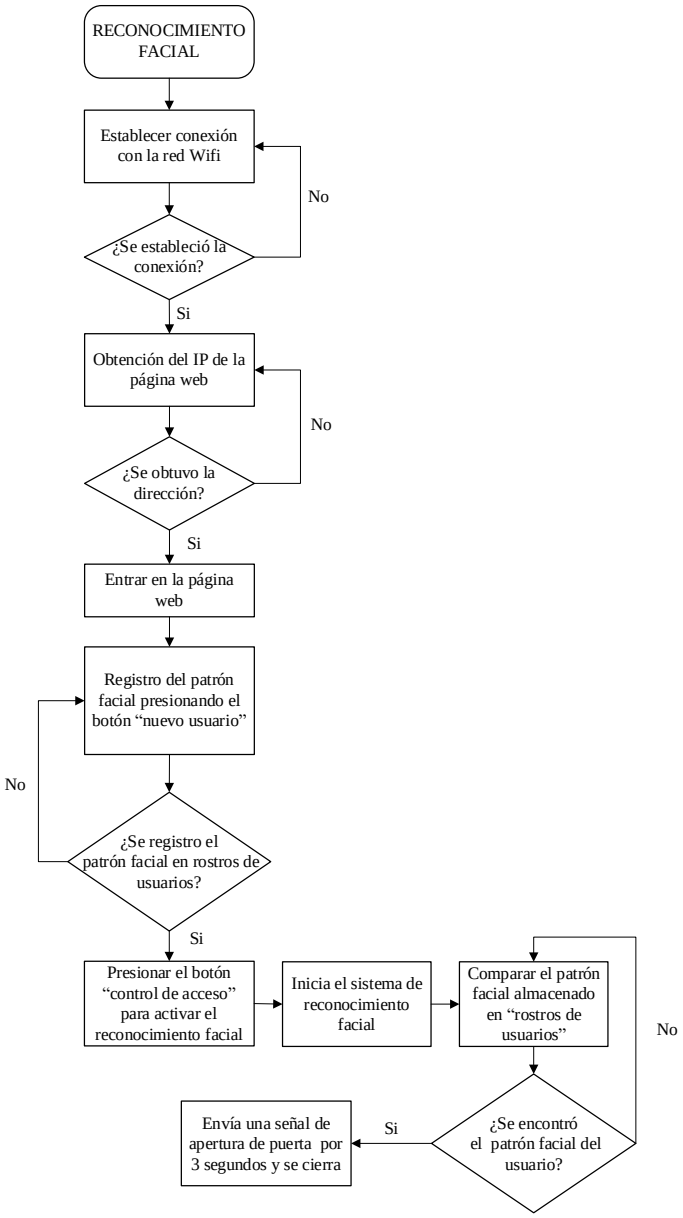


Figura 29. Flujograma del sistema de reconocimiento facial.

En la Figura 29, se puede observar que, al iniciar el programa, se requiere la conexión a una red Wi-Fi. Una vez conectado a la red, se asignará una dirección IP que llevará al usuario a una página web, ilustrada en la Figura 16. En esta página web, es posible ingresar patrones faciales de nuevos usuarios, asignándoles un nombre y guardándolos en la base de datos de rostros de usuarios.

Una vez almacenados los rostros, es posible activar el sistema al presionar el botón "Control de Acceso". Esto dará inicio al proceso de reconocimiento facial. Cuando un usuario registrado se coloque frente a la cámara, el dispositivo lo reconocerá y enviará una señal para abrir la puerta, permitiendo el acceso. En el caso contrario, si el usuario no está registrado en el sistema, no se enviará ninguna señal, lo que resultará en la negación de acceso.

En esta situación, si el administrador del sistema necesita otorgar acceso a otra persona, deberá registrarla en la base de datos. Solo el administrador puede llevar a cabo este registro, ya que únicamente él conocerá la dirección de la página web para el registro. Además, dicha página solo puede abrirse en un único dispositivo y con la red que se encuentra especificada en el código. Esto evita que personas no autorizadas puedan registrarse en el sistema.

4.2.4.2. Flujograma del sistema RFID

El diagrama de flujo detallado del sistema de detección de tarjetas y llaveros RFID está disponible en la Figura 30, proporcionando una representación visual de su operación.

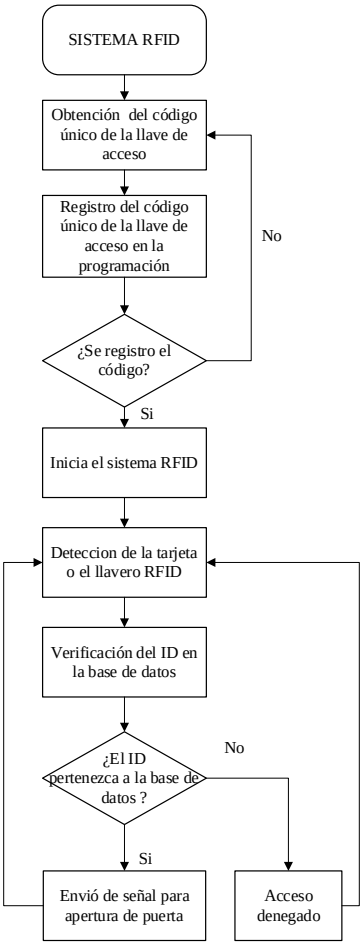


Figura 30. Flujograma del sistema RFID.

El sistema funciona de la siguiente manera: cuando una tarjeta o llavero se desliza sobre el sensor RFID, este compara las claves con la base de datos almacenada en el sistema. Si la coincidencia es positiva, el sistema enviará una señal para activar la apertura de la puerta, permitiendo el acceso. Por otro lado, si la clave no está en la base de datos, el sistema restringirá el acceso a la persona no registrada. Para registrar un nuevo usuario, el administrador del laboratorio deberá obtener el código de la tarjeta o llavero y añadirlo al programa, luego subir el nuevo código al microcontrolador.

4.2.4.3. Flujograma del sistema de fotografía de registro

El sistema de registro fotográfico se divide en dos componentes principales. El primero, que se muestra en el diagrama de flujo de la Figura 31, consiste en esperar un mensaje en Telegram. En caso de recibir una solicitud, se procede a enviar la fotografía correspondiente.

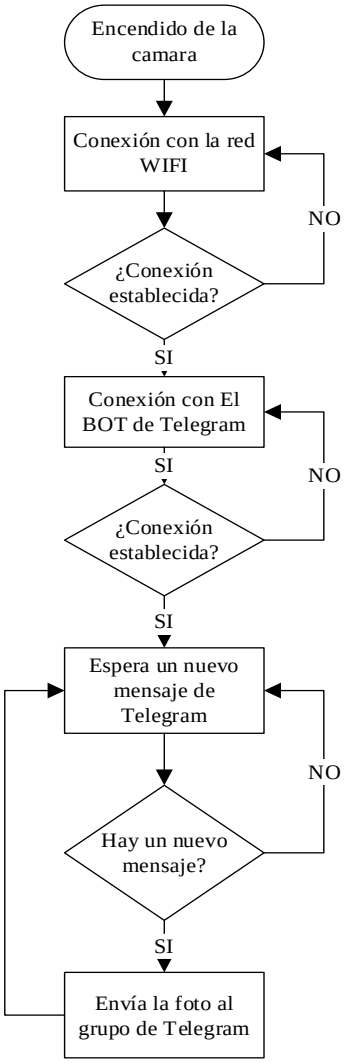


Figura 31. Flujograma del sistema de fotografía de registro con Telegram.

En segundo lugar, el sistema ha sido concebido para supervisar la detección de movimiento mediante el uso de un sensor de movimiento. Cuando esta función es activada, la captura y envío de fotografías se desencadenan automáticamente al detectar movimiento, como se representa en el diagrama de flujo de la Figura 32.

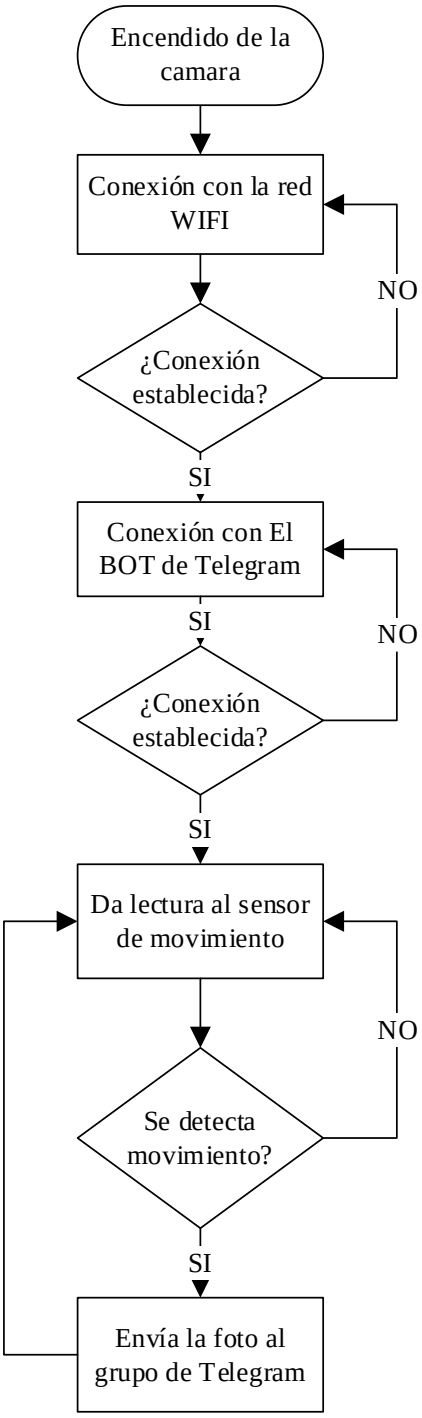


Figura 32. Flujograma del sistema de fotografía de registro con el sensor PIR.

4.2.4.4. Flujograma del sistema de control IoT

El sistema de control IoT se descompone en tres partes esenciales:

- **Funcionamiento Manual:** Incluye una botonera que habilita la apertura de la puerta y el encendido de las luces tanto internas como externas.
- **Funcionamiento Automático:** Aborda la función de apagado automático de las luminarias tras un período de inactividad.
- **Funcionamiento a través de IoT:** Engloba la habilidad de controlar la puerta, así como activar las luces internas y externas de manera remota por medio de la plataforma de Telegram.

4.2.4.4.1. Flujograma del control manual del sistema de control IoT

El sistema de control manual se implementará mediante tres pulsadores que habilitarán la apertura de la puerta, así como el encendido y apagado de las luminarias internas y externas, como se muestra en el diagrama de flujo de la Figura 33. Esta funcionalidad ha sido concebida para operar de manera autónoma, sin depender de una conexión a Internet.

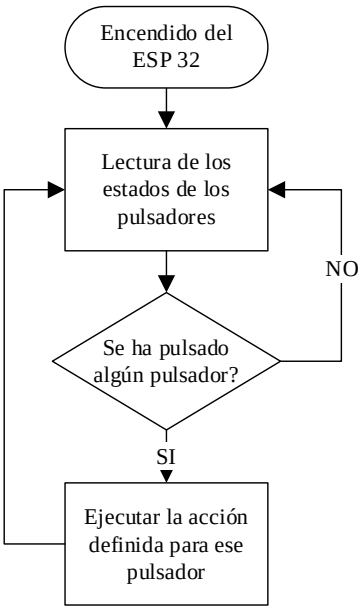


Figura 33. Flujograma del control manual del sistema de control IoT.

4.2.4.4.2. Flujograma del control automático del sistema de control IoT

El flujograma representado en la Figura 34 ilustra el funcionamiento del sistema de control automático. Principalmente, actúa como un temporizador que permite apagar las luces después de un período de inactividad registrado por el sensor. Esto se hace con el propósito de evitar

que las luces permanezcan encendidas constantemente, reduciendo así el consumo de electricidad y evitando el desperdicio de energía.

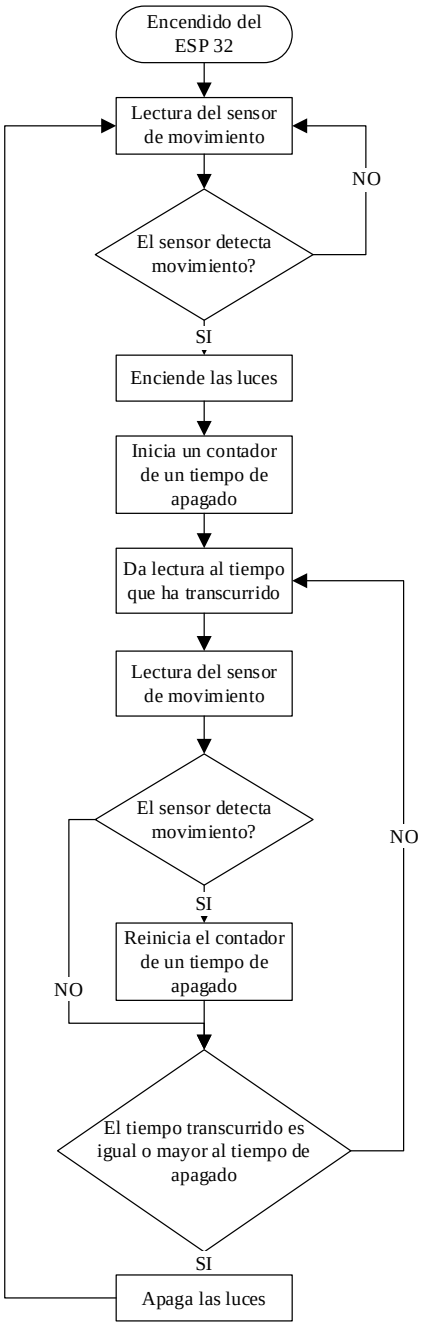


Figura 34. Flujograma del control automático del sistema de control IoT.

4.2.4.4.3. Flujograma del control remoto del sistema de control IoT

La Figura 35 muestra un diagrama de flujo del sistema de control a través de IoT. Este proceso inicia con la conexión a Internet, seguida por la interacción con el Bot de Telegram y, finalmente, la espera de nuevos mensajes para ejecutar las acciones programadas.

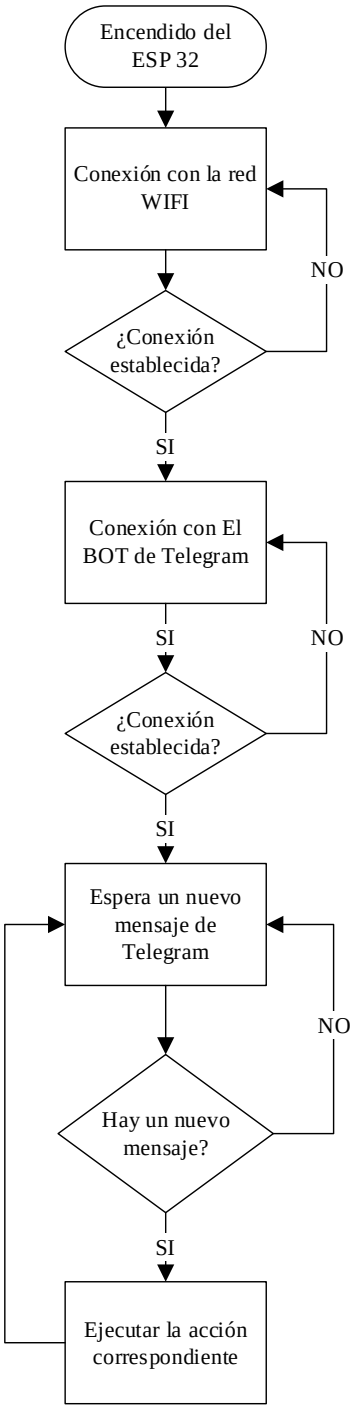


Figura 35. Flujograma del control remoto del sistema de control IoT.

4.2.5. Funcionamiento

En esta sección, se detalla el propósito y la función de cada uno de los comandos presentes en la interfaz de Telegram, tanto en relación con la cámara de registro fotográfico como en el control de las luminarias, así como en la interfaz del reconocimiento facial.

4.2.5.1. Comandos del sistema de fotografía de registro

El sistema de registro fotográfico tiene la función de capturar imágenes de las personas que ingresan al laboratorio, lo que posibilita el seguimiento de las entradas y salidas. Para acceder a las opciones del sistema a través del bot, es necesario enviar el comando /config, como se muestra en la Figura 36. Asimismo, se cuentan con comandos específicos en la Tabla 15 para activar o desactivar las distintas funciones de la cámara según se requiera.

Tabla 15 Comandos del sistema de fotografía de registro.

COMANDO	ACCIÓN
/CONFIG	Muestra un listado de opciones
/FOTO	Realiza la acción de capturar una fotografía y luego la remite a través de la plataforma de Telegram.
/PIRON	Habilita el sensor de movimiento (PIR) para detectar cualquier movimiento y procede a enviar fotografías cuando se detecte actividad.
/PIROFF	Desactiva el sensor de movimiento y detiene el envío de fotos en caso de detectar movimiento.

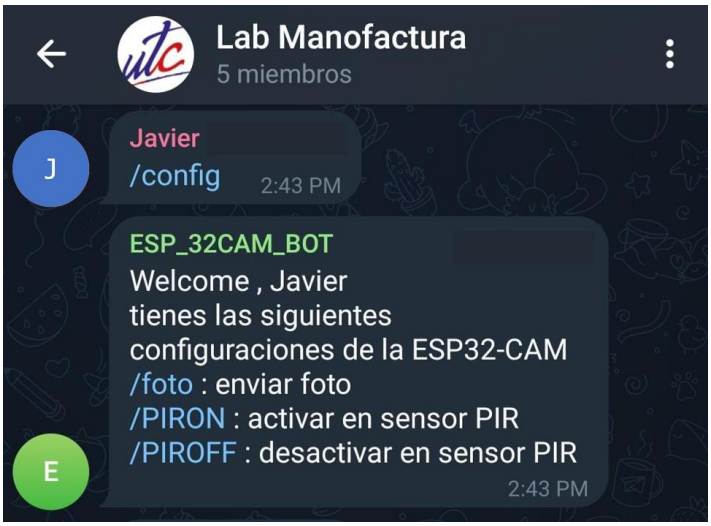


Figura 36. Comandos mostrados al enviar el comando “/config”.

4.2.5.2. Comandos para el sistema de control IoT

El sistema ofrece la posibilidad de controlar las luminarias, los tomacorrientes y la apertura de la puerta a través de un teclado integrado en Telegram. Para acceder a este teclado, simplemente se debe ingresar el comando "opciones", tal como se ilustra en la Figura 37.

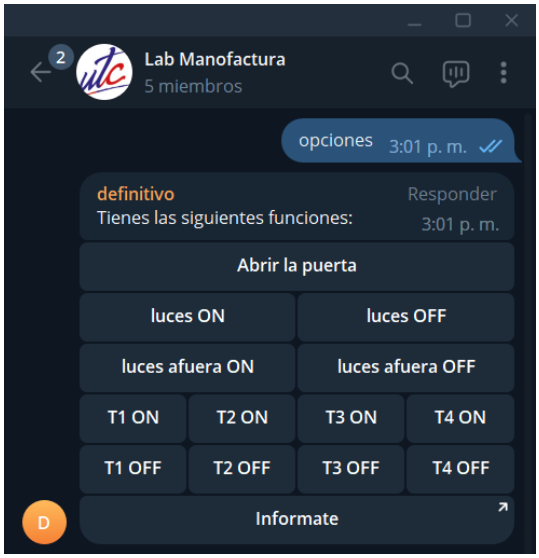


Figura 37. Comando “opciones” del sistema IoT.

Las funciones se detallan en la Tabla 16 en donde se encuentran cada uno de los elementos.

Tabla 16 Funciones del teclado del sistema IoT en Telegram.

BOTON	ACCIÓN
Comando “Opciones”	Devuelve la botonera en donde se encuentran las diferentes acciones que se pueden realizar.
Abrir la puerta	Permite la apertura de la puerta.
LUCES ON	Enciende las luces internas del laboratorio.
LUCES OFF	Apaga las luces internas del laboratorio.
LUCES AFUERA ON	Enciende las luces exteriores del laboratorio.
LUCES AFUERA ON	Apaga las luces exteriores del laboratorio.
T1 ON	Activa la alimentación del tomacorriente número uno.
T1 OFF	Desactiva la alimentación del tomacorriente número uno.
T2 ON	Activa la alimentación del tomacorriente número dos.
T2 OFF	Desactiva la alimentación del tomacorriente número dos.
T3 ON	Activa la alimentación del tomacorriente número tres.
T3 OFF	Desactiva la alimentación del tomacorriente número tres.
T4 ON	Activa la alimentación del tomacorriente número cuatro.
T4 OFF	Desactiva la alimentación del tomacorriente número cuatro.
Infórmate	Abre un link en donde está el manual de usuario del sistema.

4.2.5.3. Comandos reconocimiento facial

El sistema de control de acceso dispone de una interfaz web que puede ser accedida a través de la dirección IP proporcionada por la ESP32-CAM, tal como se detalló previamente en la sección de programación. A continuación, se destacan las funciones asociadas a cada uno de los botones de la interfaz web, la Tabla 17 detalla la función que cumple cada botón.

Tabla 17 Acciones de los botones de la interfaz del reconocimiento facial

BOTONES	ACCIÓN
INICIAR CAMARA	Inicia la cámara de la placa ESP32-CAM.
DETECTAR ROSTRO	Detecta rostros
NUEVO USUARIO	Registra al nuevo usuario que se desea agregar.
CONTROL DE ACCESO	Inicia el sistema para su funcionamiento y comienza a comparar los rostros capturados con los rostros previamente registrados.
ELIMINAR TODO	Elimina a todos los usuarios agregados.

En la Figura 38 se presenta la interfaz que incluye un campo de texto destinado a ingresar el nombre del nuevo usuario que se desea registrar. Una vez que se ha ingresado el nombre, al presionar el botón "Nuevo Usuario", el sistema procederá a almacenar el rostro del usuario en la sección de "Rostros de Usuarios".

Figura 38. Interfaz del reconocimiento facial.

Una vez que los rostros han sido almacenados, simplemente se debe presionar el botón "Control de Acceso" para poner en funcionamiento el sistema.

4.2.6. Diseño de placas electrónicas

En esta sección se presenta un análisis detallado del diseño de las placas electrónicas relacionadas con los sistemas de control de acceso, registro fotográfico y IoT. Además, se suministran descripciones de los diagramas esquemáticos asociados con cada uno de estos sistemas.

4.2.6.1. Diseño de la PCB del sistema cámara de fotografía de registro

La Figura 39 muestra el diseño de la placa, ha sido planteado para mantener una estructura compacta de 40x40 mm. Se ha considerado cuidadosamente la disposición de los pines de salida GND, RX y TX, lo que permite programar el módulo sin tener que desconectarlo de la placa.

Además, se ha incorporado el uso de conectores hembra para el sensor PIR y el módulo ESP32CAM, lo que facilita tanto su conexión como su desconexión.

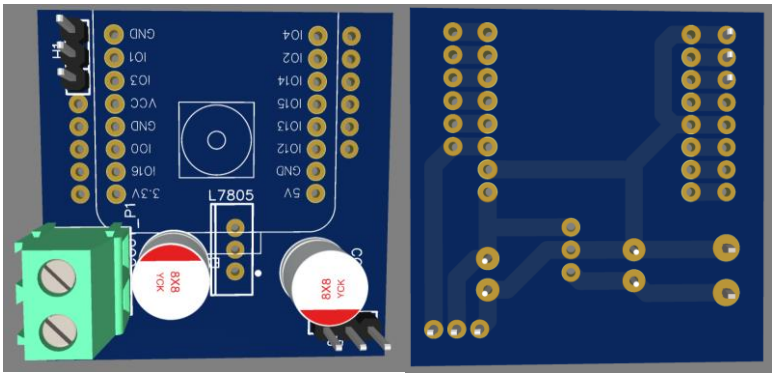


Figura 39. PCB del sistema de fotografía de registro.

El módulo regulador de voltaje incluye condensadores de filtrado con el propósito de mitigar cualquier interferencia proveniente de la fuente de alimentación, tal como se expone en el esquema de la Figura 40. En la placa, únicamente se presentan pines de conexión que están dispuestos en una bornera para suministrar una tensión de 12V al circuito.

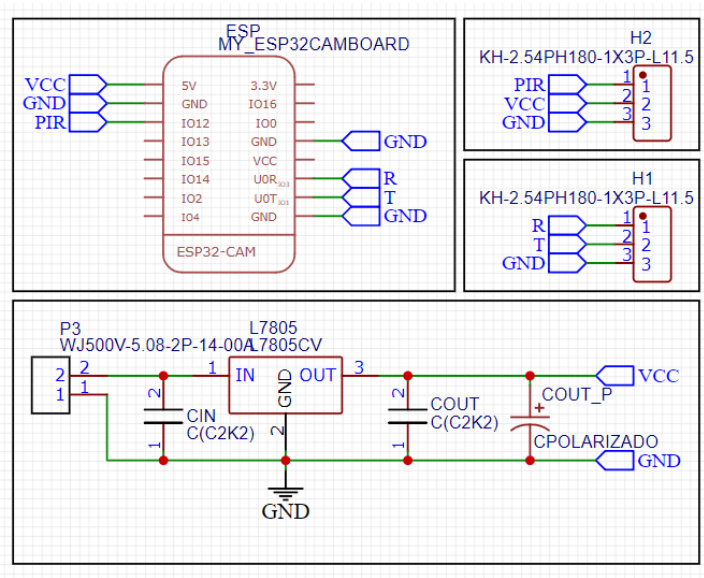


Figura 40. Esquemático del sistema de fotografía de registro.

4.2.6.2. Diseño de la PCB del sistema de control de acceso al laboratorio

El diseño de la PCB que se presenta en la Figura 41 está compuesto por una placa de dimensiones 4x7 centímetros en ancho y largo, respectivamente. En esta placa se encuentran ubicados los componentes electrónicos esenciales para garantizar su funcionamiento adecuado. Entre estos elementos, destacan la ESP32 CAM, los LEDs de indicación visual junto con sus

correspondientes resistencias, además de la fuente de alimentación de la placa y las salidas de control.

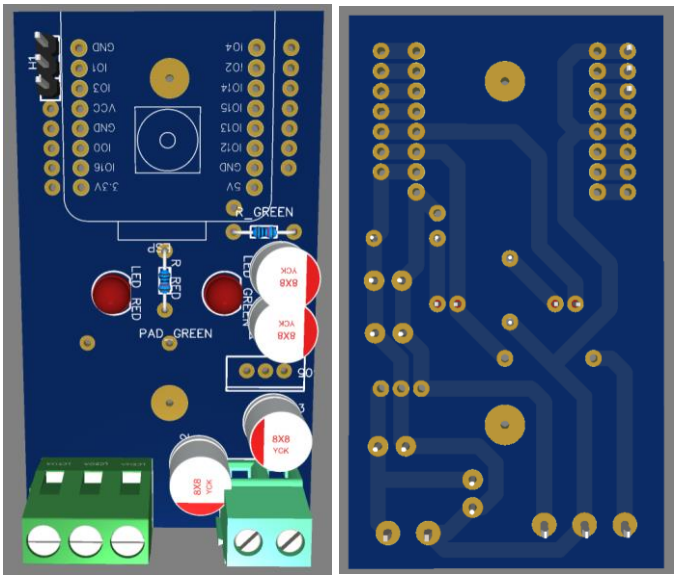


Figura 41. PCB del sistema de control de acceso.

Adicionalmente, esta placa incluye un componente integrado que permite la regulación del voltaje procedente del UPS, que originalmente es de 12V, como se indica en el esquema de la Figura 42. Este componente ajusta la alimentación del sistema a 5V, el voltaje necesario para el funcionamiento adecuado del dispositivo.

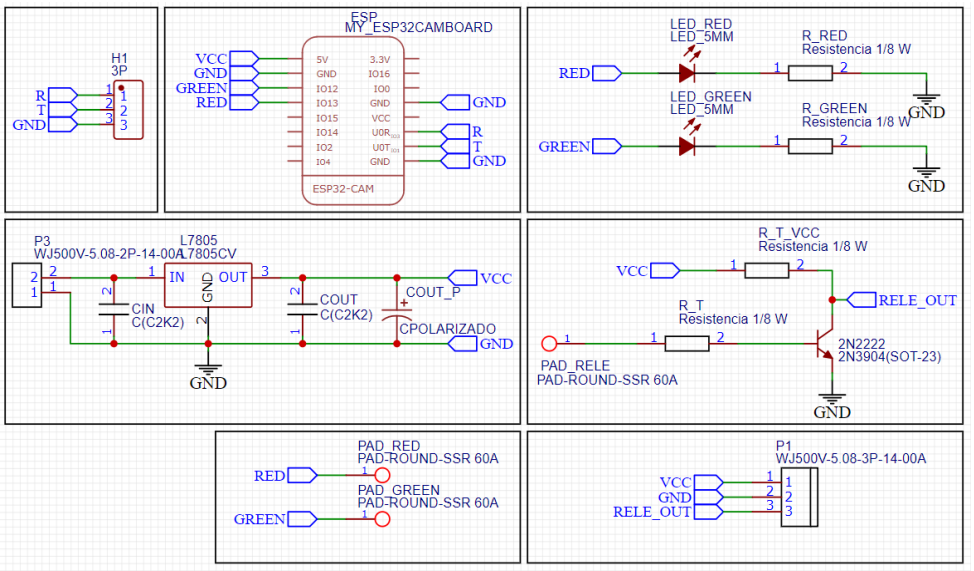


Figura 42. Esquemático sistema de control de acceso.

4.2.6.3. Diseño de la PCB del sistema de control IoT

En la Figura 43 se presenta el diseño de la placa de circuito impreso (PCB), la cual ha sido concebida para simplificar la interconexión de un módulo ESP32 y para permitir una fácil conexión de los pines de control hacia los diversos componentes del sistema, como luminarias, tomas de corriente, sensores y actuadores.

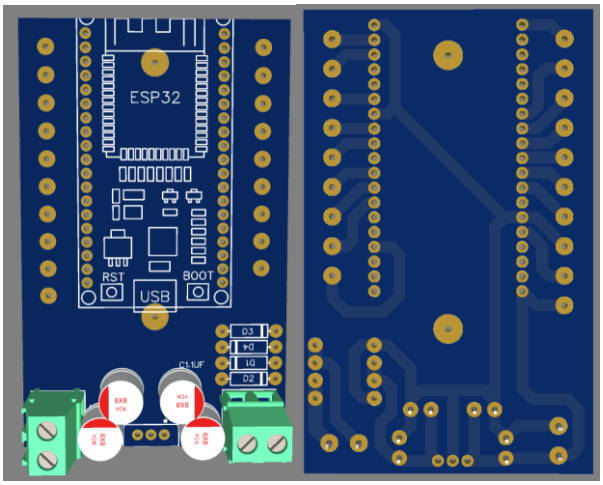


Figura 43. PCB del sistema de control IoT.

Adicionalmente, se ha implementado un sistema de alimentación que garantiza una salida constante de 5V, independientemente de la polaridad del voltaje de entrada. Este sistema de alimentación también provee la energía necesaria para la ESP32, como se ilustra en el esquema de la Figura 44.

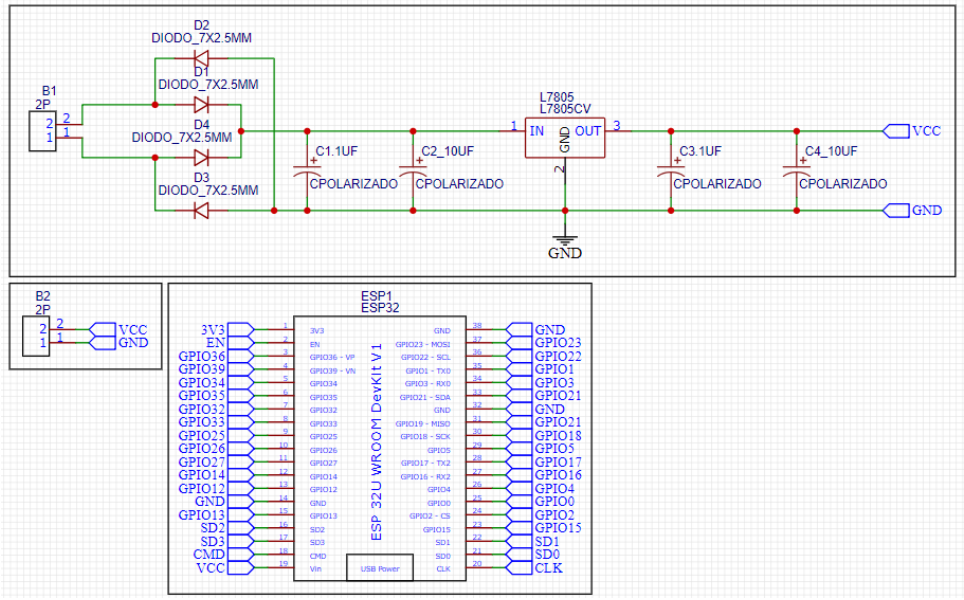


Figura 44. Esquemático del sistema de control IoT.

4.2.7. Diseño 3D

En esta sección se presentan los diseños en tres dimensiones (3D) que se elaboraron, abarcando elementos tales como el portero eléctrico, el sistema de registro fotográfico y la botonera. Estos diseños se han desarrollado utilizando la herramienta de modelado Fusión 360, conocida por su eficacia en este tipo de proyectos. Para todas las impresiones, se ha empleado el material PLA, que se destaca por su resistencia y capacidad para mantener su estructura sin deformaciones, asegurando de esta manera la durabilidad de los componentes.

4.2.7.1. Diseño 3D del sistema de fotografía de registro

Dado que la cámara de registro fotográfico se ubicará en el techo, es esencial proporcionarle una carcasa que la mantenga y proteja. Para esta finalidad, se ha desarrollado un diseño tridimensional (3D), como se muestra en la Figura 45. Este diseño dispone de un amplio espacio interno para alojar diversos componentes, como un sensor PIR, la placa de la cámara y el módulo ESP32-CAM. Adicionalmente, se ha implementado un mecanismo de ajuste que permite modificar los ángulos de visión de la cámara y realizar rotaciones según las necesidades. Puedes consultar los planos detallados en el ANEXO H.

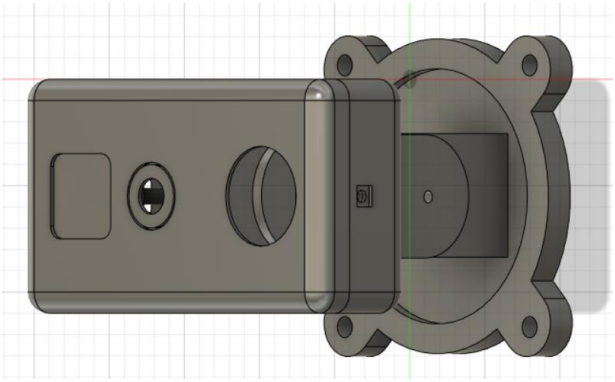


Figura 45. Diseño 3D del sistema de fotografía de registro.

4.2.7.2. Diseño 3D del sistema de control de acceso (Portero electrónico)

El diseño actual se corresponde con un modelo de portero electrónico, representado en la Figura 46, que incluye áreas designadas para la integración de los componentes de reconocimiento facial y del sistema de Identificación por Radio Frecuencia (RFID). Las medidas del portero electrónico se encuentran especificadas en el ANEXO H para su consulta.

Figura 46. Diseño 3D del sistema de control de acceso (Portero electrónico).

4.2.7.3. Diseño 3D de la botonera

Dado que se reconoce la importancia de contar con un control manual, se ha tomado en consideración la elaboración de una botonera, cuyo diseño se muestra en la Figura 47. Esta botonera habilita el control de las luces tanto en el interior como en el exterior, además de facilitar la apertura de la puerta. Es relevante señalar que este diseño está posicionado en el interior del laboratorio.

Figura 47. Diseño 3D de la Botonera.

4.2.8. Dimensionamiento sistema de respaldo de energía

4.2.8.1. Dimensionamiento del UPS para el diseño del sistema

Para dimensionar adecuadamente el sistema de respaldo de energía, se realizó una evaluación del consumo en vatios de cada componente del diseño. Esta información se multiplicó por la cantidad necesaria de cada elemento que se requiere instalar. Una vez recopilados estos datos, se efectuó la conversión a voltamperios (VA) mediante la multiplicación de los vatios por el factor de potencia correspondiente.

Posteriormente, todos los valores en VA se sumaron para obtener el consumo total del sistema. Una vez que se determinó el consumo total, se aplicó una estrategia de sobredimensionamiento.

En la mayoría de los casos, se opta por un sobredimensionamiento del 50%. Esta práctica se adopta con el fin de garantizar una reserva de energía en caso de conectar dispositivos adicionales, además de aquellos propuestos originalmente en el sistema el proceso descrito se puede observar en la Tabla 18 .

Tabla 18 Dimensionamiento del UPS para el diseño del sistema.

DESCRIPCIÓN	CANTIDAD	CONSUMO(W)	TOTAL(W)	TOTAL(VA)
ESP32	1	0.5	0.5	0.6
ESP32-CAM CON LA OV2640	2	1	2	2.2
ESP8266	1	0.3	0.3	0.3
MODULO RFID	1	0.3	0.3	0.3
SENSOR PIR	6	0.05	0.3	0.3
MODULO RELE 2 VIAS	2	0.5	1	1.1
MODULO RELE 4 VIAS	1	0.7	0.7	0.8
CERRADURA ELÉCTRICA	1	10	10	11.1
LUMINARIA OJO DE BUEY	1	5	5	5.6
REUTER	1	20	20	22.2
SENSOR SW-18010P	22	0.05	1.1	1.2
BOCINA DE ALARMA DE 116DB	3	10	30	33.3
ESP32-CAM CON LA OV5640	10	1	10	11.1
LUMINARIAS CON LUCES NEUTRAS O FRIAS (4000K - 5000K) DE 1200 - 2000 LM A 35 - 40W	10	40	400	444.4
LUMINARIAS CON LUCES FRIAS (5000K - 6500K) DE 2000 - 3000 LM A 45 - 60W	6	60	360	400.0
SENSOR MQ-2	2	0.5	1	1.1
TUBO FLUORESCENTE	6	20	120	133.3
INPRESORA 3D	5	500	2500	2777.8
LAPTOP	8	200	1600	1777.8
TOTAL			5062.2	5624.7
SOBREDIMENCIONAMIENTO 50%			1.5	8437.0

Tal como se detalla en la Tabla 18 se identificó la necesidad de adquirir un sistema de alimentación ininterrumpida (UPS) capaz de cubrir la demanda total de 8437 VA. Tras una búsqueda exhaustiva, se seleccionó un UPS comercial que cumple con este requisito: el modelo UPS CDP ON LINE UPO22-10AX.

Este UPS presenta una capacidad de suministro de 9000W, lo que lo hace idóneo para satisfacer el consumo total requerido. Este modelo se encuentra representado en la Figura 48.

Figura 48. UPS CDP ON LINE UPO22-10AX.

Para determinar la duración del UPS, es crucial obtener los datos precisos de las baterías. Esta información se localiza en el datasheet del propio UPS. Al consultar dicho documento, se estableció que el UPS requiere de 20 baterías de 12V con una capacidad de 9Ah, como se ilustra en la Figura 49.

Baterías		
Tipo/cantidad batería		12V/9Ah x 20
Tiempo de recarga		4 a 5 horas al 90%
Corriente de carga		1,0 Ah (opcional 4 Ah)
Voltaje de carga		273VDC +/-1%
Tiempo de autonomía		5 minutos a plena carga - 10 minutos a media carga

Figura 49. Datos de las baterías del UPS.

El proceso inicial involucra la multiplicación del voltaje por la capacidad en amperios-hora (Ah). Luego, se multiplica este resultado por el número total de baterías para obtener el total en voltamperios-hora (VAh). Posteriormente, se divide el consumo total sin considerar el sobredimensionamiento por los VAh totales de las baterías. Este cálculo arroja un resultado en horas, que equivale a 0.3840 horas. Si lo convertimos a minutos, obtenemos 23.0413 minutos. No obstante, es crucial ajustar este valor por las pérdidas de descarga funcional para determinar la duración real de la batería, que es de 18.433 minutos, tal como se detalla en la Tabla 19 .

Tabla 19 Autonomía del UPS con el consumo total.

	V	AH	N° BATERIAS	TOTAL (VAH)
BATERIA	12	9	20	2160
TIEMPO DE FUNCIONAMIENTO			0.38402276	Horas
			23.0413654	Minutos
PERDIDAS POR FUNCIONALIDAD DE DESCARGA			18.4330923	Minutos

Es relevante destacar que esta duración puede aumentar en caso de que elementos como las impresoras 3D y las laptops mencionadas en la Tabla 18 no estén conectadas. Al realizar el cálculo pertinente, se observa una autonomía de 96.977 minutos o 1.30 horas, como se aprecia

en la Tabla 20 . Esta consideración demuestra cómo el sistema puede adaptarse a diferentes escenarios de consumo para garantizar una óptima duración durante un corte de energía.

Tabla 20 Autonomía del UPS sin impresoras 3D y laptops.

	V	AH	N° BATERIAS	TOTAL (VAH)
BATERIA	12	9	20	2160
TIEMPO DE FUNCIONAMIENTO			2.02036999	Horas
			121.222199	Minutos
PERDIDAS POR FUNCIONALIDAD DE DESCARGA			96.9777593	Minutos

4.2.8.2. Dimensionamiento del UPS para la implementación

El sistema respaldo de energía debe tener la capacidad de ofrecer una fuente de respaldo en caso de interrupciones en el suministro eléctrico. Esto es crucial ya que el sistema de cierre de la puerta opera con electricidad y necesita un suministro constante de energía. Para elegir la fuente de energía apropiada, varios factores deben ser tomados en cuenta.

En primer lugar, es esencial considerar la tensión necesaria, tal como se presenta en la Tabla 21 para los sistemas instalados, así como para la cerradura magnética utilizada en el mecanismo de cierre de la puerta.

Tabla 21 Tenciones de alimentación de los distintos sistemas.

DESCRIPCIÓN	TENCIÓN DE ALIMENTACIÓN
CHAPA MAGNÉTICA	12 V – 24 V
SISTEMA CONTROL IOT	7.5 V – 37 V
SISTEMA DE CONTROL DE ACCESO	7.5 V – 37 V

Adicionalmente, es esencial considerar los consumos individuales detallados en la Tabla 22 Tabla 22 para cada uno de los componentes presentes en el sistema. Esto permitirá calcular la capacidad necesaria de la fuente de alimentación de respaldo.

Tabla 22 Consumo energético de los distintos sistemas.

DESCRIPCIÓN	CONSUMO
CHAPA MAGNÉTICA	500 mA
SISTEMA DE RECONOCIMIENTO FACIAL	250 mA
SISTEMA RFID	170 mA
SISTEMA DE CONTROL IOT	260 mA
SISTEMA DE VIGILANCIA REMOTA	225 mA
CONSUMO TOTAL	1405 mA

Dentro de los requisitos, se optó por un sistema respaldo de energía ZKTeco de 12V. Esta fuente es de regulación lineal, lo que evita la generación de ruido en contraste con las fuentes conmutadas. Además, se acompaña de una batería de 12V y 7A. A continuación, procederemos a realizar el cálculo correspondiente para determinar la duración de la batería.

Para hallar el tiempo en horas de autonomía se considera la ecuación 1.

$$h = \frac{W_B}{W_C} \tag{1}$$

En donde W_b es la potencia de la batería y W_c la potencia de la carga ambas en [Wh], para determinar la potencia se utiliza la ecuación 2.

$$W = V \cdot I \tag{2}$$

Sustituyendo los valores de la capacidad de la batería y la carga total en la ecuación:

$$h = \frac{12 \cdot 7}{12 \cdot 1.405} = 4.98$$

La estimación proporciona una duración aproximada de 5 horas para la autonomía del sistema. Esto asegura la capacidad del sistema respaldo de energía que la fuente de alimentación pueda mantener la operación del sistema de cierre de la puerta y otros componentes críticos en situaciones de cortes de energía.

4.3. DIAGRAMA DE CONEXIÓN GENERAL DEL SISTEMA DESARROLLADO

La Figura 50 ilustra la interconexión de los sistemas denominados control IoT, reconocimiento facial, RFID y de vigilancia. En este diagrama, se presenta cómo el sistema RFID tiene la función de controlar la apertura de la puerta, activado por medio de la identificación de tarjetas, llaveros, el sistema de reconocimiento facial o el sistema de control IoT. Además, los sistemas de control IoT y de registro fotográfico se ocupan de establecer la conexión con Telegram.

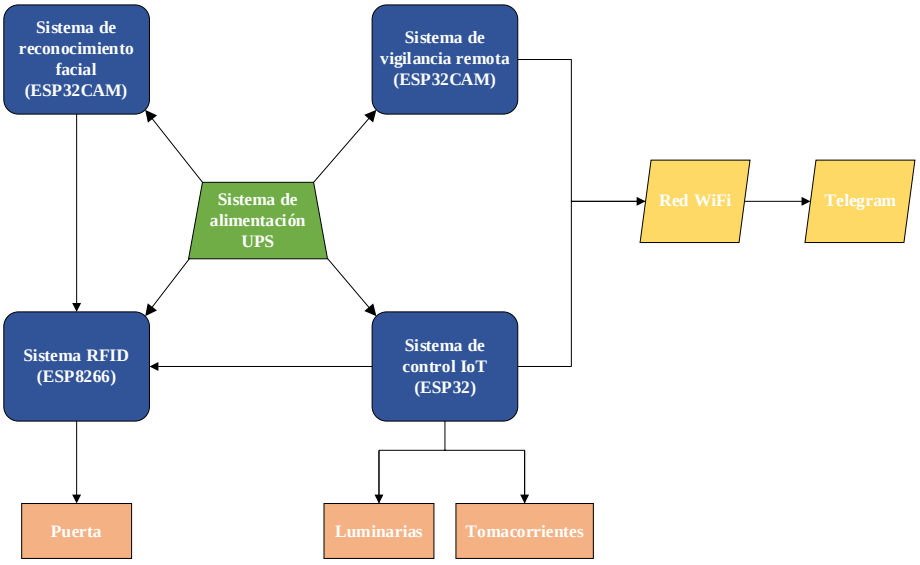


Figura 50. Diagrama de conexión general del sistema.

Es importante destacar que todos estos sistemas están alimentados mediante una fuente de energía de 12V respaldada por una UPS, asegurando un suministro continuo e ininterrumpido de electricidad para todos los componentes, incluyendo la alimentación de la cerradura de la puerta.

4.4. IMPLEMENTACIÓN DEL SISTEMA EN EL LABORATORIO DE MANUFACTURA ADITIVA Y SUSTRACTIVA DE LA FACULTAD DE CIYA

En relación a la implementación, se abordó la gestión de accesos de manera integral. Esto incluyó la integración de reconocimiento facial, lectura de tarjetas RFID y apertura mediante IoT a través de Telegram. Adicionalmente, se llevó a cabo la instalación y configuración del sistema de control de iluminación y enchufes.

4.4.1. Adecuación del sistema eléctrico

En el Laboratorio de Manufactura Aditiva y Sustractiva, inicialmente solo se contaba con la infraestructura eléctrica destinada al sistema de iluminación, como se ilustra en la Figura 51. Sin embargo, con la intención de incorporar impresoras 3D y acomodar las necesidades de los estudiantes en el laboratorio, se llevó a cabo una expansión eléctrica que involucró la instalación de tomacorrientes, como se observa en la Figura 52.

Figura 51. Estado inicial del Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA.

Esta ampliación fue indispensable para atender los requerimientos energéticos tanto de las impresoras 3D como de las actividades de los alumnos. Para lograrlo, se emplearon elementos como canaletas, tomacorrientes, cables calibre 10 AWG, así como consumibles y herramientas específicas.

Figura 52. Estado actual del Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA.

La implementación de esta infraestructura eléctrica adicional no solo permitió un funcionamiento adecuado de las impresoras 3D, sino que también garantizó que los estudiantes tuvieran acceso a los recursos eléctricos necesarios para sus proyectos y actividades en el laboratorio.

4.4.2. Ubicación de los elementos

En esta sección se muestra la ubicación de los elementos que componen el sistema implementado.

4.4.2.1. Ubicación del sistema de control de acceso

Para la instalación del portero electrónico, es esencial considerar su accesibilidad para todas las personas. Por lo tanto, se recomienda ubicarlo a una altura de entre 1.2 y 1.7 metros sobre el nivel del suelo, como se ilustra en la Figura 53.

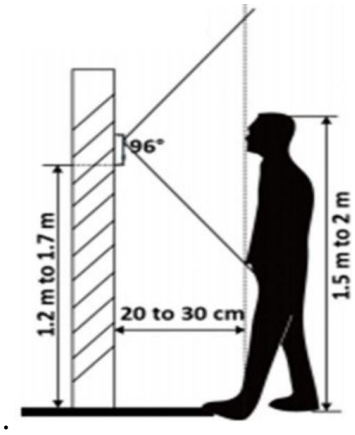


Figura 53. Altura para colocación del portero.

Además de lo mencionado anteriormente, existen pautas clave a considerar para la ubicación del sistema de control de acceso:

- **Accesibilidad:** Coloca el sistema de control de acceso en un lugar de fácil acceso para los usuarios autorizados. Debe estar en una ubicación conveniente y visible para que las personas puedan acceder y utilizar el sistema sin dificultad.
- **Cercanía a la Entrada:** Instala el sistema cerca de la entrada principal del área o edificio que deseas proteger. Esto facilita el proceso de acceso y evita que las personas tengan que recorrer largas distancias para llegar al sistema.
- **Visibilidad:** Asegúrate de que el sistema sea claramente visible para las personas que se acerquen. Esto puede disuadir a posibles intrusos y transmitir una sensación de seguridad a los usuarios.
- **Protección contra las Inclemencias del Tiempo:** Si el sistema se encuentra en el exterior, asegúrate de que esté protegido de las condiciones climáticas adversas, como la lluvia directa o la luz solar intensa. Utiliza carcasas o cubiertas protectoras para mantener el sistema en buen estado.
- **Evitar Obstáculos:** Coloca el sistema en un lugar donde no haya obstáculos que bloqueen su acceso o visibilidad. Asegúrate de que no haya puertas, muebles u otros elementos que dificulten el uso del sistema.

Siguiendo las pautas anteriores, se ha decidido instalar el sistema a una altura de 1.7 metros sobre el nivel del suelo como se muestra en la Figura 54, en el marco de aluminio de la puerta de ingreso al laboratorio. Esta ubicación fue elegida debido a su proximidad a la entrada, lo que proporciona un acceso conveniente para los usuarios, y además ofrece una visibilidad óptima.

Figura 54. Ubicación del portero.

4.4.2.2. Ubicación del sistema de fotografía de registro

La ubicación del sistema de fotografía de registro se ha elegido estratégicamente cerca de la puerta de entrada. Esta decisión se basa en diversas consideraciones que garantizan su efectividad y rendimiento óptimos. Al estar colocado cerca de la puerta de entrada, el sistema tiene la capacidad de capturar imágenes de las personas que ingresan al laboratorio. Además, esta ubicación aprovecha la iluminación natural que entra por la entrada, lo que asegura una buena iluminación para las fotografías.

Esta elección de ubicación se basa en pautas importantes:

- **Proximidad a la Entrada:** La ubicación cercana a la puerta permite que el sistema capture las imágenes en el momento exacto en que las personas entran al laboratorio, maximizando así la exactitud y utilidad de las fotos tomadas.
- **Buena Iluminación:** Al estar cerca de la puerta, el sistema se beneficia de la luz natural que entra al espacio, lo que garantiza que las fotografías tengan una iluminación adecuada y nítida.
- **Facilidad de Uso:** Al colocar el sistema cerca de la entrada, se simplifica el proceso para las personas que ingresan, ya que no deben desviarse de su ruta habitual para ser capturadas por la cámara.

- **Visibilidad y Disuasión:** Al ser visible para quienes ingresan, el sistema puede tener un efecto disuasorio sobre cualquier comportamiento inapropiado, ya que las personas son conscientes de que están siendo registradas visualmente.

4.4.2.3. Ubicación del sistema control IoT

El sistema control IoT ha sido situado en la viga ubicada en la esquina derecha del laboratorio, justo encima del sistema de respaldo de energía. La decisión de colocar el sistema en esta viga específica refleja la consideración de varios factores:

- **Accesibilidad y Comodidad:** La ubicación facilita que el sistema de control IoT esté accesible tanto para el personal como para los usuarios del laboratorio. Esta ubicación de fácil acceso en caso de ser necesario.
- **Distribución de Dispositivos:** La elección de la viga como ubicación central permite una ubicación cercana a los dispositivos como sensores y controladores etc.
- **Futuras Expansiones:** La ubicación en la esquina derecha permite una distribución correcta de dispositivos, la disposición facilita futuras expansiones del sistema, ya que se ha considerado espacio adicional para incorporar nuevos dispositivos según las necesidades cambiantes del laboratorio.

La ubicación se muestra en la Figura 55.

Figura 55. Ubicación del control IoT.

4.4.2.4. Ubicación del sistema de respaldo de energía

Se ha tomado en cuenta la biga en la esquina derecha del laboratorio para ubicar el sistema de respaldo de energía, considerando los criterios relevantes de la norma NFPA 110: Standard for

Emergency and Standby Power Systems [22]. Este lugar del laboratorio ha sido elegido, siguiendo los criterios esenciales que garantizan su funcionamiento y protección adecuada. Los criterios aplicados son los siguientes:

- **Ubicación del sistema de respaldo:** La biga ubicada en la esquina derecha del laboratorio proporciona un espacio que se encuentra antes de las impresoras 3D.
- **Distancias y separación:** En esta ubicación, se asegura una apropiada separación de otras zonas, incluyendo la destinada a los estudiantes.
- **Combustibles y líquidos inflamables:** Dado que la ubicación seleccionada no involucra la presencia de combustibles ni líquidos inflamables cercanos, no existe riesgo de propagación de incendios u otros peligros relacionados con sustancias inflamables.
- **Resistencia al impacto y vandalismo:** Al estar dentro del laboratorio en una ubicación relativamente protegida, el sistema de respaldo se encuentra fuera del alcance directo y es menos susceptible a impactos accidentales o actos de vandalismo.
- **Requisitos eléctricos y conexiones:** En esa ubicación del laboratorio permite un acceso conveniente a las conexiones eléctricas necesarias para el sistema de respaldo.

El resto de criterios como Condiciones ambientales, Ruido y vibración etc. no aplican por ende no se consideran. En resumen, la ubicación del sistema de respaldo de energía en la biga ubicada en la esquina derecha del laboratorio cumple con los criterios esenciales para su funcionamiento la ubicación se muestra en la Figura 56.

Figura 56. Ubicación del sistema de respaldo de energía.

4.4.3. Conexión del sistema respaldo de energía

Dentro del esquema de conexión se ubica el sistema de suministro de 110V, el cual alimenta a los sistemas de respaldo de energía. Estos sistemas de respaldo, a su vez, suministran energía en forma de corriente continua de 12V a los componentes del sistema de control de acceso, el sistema IoT y el sistema de fotografía de registro, tal como se ilustra en la Figura 57.

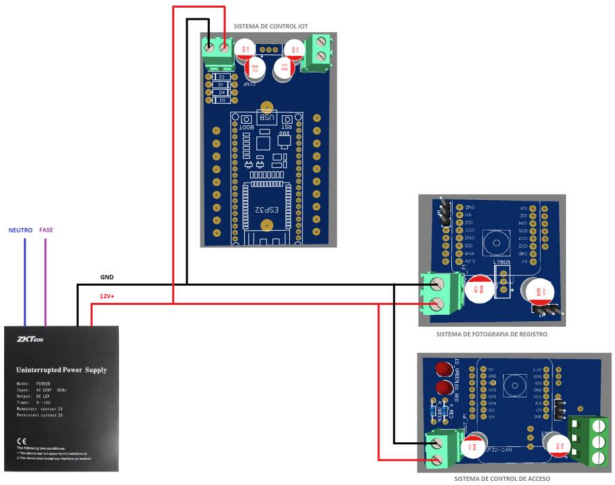


Figura 57. Diagrama de conexión del sistema de respaldo de energía.

El resto de conexiones realizadas se detallan en el ANEXO I, ya que se dividen en varias partes.

4.4.4. Diagramas del sistema implementado

La Figura 58 presenta el diagrama implementado en el Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA. Se trata de un esquema unifilar que visualiza todos los elementos involucrados.

Figura 58. Plano actual del Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA.

La Figura 59 proporciona una descripción detallada de cada uno de los elementos presentes en el diagrama. Además, para una visualización completa de los planos, se encuentran disponibles en el ANEXO I.

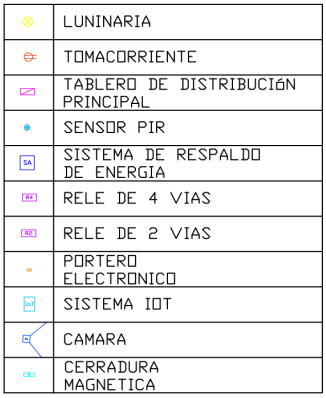


Figura 59. Nomenclatura del sistema implementado.

5. ANÁLISIS DE RESULTADOS

Esta sección engloba las pruebas de operatividad del sistema, las cuales comprenden evaluaciones de la conectividad Wi-Fi, el funcionamiento del reconocimiento facial, el sistema RFID y el control a través de IoT, entre otros aspectos a evaluar.

5.1. PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA

5.1.1. Conectividad Wi-Fi

Para evaluar la conectividad, se analiza el tiempo necesario para que los módulos se conecten al Wi-Fi. En la Tabla 23 se presenta el promedio de tiempo requerido para que las dos ESP32-CAM y la ESP32 se conecten exitosamente a la red WiFi.

Tabla 23 Tiempo de conexión Wifi de los módulos.

DESCRIPCION	TIEMPO PROMEDIO
RECONOCIMIENTO FACIAL (ESP32CAM)	1.8 s
CÁMARA DE FOTOGRAFÍA (ESP32CAM)	2.1 s
CONTROL DE LUMINARIAS Y TOMACORRIENTES (ESP32)	1.5 s

5.1.2. Pruebas del sistema de control IoT

El sistema de control opera en tres modos diferentes: manual, automático y a través de IoT (Telegram). Con el fin de llevar a cabo la evaluación, se realizaron 100 pruebas de encendido y apagado para cada uno de estos modos, lo que suma un total de 300 pruebas. Estas pruebas

incluyen el encendido de las luces tanto en el exterior como en el interior del laboratorio, así como la apertura de la puerta. Para ejercer el control a través de Telegram, es necesario enviar el comando "opciones", tal y como se muestra en la Figura 60.

Figura 60. Comando “opciones” de Telegram.

La Tabla 24 presenta el recuento de éxitos y fallos en cada uno.

Tabla 24 Pruebas del sistema de control IoT.

MODOS	ÉXITO	FALLO	TOTAL
MANUAL	95	5	100
AUTOMÁTICO	98	2	100
IOT (TELEGRAM)	99	1	100

Al realizar una evaluación integral del sistema, en la Tabla 25 se muestran los índices de tasa de éxito.

Tabla 25 Porcentaje de tasa de éxito del sistema de control IoT.

TOTAL	100%
PORCENTAJE ÉXITO (%)	97.33
PORCENTAJE FALLOS (%)	2.66

La Figura 61 muestra un gráfico circular que representa el porcentaje de aciertos y errores. De las 300 pruebas efectuadas, el sistema alcanzó un total de 292 aciertos y tuvo 8 fallos, lo que equivale a un índice de aciertos del 97.33% y un índice de fallos del 2.66%.

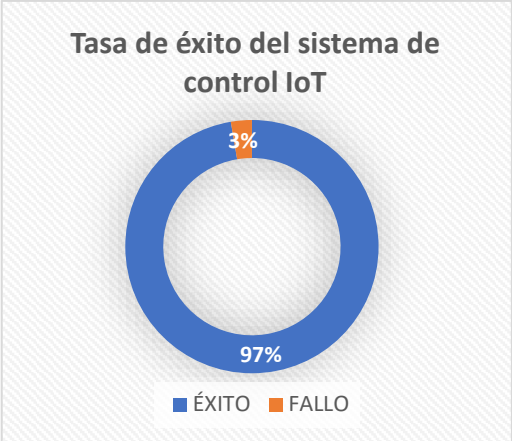


Figura 61. Porcentaje de la tasa de éxito del sistema de control IoT.

Dado que el microcontrolador opera a través de IoT y se enlaza con Telegram, es crucial considerar el tiempo de respuesta. Tanto en los modos manual como automático, la respuesta es prácticamente instantánea. Sin embargo, en la Tabla 26 se especifica el tiempo de respuesta a través de IoT.

Tabla 26 Tiempo de acción del sistema de control IoT.

TIEMPO DE RESPUESTA	NUMERO DE EXITOS
1 SEGUNDO	83
2 SEGUNDO	9
3 SEGUNDO	8
PROMEDIO	1.25 s

El sistema demuestra un tiempo de respuesta con un promedio de funcionamiento de 1.25 segundos a partir del instante en que el mensaje se envía a través de Telegram. Este resultado puede verse influenciado por la calidad de la conexión a Internet, tanto por parte del usuario como del sistema IoT.

5.1.3. Pruebas de envió de fotografías

Antes de llevar a cabo el ensayo, es importante asegurarse de que el sensor PIR de la cámara esté activado, tal como se ilustra en la Figura 62. El sistema de captura de fotografías para el registro funciona en dos modos diferentes. El primero se basa en el uso del sensor de movimiento, que, al detectar actividad, envía una fotografía mediante Telegram. El segundo modo se activa cuando se solicita una fotografía a través de Telegram.

Figura 62. Activación del sensor PIR de la cámara.

Con el objetivo de realizar este evaluación, se ejecutaron en total 50 pruebas de acceso al laboratorio, tal como se ilustra en la Figura 63. En cada una de estas pruebas, se tomó una fotografía de la persona que ingresaba y posteriormente se envió dicha imagen a través de Telegram.

Figura 63. Prueba de acceso del laboratorio con el sensor PIR.

Para el pedido de fotografías se debe ingresar el comando “/foto” como se muestra en la Figura 64.

Figura 64. Pedido de fotografía de la cámara.

Los resultados de las 25 pruebas realizadas están documentados en la Tabla 27 , proporcionando un desglose tanto de la cantidad de fallos como de los éxitos alcanzados.

Tabla 27 Pruebas de toma de fotografías.

SISTEMA	ÉXITO	FALLO	TOTAL
PIR	22	3	25
TELEGRAM	23	2	25
TOTAL	45	5	50

El porcentaje de éxito se muestra en la Tabla 28 así como la tasa de fallos.

Tabla 28 Porcentaje de tasa de éxito en la toma de fotografías.

PORCENTAJE ÉXITO (%)	**90**
PORCENTAJE FALLOS (%)	10

De las 50 pruebas que se llevaron a cabo, el sistema obtuvo un total de 45 éxitos y experimentó cinco fallos, como se describen en la Tabla 28 . Esto se traduce en un índice de éxito del 90% y un índice de fallos del 10%.

Otro factor de importancia consiste en la evaluación del tiempo de respuesta de Telegram. La Tabla 29 detalla el intervalo necesario para enviar la fotografía a través de Telegram, tanto cuando el sensor de movimiento lo activa como cuando se solicita la imagen desde Telegram. Estas pruebas derivan del punto anterior, representando las mismas 50 pruebas para cada uno de los casos.

Tabla 29 Promedio del tiempo de acción en la toma de fotografías.

TIEMPO DE RESPUESTA	SENSOR DE MOVIMIENTO	TELEGRAM
2 SEGUNDO	3	2
3 SEGUNDO	11	5
4 SEGUNDO	8	16
PROMEDIO	3.2 s	3.6 s

El uso del sensor de movimiento permite que el sistema opere a una velocidad más rápida, dado que no requiere establecer una comunicación previa con Telegram antes de enviar la fotografía. Esto se evidencia en un promedio de 2.2 segundos. En contraposición, al solicitar imágenes mediante Telegram, el procedimiento implica que el mensaje debe ser procesado por la ESP32CAM, lo que resulta en un aumento del tiempo de respuesta a 3.6 segundos. Es importante señalar que la velocidad de conexión a internet también desempeña un papel en este aspecto.

5.1.4. Pruebas del reconocimiento facial y RFID

El sistema de control de acceso está compuesto por tres componentes principales: el reconocimiento facial, la lectura de tarjetas RFID y la apertura remota. La operación de apertura remota es controlada por el mismo sistema encargado de gestionar las luces y tomacorrientes que ya han sido evaluados previamente. En consecuencia, se procedió a evaluar los otros dos sistemas restantes, realizando un total de 100 pruebas individuales para cada uno, lo que suma un total de 200 pruebas. La Tabla 30 muestra el registro de tasas de éxito y fallos de ambos sistemas durante estas evaluaciones.

Tabla 30 Pruebas del sistema de control de acceso.

SISTEMA	ÉXITO	FALLO	TOTAL
RFID	99	1	100
RECONOCIMIENTO FACIAL	95	5	100
TOTAL	194	6	200

Al realizar una evaluación control de acceso, en la Tabla 31 se muestran los índices de la tasa de éxito en porcentaje.

Tabla 31 Porcentaje de tasa de éxito del sistema de control de acceso.

PORCENTAJE ÉXITO (%)	**97**
PORCENTAJE FALLOS (%)	3

La Figura 65 muestra un gráfico circular que representa el porcentaje de aciertos y errores en el sistema de control de acceso. De las 200 pruebas efectuadas, el sistema obtuvo un total de 194 aciertos y enfrentó 6 fallos, lo que se traduce en una tasa de aciertos del 97% y una tasa de fallos del 3%.

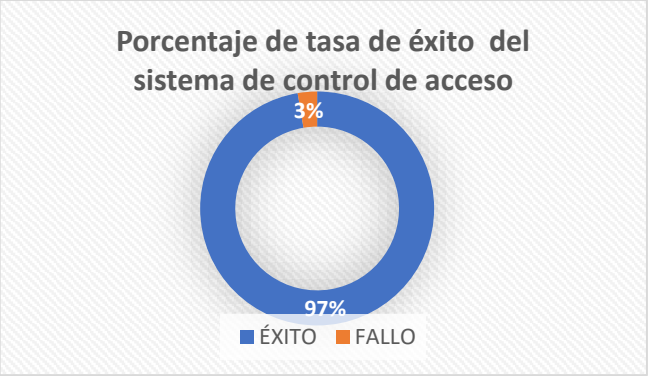


Figura 65. Porcentaje de tasa de éxito del sistema de control de acceso.

Otra faceta esencial de la evaluación involucra el tiempo de reacción de los sistemas. La identificación mediante tarjetas RFID demuestra una respuesta inmediata. En lo que respecta al reconocimiento facial, la velocidad de respuesta está especificada en la Tabla 32 exponiendo la rapidez con la cual el sistema de detección facial se activa.

Tabla 32 Promedio del tiempo de acción del reconocimiento facial.

TIEMPO DE RESPUESTA	NUMERO DE EXITOS
1 SEGUNDO	9
2 SEGUNDO	15
3 SEGUNDO	76
PROMEDIO	2.67 s

El rendimiento promedio del sistema es de aproximadamente 2.67 segundos en términos de tiempo de respuesta desde que una persona se coloca frente al sistema de detección facial.

5.1.5. Prueba de autonomía del sistema

La autonomía desempeña un rol esencial en el sistema, ya que establece la duración operativa en caso de un corte en el suministro eléctrico. Para evaluar este aspecto, se realizaron 10 pruebas donde se desconectó el suministro eléctrico y se registró el tiempo en el cual el sistema estuvo antes de quedarse sin energía. En la Tabla 33 se presentan los resultados de estas pruebas.

Tabla 33 Prueba de autonomía del sistema.

N PRUEBA	TIEMPO
1	5h 45min
2	5h 33min
3	5h 26min
4	5h 38min
5	5h 25min
6	5h 37min
7	5h 15min
8	5h 23min
9	5h 25min
10	5h 34min
PROMEDIO	5h 30 min

Los resultados de la autonomía evidencian que el sistema posee una duración operativa aproximadamente 30 minutos más extensa. Este cálculo se basa en la utilización de la ecuación 1 y la estimación de la corriente:

$$I_{de\ carga} = \frac{7A}{5.5h} = 1.27Ah$$

A partir de las horas de autonomía obtenidas, es posible concluir que la corriente de carga del sistema se sitúa en 1.27 Ah, lo cual muestra una disminución de 0.135 Ah en comparación con la corriente previamente calculada.

5.2. COSTO DEL PROYECTO

5.2.1. Costos del diseño

La Tabla 34 presenta un desglose de las cantidades, costos unitarios y el total estimado para la implementación del sistema de seguridad y control mediante IoT.

Tabla 34 Costos estimados del diseño completo

DESCRIPCIÓN	UNIDAD	CANTIDAD	P. UNITARIO	P. TOTAL
ESP32	U	1	12	12
ESP32-CAM CON LA OV2640	U	2	16	32
ESP8266	U	1	7	7
MODULO RFID	U	1	4.5	4.5
SENSOR PIR	U	6	2.5	15
MODULO RELE 2 VIAS	U	2	2.55	5.1
MODULO RELE 4 VIAS	U	1	5.8	5.8
IMPRESIÓN DE PLACA PCB	U	13	8	104
IMPRESIÓN 3D	U	28	6	168
CABLE 22 AWG	M	100	0.35	35
CABLE 18 AWG	M	35	0.4	14
CABLE 10 AWG	M	15	0.8	12
CONDENSADORES	U	30	0.2	6
RESISTENCIAS	U	15	0.1	1.5
ESPIRAL	M	1	1	1
LM7805	U	14	0.35	4.9
CERRADURA ELÉCTRICA	U	1	30	30
FUENTE DE ALIMENTACIÓN	U	1	55	55
LUMINARIA OJO DE BUEY	U	1	5.55	5.55
CAJA DE PROYECTOS	U	1	5.8	5.8
TOMACORRIENTE	U	9	2.6	23.4
CAJA PARA TOMACORRIENTE	U	9	2.3	20.7
CANALETA	U	8	3.8	30.4

DESCRIPCIÓN	UNIDAD	CANTIDAD	P. UNITARIO	P. TOTAL
PUERTA LÓGICA	U	2	0.75	1.5
OPTOACOPLADORES	U	4	0.32	1.28
REUTER	U	1	25	25
SENSOR SW-18010P	U	22	2.5	55
BOCINA DE ALARMA DE 116DB	U	3	10	30
ESP32-CAM CON LA OV5640	U	10	22	220
LUMINARIAS CON LUCES NEUTRAS O FRIAS (4000K - 5000K)	U	10	13	130
LUMINARIAS CON LUCES FRIAS (5000K - 6500K)	U	6	15	90
SENSOR MQ-2	U	2	3	6
HERRAMIENTAS Y CONSUMIBLES	U	1	60	60
TOTAL				1217.43

5.2.2. Costos de implementación

La Tabla 35 presenta una lista de los materiales empleados en el proyecto, además de aquellos necesarios para la adecuación del sistema eléctrico del laboratorio. Cabe señalar que no se han incluido el acceso a internet, ya que este servicio es suministrado por la propia Universidad.

Tabla 35 Costos del sistema de control de acceso y tomacorrientes.

DESCRIPCIÓN	UNIDAD	CANTIDAD	P. UNITARIO	P. TOTAL
ESP32	U	1	12	12
ESP32CAM	U	2	16	32
ESP8266	U	1	7	7
MODULO RFID	U	1	4.5	4.5
SENSOR PIR	U	3	2.5	7.5
MODULO RELE 2 VIAS	U	2	2.55	5.1
MODULO RELE 4 VIAS	U	1	5.8	5.8
IMPRESIÓN DE PLACA PCB	U	3	8	24
IMPRESIÓN 3D	U	8	8	64
CABLE 22 AWG	M	40	0.35	14
CABLE 18 AWG	M	17	0.4	6.8
CABLE 10 AWG	M	15	0.8	12
CONDENSADORES	U	10	0.2	2
RESISTENCIAS	U	15	0.1	1.5
ESPIRAL	M	1	1	1
LM7805	U	4	0.35	1.4
CERRADURA ELÉCTRICA	U	1	30	30
FUENTE DE ALIMENTACIÓN	U	1	55	55
LUMINARIA OJO DE BUEY	U	1	5.55	5.55
CAJA DE PROYECTOS	U	1	5.8	5.8
TOMACORRIENTE	U	9	2.6	23.4

CAJA PARA TOMACORRIENTE	U	9	2.3	20.7
CANALETA	U	8	3.8	30.4
PUERTA LÓGICA	U	2	0.75	1.5
OPTOACOPLADORES	U	4	0.32	1.28
REUTER	U	1	25	25
HERRAMIENTAS Y CONSUMIBLES	U	1	50	50
TOTAL				**449.23**

5.3. COMBATIVA CON OTROS SISTEMAS COMERCIALES

En el panorama actual del mercado, se pueden encontrar múltiples alternativas que ofrecen funcionalidades similares a las del sistema que se ha desarrollado en la Tabla 36 proporciona los diversos sistemas comerciales, sus características y costos asociados.

Tabla 36 Comparación con sistemas comerciales.

SISTEMA	SERVICIOS	COSTO
SMARTTHINGS HUB DE SAMSUNG	Control de luces y tomas de corriente. Apertura de puertas mediante sensores. Posibilidad de integrar cámaras con reconocimiento facial y captura de imágenes.	$100
AMAZON ECHO PLUS CON ALEXA	Control de luces y tomacorrientes inteligentes. Posibilidad de integración con cerraduras inteligentes y sistemas de seguridad con reconocimiento facial.	$150
GOOGLE NEST HUB MAX	Control de iluminación y electrodomésticos conectados. Posibilidad de integración con cerraduras inteligentes y sistemas de seguridad. Puede usarse con cámaras que admitan reconocimiento facial y captura de imágenes.	$230
APPLE HOMEKIT	Control de luces y dispositivos inteligentes. Posibilidad de integración con cerraduras inteligentes y sistemas de seguridad. Puede usarse con cámaras compatibles con reconocimiento facial y captura de imágenes.	$500
LUTRON CASETA SMART LIGHTING	Control de iluminación con tomacorrientes inteligentes. Posibilidad de integración con cerraduras y cámaras compatibles.	$100
SISTEMA DESARROLLADO	Control de luces y tomas de corriente. Apertura de puertas mediante reconocimiento facial. Apertura de puertas mediante lectura de tarjetas RFID. Cámaras con reconocimiento facial Captura de imágenes. Control del sistema mediante IoT.	$290

A pesar de que el costo total del proyecto, mostrado en la Tabla 36 incluye la adecuación de las instalaciones eléctricas del laboratorio, es importante considerar que si excluimos este aspecto y asumimos que las instalaciones y el acceso a internet ya están disponibles, el costo se reduce a 290 $.

Aunque ciertas soluciones comerciales ofrezcan funciones como reconocimiento facial y sistemas RFID etc., sus precios no consideran estos aspectos. En contraposición, el sistema

desarrollado combina todas estas funciones. Además, destaca por su potencial de evolución y mejoras futuras, ya que el proyecto cuenta con microcontroladores programables.

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- Tras realizar la revisión del estado del arte en sistemas de control de acceso a espacios, se identificaron tecnologías pertinentes que proporcionaron una base para el diseño y desarrollo del sistema integral en el Laboratorio de Manufactura Aditiva y Sustractiva. Esta revisión preliminar permitió destacar el suso de microcontroladores programables de la familia ESP y que la plataforma de programación Arduino ya que proveer una serie de herramientas como librerías y controladores para diversas placas etc.
- En el diseño se consideraron, diferentes métodos de control de acceso como el reconocimiento facial, la lectura de tarjetas RFID y la conectividad con IoT. De manera agilice y facilite el proceso de entrada al laboratorio, a la vez que se estableció una base para la automatización de la iluminación y control de los tomacorrientes.
- La implementación del sistema en el Laboratorio de Manufactura Aditiva y Sustractiva resultó exitosa logrando la colocación de los sistemas diseñados y considerando la ubicación de los elementos, cumpliendo con las normativas y criterios de emplazamiento.
- Las pruebas realizadas muestran una mayor facilidad de ingreso, confirmando su adecuado funcionamiento en situaciones prácticas. Estos ensayos también han arrojado resultados que demuestran una tasa de éxito superior al 95% en el manejo del control de acceso, iluminación y tomacorrientes, además de tiempos de espera menores a cuatro segundos en el control a través de IoT.

6.2. RECOMENDACIONES

- Para futuras mejoras en la seguridad del Laboratorio, se sugiere la implementación de sistemas de vigilancia planteado que abarca la totalidad del espacio, posibilitando la detección de cualquier sustracción de elementos por parte de personas no autorizadas.
- Se aconseja la implementación de un sistema de alarmas tanto local como remoto para salvaguardar las instalaciones en caso de intrusiones que puedan causar daños, permitiendo así alertar de manera efectiva a los responsables del laboratorio.

- Se recomienda utilizar los módulos montados en las PCB diseñadas para proyectos similares, ya que ofrecen una mayor flexibilidad en términos de programación, alimentación y manejo de los pines de salida de las placas ESP, estas PCB permiten una mejor integración de los módulos ESP y facilitan la conexión y configuración de los pines de salida según los requisitos específicos del proyecto.

7. REFERENCIAS

[1] Gobierno del Ecuador, "Entrega de la Estrategia Nacional de Seguridad Ciudadana y Prevención del Delito," vol. 4, no. 1, pp. 88–100, 2023.

[2] Nanotec, "La evolución del control de accesos," 2016.

[3] A. De La Cruz and R. Ayala, "Propuesta de un manual de prácticas para el desarrollo de la plataforma Arduino y NodeMcu en un prototipo simulado y práctico para diferentes áreas del departamento de ingeniería y arquitectura de la facultad multidisciplinaria de occidente de la Universi," *Angew. Chemie Int. Ed. 6(11), 951–952.*, pp. 2013–2015, 2020.

[4] Z. Vargas, "Sistema de Control de Acceso y Monitoreo con la Tecnología RFID para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil," 2013.

[5] J. La Cruz and A. A. Otazú, "Diseño e implementación de un sistema domótico utilizando plataformas de desarrollo como controlador," *Univ. Lima*, p. 147, 2018, [Online]. Available: http://repositorio.ulima.edu.pe/bitstream/handle/ulima/8026/La_Cruz_Chacón_Jonatán?sequence=3&isAllowed=y

[6] N. Hema and J. Yadav, "Secure Home Entry Using Raspberry Pi with Notification via Telegram," *2020 6th Int. Conf. Signal Process. Commun. ICSC 2020*, pp. 211–215, 2020, doi: 10.1109/ICSC48311.2020.9182778.

[7] F. I. Rukmana, Akmaliyah, E. Mulyana, A. Kusnawan, L. Kamelia, and W. Darmalaksana, "All-in-one application for smart home system base on telegram controlled," *Proc. - 2020 6th Int. Conf. Wirel. Telemat. ICWT 2020*, pp. 30–33, 2020, doi: 10.1109/ICWT50448.2020.9243631.

[8] P. A. Lascano Endara, Neptaly Alexander y Pico Benitez and Departamento, "Desarrollo

de sistema de identificación de personas basado en aprendizaje automático y gafas inteligentes para aplicaciones de seguridad Lascano," *Front. Neurosci.*, vol. 14, no. 1, pp. 1–13, 2021.

[9] J. López, "Desarrollo de un sistema de seguridad inalámbrico mediante el uso de una aplicación móvil y módulos ESP32," 2022.

[10] J. D. T. López, "Desarrollo de un sistema de seguridad inalámbrico mediante el uso de una aplicación móvil y módulos esp32," 2022.

[11] Romel Daniel Castro Arias, "Sistema de control de acceso al personal de la lavadora de jeans fashion mediante reconocimiento facial," Universidad Técnica De Ambato, 2016. [Online]. Available: https://repositorio.uta.edu.ec/bitstream/123456789/20347/1/Tesis_t1107ec.pdf

[12] C. T. Borja and Á. G. Bueno, "Sistemas Biométricos." p. 39, 2006.

[13] P. W. P. Angamarca, "Diseño de un sistema de control de acceso utilizando la tecnología de identificación RFID para la empresa soluciones g cuatro del ecuador CIA. Ltda," 2009.

[14] W. Cruz, "Diseño del sistema de seguridad y de control de iluminación para el conjunto cerrado el portal del bosque en la ciudad de Tunja," 2018, [Online]. Available: http://dx.doi.org/10.1186/s13662-017-1121-6%0Ahttps://doi.org/10.1007/s41980-018-0101-2%0Ahttps://doi.org/10.1016/j.cnsns.2018.04.019%0Ahttps://doi.org/10.1016/j.cam.2017.10.014%0Ahttp://dx.doi.org/10.1016/j.apm.2011.07.041%0Ahttp://arxiv.org/abs/1502.020

[15] M. Barrera Durango, N. Londoño Ospina, J. Carvajal, and A. Fonseca, "Analysis and design of a low cost home automation prototype system," *Rev. Fac. Ing.*, no. 63, pp. 117–128, 2012.

[16] J. E. Guarella, J. P. Heredia, L. Rodríguez, and I. Bagatto, "Sensores y actuadores en motores." p. 27, 2011.

[17] M. Domínguez, "¿Qué es la domótica? ▷▷ Cómo funciona una casa inteligente," *Caloryfrio.com portal sectorial de las instalaciones*. https://www.caloryfrio.com/calefaccion/herramientas-y-regulacion/que-es-la-domotica-

y-como-funciona-una-casa-domotica.html

[18] C. Valencia, “Hacking etico al IoT mediante SDR.” p. 144, 2018. [Online]. Available: https://repositorio.uta.edu.ec/bitstream/123456789/28812/1/Tesis_ t1489ec.pdf

[19] Jorge Jarne Brun, “Smart Home usando IoT y Chatbots,” Universidad Complutense de Madrid, 2018. [Online]. Available: https://eprints.ucm.es/id/eprint/49433/1/Memoria_Jorge_Jarne.pdf

[20] J. J. Segura Garrido, “Control y monitorización de una vivienda mediante Arduino y Telegram,” 2016.

[21] R. Loachamín, “Análisis de una red inalámbrica mallada autoconfigurable, utilizando el módulo NodeMcu ESP32 con el estándar 802,” Escuela Politécnica Nacional, 2020.

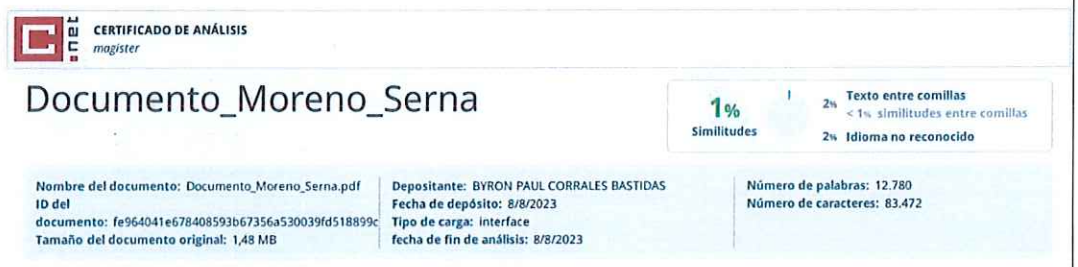
[22] NFPA, “NFPA 110 Standard for Emergency and Standby Power Systems,” 2022.

8. ANEXOS

ANEXO 1. INFORME ANTIPLAGIO PROYECTO DE TITULACIÓN

Facultad:	Ciencias de la Ingeniería y Aplicadas
Carrera:	Ingeniería en Electricidad
Nombre del docente evaluador que emite el informe:	Ing. Byron Paúl Corrales Bastidas
Documento evaluado:	Propuesta Tecnológica presentada previo a la obtención del Titulo de Ingeniero en Electricidad.
Autores del documento:	Moreno Chuqui Washington Rafael Serna Moreno Dilan Javier
Programa de similitud utilizado:	Sistema COMPILATION
Porcentaje de Similitud según el programa utilizado.	<1 %
Observaciones: **Calificación de originalidad atendiendo a los siguientes criterios:** • El documento cumple criterios de originalidad, sin observaciones. • El documento cumple criterios de originalidad, con observaciones. • El documento no cumple criterios de originalidad.	 -x- --- ---
Fecha de realización del informe:	07/08/2023

Captura de pantalla del documento analizado:



Ing. Byron Paúl Corrales Bastidas
Director de la Propuesta Tecnológica

ANEXO B	CREACIÓN DE UN BOT EN TELEGRAM	

Para iniciar el proceso de creación del bot, la persona debe buscar "BotFather" en el buscador de Telegram Figura 1. Una vez que aparezcan varias opciones relacionadas, debe seleccionar la que cuenta con el sello de verificación, ya que esto garantiza su autenticidad y ayuda a evitar posibles problemas futuros. Con BotFather como punto de partida, se puede comenzar la personalización del bot para que se adapte perfectamente a las necesidades y preferencias del usuario.

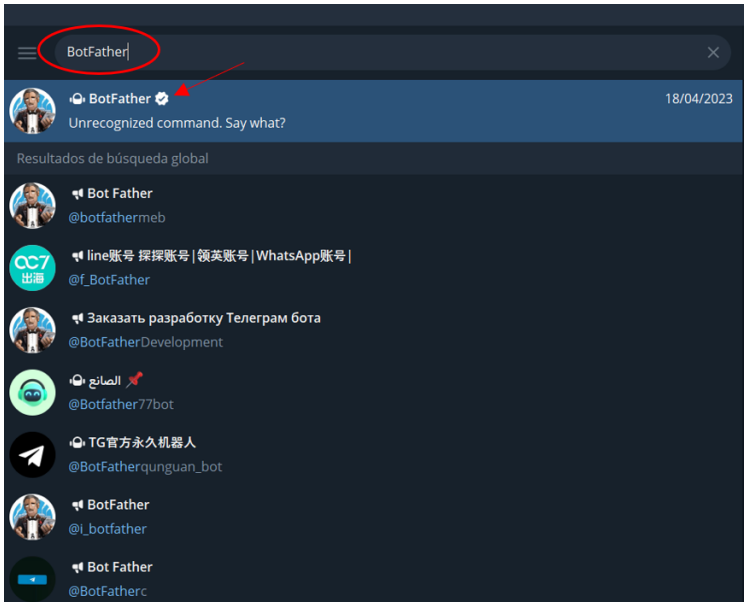


Fig. 1. BotFather en el buscador de Telegram.

Una vez que se ha localizado a BotFather en la plataforma, se inicia una conversación con el bot y luego se procede a hacer clic en el botón "Iniciar" o "Start". Al realizar esta acción, se presentará una lista completa de todos los comandos que BotFather tiene la capacidad de entender y responder Figura 2. Esto brinda la oportunidad de explorar y utilizar las funcionalidades de manera efectiva. De esta manera, a través de esta sencilla interacción, la persona estará preparada para aprovechar todas las capacidades y oportunidades que BotFather ofrece en términos de creación y control de bots personalizados en Telegram.

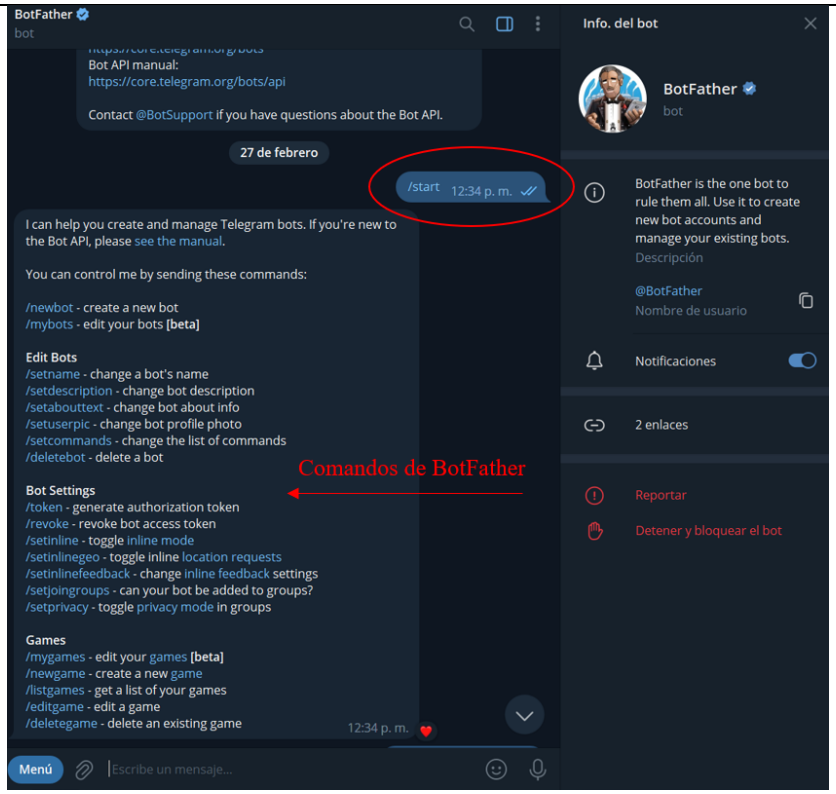


Fig. 2. Lista de todos los comandos que ofrece BotFather.

Dentro de la lista de comandos, se localiza la opción "crear un nuevo bot", la cual se selecciona. Inmediatamente, se recibe un mensaje que solicita proporcionar un nombre para el nuevo bot. Una vez que se ha asignado un nombre, se recibe otro mensaje que pide ingresar un nombre de usuario para el bot, este último debe concluir con la palabra "bot". Es importante tener en consideración que el nombre del bot y el nombre de usuario son dos elementos distintos y necesitan ser diferentes entre sí para lograr una configuración adecuada.

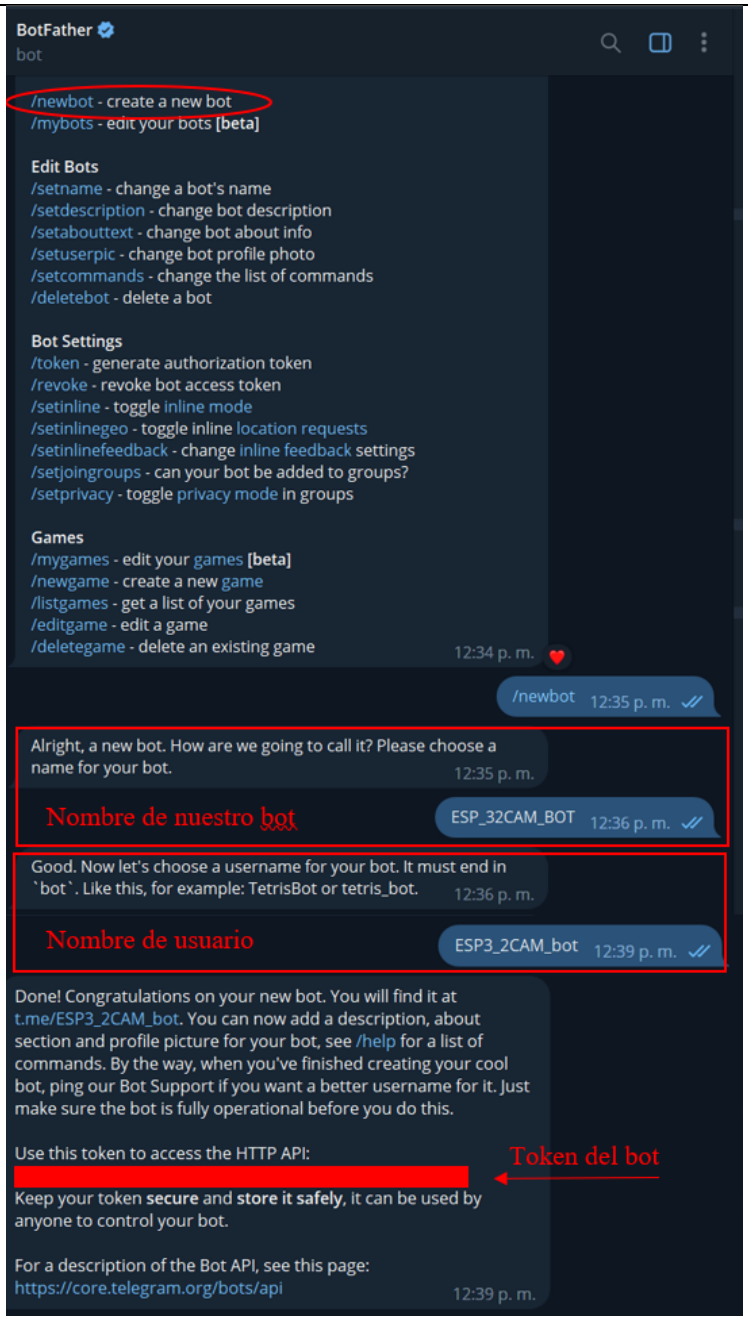


Fig. 3. Creación de un bot en Telegram y obtención del Token.

Al finalizar el procedimiento, se recibe un mensaje de confirmación que notifica la exitosa creación del bot y, además, suministra un token exclusivo Figura 3. Dicho token será de considerable utilidad en tareas de control, particularmente en el contexto del sistema IoT (Internet de las cosas). Gracias a este token, se adquiere la capacidad de administrar y operar el bot de manera eficaz, lo que posibilita aprovechar plenamente todas las funcionalidades para automatizar y controlar el sistema.

ANEXO C	INSTALACIÓN DE LOS DRIVER DE LAS PLACAS ESP32-CAM, ESP32 Y ESP8266	

Para utilizar las placas ESP32-CAM, ESP32 y ESP8266 en el entorno de desarrollo Arduino IDE, es necesario llevar a cabo la instalación correspondiente.

Para iniciar este proceso, primero debemos abrir el entorno de desarrollo Arduino IDE en nuestra computadora. Una vez que esté abierto, dirigimos nuestra atención a la pestaña "Archivos" y posteriormente seleccionamos "Preferencias" Figura 4.

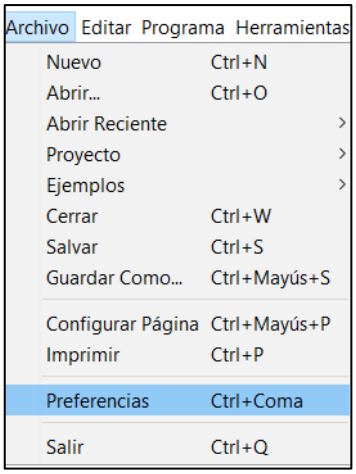


Fig. 4. Pasos para abrir la ventana de preferencias.

En la ventana emergente, pegamos la URL correspondiente en el campo denominado "Gestor de URLs adicionales de Tarjetas" y luego presionamos el botón "Ok" Figura 5.

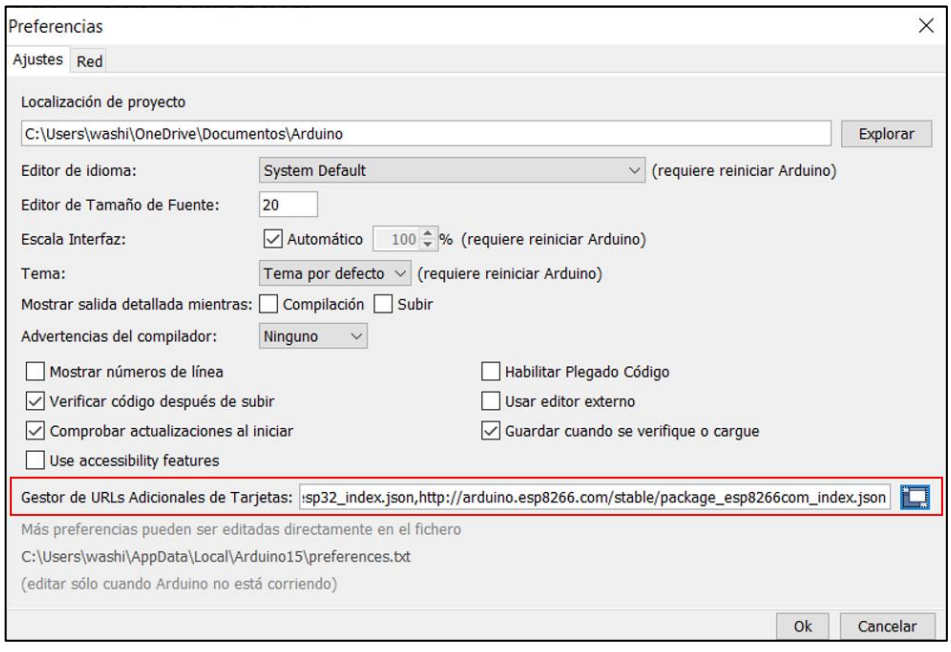


Fig. 5. Colocación de la URL de la placa en gestor de URLs

Tabla 1.URLs de las placas ESP32, ESP32-CAM y ESP8266.

ESP32 y ESP32-CAM	https://dl.espressif.com/dl/package_esp32_index.json
ESP8266	http://arduino.esp8266.com/stable/package_esp8266com_index.json

A continuación, se debe dirigir al menú denominado "Herramientas" y optar por la alternativa denominada "Placa". Dentro de esta sección, se localiza la entrada etiquetada como "Gestor de Tarjetas" Figura 6. Al hacer clic en esta opción, se habilitará el avance en el proceso.

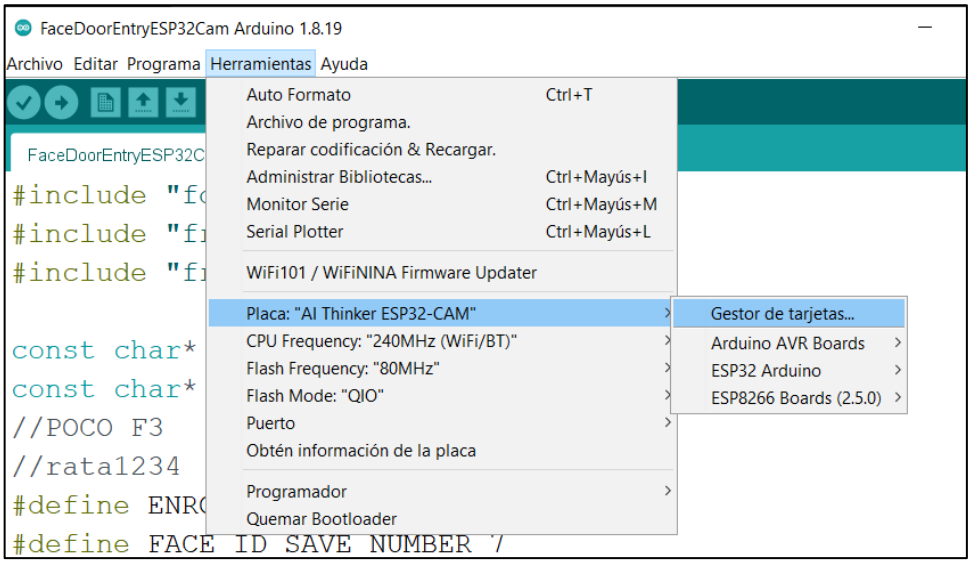


Fig. 6. Pasos para entrar en la ventana gestor de tarjetas.

Dentro de la ventana del Gestor de Tarjetas, se debera ingresar el término "ESP32". Luego, se elige la opción adecuada en los resultados obtenidos y se presiona el botón "Instalar" para dar continuidad al proceso Figura 7.

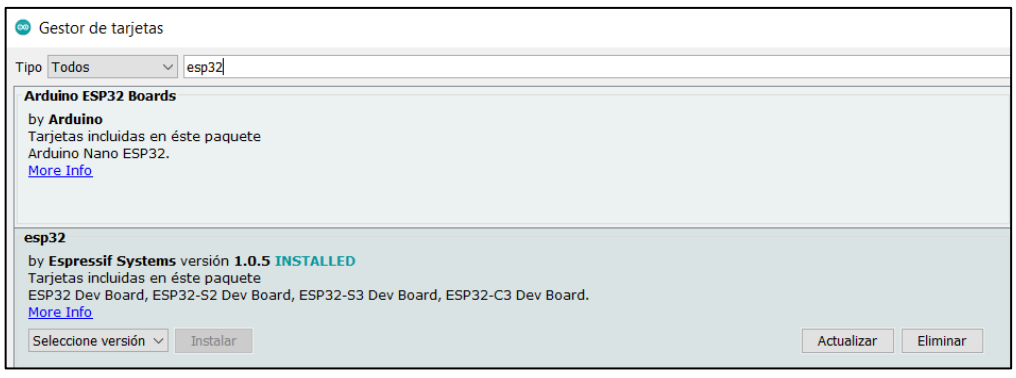


Fig. 7. Ventana de gestor de tarjetas.

Una vez que el procedimiento se ha completado, es momento de dirigirse al menú "Herramientas > Placa". En este punto, se observará que se han habilitado diversas alternativas de placas basadas en la plataforma ESP32 Figura 8. Esto también incluirá la opción de seleccionar una placa específica, la cual dependerá de la URL que se haya empleado previamente.

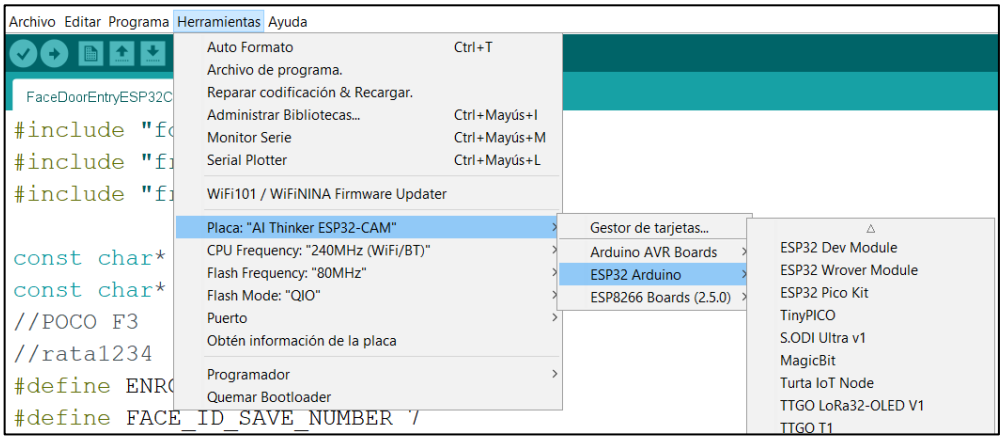


Fig. 8. Placas disponibles para la ESP32-CAM

ANEXO D	INSTALACIÓN DE LIBRERÍAS EN EL ID DE ARDUINO	

En el entorno de desarrollo Arduino IDE, se emplea una variedad de bibliotecas que ofrecen comandos específicos para distintas funciones. Para adquirir estas bibliotecas y agregarlas al Arduino IDE, se deben seguir los pasos que se detallan a continuación:

En un primer paso, se procede a iniciar el Arduino IDE en la computadora. A continuación, se dirige a la pestaña denominada "Herramientas" y se selecciona la opción titulada "Administrador de bibliotecas " como muestra la figura 9.

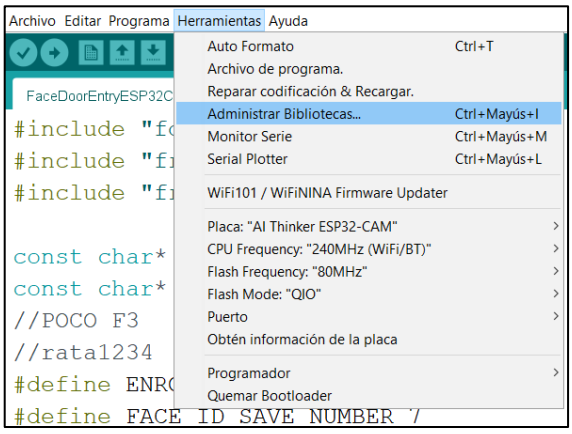


Fig. 9. Pasos para entrar en la ventana administrador de bibliotecas.

Dentro de la ventana emergente, se inicia la búsqueda de la biblioteca necesaria a través del campo de búsqueda proporcionado. Al localizar la biblioteca requerida, se elige la versión deseada y se procede a realizar la descarga. Esto habilita la posibilidad de utilizar la biblioteca seleccionada en el proyecto, como se muestra en la figura 10.

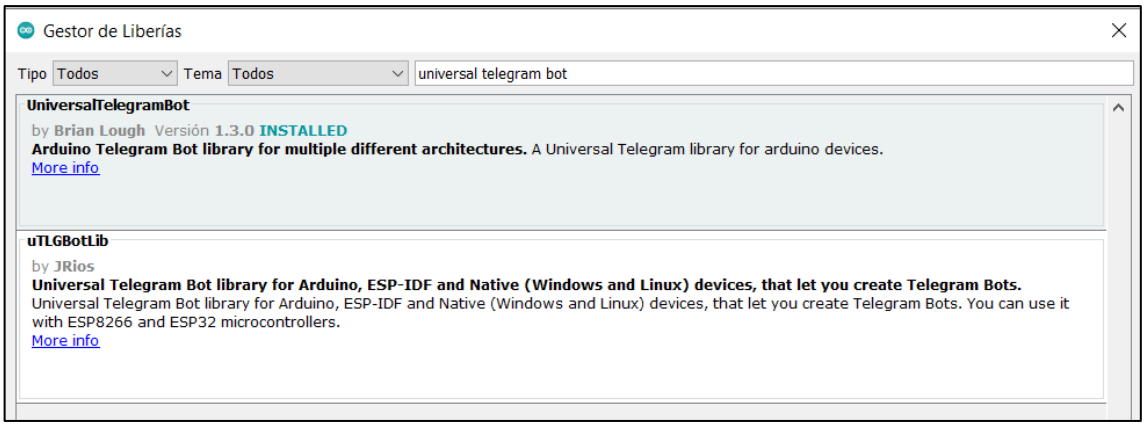


Fig. 10. Ventana de gestor de librerias

En caso de no lograr ubicar la biblioteca necesaria en el administrador de bibliotecas, se recomienda llevar a cabo una búsqueda empleando el navegador de su elección. Simplemente

se debe introducir el nombre de la biblioteca seguido por "Arduino library" para localizarla. En situaciones como estas, se aconseja obtener y descargar estas bibliotecas directamente desde la plataforma GitHub como muestre la figura 11.

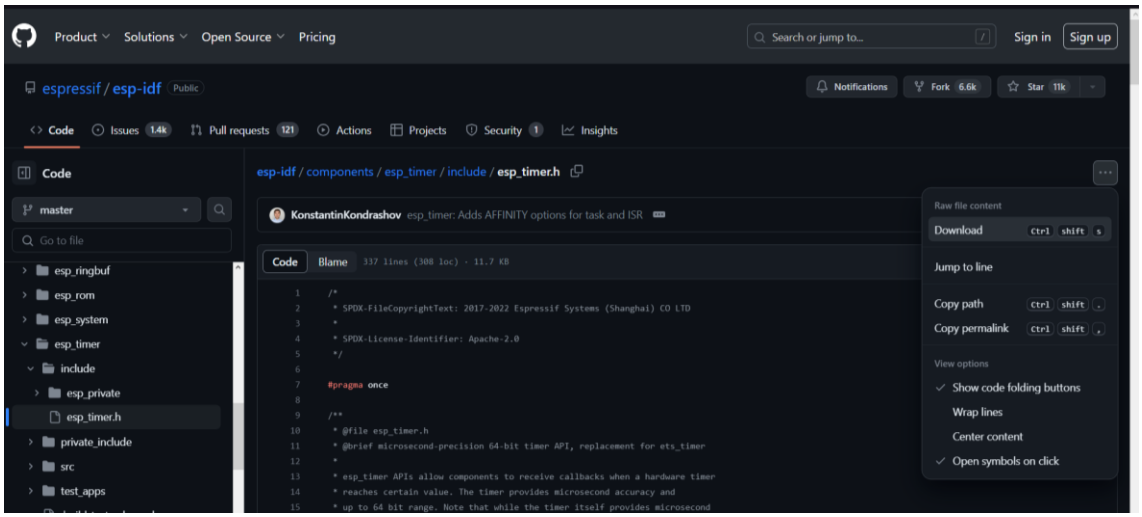


Fig. 11. Librerías de Arduino en GitHub

Tras haber descargado la biblioteca, es necesario localizar la carpeta de Arduino en la computadora. Al acceder a esta carpeta, se identifica la subcarpeta denominada "libraries", la cual aloja todas las bibliotecas que han sido descargadas. En este contexto, se lleva a cabo la acción de pegar la biblioteca que ha sido previamente descargada en esta ubicación, lo cual habilita su uso en los proyectos en curso como muestre la figura 12.

Fig. 12. Inserción de librería descargada en la carpeta de librerías de Arduino

ANEXO E	DESCRIPCIÓN DE LAS LIBRERÍAS UTILIZADAS EN LA PROGRAMACIÓN	

Librerías	Descripción
Ticker.h	La librería Ticker.h es una herramienta útil en proyectos de Arduino que requieren eventos periódicos. Permite programar acciones o funciones que se ejecutan en intervalos regulares de tiempo utilizando temporizadores internos. Esta librería proporciona gran facilidad de uso para implementar temporizaciones periódicas en proyectos de Arduino.
CTBot.h	La librería "CTBot.h" es una herramienta de código abierto diseñada para simplificar la interacción con la plataforma de mensajería Telegram a través del módulo ESP8266. Esta librería permite la creación de bots de Telegram que pueden responder a comandos, enviar actualizaciones o notificaciones a los usuarios, y realizar una variedad de tareas automatizadas.
WiFi.h	La libreria WiFi.h se utiliza para habilitar la conexión de red (local e internet) utilizando el Arduino WiFi shield, permite que una placa Arduino se conecte a internet y proporciona una amplia colección de funciones en C++ para configurar y operar un módulo ESP32 en modo estación y/o punto de acceso suave.
esp_camera.h	Es una libreria específica de la plataforma ESP32 que proporciona funcionalidad para la captura y procesamiento de imágenes utilizando la cámara integrada en el módulo ESP32. Esta biblioteca es ampliamente utilizada en proyectos que involucran aplicaciones de visión por computadora, videovigilancia, reconocimiento de objetos y más.
Arduino.h	La librería Arduino.h es esencial en el desarrollo de proyectos de Arduino, ya que proporciona las funciones y clases necesarias para controlar los dispositivos y aprovechar los recursos del microcontrolador. Simplifica la programación, ofrece funcionalidades comunes y promueve la modularidad en el código, lo que facilita el desarrollo de proyectos con placas Arduino.
WiFiClientSecure.h	La librería WiFiClientSecure.h es una biblioteca importante en Arduino que permite establecer conexiones seguras a través de Wi-Fi utilizando sockets seguros (SSL) o Transport Layer Security (TLS). Proporciona una forma fácil de transmitir datos de forma segura y autenticada, lo que la hace útil en aplicaciones de IoT y en cualquier proyecto donde se requiera seguridad en las comunicaciones Wi-Fi.

soc/soc.h	La librería soc/soc.h es una biblioteca específica de la plataforma ESP32 que permite acceder y controlar las funciones y características del System-on-a-Chip (SoC). Proporciona una interfaz de bajo nivel para configurar los periféricos, los pines de E/S, el reloj y las interrupciones del ESP32.
soc/rtc_cntl_reg.h	La librería soc/rtc_cntl_reg.h es una biblioteca específica de la plataforma ESP32 que permite acceder y controlar los registros de control del Real-Time Clock del ESP32. Proporciona una interfaz para configurar y ajustar parámetros relacionados con la medición y el seguimiento del tiempo.
UniversalTelegramBot.h	La librería UniversalTelegramBot.h es una herramienta útil para crear bots de Telegram con Arduino. Proporciona una interfaz sencilla para la comunicación y el manejo de mensajes, comandos y archivos a través de la API de Telegram.
ArduinoJson.h	La librería ArduinoJson.h es una biblioteca esencial en proyectos de Arduino que implican el manejo y procesamiento de datos en formato JSON (JavaScript Object Notation). Facilita la creación, modificación y análisis de datos JSON, y proporciona una interfaz eficiente y de bajo consumo de memoria para trabajar con este formato.

ANEXO F	DESENCRIPTAR Y ENCRIPTAR CÓDIGO HEXADECIMAL	

La ESP32-CAM cuenta con una interfaz web integrada en el código, la cual está encriptada en formato hexadecimal, esto limita la capacidad de realizar modificaciones directas en la programación. Para revertir esta encriptación y acceder al código original, se utiliza la herramienta en línea CyberChef. El proceso implica los siguientes pasos:

1. Accede al sitio web de CyberChef a través del siguiente enlace.

https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')Gunzip()

2. Una vez en la página, copia el código hexadecimal de la programación de Arduino. Este código debe pegarse en la sección "Input" de la herramienta.

3. Luego, presiona el botón "Bake" en la página, lo que generará el código original en la sección "Output". Este código original se podrá modificar según sea necesario para su posterior incorporación en la programación como se muestra en la figura 13.

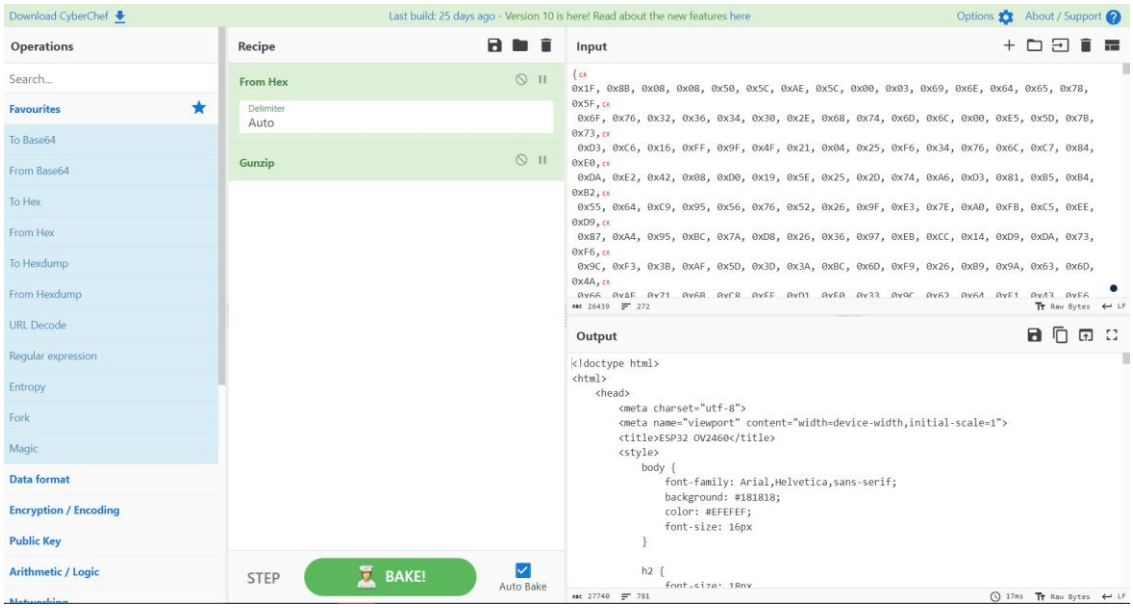


Fig. 13. Página web CyberChef para descifrar código hexadecimal.

4. Si es necesario encriptar el código modificado, se deben seguir los mismos pasos mencionados anteriormente, pero utilizando el siguiente enlace como se muestra en la figura 14.

https://gchq.github.io/CyberChef/#recipe=Gzip('Dynamic%20Huffman%20Coding','index.html.gz',",false)To_Hex('0x',0)Split('0x',',%200x')

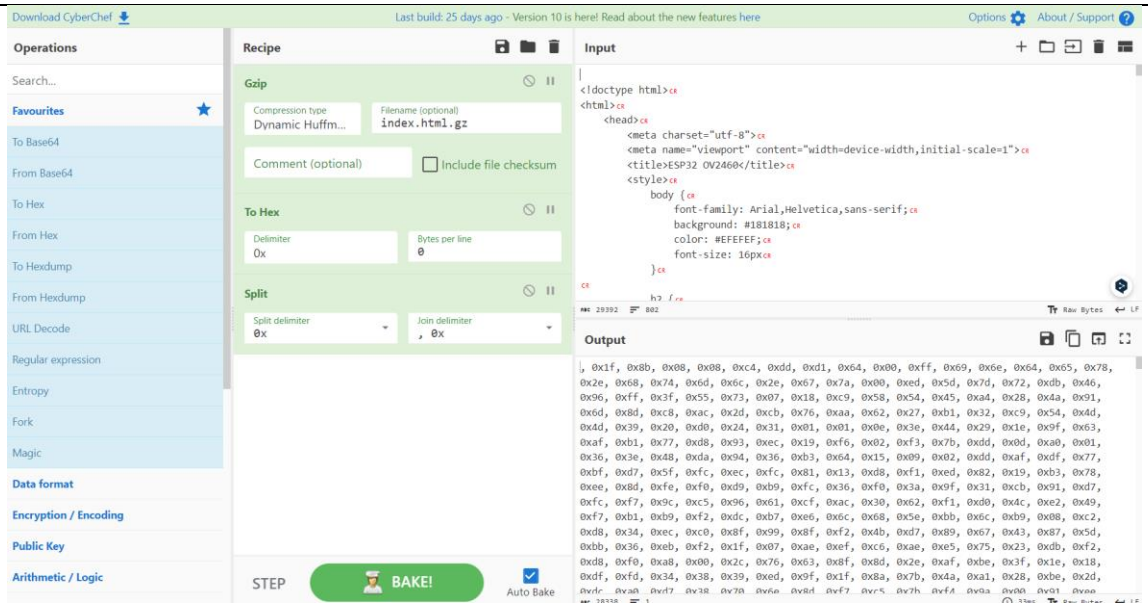
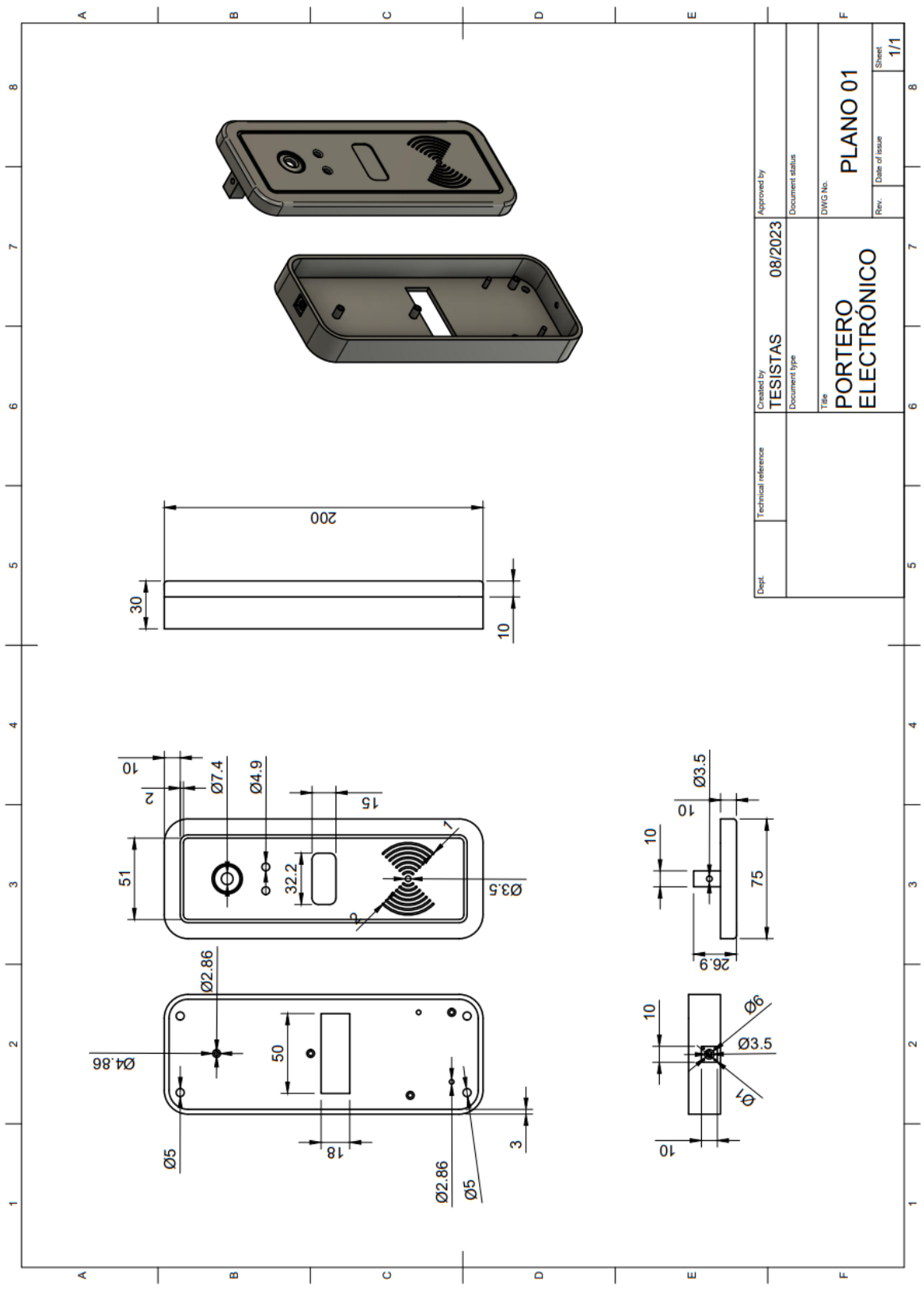


Fig. 14. Página web CyberChef para encriptar código a hexadecimal.

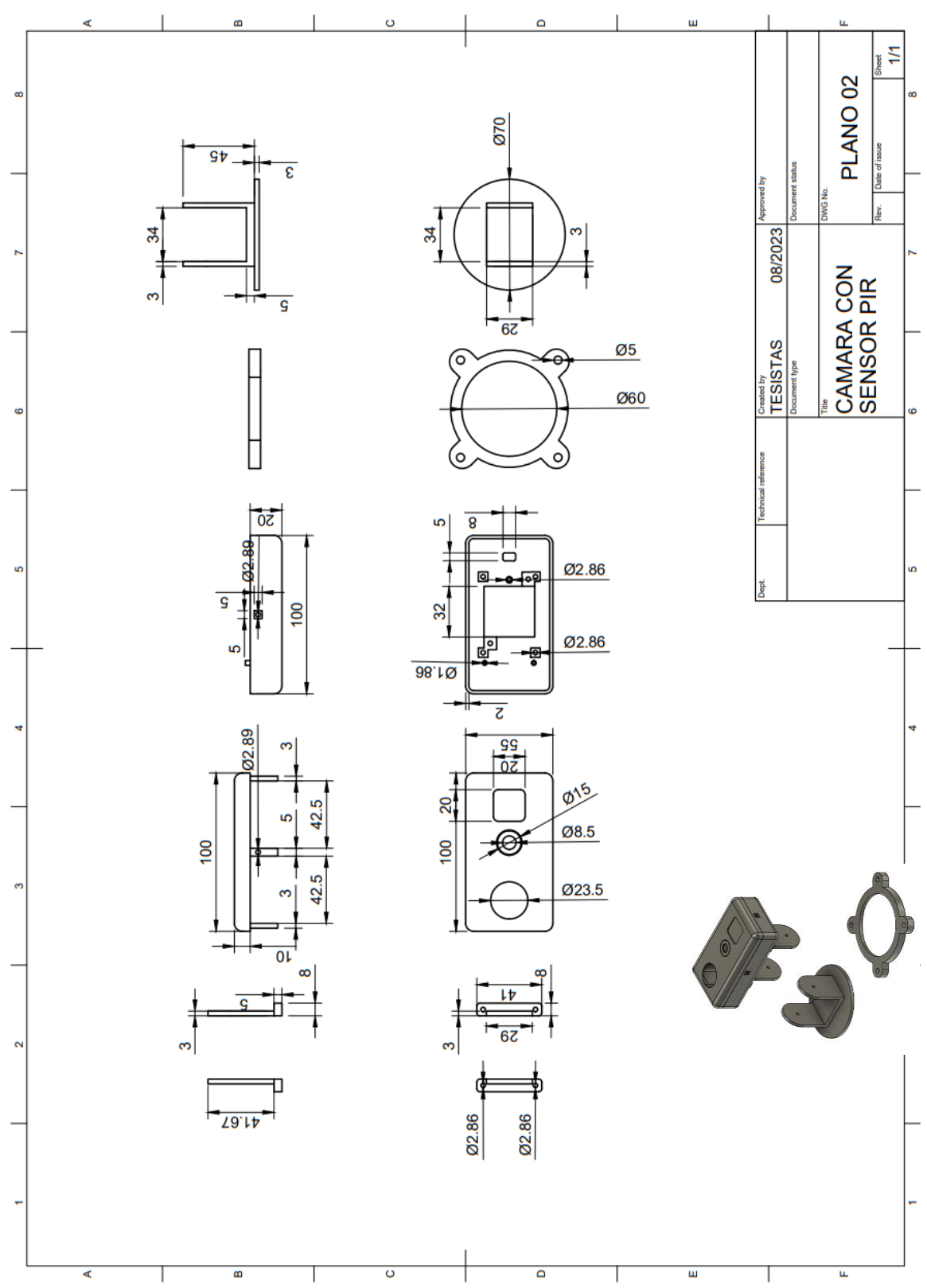
Esta serie de pasos permitirá desencriptar y encriptar el código hexadecimal de la interfaz web de la ESP32-CAM, lo que facilitará la modificación y personalización de la programación según los requisitos específicos del usuario.

ANEXO G	PLANOS DE LOS MODELOS 3D REALIZADOS	

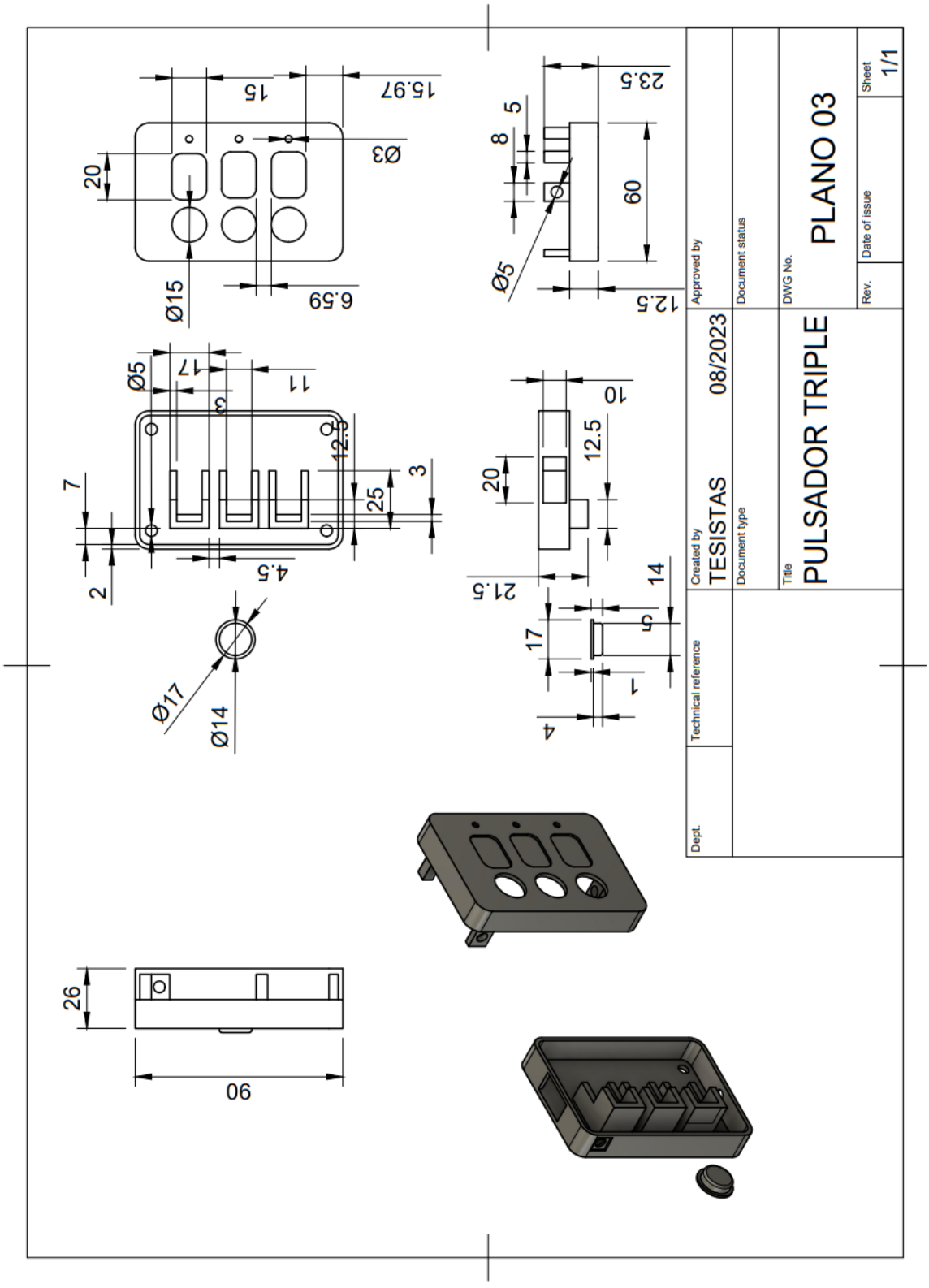
PORTERO ELECTRÓNICO



CAMARA CON SENSOR PIR



PULSADORES TRIPLES



ANEXO H	MANUAL DE MANTENIMIENTO Y ACTUALIZACIÓN DEL SISTEMA	

Introducción El presente manual tiene como objetivo proporcionar las instrucciones necesarias para el mantenimiento adecuado del sistema domótico propuesto. Este sistema está diseñado para gestionar la seguridad del control de acceso al Laboratorio de Manufactura Aditiva y Sustractiva de la Facultad de CIYA utilizando IoT.

Mantenimiento Preventivo El mantenimiento preventivo es fundamental para garantizar el correcto funcionamiento del sistema a largo plazo. A continuación, se detallan las tareas de mantenimiento preventivo recomendadas:

1. Verificación de conexiones: Regularmente, se debe revisar y asegurar que todas las conexiones eléctricas y de comunicación estén firmes y sin signos de deterioro.
2. Limpieza: Es importante mantener limpios los componentes del sistema, como los sensores, actuadores y microcontroladores. Se recomienda utilizar un paño suave y seco para limpiar suavemente las superficies.
3. Revisión de baterías: En caso de contar con baterías en el sistema, se debe verificar periódicamente su estado de carga y reemplazarlas si es necesario.

Mantenimiento Correctivo En caso de presentarse alguna falla o avería en el sistema, se deben seguir los siguientes pasos:

1. Identificación del problema: Es necesario identificar el componente o área del sistema que está presentando la falla. Para ello, se pueden utilizar herramientas de diagnóstico y pruebas.
2. Reparación o reemplazo: Una vez identificado el problema, se debe proceder a reparar o reemplazar el componente defectuoso. Se recomienda contar con repuestos y herramientas adecuadas para llevar a cabo estas tareas.
3. Pruebas de funcionamiento: Después de realizar la reparación o reemplazo, se deben realizar pruebas para asegurarse de que el sistema esté funcionando correctamente.

Actualizaciones y Mejoras Es importante estar al tanto de las actualizaciones y mejoras disponibles para el sistema domótico propuesto. Esto garantizará que el sistema esté

actualizado con las últimas funcionalidades y mejoras de rendimiento. A continuación, se detallan las recomendaciones para las actualizaciones y mejoras del sistema:

1. Actualizaciones de firmware: Se recomienda verificar regularmente si hay actualizaciones de firmware disponibles para los componentes del sistema, como los microcontroladores y los dispositivos de comunicación. Estas actualizaciones pueden mejorar la estabilidad, la seguridad y el rendimiento del sistema.
2. Actualizaciones de software: Además de las actualizaciones de firmware, es importante estar al tanto de las actualizaciones de software para las aplicaciones y plataformas utilizadas en el sistema domótico. Estas actualizaciones pueden agregar nuevas funcionalidades y corregir posibles errores o vulnerabilidades de seguridad.
3. Mejoras de hardware: A medida que avanza la tecnología, pueden surgir nuevos componentes o dispositivos que mejoren el rendimiento o la eficiencia del sistema domótico. Se recomienda estar informado sobre las últimas tendencias y avances en hardware y considerar la posibilidad de realizar mejoras en el sistema.
4. Evaluación de nuevas funcionalidades: A medida que se desarrollan nuevas funcionalidades y tecnologías en el campo de la domótica, es importante evaluar si estas pueden ser beneficiosas para el sistema domótico propuesto. Se recomienda investigar y analizar las nuevas funcionalidades disponibles y determinar si pueden ser implementadas en el sistema existente.
5. Pruebas y validación: Antes de implementar cualquier actualización o mejora en el sistema domótico, es importante realizar pruebas para asegurarse de que no afecten negativamente el funcionamiento del sistema. Se recomienda realizar pruebas en un entorno controlado y validar el correcto funcionamiento antes de implementar los cambios en el sistema.

ANEXO I	MANUAL DE USUARIO	

MANUAL DE USUARIO

GUÍA N°	LABORATORIO:	Manufactura Aditiva y Sustractiva
	ÁREA:	Bloque B
01	NOMBRE DE LA GUÍA:	Manual de usuario del sistema

DESARROLLO

1. OBJETIVO

- Desarrollar un manual que explique cómo operar el sistema implementado en el laboratorio de Manufactura Aditiva y sustractiva de la facultad de CIYA.

2. INTRODUCCIÓN

El sistema de control de accesos implementado tiene como finalidad mejorar el proceso de ingreso al laboratorio al eliminar la dependencia de un responsable para abrir la puerta. Se emplean tres métodos de acceso: el primero se basa en tarjetas electromagnéticas RFID, permitiendo la apertura al acercarlas al sensor correspondiente. El segundo método, mediante reconocimiento facial, utiliza una cámara exterior para identificar a personas registradas. Ambos métodos se integran en una unidad de control tipo portero eléctrico. El tercer método emplea Telegram como interfaz remota para gestionar la apertura de la puerta. Además del acceso, el proyecto incluye una cámara interna que captura fotos de usuarios que ingresan al laboratorio y las envía a Telegram.

Al automatizar la iluminación para ahorrar energía, las luces se activan al detectar ingresos y se apagan tras la inactividad. También, es posible controlar las luces a distancia mediante Telegram. Otro aspecto es el control IoT de tomas de corriente, permitiendo el encendido/apagado remoto de dispositivos conectados.

INSTRUCCIONES

PORTERO ELECTRÓNICO

Fig. 15. Portero Electrónico.

CONEXIONES

El diagrama de conexión del portero se encuentra detallado en la Figura 16.

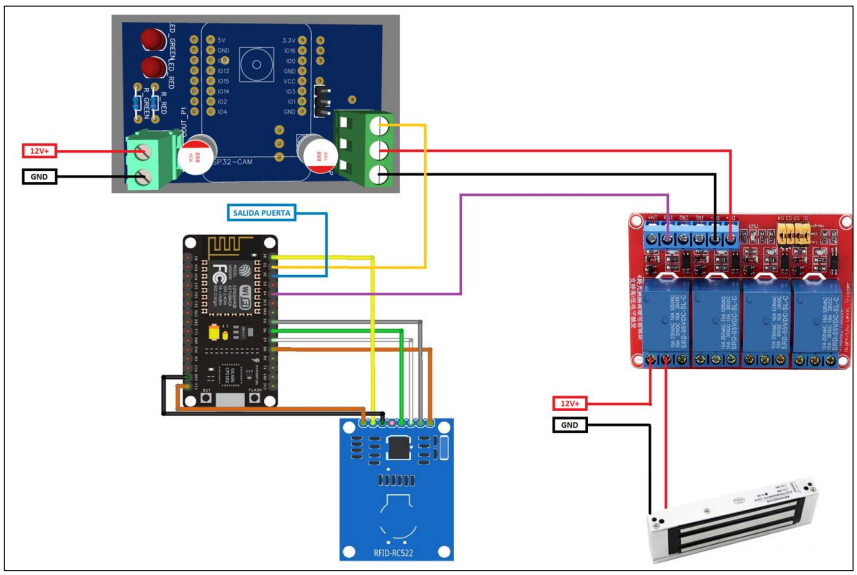


Fig. 16. Conexión del portero.

COMO USARLO

A continuación, se detallará el proceso para agregar un nuevo usuario al sistema de reconocimiento facial. Asegúrese de seguir cada paso cuidadosamente para garantizar un registro exitoso.

Paso 1: Obtención de la Dirección IP de la Página Web

1. Conecte la ESP32-CAM a su computadora mediante el programador correspondiente figura 17.

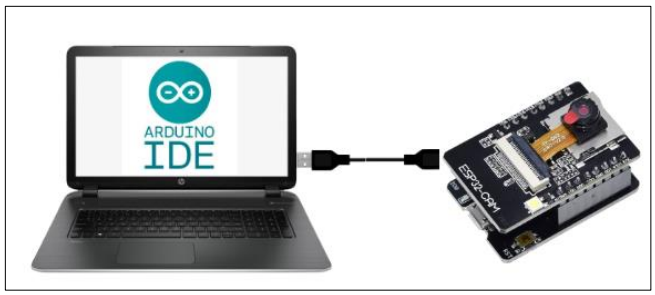


Fig. 17. Conexión de la ESP32-CAM con el computador

2. Abra el "Monitor Serial" en el entorno de desarrollo de Arduino.
3. Realice un reinicio del módulo ESP32-CAM.
4. En el "Monitor Serial", se mostrará la dirección IP de la página web. Anote esta dirección, ya que la necesitará para acceder a la interfaz de usuario figura 18.

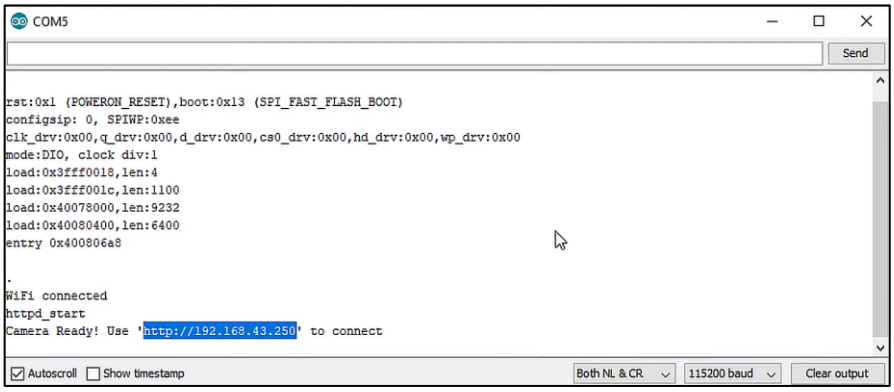


Fig. 18. Monitor serial del IDE de Arduino

Nota: Este proceso se debe realizar solo una vez o cuando cambie las credenciales de usuario y contraseña de la red Wi-Fi. La dirección IP de la página web solo cambiará si se modifica la red Wi-Fi a la que está conectada la ESP32-CAM.

Paso 2: Acceso a la Página Web e Ingreso del Nuevo Usuario

1. Abra un navegador web en su computadora.
2. Ingrese la dirección IP obtenida en el paso anterior en la barra de direcciones del navegador y presione "Enter" figura 19.

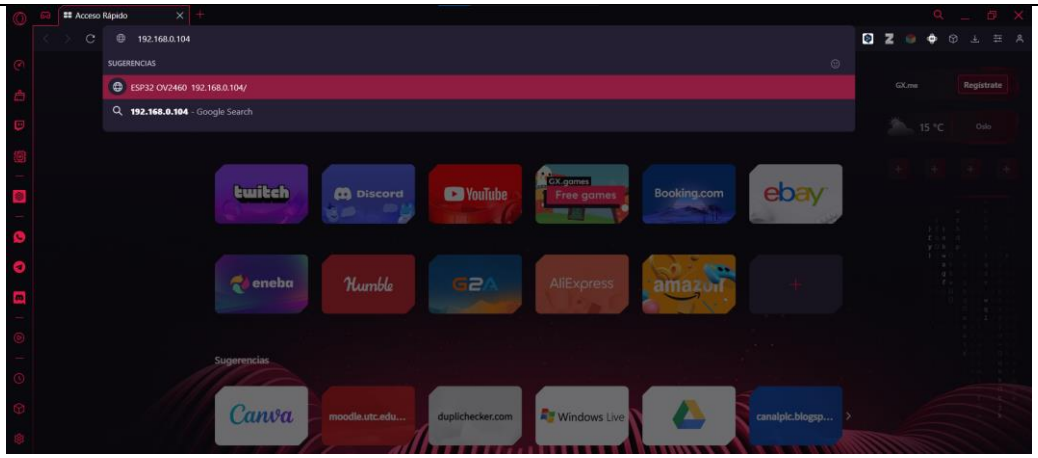


Fig. 19. Colacacion de la IP en el navegador

3. Se abrirá la interfaz de usuario del sistema de reconocimiento facial.

Paso 3: Registro del Nuevo Usuario

1. En la interfaz de usuario, localice el cuadro de texto etiquetado como "Nuevo Usuario".
2. Escriba el nombre del nuevo usuario en el cuadro de texto.
3. Posicione al nuevo usuario frente a la cámara de la ESP32-CAM.

Paso 4: Inicio del Proceso de Registro

1. Presione el botón etiquetado como "Nuevo Usuario" en la interfaz de usuario Figura 6.
2. El sistema comenzará a capturar y guardar el patrón facial del nuevo usuario en la sección correspondiente como muestre la figura 20.

Fig. 20. Ingreso de nuevos usuarios

Nota: Asegúrese de permanecer quieto frente a la cámara hasta que el proceso de registro se complete por completo.

Paso 5: Activación del Sistema de Reconocimiento Facial

1. Una vez finalizado el registro, vuelva a la interfaz de usuario.
2. Localice y presione el botón etiquetado como "Control de Acceso" muestre la figura 21.

Fig. 21. Activación del sistema de reconocimiento facial

Paso 6: Detección de Rostros y Reconocimiento

1. El sistema se activará y comenzará a detectar rostros en tiempo real.
2. Si el nuevo usuario está presente en el área de detección, el sistema lo reconocerá y permitirá el acceso.

¡Enhorabuena! Ha agregado exitosamente un nuevo usuario al sistema de reconocimiento facial. Ahora, el nuevo usuario podrá acceder al área protegida mediante su patrón facial registrado. Recuerde que este proceso garantiza la seguridad y eficacia del sistema. Si tiene alguna pregunta o necesita asistencia adicional, consulte la sección de soporte en el manual del usuario.

SISTEMA DE LECTURA DE TARJETAS RFID

Agregar Nuevos Usuarios al Sistema

Paso 1: Preparación de Hardware y Software

Asegúrate de tener el hardware necesario en funcionamiento:

- Arduino (modelo y versión específicos)
- Módulo lector RFID (por ejemplo, MFRC522)
- Tarjetas o etiquetas RFID en blanco
- Computadora con el IDE de Arduino instalado

Abre el IDE de Arduino en tu computadora y asegúrate de que el entorno esté configurado correctamente para el modelo de Arduino y el módulo lector RFID que estás utilizando.

Paso 2: Código y Configuración

- Abre el archivo de código fuente de tu proyecto en el IDE de Arduino.
- Localiza la sección del código que maneja la lectura de las tarjetas RFID y la identificación de usuarios. Esta sección podría estar en una función llamada setup().
- Para agregar nuevos usuarios, busca la parte del código donde se gestionan las comparaciones de identificación de tarjetas. Deberías ver algo similar a esto :

```
byte Usuario1[4]= {0x45, 0x7D, 0x08, 0x6D} ; //código del usuario 1
byte Usuario2[4]= {0xCC, 0xD7, 0x3A, 0x45} ; //código del usuario 2
```

Agrega una nueva sección similar para cada nuevo usuario que desees agregar. Asegúrate de definir los UID únicos para cada tarjeta RFID en blanco.

Paso 3: Agregar Usuarios

- Abre el archivo de código fuente de tu proyecto en el IDE de Arduino.
- Identifica la sección donde se agregan usuarios nuevos. Esto podría estar al comienzo del código o en una sección designada.
- Agrega un nuevo conjunto de definiciones de UID para el nuevo usuario, utilizando el formato similar al siguiente:

```
byte Usuario3[4]= {0x99, 0x29, 0x22, 0xA3} ; //código del usuario 3
```

  Agrega la lógica necesaria para identificar al nuevo usuario en la sección de comparaciones del paso 2. Por ejemplo:

```
else if(compareArray(ActualUID,Usuario3)){
                    Serial.println("Acceso concedido...");
                    Apertura_Puerta();
                  }
```

- Carga el nuevo código en tu Arduino y prueba el sistema con la nueva tarjeta RFID.

Paso 4: Pruebas y Verificación

- Carga el nuevo código en el Arduino y realiza pruebas para asegurarte de que el nuevo usuario sea identificado correctamente y se realicen las acciones apropiadas.

- Verifica que todas las tarjetas RFID que desees agregar como nuevos usuarios estén configuradas correctamente en el código.

Realiza pruebas para garantizar que el sistema funcione según lo esperado y que los nuevos usuarios sean identificados y tratados de manera adecuada muestre la figura 22.

CAMARA DE FOTOGRAFIA DE REGISTRO

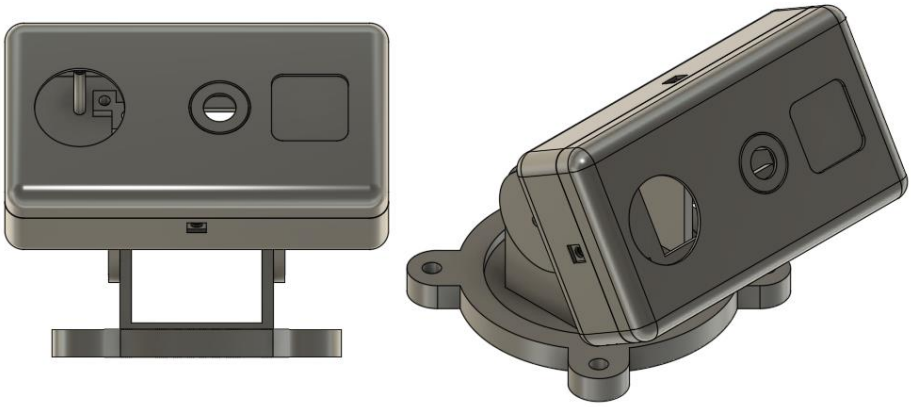


Fig. 22. Cámara de fotografía de registro

CONEXIONES

El diagrama de conexión de la cámara se encuentra detallado en la Figura 23.

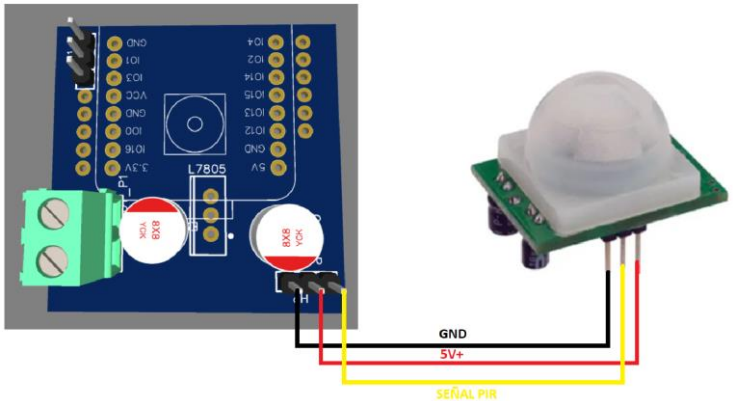


Fig. 23. Conexión de la cámara de registro

COMO USARLO

El sistema de registro fotográfico proporciona una manera eficaz de capturar imágenes de las personas que ingresan y salen del laboratorio, permitiendo llevar un seguimiento de las actividades. Este manual detalla cómo utilizar el sistema paso a paso.

Paso 1: Acceso a las Opciones del Sistema

- Abra la aplicación de mensajería Telegram en su dispositivo Figura 24.

Fig. 24. Telegram en un dispositivo móvil.

- Para acceder a las opciones del sistema, envíe el comando /config en el chat Figura 25.

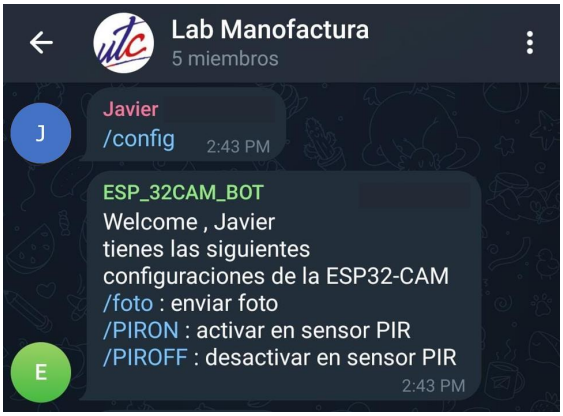


Fig. 25.Comando "/config" en el chad.

Paso 2: Captura y Envío de Fotografía

- Una vez en el menú de opciones (/config), seleccione la opción /foto.
- El sistema capturará automáticamente una fotografía utilizando la cámara Figura 26.

Fig. 26. Comando /foto

La fotografía capturada se enviará a través de Telegram al grupo correspondiente.

Paso 3: Activación del Sensor de Movimiento

Si desea habilitar el sensor de movimiento (PIR) para detectar actividad, utilice el comando /PIRON muestre la figura 27.

Fig. 27. Comando "/PIRON"

Una vez activado, el sistema enviará fotografías cuando se detecte movimiento en la zona.

Paso 4: Desactivación del Sensor de Movimiento

Si desea desactivar el sensor de movimiento, utilice el comando /PIROFF muestre la figura 28.

Fig. 28.Comando "/PIROFF"

La detección de movimiento se desactivará y se dejará de enviar fotografías en caso de actividad.

Nota Importante:

Asegúrese de que el laboratorio tenga una adecuada iluminación para obtener imágenes de calidad.

Mantenga el entorno del sensor de movimiento despejado para una detección precisa.

¡Listo! Ahora está familiarizado con las funciones básicas del sistema de registro fotográfico. Utilice los comandos mencionados para capturar imágenes y controlar el envío de fotos a través de Telegram.

SISTEMA DEL CONTROL IOT

Fig. 29.Sistema de control IoT.

CONEXIONES

El diagrama de conexión para el control del sistema IoT se presenta en la Figura 30.

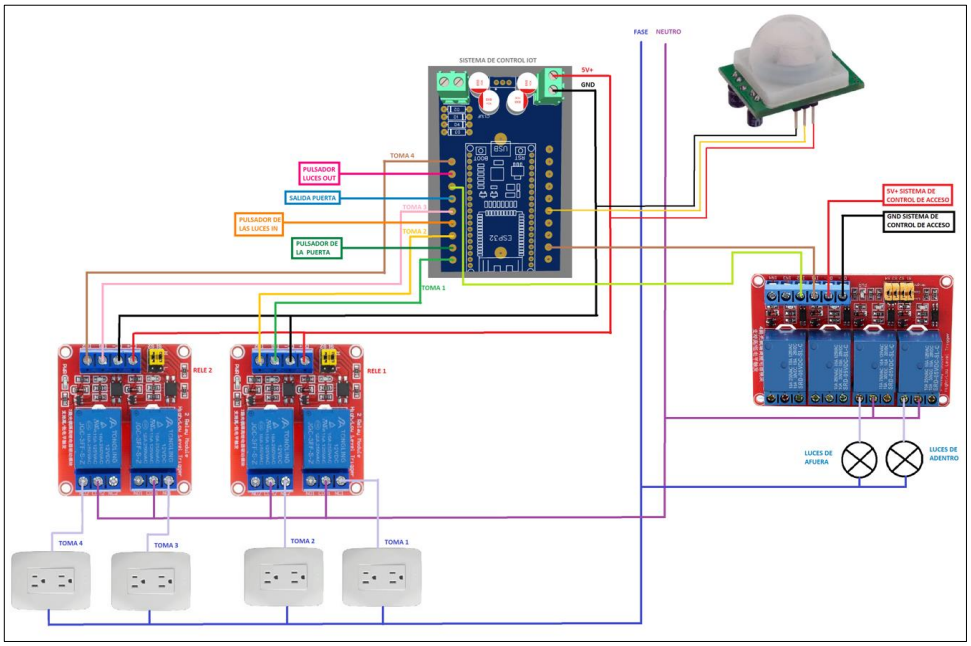


Fig. 30. Conexión del sistema IoT.

COMO USARLO

El sistema ofrece una manera conveniente de gestionar las luminarias, tomacorrientes y la apertura de la puerta mediante un teclado integrado en Telegram. Para acceder a este teclado, sigue los pasos a continuación:

Paso 1: Abre la aplicación Telegram en tu dispositivo móvil o de escritorio muestre la figura 31.

Fig. 31.Telegram en un dispositivo móvil.

Paso 2: En el campo de mensajes, ingresa el comando "opciones" y presiona "Enviar".

Paso 3: El sistema responderá mostrando un teclado con varias opciones de control, como se muestra en la Figura 32.

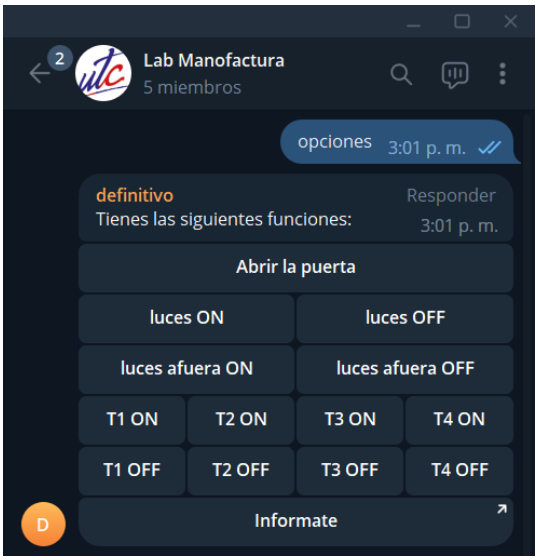


Fig. 32. Comando “opciones” enviado por Telegram.

Paso 4: Selecciona una de las opciones disponibles en el teclado para realizar la acción correspondiente. A continuación, se detallan las funciones de cada botón en la Tabla 2.

Tabla 2. Funciones del teclado del sistema IoT en Telegram

BOTON	ACCIÓN
Comando “Opciones”	Devuelve la botonera en donde se encuentran las diferentes acciones que se pueden realizar.
Abrir la puerta	Permite la apertura de la puerta.
LUCES ON	Enciende las luces internas del laboratorio.
LUCES OFF	Apaga las luces internas del laboratorio.
LUCES AFUERA ON	Enciende las luces exteriores del laboratorio.
LUCES AFUERA ON	Apaga las luces exteriores del laboratorio.
T1 ON	Activa la alimentación del tomacorriente número uno.
T1 OFF	Desactiva la alimentación del tomacorriente número uno.
T2 ON	Activa la alimentación del tomacorriente número dos.
T2 OFF	Desactiva la alimentación del tomacorriente número dos.
T3 ON	Activa la alimentación del tomacorriente número tres.

T3 OFF	Desactiva la alimentación del tomacorriente número tres.
T4 ON	Activa la alimentación del tomacorriente número cuatro.
T4 OFF	Desactiva la alimentación del tomacorriente número cuatro.
Infórmate	Abre un link en donde está el manual de usuario del sistema.

Con estos sencillos pasos, podrás controlar las funciones del sistema IoT de manera conveniente a través de Telegram.

ANEXO J	DIAGRAMAS DE CONEXIÓN	

En la figura 33 se muestran las borneras de salida de la placa del sistema de control IoT.

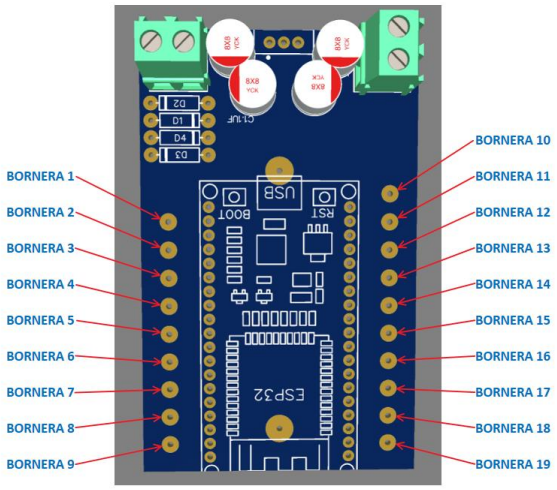


Fig. 33. Borneras de salida del sistema de control IoT.

En la figura 34 se muestra el diagrama de conexión del sistema de accionamiento de los tomacorrientes.

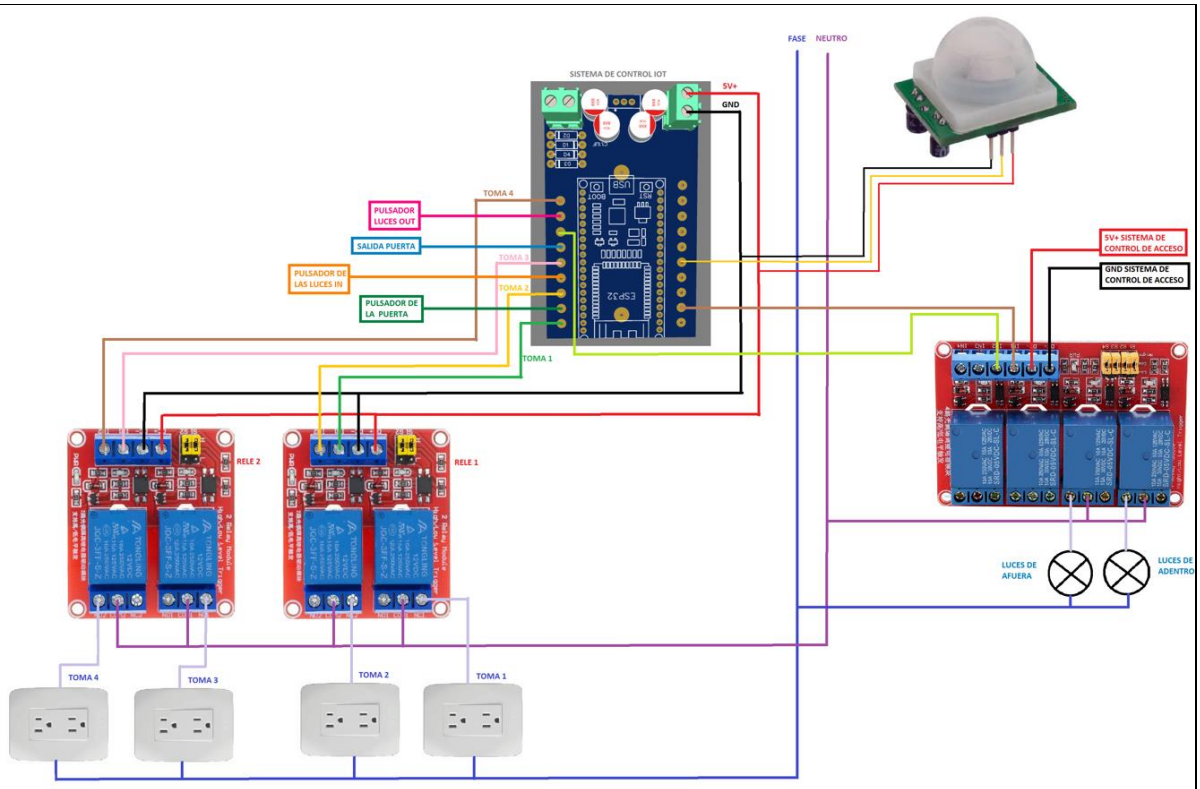


Fig. 34. Diagrama de conexión del sistema de accionamiento de los tomacorrientes.

En la figura 35 se muestra el diagrama de conexión del sistema de control de acceso.

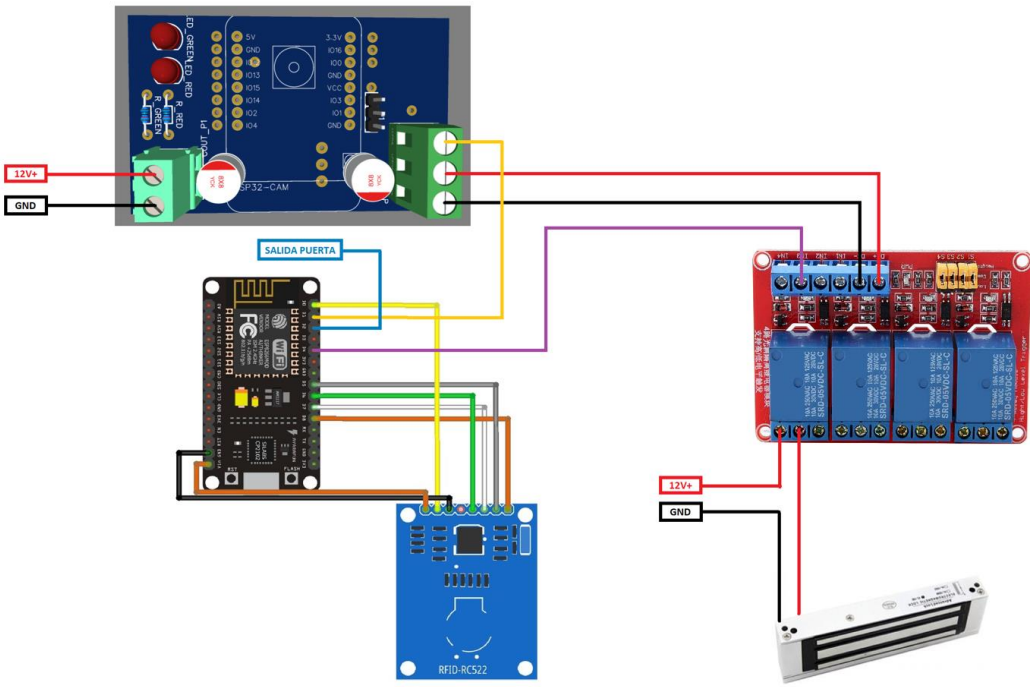


Fig. 35.Diagrama de conexión del sistema de control de acceso.

En la figura 36 se muestra el diagrama de conexión del sistema de fotografía de registro

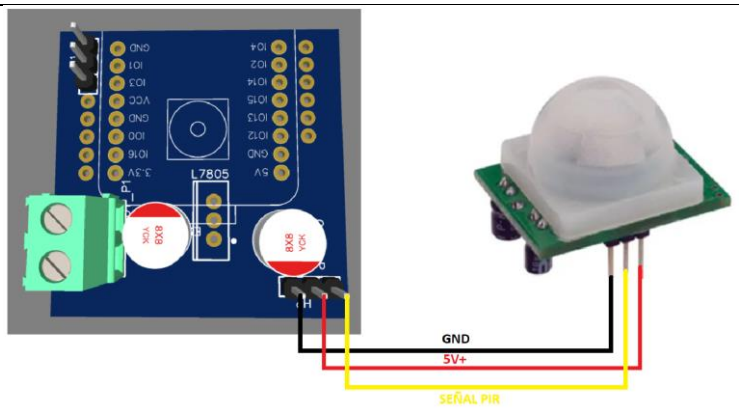


Fig. 36. Diagrama de conexión del sistema de fotografía de registro.

En la figura 37 se muestra el diagrama de conexión de alimentación del sistema.

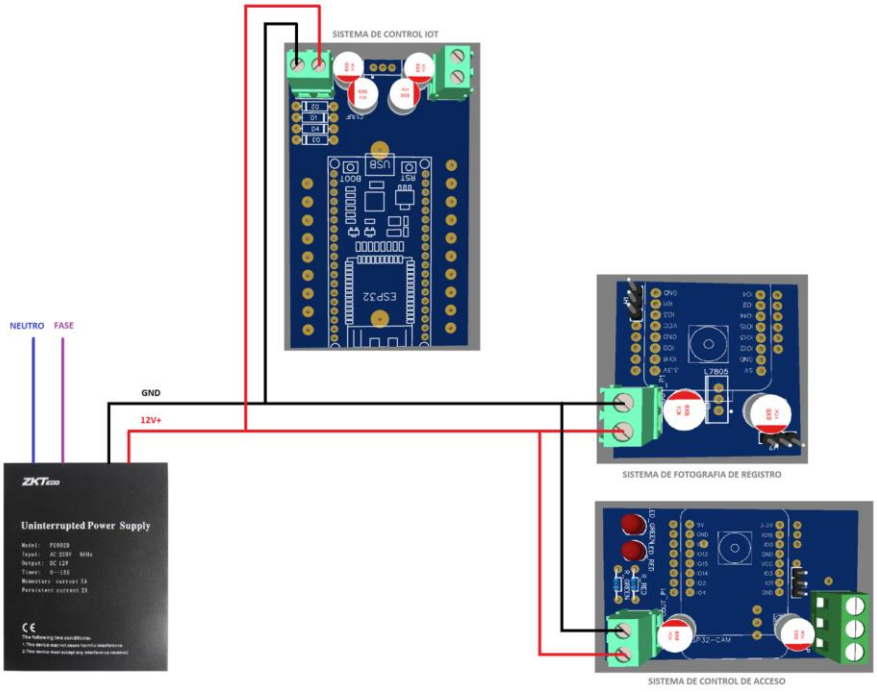


Fig. 37. Diagrama de conexión de alimentación del sistema.

ANEXO K	PLANOS DE LOS MODELOS 3D REALIZADOS	

ANEXO L	COMPONENTES EMPLEADOS EN EL DISEÑO	

PARTE ELECTRICA

Conductores

Especificaciones técnicas de los conductores.

USO	CALIBRE (AWG)	DIÁMETRO APROX. (MM)	CORRIENTE NOMINAL (A)	MATERIAL
ALIMENTACIÓN	12	2.05	20	Cobre
ALIMENTACIÓN	14	1.63	15	Cobre
CONEXIÓN A TIERRA	14	1.63	15	Cobre
ALIMENTACIÓN	18	1.02	7	Cobre
ALIMENTACIÓN	22	0.64	3	Cobre

Protecciones

CARACTERÍSTICA	DISYUNTOR DE 25A	DISYUNTOR DE 10A
AMPERAJE NOMINAL	25A	10A
TIPO	Térmico-magnético	Térmico-magnético
CAPACIDAD DE INTERRUPCIÓN	1000-5000A (depende del modelo)	1000-5000A (depende del modelo)
VOLTAJE NOMINAL	Dependerá del sistema eléctrico	Dependerá del sistema eléctrico
USO	Protección contra sobrecargas y cortocircuitos	Protección contra sobrecargas y cortocircuitos
CARACTERÍSTICAS ADICIONALES	Manija de operación, indicador de estado, capacidad de reinicio después de sobrecarga	Manija de operación, indicador de estado, capacidad de reinicio después de sobrecarga

Luminarias

Especificaciones técnicas de las luminarias leds.

NIVELES DE LÚMENES	TIPO DE LUZ RECOMENDADO	APLICACIÓN	POTENCIA ESTIMADA (W)
1200 - 2000	Neutra/Fría (4000K - 5000K)	Áreas de trabajo detallado, garajes, espacios comerciales	10 - 15
2000 - 3000	Fría (5000K - 6500K)	Iluminación exterior, seguridad, áreas de alto contraste	15 - 20

UPS del sistema

Consumo de los elementos que debe abastecer el UPS

DESCRIPCIÓN	CANTIDAD	CONSUMO(W)	TOTAL(W)	TOTAL(VA)
ESP32	1	0.5	0.5	0.6
ESP32-CAM CON LA OV2640	2	1	2	2.2
ESP8266	1	0.3	0.3	0.3
MODULO RFID	1	0.3	0.3	0.3
SENSOR PIR	6	0.05	0.3	0.3
MODULO RELE 2 VIAS	2	0.5	1	1.1
MODULO RELE 4 VIAS	1	0.7	0.7	0.8
CERRADURA ELÉCTRICA	1	10	10	11.1
LUMINARIA OJO DE BUEY	1	5	5	5.6

REUTER	1	20	20	22.2
SENSOR SW-18010P	22	0.05	1.1	1.2
BOCINA DE ALARMA DE 116DB	3	10	30	33.3
ESP32-CAM CON LA OV5640	10	1	10	11.1
LUMINARIAS CON LUCES NEUTRAS O FRIAS (4000K - 5000K) DE 1200 - 2000 LM A 35 - 40W	10	40	400	444.4
LUMINARIAS CON LUCES FRIAS (5000K - 6500K) DE 2000 - 3000 LM A 45 – 60W	6	60	360	400.0
SENSOR MQ-2	2	0.5	1	1.1
TUBO FLUORESCENTE	6	20	120	133.3
INPRESORA 3D	5	500	2500	2777.8
LAPTOP	8	200	1600	1777.8
TOTAL			5062.2	5624.7
SOBREDIMENCIONAMIENTO 50%			1.5	8437.0

El UPS elegido es el UPS CDP ON LINE UPO22-10AX con capacidad de 10000W para que pueda abastecer la demanda del sistema

UPS CDP ON LINE UPO22-10AX

CARACTERÍSTICA	VALOR
CAPACIDAD	10000VA/10000W
BATERÍAS	20 baterías de 12V, 9Ah cada una
FORMA DE ONDA	Onda sinusoidal pura
PESO	142 kg
RANGO DE VOLTAJE DE ENTRADA	110 a 300 Vca +/-3 (LL)
RANGO DE VOLTAJE DE SALIDA	104/110/115/120Vac o 208/220/230/240Vac
DIMENSIONES	250 x 826 x 592 mm
CERTIFICACIONES	CIDET, ISO9001, ISO14001, NOM, TABLA, UL

Electrónicos

Alarma

Especificaciones técnicas de las alarmas lo que se toma en cuenta para esta elección son los decibelios.

ALARMA - SIRENA ELECTRÓNICA 116DB

ESPECIFICACIONES TÉCNICAS
VOLTAJE: 12-24VCC
TONOS: 32 SELECCIONABLES
PESO: 1 KG
NIVEL DE SONIDO: 116 DB
DIMENSIONES: AMA

Cámara

Especificaciones técnicas de la carama ESP32-CAM con el módulo de cámara OV5640.

CARACTERÍSTICA	ESP32-CAM	MÓDULO DE CÁMARA OV5640
MICROCONTROLADOR	ESP32-D0WDQ6	OV5640
FRECUENCIA DE RELOJ	Hasta 240 MHz	-
CONECTIVIDAD	Wi-Fi, Bluetooth	-
RAM	520 KB SRAM	-
ALMACENAMIENTO	4 MB Flash	-
INTERFAZ DE CÁMARA	SCCB	SCCB
ALIMENTACIÓN	5V (micro USB o batería Li-Po)	2.8V ~ 3.3V
INTERFAZ DE SALIDA DE IMAGEN	-	JPEG / YUV422 / RGB565
RESOLUCIÓN MÁXIMA	-	5 MP (2592 x 1944)
TAMAÑO DEL PÍXEL	-	1.4 µm x 1.4 µm
ENFOQUE	-	Autofocus (20 cm al infinito)
DIMENSIONES	27 mm x 40 mm	-

Sensor para detectar incendios MQ-2

Especificaciones técnicas del sensor contra incendios MQ-2.

CARACTERÍSTICA	VALOR
NOMBRE DEL SENSOR	MQ-2
DETECTA	Gas inflamable (LPG, butano, etc.), humo, alcohol, CO y otros gases inflamables
VOLTAJE DE OPERACIÓN	5V DC
CONSUMO DE CORRIENTE	150 mA (en calefacción), 5 mA (en reposo)
SALIDA ANALÓGICA	Sí (varía según la concentración de gas)
SENSIBILIDAD	Ajustable mediante potenciómetro
TIEMPO DE RESPUESTA	<10 segundos
TIEMPO DE PRE-CALENTAMIENTO	1-2 minutos
RANGO DE CONCENTRACIÓN DETECTABLE	300-10,000 ppm (gases inflamables), 300-5000 ppm (CO)
TEMPERATURA DE OPERACIÓN	-10°C a 50°C
HUMEDAD DE OPERACIÓN	95% RH máx
VIDA ÚTIL ESTIMADA	Más de 5 años

Sensor para detectar ruptura de ventanas SW-18010P

Especificaciones técnicas del sensor para detectar la ruptura de ventanas SW-1810P

CARACTERÍSTICA	VALOR
NOMBRE DEL SENSOR	SW-18010P
TIPO	Interruptor de vibración
SENSIBILIDAD	> 1.8 g
VOLTAJE DE OPERACIÓN	2.7V - 5.2V
CORRIENTE DE OPERACIÓN	< 5 mA
SALIDA	Salida de contacto momentáneo
RESISTENCIA DE CONTACTO	< 10 Ω
VIDA ÚTIL ESTIMADA	Más de 50,000 ciclos
TIEMPO DE RESPUESTA	< 2 ms
TEMPERATURA DE OPERACIÓN	-10°C a 60°C
DIMENSIONES	4.7 mm x 12.8 mm

Sensor RFID

Características técnicas del sensor RFID

CARACTERÍSTICA	VALOR
MODELO	RFID RC522
FRECUENCIA DE OPERACIÓN	13.56 MHz
PROTOCOLO DE COMUNICACIÓN	SPI

DISTANCIA DE LECTURA	Hasta varios centímetros
TIPO DE ETIQUETA	Pasiva (requiere energía del lector)
MODULACIÓN	ASK (Amplitude Shift Keying)
VELOCIDAD DE COMUNICACIÓN	Hasta 10 Mbps
ALIMENTACIÓN	3.3V
INTERFACES	SPI, UART (dependiendo del módulo)
MEMORIA INTERNA	Memoria para almacenar datos y claves
USO	Identificación, control de acceso, etc.

Sensor de detección de movimiento PIR

Características técnicas del sensor PIR

CARACTERÍSTICA	VALOR
TIPO DE SENSOR	PIR (Passive Infrared)
VOLTAJE DE OPERACIÓN	3.3V - 5V
CORRIENTE EN REPOSO	< 50 µA
CORRIENTE EN DETECCIÓN	15 mA - 20 mA
ALCANCE DE DETECCIÓN	5 - 7 metros
ÁNGULO DE DETECCIÓN	120 grados
TIEMPO DE RETARDO	Ajustable (segundos)
SENSIBILIDAD	Ajustable (distancia)
SALIDA	Digital (HIGH/LOW)
TEMPERATURA DE OPERACIÓN	-20°C a 60°C
HUMEDAD DE OPERACIÓN	5% - 95%
DIMENSIONES	Variable

Modulo relé de 4 vías

Relé de cuatro vías para automatizar tomacorrientes y luminarias

CARACTERÍSTICA	VALOR
TIPO DE RELÉ	4 Vías (4 Canales)
CORRIENTE NOMINAL	10:00 a. m.
VOLTAJE DE OPERACIÓN	110 V
VOLTAJE DE CONTROL (ARDUINO)	5V
TIPO DE CONTACTO	SPDT (Form C)
CARGA MÁXIMA	1100W
TIPO DE CONEXIÓN	Terminal de tornillo
TIEMPO DE CONMUTACIÓN	Milisegundos
DIMENSIONES	Variable
PROTECCIÓN CONTRA CORRIENTE INVERSA	Diodo de protección
USO	Control de cargas eléctricas

Modulo ESP32

ESP32 para que funcione como cerebro del sistema

CARACTERÍSTICA	VALOR
MICROCONTROLADOR	ESP32-D0WDQ6 (dual-core 32-bit MCU)
FRECUENCIA DE OPERACIÓN	Hasta 240 MHz
MEMORIA RAM	520 KB
ALMACENAMIENTO FLASH	4 MB
CONECTIVIDAD	Wi-Fi 802.11 b/g/n, Bluetooth 4.2
GPIO	34 pines GPIO
INTERFACES	UART, SPI, I2C, I2S, PWM, ADC, DAC
VOLTAJE DE OPERACIÓN	2.2V - 3.6V

CONSUMO DE CORRIENTE	Depende de la actividad
DIMENSIONES	Varias dimensiones y formatos
SISTEMA OPERATIVO	FreeRTOS
PERIFÉRICOS ADICIONALES	RMT, LEDC, SDMMC, CAN, IR, etc.

Modulo ESP8266

Características técnicas del módulo ESP8266

CARACTERÍSTICA	VALOR
MICROCONTROLADOR	ESP8266
FRECUENCIA DE OPERACIÓN	Hasta 160 MHz
MEMORIA RAM	80 KB
ALMACENAMIENTO FLASH	512 KB
CONECTIVIDAD	Wi-Fi 802.11 b/g/n
GPIO	17 pines GPIO
INTERFACES	UART, SPI, I2C
VOLTAJE DE OPERACIÓN	3.3V
CONSUMO DE CORRIENTE	Depende de la actividad
DIMENSIONES	Varias dimensiones y formatos
SISTEMA OPERATIVO	FreeRTOS
PERIFÉRICOS ADICIONALES	PWM, ADC, GPIO Interrupts, etc.

Costos de los elementos descritos

Descripción	Unidad	Cantidad	P. Unitario	P. Total
ESP32	U	1	12	12
ESP32-CAM CON LA OV2640	U	2	16	32
ESP8266	U	1	7	7
MODULO RFID	U	1	4.5	4.5
SENSOR PIR	U	6	2.5	15
MODULO RELE 2 VIAS	U	2	2.55	5.1
MODULO RELE 4 VIAS	U	1	5.8	5.8
IMPRESIÓN DE PLACA PCB	U	13	8	104
IMPRESIÓN 3D	U	28	6	168
CABLE 22 AWG	M	100	0.35	35
CABLE 18 AWG	M	35	0.4	14
CABLE 10 AWG	M	15	0.8	12
CONDENSADORES	U	30	0.2	6
RESISTENCIAS	U	15	0.1	1.5
ESPIRAL	M	1	1	1
LM7805	U	14	0.35	4.9
CERRADURA ELÉCTRICA	U	1	30	30
FUENTE DE ALIMENTACIÓN	U	1	55	55
LUMINARIA OJO DE BUEY	U	1	5.55	5.55
CAJA DE PROYECTOS	U	1	5.8	5.8
TOMACORRIENTE	U	9	2.6	23.4
CAJA PARA TOMACORRIENTE	U	9	2.3	20.7
CANALETA	U	8	3.8	30.4
PUERTA LÓGICA	U	2	0.75	1.5
OPTOACOPLADORES	U	4	0.32	1.28

REUTER	U	1	25	25
SENSOR SW-18010P	U	22	2.5	55
BOCINA DE ALARMA DE 116DB	U	3	10	30
ESP32-CAM CON LA OV5640	U	10	22	220
LUMINARIAS CON LUCES NEUTRAS O FRIAS (4000K - 5000K)	U	10	13	130
LUMINARIAS CON LUCES FRIAS (5000K - 6500K)	U	6	15	90
SENSOR MQ-2	U	2	3	6
HERRAMIENTAS Y CONSUMIBLES	U	1	60	60
TOTAL				1217.43