ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN

DISEÑO Y CONSTRUCCIÓN DE UN PROTOTIPO DE SISTEMA EMBEBIDO DE SEGURIDAD, SUPERVISADO MEDIANTE UNA RED SOCIAL, PARA EL CENTRO "PSICOLÓGICO INFANTIL - PSICOVID"

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA Y AUTOMATIZACIÓN

AUTOR:

HERNÁN DAVID CHAFLA POMA

Riobamba - Ecuador

2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN

DISEÑO Y CONSTRUCCIÓN DE UN PROTOTIPO DE SISTEMA EMBEBIDO DE SEGURIDAD, SUPERVISADO MEDIANTE UNA RED SOCIAL, PARA EL CENTRO "PSICOLÓGICO INFANTIL - PSICOVID"

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA Y AUTOMATIZACIÓN

AUTOR: HERNÁN DAVID CHAFLA POMA

DIRECTOR: Ing. José Enrique Guerra Salazar Msc.

Riobamba - Ecuador

2022

Yo, Hernán David Chafla Poma, declaro que el presente trabajo de integración curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

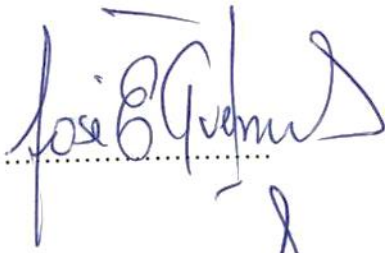
Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de integración curricular, el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 25 de octubre del 2022

Hernán David Chafla Poma
060572965-6

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN

El Tribunal del Trabajo de Integración Curricular certifica que: El trabajo de Integración Curricular; Tipo: Proyecto Técnico, **DISEÑO Y CONSTRUCCIÓN DE UN PROTOTIPO DE SISTEMA EMBEBIDO DE SEGURIDAD, SUPERVISADO MEDIANTE UNA RED SOCIAL, PARA EL CENTRO "PSICOLÓGICO INFANTIL -PSICOVID"**, realizado por el señor **HERNÁN DAVID CHAFLA POMA**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribuna Autoriza su presentación.

	FIRMA	**FECHA**
Ing. Pablo Eduardo Lozada **PRESIDENTE DEL TRIBUNAL**		2022-10-25
Ing. José Guerra Salazar **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2022-10-25
Ing. Franklin Moreno Montenegro **ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2022-10-25

DEDICATORIA

A Dios por absolutamente todo lo que soy, lo que me rodea y lo que me espera. A mi padre Julio Hernán Chafla Méndez por enseñarme el verdadero sentido, valor e importancia de hacer un buen trabajo, y compartir conmigo los frutos obtenidos de hacer el suyo. A mi madre Carmen Elisa Poma Ramos por formarme como una persona con valores y enseñarme que verdaderamente es lo que nos diferencia del resto. A mis hermanos Jimena y Anthony por extender su mano en mis momentos de necesidad. A mi familia entera, que hasta el día de hoy ha sido soporte para mi formación como persona y como profesional.

David

AGRADECIMIENTO

A Dios, mis padres, hermanos y familia por su amor sobre mí y la lucha que enfrentan a diario por ver que cumpla mis sueños. A los docentes de mi querida Escuela Superior Politécnica de Chimborazo por compartir su saber para mi formación profesional, especialmente a mi docente tutor el Ing. José Guerra por su instrucción y el tiempo que empleo en la guía para la elaboración de este proyecto de integración curricular.

David

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS ..... **ix**
ÍNDICE DE ILUSTRACIONES ..... **xi**
ÍNDICE DE ANEXOS ..... **xiv**
RESUMEN ..... **xv**
SUMMARY ..... **xvi**
INTRODUCCIÓN **1**
CAPÍTULO I
1. DIAGNÓSTICO DEL PROBLEMA **2**
1.1. Antecedentes **2**
1.2. Planteamiento del problema **4**
1.2.1. Sistematización del problema ***4***
1.3. Justificación Teórica **5**
1.3.1. Justificación Aplicativa ***7***
1.4. Objetivo General **8**
1.4.1. Objetivos específicos ***9***
1.5. Metodología **9**
CAPÍTULO II
2. MARCO TEÓRICO **10**
2.1. Sistemas de seguridad comerciales **10**
2.1.1. Vulnerabilidades de los sistemas de seguridad comerciales ***11***
2.2. Control de acceso **13**
2.2.1. Tecnologías aplicadas al control de acceso ***13***
2.2.2. Comparativa de tecnologías aplicadas al control de acceso ***17***
2.3. Realidad de la zona **19**
2.4. Normativas **21**
2.5. Arquitectura **23**
2.5.1. Elementos de adquisición de datos ***25***
2.5.1.1. Comparativa entre elementos de adquisición de datos *26*
2.5.2. Elementos de actuación ***27***
2.5.3. Baterías ***28***
2.5.3.1. Comparativa entre baterías *29*
2.5.4. Tarjeta de desarrollo ***29***
2.5.4.1. Comparativa entre tarjetas de desarrollo *30*

2.6. Redes sociales y su frecuencia de uso **31**
2.6.1. Comparativa entre redes sociales de mensajería ***32***
2.6.2. Prácticas de seguridad para la utilización de redes sociales ***33***
CAPÍTULO III
3. MARCO METODOLÓGICO **35**
3.1. Requerimientos del PSES **35**
3.2. Concepción de la arquitectura general del prototipo **36**
3.2.1. Módulo de adquisición de datos ***37***
3.2.2. Módulo de control y actuación ***37***
3.2.3. Módulo de administración, control y visualización de la información ***38***
3.3. Diseño de la arquitectura de los módulos del PSES **38**
3.3.1. Módulo de adquisición de datos ***38***
3.3.2. Módulo de control y actuación ***39***
3.4. Selección del *hardware* para el PSES **40**
3.4.1. ESP8266 Wemos D1 mini ***40***
3.4.2. Sensor magnético MC-38 ..... ***41***
3.4.3. Sensor de movimiento DSC LC-100-PI ***42***
3.4.4. Módulo sensor de vibración Ky-002 ..... ***43***
3.4.5. Módulo RFID/NFC PN532 ..... ***44***
3.4.6. Cerradura magnética ZE-280-5T ***45***
3.4.7. Alarma audible 12V Opalux ***46***
3.4.8. Otros elementos ***47***
3.4.9. Batería para el PSES ***49***
3.5. Esquema de conexión del PSES **52**
3.5.1. Esquema de conexión del bloque de alimentación ***52***
3.5.2. Esquema de conexión del módulo de adquisición de datos ***53***
3.5.2.1. Adquisición de datos para el control de acceso *53*
3.5.2.2. Adquisición de datos para el sistema de alarma *55*
3.5.3. Esquema de conexión del módulo de control y actuación ***59***
3.6. Diseño del *software* para el PSES **61**
3.6.1. Software de desarrollo para el PSES ***62***
3.6.2. Software requerido para la comunicación del PSES ***63***
3.6.2.1. Creación de base de datos en Firebase *63*
3.6.2.2. Creación de bot Telegram *63*
3.6.3. Programas software del PSES ***64***
3.6.3.1. Programa software del módulo de adquisición de datos *64*

3.6.3.2. Programas software del módulo de control y actuación 73
3.7. Interfaces gráficas del módulo de administración, control y visualización de la información 76
3.7.1. Interfaz de control y visualización de la información -Telegram 76
3.7.2. Software para el dispositivo móvil 77
3.8. Diseño estructural del prototipo 79
3.8.1. Estructura para el módulo de adquisición de datos orientado al control de acceso 79
3.8.2. Estructura para el módulo de adquisición de datos orientado al sistema de alarma 81
CAPÍTULO IV
4. MARCO DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 83
4.1. Caracterización de los módulos de adquisición de datos 85
4.1.1. Validación de los elementos de sensado del módulo de adquisición de datos 1 85
4.1.2. Validación de los elementos de sensado del módulo de adquisición de datos 2 88
4.1.3. Validación de los elementos de sensado del módulo de adquisición de datos 3 90
4.1.4. Validación de los elementos de sensado del módulo de adquisición de datos 4 91
4.2. Caracterización del módulo de control y actuación 93
4.2.1. Repetibilidad en la comunicación entre el módulo de control y actuación y los módulos de adquisición de datos 93
4.2.2. Repetibilidad en la activación de la cerradura magnética 100
4.3. Caracterización del módulo de administración, control y visualización de la información 101
4.3.1. Pruebas de transmisión de la información para el control del PSES 101
4.3.2. Prueba de registro de usuarios para el control de acceso 104
4.4. Caracterización de la comunicación para los módulos de PSES 106
4.5. Pruebas de la alimentación del PSES 109
4.5.1. Consumo energético del PSES 109
4.5.2. Estimación de la carga y descarga de la batería 110
4.6. Funcionamiento general del PSES 111
4.7. Análisis económico para la construcción del PSES 114
4.7.1. Comparativa con un sistema comercial 115
CONCLUSIONES 117
RECOMENDACIONES 119
BIBLIOGRAFÍA
ANEXOS

ÍNDICE DE TABLAS

Tabla 1-2: Vulnerabilidades de los sistemas de seguridad comerciales 11
Tabla 2-2: Comparativa de tecnologías aplicadas al control de acceso 18
Tabla 3-2: Comparativa entre elementos de adquisición de datos 26
Tabla 4-2: Comparativa entre baterías 29
Tabla 5-2: Comparativa entre tarjetas de desarrollo 30
Tabla 6-2: Comparativa entre redes sociales de mensajería 32
Tabla 1-3: Especificaciones técnicas principales de la ESP8266 Wemos D1 mini 41
Tabla 2-3: Especificaciones técnicas principales del sensor magnético MC-38 42
Tabla 3-3: Especificaciones técnicas principales del sensor de movimiento DSC LC-100-PI 43
Tabla 4-3: Especificaciones técnicas principales del módulo sensor de vibración Ky-002 . 44
Tabla 5-3: Especificaciones técnicas principales del módulo RFID/NFC PN532 45
Tabla 6-3: Especificaciones técnicas principales de la cerradura magnética ZE-280-5T 46
Tabla 7-3: Especificaciones técnicas principales de la alarma audible 47
Tabla 8-3: Cálculo de consumo de corriente en el PSES 50
Tabla 9-3: Especificaciones técnicas de la batería Rekoser RKE12-7 51
Tabla 10-3: Medidas más importantes para la estructura del módulo de adquisición de datos 1 81
Tabla 11-3: Medidas más importantes para la estructura del módulo de adquisición de datos 2, 3 y 4 82
Tabla 1-4: Validación del sensor magnético 1 MC-38 85
Tabla 2-4: Repetibilidad de lecturas NFC para un estado activo 87
Tabla 3-4: Repetibilidad de lecturas NFC para un estado inactivo 88
Tabla 4-4: Validación del sensor de movimiento 1 DSC LC-100-PI 89
Tabla 5-4: Validación del sensor magnético 2 MC-38 90
Tabla 6-4: Validación del sensor de movimiento 2 DSC LC-100-PI 92
Tabla 7-4: Comunicación entre el módulo de control y actuación- módulo de adquisición de datos 1 94
Tabla 8-4: Comunicación entre el módulo de control y actuación- módulo de adquisición de datos 2 95
Tabla 9-4: Comunicación entre el módulo de control y actuación- módulo de adquisición de datos 3 97

Tabla 10-4: Comunicación entre el módulo de control y actuación-módulo de adquisición de datos 4 99
Tabla 11-4: Repetibilidad en la activación de la cerradura magnética..... 101
Tabla 12-4: Pruebas de transmisión de la información para el control del PSES 103
Tabla 13-4: Consumo de corriente del PSES para un estado activo e inactivo..... 109
Tabla 14-4: Análisis económico para la construcción del PSES..... 114
Tabla 15-4: Comparativa entre las características del PSES y un sistema comercial..... 115

ÍNDICE DE ILUSTRACIONES

Ilustración 1-2: Componentes más comunes de un sistema de control de acceso autónomo14
Ilustración 2-2: Plano estructural del centro "Psicológico Infantil PSICOVID" 20
Ilustración 3-2: Horas de desconexión de energía eléctrica en Ecuador..... 21
Ilustración 4-2: Arquitectura centralizada de un sistema de seguridad 23
Ilustración 5-2: Arquitectura distribuida de un sistema de seguridad 24
Ilustración 6-2: Componentes que conforman un sistema de seguridad social 24
Ilustración 1-3: Arquitectura general del PSES..... 36
Ilustración 2-3: Diagrama de bloques del módulo de adquisicion de datos 39
Ilustración 3-3: Diagrama de bloques del módulo de control y actuación..... 40
Ilustración 4-3: ESP8266 Wemos D1 mini..... 41
Ilustración 5-3: Sensor magnético MC-38 42
Ilustración 6-3: Sensor de movimiento DSC LC-100-PI..... 43
Ilustración 7-3: Módulo sensor de vibración Ky-002..... 44
Ilustración 8-3: Módulo RFID/NFC PN532..... 45
Ilustración 9-3: Cerradura magnética ZE-280-5T..... 46
Ilustración 10-3: Alarma audible 12V Opalux 47
Ilustración 11-3: Convertidor DC-DC MP2307 48
Ilustración 12-3: Módulo DFPlayer Mini MP3 48
Ilustración 13-3: Módulo relé de 1 canal..... 49
Ilustración 14-3: Fuente de alimentación UHPPOTE 49
Ilustración 15-3: Bateria Rekoser RKE12-7 51
Ilustración 16-3: Esquema de conexión del bloque de alimentación 53
Ilustración 17-3: Adquisición de datos para el control de acceso..... 54
Ilustración 18-3: PCB y construcción del módulo de adquisición de datos para el control de acceso 55
Ilustración 19-3: Módulo de adquisición de datos 2 56
Ilustración 20-3: PCB y construcción del módulo de adquisición de datos 2 56
Ilustración 21-3: Módulo de adquisición de datos 3 57
Ilustración 22-3: PCB y construcción del módulo de adquisición de datos 3 58
Ilustración 23-3: Módulo de adquisición de datos 4 59
Ilustración 24-3: PCB y construcción del módulo de adquisición de datos 4 59
Ilustración 25-3: Esquema de conexión del módulo de control y actuación..... 61
Ilustración 26-3: PCB y construcción del módulo de control y actuación..... 61

Ilustración 27-3: Diagrama de flujo del módulo de adquisición de datos orientado al control de acceso 67
Ilustración 28-3: Diagrama de flujo para el módulo de adquisición de datos 2 69
Ilustración 29-3: Diagrama de flujo para el módulo de adquisición de datos 3 71
Ilustración 30-3: Diagrama de flujo para el módulo de adquisición de datos 4 73
Ilustración 31-3: Diagrama de flujo del módulo de control y actuación 75
Ilustración 32-3: Mensajes del PSES enviados a Telegram..... 76
Ilustración 33-3: Ventana principal de la aplicación móvil 77
Ilustración 34-3: Ventanas para el registro de un nuevo usuario NFC..... 78
Ilustración 35-3: Ventana con usuarios registrados en Firebase..... 79
Ilustración 36-3: Estructura para el módulo de adquisición de datos 1..... 80
Ilustración 37-3: Parte del plano estructural del módulo de adquisición de datos 1 80
Ilustración 38-3: Estructura para los módulo de adquisición de datos 2, 3 y 4 81
Ilustración 39-3: Parte del plano estructural de los módulo de adquisición de datos 2, 3 y 4 82
Ilustración 1-4: Módulos que componen la arquitectura general del PSES..... 83
Ilustración 2-4: Usuarios registrados para el control de acceso..... 87
Ilustración 3-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha) 94
Ilustración 4-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha) 95
Ilustración 5-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha) 97
Ilustración 6-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha) 99
Ilustración 7-4: Pantalla serial de arduino del módulo de control y actuación..... 100
Ilustración 8-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha), para el comando “/alarma_on”, “/alarma_off” 102
Ilustración 9-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha), para el comando “/sirana_on”, “/sirena_off”..... 103
Ilustración 10-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha), para el comando “/abrir” 103
Ilustración 11-4: Ventanas que conforman la aplicación móvil para el control de acceso .. 104
Ilustración 12-4: Lectura de tarjeta NFC para su registro..... 105
Ilustración 13-4: Informacion registrada en Firebase..... 105
Ilustración 14-4: Alcance de comunicación con interferencia 106
Ilustración 15-4: Alcance de comunicación con línea de vista..... 107

Ilustración 16-4: Nivel de recepción de datos en función a la distancia, con linea de vista. 108
Ilustración 17-4: Nivel de recepción de datos en función a la distancia, con interferencia. 108
Ilustración 18-4: Caracteristica de descarga de la batería Rekoser 12V7Ah 110
Ilustración 19-4: Implementación del PSES dentro de las instalaciones del centro "Psicológico Infantil PSICOVID"..... 112
Ilustración 20-4: Certificado de aceptacion del proyecto de integración curricular emitido por el centro "Psicológico Infantil -PSICOVID" 113

ÍNDICE DE ANEXOS

ANEXO A: Hoja de datos de la ESP8266 Wemos D1 Mini
ANEXO B: Hoja de datos del sensor magnético MC-38
ANEXO C: Hoja de datos del sensor de movimiento DSC LC-100-PI
ANEXO D: Hoja de datos del sensor de vibración KY-002
ANEXO E: Hoja de datos del módulo RFID/NFC PN532
ANEXO F: Hoja de datos de la cerradura magnética ZE-280-5T
ANEXO G: Hoja de datos de la batería Rekoser RKE12-7
ANEXO H: Creación de base de datos en Firebase
ANEXO I: Creación de bot Telegram
ANEXO J: Programa en Arduino IDE para el módulo de adquisición de datos 1
ANEXO K: Programa en Arduino IDE para el módulo de adquisición de datos 2
ANEXO L: Programa en Arduino IDE para el módulo de adquisición de datos 3
ANEXO M: Programa en Arduino IDE para el módulo de adquisición de datos 4
ANEXO N: Programa en Arduino IDE para el módulo de control y actuación
ANEXO O: Programación realizada para el desarrollo de la App móvil orientada al control de acceso
ANEXO P: Plano estructural del módulo de adquisición de datos orientado al control de acceso
ANEXO Q: Plano estructural del módulo de adquisición de datos orientado al sistema de alarma
ANEXO R: Evidencia del marco de análisis e interpretación de resultados

RESUMEN

El objetivo del trabajo de integración curricular fue diseñar y construir un prototipo de sistema embebido de seguridad para el centro Psicológico Infantil Psicovid, el cual es monitoreado y controlado mediante el uso de la App Telegram. El diseño modular del prototipo es escalable, tiene incorporado un sistema de seguridad con dos funciones diferentes: un sistema de alarma que cumple con la Norma Ecuatoriana INEN-IEC 62851-1 y un sistema de control de acceso que utiliza comunicación de campo cercano (NFC) y una aplicación móvil desarrollada en *Android Studio* para su administración. El prototipo está compuesto por tres módulos, los dos primeros están implementados en tarjetas de desarrollo ESP8266: módulo de adquisición de datos, módulo de control-actuación y el módulo de administración, control y visualización de la información. A través de las pruebas realizadas se comprobó la integridad de la información y las distancias de comunicación, este último valor arrojó distancias máximas de 35m con línea de vista y 19m con interferencia, se midieron retardos de tiempo entre 2 y 3 segundos, la validación de los sensores se realizó calculando el error relativo máximo, se obtuvo los valores de: Er=7.14% para los sensores magnéticos y Er=5.56% para los sensores de movimiento, teniendo un resultado experimental aceptable para ambos casos. Para los sensores de vibración, lecturas del módulo NFC y la activación de la cerradura magnética se realizaron pruebas de repetibilidad, obteniendo un coeficiente de variación del 10%, 0% y 0% respectivamente, significando un trabajo aceptable, se evidenció un consumo energético de 504.3 mA para un estado activo y de 264.9 mA para un estado inactivo. El prototipo puede ser utilizado como herramienta de seguridad para distintos establecimientos, siendo un sistema confiable, de calidad, de bajo consumo energético y un 23.56% más económico que dispositivos comerciales. Se recomienda usar una placa de circuito SW-420 para tener control sobre el sensor de vibración el cual a su vez pueda trabajar en conjunto con un sistema de visión artificial para la identificación de un falso o verdadero intento de robo.

Palabras clave: <SISTEMA EMBEBIDO> <SISTEMA DE SEGURIDAD> <COMUNICACIÓN DE CAMPO CERCANO (NFC)> <ARDUINO (SOFTWARE-HARDWARE)> <PLATAFORMA DE MENSAJERÍA TELEGRAM>

SUMMARY

The objective of the curricular integration research project was to design and build a prototype of an embedded security system for the Psicovid Children's Psychological Center, which is monitored and controlled through the use of the Telegram App. The prototype modular design is scalable; it has a built-in security system with two different functions: an alarm system that complies with the Ecuadorian Standard INEN-IEC 62851-1 and an access control system that uses near field communication (NFC) and a mobile application developed in *Android Studio* for its administration. The prototype comprises three modules; the first two modules are implemented on ESP8266 development boards: the data acquisition module, the control-actuator module, and the module of management, control, and information display. Through the tests carried out, the integrity of the information and the communication distances were verified; this last value delivered maximum distances of 35m with Line-Of-Sight and 19m with interference, time delays between 2 and 3 seconds were measured, the validation of the sensor were performed by calculating the maximum relative error, obtaining the following values: Er=7.14% for the magnetic sensors and Er=5.56% for the motion sensors, getting an acceptable experimental result for both cases. For the vibration sensors, NFC module readings, and the activation of the magnetic lock, repeatability tests were carried out, obtaining a coefficient of variation of 10%, 0%, and 0%, respectively, representing an acceptable job, Showing an energy consumption of 504.3 mA for an active state and 264.9 mA for an inactive state. The prototype can be used as a security tool for different establishments, being reliable, quality, low energy consumption system, and 23.56% cheaper than commercial devices. It is recommended to use an SW-420 circuit board to control the vibration sensor which it can work together with an artificial vision system to identify a fake or real robbery attempt.

Keywords: <EMBEDDED SYSTEM> <SECURITY SYSTEM> <NEAR FIELD COMMUNICATION (NFC)> <ARDUINO (SOFTWARE-HARDWARE)> <TELEGRAM MESSAGING PLATFORM>.

Lenin Lara
0602546103

INTRODUCCIÓN

En función a su esquema metodológico el presente trabajo de integración curricular cuenta con cuatro capítulos desglosados en: capítulo 1 diagnóstico del problema, capítulo 2 marco teórico, capítulo 3 marco metodológico, capítulo 4 marco de análisis e interpretación de resultados.

En el primer capítulo se menciona varios puntos de apertura para el desarrollo del tema planteado, tales como, antecedentes, planteamiento del problema, justificación teórica, justificación aplicativa, los objetivos que se pretende alcanzar en el desarrollo del presente trabajo de integración curricular y la metodología utilizada.

En el segundo capítulo se realiza una revisión bibliográfica orientado a los sistemas de seguridad comerciales, control de acceso, realidad de la zona, normativas, arquitectura, componentes de un sistema de alarma y redes sociales con su frecuencia de uso. Esto con el fin de seleccionar las tecnologías o familias que mejores características presenten, además de ayudar a que el lector perciba conocimientos teóricos respecto al tema.

En el tercer capítulo se abordan puntos importantes para el desarrollo físico del prototipo de sistema embebido de seguridad, desde ahora también llamado PSES, tal como: planteamiento de los requerimientos, concepción de la arquitectura general del prototipo, diseño de la arquitectura de sus módulos, selección del hardware, esquemas de conexión, diseño de software, interfaces gráficas del módulo de administración, control y visualización de la información y diseño estructural del prototipo.

Finamente, en el cuarto capítulo se realiza el análisis e interpretación de resultados post-construcción del PSES, para ello se desarrolla la caracterización de: los módulos de adquisición de datos, módulo de control y actuación, módulo de administración- control- visualización de la información, y caracterización de la comunicación para los módulos del PSES. Por último, se realizan pruebas de alimentación y análisis económico para la construcción del PSES.

CAPÍTULO I

1. DIAGNÓSTICO DEL PROBLEMA

El presente capítulo cuenta con los siguientes apartados:

1.1. Antecedentes

A medida que la población aumenta, aumenta la delincuencia (Jiménez Ornelas, 2005, p. 239), factor que perjudica directamente a aquellas personas que se esfuerzan por vivir de una manera justa a raíz de cumplir un trabajo integro.

Al contrastar los diferentes derivados de la delincuencia ocurridos en Ecuador entre los meses de enero y octubre de los años 2020 y 2021, se tiene que; según la Fiscalía General del Estado, absolutamente todos los tipos y niveles de robo fueron en ascenso, por ejemplo, el robo a personas creció en un 25.6%, robo a domicilios 12.3%, robo de carros 51.4%, robo de motos 30.1%, unidades económicas 14.9%, entre bienes, accesorios y autopartes de vehículos 30.3%, siendo la noche el horario utilizado con mayor frecuencia para cometer estos hurtos (Fiscalía General del Estado, 2021, p. 1–5).

Al tomar como problema principal el robo a inmuebles, según el Instituto Nacional de Estadísticas y Censos (2021), entre los meses de enero a noviembre del año 2020, se registró una cifra total de 6643, produciendo una disminución de -34.3% respecto al año 2019, sin embargo, entre los meses de enero a noviembre del año 2021 el valor de robos a domicilios registrado fue de 7449 significando un aumento del 12.1% en comparación al año pasado.

Según el Servicio Integrado de Seguridad ECU-911 (ECU-911, 2020, p. 8), el Centro Local - Riobamba coordino 108.258 llamados de emergencias hechos en la provincia de Chimborazo, de los cuales el 68.1% corresponden a emergencias de seguridad ciudadana, siendo la emergencia por servicio con mayor demanda en la provincia. Con base a las estadísticas manejadas por la policía del Distrito "Riobamba-Chambo" con fecha del 1 de enero al 17 de septiembre del 2021, 182 inmuebles han sido afectos por antisociales (La Prensa Chimborazo, 2021).

Con ayuda de las herramientas tecnológicas que cada vez se encuentran más desarrolladas e inmersas en el diario vivir (Palomino, 2022, p. 4), la humanidad ha tratado de erradica o al menos disminuir en un cierto porcentaje este problema. Actualmente existen diferentes maneras de

asegurar el interior o exterior de una vivienda, plantel, empresa, etc. La videovigilancia es uno de los métodos utilizados hoy en día como medida de precaución en cuando a seguridad se refiere, seguido por la instalación de sensores, alarmas, cercos eléctricos, etc.

En Europa existen empresas dedicadas a ofrecer servicios de seguridad, entre ellas "Loxone" (Ensaco, 2022), ofrece una extensa lista de servicios de seguridad para casi cualquier tipo de establecimiento, sin embargo, al ser una empresa reconocida mundialmente los precios que maneja tienden a ser elevados. Ahora, las empresas que ofrecen servicios de seguridad se están volviendo una alternativa contraproducente para la seguridad gracias al tipo de armas que poseen, por la cantidad y formación profesional de sus trabajadores y por sus lazos con actos delictivos (Castellanos, 2000, p. 1).

Es justo mencionar también que una gran cantidad de estas empresas de seguridad realizan un trabajo considerable, trayendo consigo una serie de ventajas, entre ellas ofrecer soluciones a través de un equipo humano y técnico que garantizan seguridad (Guaña and Lema, 2013, p. 14). Sin embargo, su principal problema se enfoca en la inversión que tienen que hacer los usuarios por adquirir el servicio, factor que se ve reflejado directamente en los ingresos anuales que perciben dichas empresas.

Según el Instituto Nacional de Estadísticas y Censos, un total de 66 empresas dedicadas a la comercialización de alarmas sociales, control de acceso, incendios, y otros sistemas de seguridad, registran $12.8 millones de dólares en cuanto a ingresos anuales. En el sentido de la comercialización de equipos como sensores, cámaras, pantallas, entre otros, perciben $114 millones de dólares al año. Esto sin hablar de los costos que los usuarios tienen que cancelar mensualmente para que la empresa contratada continúe prestando sus servicios de seguridad (El Comercio, 2021).

A nivel latinoamericano se han desarrollado trabajos de tesis que indirectamente suplen a las empresas de seguridad ofreciendo como alternativa sistemas de seguridad basados en un Circuito Integrado Programable "PIC" (Cholan and Varas, 2017, pp. 15–19), otros haciendo uso de videovigilancia y *software* libre (Rivas and Velazquez, 2011, pp. 4–6), sin embargo, algunos de estos sistemas se limitan a ser implementados únicamente en viviendas o su configuración resulta ser compleja.

En Guayaquil-Ecuador estudiantes de la Universidad Politécnica Salesiana, realizaron el diseño e implementación de un sistema de seguridad para un centro de acogida (Aviles and Cobeña, 2015, p.

2–4), haciendo uso de sensores y cámaras como medios de detección de presencia, y de una sirena como elemento de respuesta al sistema, el control se realiza telemétricamente, es decir, se utilizó un control a distancia. Sin embargo, en sus conclusiones se indica un costo elevado para su implementación.

En 2018, Karina Gaibor y Fernando Loor, realizaron como proyecto de titulación el diseño de un sistema de alarma controlado inalámbricamente para salvaguardar la seguridad de las viviendas enfocados a sectores de bajos recursos económicos, los autores proponen e incitan al desarrollo de proyectos que ofrezcan una solución al problema de la delincuencia producida en las diferentes ciudades del Ecuador, considerando parámetros de seguridad, tecnología, costo y confianza.

Un estudiante de la Universidad Estatal del Sur de Manabí a (Aguayo, 2018, p. 1–5) realizó como proyecto de titulación la implementación de un sistema de alarma basado en tecnología Arduino y telefonía móvil, sin embargo, para mantener al sistema funcional es necesario renovar el contrato mensual del plan de mensajes con la empresa de telefonía. Por tal motivo el autor recomienda que el sistema sea activado solo en horas no laborables y se propone el desarrollo de nuevos proyectos tecnológicos relacionados con la seguridad.

Con base a la investigación se puede deducir que el Ecuador posee altos índices de delincuencia enfocados a robos de inmuebles y los sucesos registrados y relacionados con esta actividad en la provincia de Chimborazo forman gran parte de ella, no obstante, existen varias alternativas por las que un usuario puede optar para evitar en lo posible ser víctima de este problema.

Dichas alternativas tienen que ser revisadas, analizadas y escogidas de tal forma que el usuario se sienta satisfecho con su elección, pues como se ha estudiado existen varios proyectos de investigación que cuentan con un mismo enfoque, pero con distintas arquitecturas, por lo que dotan de ventajas y desventajas diferentes.

1.2. Planteamiento del problema

¿Cómo se podría realizar el diseño y construcción de un prototipo de sistema embebido de seguridad, supervisado mediante una red social, para el centro “Psicológico Infantil - PSICOVID”?

1.2.1. Sistematización del problema

- ¿Qué sistemas de seguridad comerciales existen y cuáles son sus componentes, normativas, arquitectura y vulnerabilidades?
- ¿Cuáles son los requerimientos que tiene que cumplir el sistema embebido de seguridad en el centro "Psicológico Infantil -PSICOVID"?
- ¿Cuál es el diseño del prototipo de sistema embebido de seguridad con módulos de detección y actuación que se adapta a los requerimientos?
- ¿Qué elementos *hardware* y *software* serán necesarios para la construcción del diseño del sistema embebido de seguridad?
- ¿Como evaluar que el sistema embebido de seguridad este cumpliendo con los requerimientos propuestos al inicio de la investigación?

1.3. Justificación Teórica

Dada la zona en la que se encuentra ubicado el Centro "Psicológico Infantil -PSICOVID", es de suma importancia instalar un sistema de seguridad que brinde tranquilidad a todos aquellos que tengan algo que ver con el establecimiento, pues según el Distrito de Policía "Riobamba-Chambo", estadísticamente la ubicación del establecimiento PSICOVID se encuentra en el puesto número uno de las cinco zonas con mayores conflictos y que además representan un mayor número en cuanto a llamadas de emergencia se trata, liderando este top con un 17% en registros de actos delictivos (La Prensa Chimborazo, 2021).

A través de una entrevista realizada a la psicóloga Maritza Poma, dueña del centro "Psicológico Infantil -PSICOVID", se constató que evidentemente el establecimiento se encuentra en una zona conflictiva, pues en ocasiones pasadas habían sido víctimas de robo, razón por lo que surge la necesidad de implementar un sistema de seguridad.

El acudir a empresas que ofrecen servicios de seguridad no siempre es la solución, pues como se menciona en los antecedentes de la presente investigación, dichas empresas se están volviendo contraproducentes ante el problema, gracias al tipo de armas que poseen, por la cantidad e integridad cuestionable de sus empleados o por sus lazos con actos delictivos (Castellanos, 2000, p. 1). Tomando en cuenta que el factor más crítico de las empresas de seguridad actuales es el tiempo, pues si se violara el área protegida, el primero en ser avisado sería la central de monitoreo de la empresa, dejando en segundo plano el aviso a los usuarios, haciendo de esta forma que ellos no cuenten con una respuesta en tiempo real acerca de lo que ocurre u ocurrió, habiendo en la mayoría de casos grandes tiempos muertos que representan brechas para que la delincuencia cumpla su propósito (Bone, 2019, pp. 1–6).

Sumándose a la lista de vulnerabilidades de los sistemas de seguridad diseñados e implementados en América latina (Aviles and Cobeña, 2015, pp. 2–4), (Rivas and Velazquez, 2011, pp. 4–6) y a nivel local (Cholan and Varas, 2017, pp. 15–19), los problemas se presentan en el hecho de que algunos de estos sistemas se limitan a ser implementados únicamente en viviendas, su configuración resulta ser compleja, o su implementación requiere de un costo elevado.

Al tomar las propuestas de continuar con el desarrollo de proyectos tecnológicos relacionados con la seguridad propuesto por varios autores (Gaibor and Loor, 2018, p. 102), (Aguayo, 2018, p. 83) con el fin de ofrecer una solución al problema de la delincuencia enfocada a inmuebles, y considerando las vulnerabilidades de los trabajos de investigación citados anteriormente es por lo que se propone el diseño y construcción de un prototipo de sistema embebido de seguridad para el centro "Psicológico Infantil -PSICOVID".

Se pretende aprovechar el uso de una red social para su monitoreo, pues se conoce que en Ecuador el porcentaje de usuarios activos en el último año dentro de estas plataformas fue del 78.8% del total de su población, además registros apuntan que el 57.3% de ellos disponen de acceso a internet (We Are Social, 2021, p. 8).

Así también, al contrastar el costo que implica al usuario utilizar una red social como medio de envío y recepción de datos respecto a un sistema que realiza esta acción vía SMS la diferencia es evidente, pues en un sistema de seguridad tradicional que utiliza GSM el costo de envío de tan solo un mensaje corto de texto en Ecuador es de $0.1946 (EnviosSMS, 2021) valor directamente relacionado al cobro mensual al usuario en función a los mensajes que se envíen.

Mientras que el costo de envío de un mensaje a través de una red social no tiene relación alguna con el cobro mensual por el servicio a internet, además actualmente el Municipio de Riobamba brinda acceso gratuito a internet a través de más de 148 puntos Wifi, ubicados en diferentes puntos de la ciudad (Colcha, 2020) por lo que los ciudadanos tienen mayor probabilidad de contar con servicio a internet cuando se encuentren fuera de sus hogares.

Otro beneficio que ofrecería el prototipo de sistema embebido supervisado mediante una red social aparte del costo de envió de datos respecto a los sistemas de seguridad tradicionales, es que el uso de las redes sociales no se ven limitadas a ser utilizadas en el celular, pues sus plataformas son usadas sin problema a través de un ordenador. Por estas razones se propone el uso de una red social para la supervisión del prototipo de sistema embebido.

Además, a través de diseñar y construir el sistema embebido de seguridad se ayudaría a cumplir con uno de los objetivos nacionales del Ecuador (objetivo 9), relacionado con la Industria, innovación e infraestructura, donde se menciona que los avances tecnológicos son de suma importancia para encontrar soluciones a desafíos a los que se enfrenta el país, tal como: economía, ambiente, eficiencia energética, oferta de nuevos empleos, etc. (PNUD, 2022).

Por todas las razones antes citadas se determina que es factible la realización de este trabajo de integración curricular, siendo un prototipo de sistema embebido de seguridad que actualmente no se lo puede encontrar en comercialización en Riobamba, abriendo así paso a futuros trabajos de investigación y desarrollo de sistemas de seguridad que se vean interesados en mejorar el prototipo o a su vez desarrollar su propio sistema partiendo del uso de alguna red social como herramienta principal para su desarrollo.

1.3.1. Justificación Aplicativa

Considerando la necesidad de implementar un sistema de seguridad en la zona se debe construir un prototipo de sistema embebido de seguridad el cual base su funcionamiento en el desarrollo de tres módulos fundamentales: "adquisición de datos", "control y actuación", "administración, control y visualización de la información".

El módulo de adquisición de datos estaría conformado por dos partes, la primera la adquisición de datos orientado al control de acceso (módulo 1) y la segunda la adquisición de datos orientado al sistema de alarma (módulo 2, 3 y 4). Estos se encargarían de la recepción y envió de los estados de sus elementos de sensado a una base de datos para su registro. Dichos elementos de sensado se ubicarían en las dos zonas del establecimiento, la zona 1 corresponde al área escolar y la zona 2 al área de la oficina.

El módulo de control y actuación estaría encargado de detectar cambios de las variables registradas en la base de datos para en función a ello emitir diferentes órdenes a los elementos de actuación, por lo que este módulo determina el comportamiento del sistema.

El módulo de administración, control y visualización de información puede ser un dispositivo móvil, el cual este compuesto por dos interfaces gráficas: la primera la interfaz de Telegram, la cual funciona como herramienta de control y visualización de la información, y la segunda la interfaz de una aplicación móvil, pudiendo actuar como herramienta de administración y

visualización, pues por medio de ella se estaría en la capacidad de observar y gestionar el proceso de administración de permisos de acceso de un solo nivel.

Los tres módulos nombrados anteriormente estarían en la capacidad de establecer comunicación vía internet utilizando wifi como puerta de acceso. Así también los dos primeros establecerían comunicación con el módulo de administración, control y visualización de información.

Se puede considerar que el sistema de seguridad cumpliría dos funciones diferentes: la primera un sistema de alarma el cual se active por medio de la red social cuando el establecimiento se encuentre vacío. En función a esto cualquier módulo de adquisición de datos estaría en la capacidad de disparar la alarma en base al cambio de estado de sus sensores, posterior a ello se actuaría sobre lo sucedido y se notificaría al administrador. La segunda función centraría su trabajo en el control de acceso al área de la oficina (zona 2), sin importar el horario el sistema siempre funciona.

Se necesita hacer uso de una base de datos como intermediaria de la comunicación, para de esta forma tener registro de: los estados de los elementos de sensado y los permisos para el control de acceso de un solo nivel, pudiendo ser modificados por un administrador de base de datos a partir del uso de una aplicación móvil.

La violación al acceso de cualquier zona cuando el sistema de alarma se encuentre activo, así como el historial de ingreso al área de la oficina (zona 2) serían notificadas al administrador a través de la comunicación establecida con la red social.

Se pudiera considerar al prototipo de sistema embebido de seguridad como escalable hasta n nodos, haciendo que si llegara a presentar la oportunidad de aumentar el área de trabajo el prototipo de sistema embebido de seguridad podría expandirse con él.

Respecto a cuestiones de alimentación es necesario tener en consideración un sistema de respaldo energético cuyo objetivo sea garantizar el suministro eléctrico en aquellos casos en donde se produzcan cortes de energía. Debido a que el área total del Centro “Psicológico Infantil - PSICOVID” es de 33.03 m2 se consideraría una arquitectura centralizada.

1.4. Objetivo General

Diseñar y construir un prototipo de sistema embebido de seguridad, supervisado mediante una red social, para el centro "Psicológico Infantil -PSICOVID".

1.4.1. Objetivos específicos

- Analizar los diferentes sistemas de seguridad comerciales, componentes, normativas, arquitectura y vulnerabilidades.
- Seleccionar los requerimientos necesarios que tendrá que cumplir el prototipo de sistema embebido de seguridad en el centro "Psicológico Infantil -PSICOVID".
- Diseñar el prototipo de sistema embebido de seguridad con módulos de sensores y actuadores que mejor se adapten a los requerimientos.
- Escoger el *Hardware* y *Software* que ayuden a que los requerimientos planteados se cumplan.
- Validar que el prototipo de sistema embebido de seguridad implementado cumpla con los requerimientos propuestos al inicio de la investigación.

1.5. Metodología

Para el desarrollo del presente trabajo de integración curricular es necesario hacer uso de manera combinada de las siguientes técnicas y métodos de investigación:

Dentro de los métodos teóricos se tiene: revisión documental, para el estudio de avances tecnológicos, blogs, libros y cualquier otro tipo de información relacionada al tema; histórico-lógico, para estudiar los cambios en función al tiempo por los que han atravesado los sistemas electrónicos que se relacionan con el tema.

Sistematización, se aplica la información experimental y la información recolectada en la revisión documental al diseño del sistema a desarrollar; análisis y síntesis, se evalúa los resultados obtenidos al finalizar el desarrollo del tema a través de los cuales se llega a las conclusiones y recomendaciones.

Dentro de los métodos empíricos a utilizarse se encuentran: experimentación, para el desarrollo de la simulación y comprobación de las diferentes etapas que conforman el sistema; medición, para evaluar las diferentes variables durante la implementación practica de la investigación; observación, para la validación del proyecto de integración curricular en función a su operabilidad dentro de su entorno.

CAPÍTULO II

2. MARCO TEÓRICO

El presente capítulo cuenta con los siguientes apartados:

2.1. Sistemas de seguridad comerciales

Es un sistema diseñado para proteger un almacén, establecimiento, oficina, tienda o fábrica, es decir tiene como objetivo principal proteger un área determinada. Esta formado de un conjunto de instalaciones y componentes necesarios para brindar protección ante robos, incendios, amenazas a usuarios o hacia bienes materiales (LAGE, 2019). Entre los cuatro más conocidos se tiene:

Sistemas conectados a una central de monitoreo. – Conformado por componentes y dispositivos electrónicos situados en puntos estratégicos, estos pueden ser; sensores de movimiento, sensores magnéticos, botones de pánico, detectores de humo, etc. La señal percibida por estos elementos es responsable de la acción que tendrá que tomar el sistema de seguridad, entre ellas la principal es comunicarse con una central de monitoreo, después se dará la comunicación con el usuario, y en la mayoría de casos la activación de una sirena como señal de alerta. Este tipo de sistemas se caracterizan porque el servicio únicamente puede ser ofrecido por una empresa legalmente acreditada, empresas que se encuentran en expansión y que el estado no regula ni controla (Castellanos, 2000, p. 1).

Sistemas con respuesta supervisada. - Son aquellos en donde la supervisión como parámetro general está presente sobre cualquier acción a efectuarse, pues se realiza de la mano del personal y operarios especializados los cuales se encargan de la detección de actividades anómalas y actúan sobre ellas, es decir, tienen que estar dispuestos a acudir a la zona supervisada cuando la ocasión lo amerite, pues tienen como objetivo aplicar supervisión y rondas disuasiva (Colomer, Meléndez and Ayza, 2022, pp. 1–2).

Videovigilancia. - Es un sistema de seguridad el cual hace uso de cámaras encargadas de grabar toda aquella actividad que ocurre dentro de su rango de alcance, produciendo la sensación de tranquilidad y seguridad en aquellos usuarios que se deciden en utilizarlas. Además, se lo considera un mecanismo de alto valor capaz de garantizar la seguridad de la ciudadanía considerando su correlativo riesgo para las libertades y derechos de los ciudadanos. Según

estudios realizados en el año 2005 por la Universidad de Florida, se demuestra que el instalar cámaras de videovigilancia produce un efecto disuasorio en clientes y en empleados del establecimiento, al considerar que el 47% de las pérdidas de un negocio son producto del robo de sus mismos trabajadores, al implementar este tipo de cámaras la cifra de robos se ve reducida (Chamarro Iglesia, 2007, pp. 213–215).

Circuito cerrado de televisión. - El objetivo principal de este sistema es la supervisión, control y registro de las eventualidades ocurridas dentro de un establecimiento, local o un área en general, este tipo de sistema tiene acceso restringido a sus usuarios respecto al contenido de sus imágenes. Este sistema de seguridad se caracteriza porque puede ser la combinación de varios sistemas, es decir, puede está conformado por videovigilancia, alarmas, puede estar supervisada por una central de monitoreo o hasta recibir servicio de respuesta supervisada. Sus áreas de cobertura suelen ser más extensas, así como su nivel de disuasión, a través de ellas se realiza la supervisión de empleados y clientes en un área comercial y resultan ser sistemas más amenazantes para las personas con malas intenciones (VÉRTICE S.L, 2011, p. 11).

Sistemas de seguridad domóticos.- Cuentan con conexión a la web, es decir, su propósito está enfocado en utilizar el internet como medio de comunicación, entre ellos se encuentran: control de acceso, detección de incendios, fugas de gas, fugas de agua, simulación de presencia. El aplicar domótica a un sistema de seguridad de alarma lo traduce a un sistema inteligente, trayendo consigo una serie de ventajas, tal como el poder controlar y monitorear el sistema remotamente desde cualquier lugar del mundo, dejando atrás a los sistemas que requieren supervisión de forma local. Cabe mencionar que es de importancia contar con una buena cobertura de internet, siendo requerimiento de comunicación, pues con ello se establece un eficiente funcionamiento e interacción de todo lo que se ve involucrado en el circuito de alarma (Carbonell, 2020).

2.1.1. Vulnerabilidades de los sistemas de seguridad comerciales

Dado los cinco sistemas de seguridad comerciales expuestos anteriormente, la *Tabla 1-2* resume las principales vulnerabilidades que poseen dichos sistemas.

Tabla 1-2: Vulnerabilidades de los sistemas de seguridad comerciales

Sistema de seguridad comercial	Vulnerabilidad
Sistemas conectados a una central de monitoreo	El factor más crítico de las empresas de seguridad actuales es el tiempo, puesto que si se violara el sistema de seguridad el primero en ser avisado seria la central de

	monitoreo de la empresa, dejando en segundo plano el aviso a los usuarios, haciendo que ellos no cuenten con una respuesta en tiempo real acerca de lo que ocurrió, habiendo en la mayoría de los casos grandes tiempos muertos que representan una brecha para que la delincuencia cumpla su propósito. Para mantener el servicio de seguridad el usuario necesita realizar pagos mensuales a la empresa.
Sistemas con respuesta supervisada	El contratar un sistema de seguridad con respuesta supervisada resulta costoso, pues el servicio implica que un profesional realice rondas y supervisiones disuasivas visitando el lugar de vez en cuando, por ende, debe ser remunerado. Para mantener el servicio de seguridad el usuario necesita realizar pagos mensuales a la empresa.
Videovigilancia	Las Apps que se utilizan como complemento del sistema de seguridad en cuanto a la visualización o control, son aplicaciones las cuales el usuario no revisa ni da seguimiento con frecuencia. Si no se cuenta con almacenamiento en memoria de respaldo o almacenamiento en la nube y simplemente se dispone del almacenamiento de la propia cámara (en caso de tenerla), si esta se llegara a perder o a dañar, las grabaciones y respaldos de seguridad se irían con ella.
Circuito cerrado de televisión	Al ser la combinación de un sistema de videovigilancia, sistema con respuesta supervisada, central de monitoreo, este sistema abarca consigo todas las vulnerabilidades antes expuestas de dichos sistemas.
Domótico	Si no se cuenta con una buena conexión a internet la comunicación entre controlador-usuario presentaría latencias. Las Apps que se utilizan como complemento del sistema de seguridad en cuanto a la visualización o control, son aplicaciones las cuales el usuario no revisa ni da seguimiento con frecuencia.

Realizado por: Chafla, Hernán, 2022

Una manera de cubrir con las vulnerabilidades mencionadas en la *Tabla 1-2* es diseñando y construyendo un prototipo de sistema embebido de seguridad cuya característica principal sea el contar con conexión a la web, sea de bajo costo, no se necesite realizar pagos periódicos a una empresa de seguridad para su monitoreo, brinde respuesta en tiempo real a los usuarios y maneje una aplicación de comunicación conocida por el administrador ya sea para la visualización, control, o ambos.

2.2. Control de acceso

Está ligado a temas de seguridad de un área, lugar o establecimiento especifico, esto se consigue mediante el monitoreo y control electrónico de la circulación de personas a través de puertas principales, secundarias, elevadores, etc. Este tipo de tecnologías se las encuentra en empresas, industrias e inclusive hogares los cuales se encuentran automatizados, con el fin de brindar protección a recursos, bienes materiales y hasta a salvaguardar la seguridad física de aquellos que se encuentren dentro del área a proteger. Dentro de las características más importantes por las cuales se utiliza en control de accesos tenemos (Johnson Controls, 2019):

- Restringir el acceso a las zonas con base a horarios laborables
- Historial de asistencias y tiempos.
- Control automatizado para ingreso de vehículos.
- Control de personal dentro de un área laboral.
- Protección de materiales, elementos delicados.
- Reemplazo de llaves.
- Elimina la presencia de supervisores o guardias los cuales se encarguen de monitorear el paso de personas o empleados.
- Generación de reportes.

2.2.1. Tecnologías aplicadas al control de acceso

En función a lo que el establecimiento, institución, comercio, o usuario lo requiera, al ser un sistema automatizado, las tecnologías utilizadas para cumplir con el objetivo de restricción de acceso a personas en función a parámetros establecidos por los administradores del lugar hacen que dicho sistema pueda ser catalogado en tres niveles diferentes: complejo, mediano o pequeño (Castaño and Alonso, 2019, p. 34). Entre algunos de ellos se tiene:

Control de acceso autónomo. – Son los controladores más sencillos, pues se caracterizan por ser sistemas que no se encuentran ligados a una unidad central u ordenador que gestione las acciones que se realicen a través de él, por lo que este sistema de control no guarda registro alguno de las entradas o salidas que se efectúan a lo largo del tiempo (Vargas, 2013, pp. 1–20).

En la *Ilustración 1-2* se observan los componentes más comunes utilizados para la implementación de un sistema de control de acceso autónomo.

Ilustración 1-2: Componentes más comunes de un sistema de control de acceso autónomo

Realizado por: Chafla, Hernán, 2022

Reconocimiento facial. – Es considerado como un sistema de control de acceso complejo debido a las técnicas y metodologías empleadas para cumplir con su objetivo. Es importante tener en consideración que, pese a que en los últimos años se han desarrollado técnicas mucho más robustas que tienen como objetivo la solución de problemas como distancias, iluminación, rotaciones, entre otros; aún no se puede decir concretamente que existen métodos para el reconocimiento facial que sean fiables o en los que se pueda confiar plenamente, pues resulta que todavía no son tolerantes a los diferentes cambios de condiciones que se pueden presentar (Galindo and Gamboa, 2016, p. 2).

Según autores (Ibarra and Paredes, 2018, pp. 286–287), existen tres fases principales que hacen posible el reconocimiento artificial, estas son:

1. Detección del rostro: Implica la adquisición de una imagen digital y la conservación de todas aquellas áreas en donde se aprecia un rostro, es decir todas aquellas que no la contengan son desechadas, existen varios métodos que permiten llegar a este resultado a través de la creación de patrones para las distintas zonas de la imagen.
2. Extracción de características: Hace referencia a la toma de datos relacionados con las características particulares de cada rostro para posteriormente ser clasificados y comparados.
3. Reconocimiento: Es considerada como la etapa final y se divide en dos partes, la primera es identificar los patrones guardados y enviados por la etapa de extracción y la segunda parte

la verificación a través de la comparación de estos mismos patrones con los obtenidos en tiempo real.

Debido a los componentes *hardware* involucrados para el desarrollo de un sistema de reconocimiento facial, su construcción requiere de una alta inversión económica, pues se necesita de una tarjeta de desarrollo robusta capaz de procesar lo requerido, además es necesario el utilizar iluminación, ópticas o lentes especiales, etc.

Reconocimiento de iris. - Utiliza una serie de tecnología de cámaras las cuales centran su principio de funcionamiento en iluminación infrarroja capaz de reducir el reflejo producido en la convexa cornea y con esto ser capaz de crear imágenes representativas a la estructura del iris, continuamente dichas imágenes se convierten en plantillas digitales para su posterior comparación con algún usuario. Este método utiliza técnicas enfocadas en el reconocimiento de patrones guardados en una base de datos (Vargas, 2013, p. 27).

RFID. - Radio Frecuency Identification, traducida al español como Identificación por Radio Frecuencia tiene el objetivo de identificar automáticamente a un objeto o producto como único. Funciona a varios metros de distancia y no necesita estar en visión directa con el lector para la conexión. Su sistema completo es considerado como un método de almacenamiento y recuperación de datos de forma remota mediante proximidad. Dentro de sistemas de seguridad puede ser utilizado para el acceso y restricción de personas a cierto tipo de zonas (Herrera, Pérez and Marciano, 2009, p. 57).

Elementos que componen un sistema RFID. – Para establecer comunicación inalámbrica esta tecnología necesita de un emisor, receptor, un intermediario y un cerebro para la comunicación, es por esto que se compone de cuatro partes básicas: una etiqueta RFID, un lector RFID, una antena y un sistema capaz de procesar y contener una base de datos también conocido como sistema de cómputo (Herrera, Pérez and Marciano, 2009, pp. 1–2). A continuación, se define las cuatro partes que componen a un sistema RFID:

a) Etiquetas RFID. - Dentro de la comunicación toma el papel de emisor, gracias a que contiene la celda encargada de enviar la señal al lector RFID que constantemente busca ondas de lectura, aunque dependiendo del tipo de etiqueta con la que se trabaje de cierta forma se puede agregar que funciona también como un dispositivo receptor. En función a su aplicación el material de construcción externo puede cambiar, ya sea para soportar el agua, polvo, altas y bajas temperaturas, etc.

Al trabajar con radiofrecuencia están obligados a transmitir los datos en una longitud de onda concreta, es decir, si se utiliza un microchip RFID de 13.56 KHz el lector debe trabajar a la misma frecuencia de 13.56 KHz, con esto se efectúa una adecuada comunicación y codificación por parte del microchip. Dichas etiquetas pueden clasificarse en (Chang and Lozano, 2013, pp. 23–32):

- *Etiquetas pasivas*. - Se caracterizan por no contar con alimentación eléctrica dentro de su estructura, esto es gracias a que la señal constante producida por la antena RFID induce una corriente pequeña que recepta la etiqueta pasiva y pone en operación a su microchip interno, permitiendo de esta manera la generación y envió de una respuesta a la antena. Una de las restricciones de este tipo de etiquetas se encuentra en el rango de los 10 centímetros hasta los 6 metros, este tipo de valores se encuentran estipulados dentro de las normas ISO 14443 y 18000-6, donde se abarcan los estándares para redes inalámbricas RFID.

- *Etiquetas activas*. - Cuentan con alimentación eléctrica propia gracias a una mini batería integrada en ellas, por este motivo se encuentran en contacto constante con el lector, este contacto permanente representa una reducción considerable de los errores por lectura, por lo que se recomienda su utilización en entornos con mucho ruido, zonas con interferencia en radio frecuencia, etc. Las distancias que pueden alcanzar son por mucho, mayores a los de una etiqueta pasiva, pues rondan los cientos de metros, así también su mini batería tiene una vida útil de hasta unos 10 años. Una de las desventajas de mayor peso es que este tipo de etiqueta activa no es para nada económica, pues cuesta de 10 a 20 veces más que una etiqueta pasiva.

b) Lector RFID. - El propósito de un lector RFID es la recepción y transmisión de señales, receptor puesto a que captura las señales de datos que envían las etiquetas pasivas o activas para posterior a ello decodificar e interpretar los datos mediante el uso de un *software* adecuado para ese trabajo. Actúa como transmisor de señales en el caso de que trabaje en conjunto a una etiqueta pasiva, pues aquí tiene la función de brindar suministro eléctrico a dichas etiquetas a través de la inducción de corrientes pequeñas por medio de una orden dictada a la antena. Existen cuatro tipos de lectores: portátiles, fijos, de mesa y de carretilla (Rodríguez, 2009, p. 17).

c) Antenas RFID. - Son considerados como intermediarios de la comunicación, pues sirven como herramientas para que los lectores RFID sean capaces de transmitir señales de radiofrecuencia, tales como pulsos de corriente de alimentación en el caso de que se utilice etiquetas pasivas, de la misma forma se necesitan de las antenas para recibir los datos enviados devuelta por las etiquetas RFID (Rodríguez and Carrión, 2016, p. 31).

d) Sistema de cómputo. - Una vez se tenga claro el funcionamiento de las etiquetas, lectores y antenas RFID lo último que se tiene que conocer es que pasa con los datos recibidos por el lector. El elemento que completa el sistema RFID es el de cómputo, los datos brindados por las etiquetas son enviados y procesados por un programa que los traduce a un lenguaje que el hombre lo interpreta con facilidad, este *software* tiene la capacidad de controlar en tiempo real todas aquellas acciones y movimientos que son detectados por el lector y posterior a ello informar al usuario sobre dicho cambio, en algunos casos se toma acciones en función a lo sucedido (Rodríguez, 2009, pp. 35–37).

NFC. - Near Field Communication, traducida al español como Comunicación de campo cercano, es considerada como una derivación del RFID con características particulares; corto alcance y trabaja en la banda de 13.56Mhz (Seguí Moreno, 2012, p. 3).

Este tipo de tecnología lo conforma un elemento el cual origina la transmisión conocida con el nombre de "Iniciator" y un elemento receptor llamado "Target", quienes establecen la comunicación basados en el principio de inducción electromagnética, por medio de la cual dos elementos inductivos colocados a una distancia máxima de 20cm son capaces de compartir energía con el fin de lograr la transmisión de datos. Entre los modos de funcionamiento de esta tecnología tenemos (Carignano, 2022, p. 3):

- *Modo activo.* - Tanto el elemento emisor (Iniciator) como el receptor (Target) tienen sus propios suministros de alimentación energética, estos elementos de comunicación se encargan de generar alternadamente su campo de radio frecuencia propio, cada vez que el dispositivo desactiva dicho campo significa que está en la espera de receptar datos.

- *Modo pasivo.* - Se caracteriza porque el elemento receptor no necesita suministro de energía propio, pues el dispositivo "initiator" es el encargado de generar el campo de radio frecuencia y el Target tendrá que, mediante modulación responder a dicha señal. El protocolo NFC en modo de uso pasivo permite a dispositivos con batería propia (teléfonos celulares) trabajar en modo ahorro de energía, lo que se traduce a una administración eficiente de suministro energético para no tener problemas futuros con la utilización de otras aplicaciones.

2.2.2. Comparativa de tecnologías aplicadas al control de acceso

La *Tabla 2-2* detalla las características más importantes de algunas de las tecnologías utilizadas para el control de accesos.

Tabla 2-2: Comparativa de tecnologías aplicadas al control de acceso

Parámetro	Control de acceso autónomo	Reconocimiento facial	Reconocimiento de iris	RFID	NFC
Contacto físico con el usuario para su activación.	Si	No	No	No	No
Guardado del registro de las entradas o salidas que se efectúen.	No	Si	Si	Si	Si
Distancia de lectura.	Necesita contacto físico	2-51 m	10-30 cm	0-100 m	0-10 cm
Velocidad.	10-100 Mbps	<= 1s	<= 1s	25Kbps	<= 424Kbps
Plataforma abierta para dispositivos móviles.	No	No	No	No	Si
Presencia de problemas a causa de una inadecuada iluminación.	No	Si	Si	No	No
Vulneración del derecho a la intimidad.	No	Si	Si	No	No

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 2-2* la tecnología a ser utilizada para el control de acceso en la zona 2 dentro del centro "Psicológico infantil PSICOVID" es la de Comunicación de campo cercano (NFC), debido a que no es un sistema invasivo, pues no se requiere que haya contacto físico entre el usuario y el propio sistema, además guarda un registro de las entradas o salidas que se efectúen en el día.

Cuenta con una alta velocidad de comunicación de hasta 424Kbps lo que se traduce a un rango corto de tiempo en la lectura y apertura de la puerta correspondiente a la zona a controlar. No vulnera el derecho a la intimidad de sus clientes y aún más importante, es de plataforma abierta por lo que los usuarios pueden hacer uso de ella mediante sus smartphones.

Finalmente, según el Instituto Nacional de Estadísticas y Censos (INEC, 2021a, p. 17) un total del 81.8% de ecuatorianos tienen a disposición teléfonos inteligentes, de los cuales cientos de los diferentes modelos existentes tienen incorporados tecnología NFC (ShopNFC, 2022), el aprovechar

de esta ventaja evitaría realizar gastos innecesarios en la compra de tecnologías alternativas, reduciendo costos en la construcción del prototipo de sistema embebido de seguridad.

2.3. Realidad de la zona

Al comparar los diferentes derivados de la delincuencia ocurridos en el Ecuador entre los meses de enero y noviembre de los años 2020-2021, se encuentra que, absolutamente todas las modalidades de robo fueron en ascenso, el robo a personas aumentó en un 24.4%, domicilios 12.1%, carros 48%, motos 31.9 %, unidades económicas 15.7% y entre bienes, autopartes de vehículos, accesorios en un 28.6% (Fiscalía General del Estado, 2021, p. 1).

El centro "Psicológico Infantil PSICOVID" está ubicado en la ciudad de Riobamba capital de la provincia de Chimborazo, específicamente en la Ciudadela la Politécnica, este circuito se caracteriza por los altos índices de delincuencia a los que se ve sujeto en cuanto a robos a domicilios respecta, pues la zona toma el primer puesto de los lugares con mayor número de sucesos de actos delictivos ocurridos y denunciados por los ciudadanos a la policía del distrito "Riobamba-Chambo", con un 17% en registros de actos delictivos, los cuales representan un total de 182 inmmuebles afectados por antisociales entre los meses de enero y septiembre del (La Prensa Chimborazo, 2021a).

Tomando como problema principal el robo a inmuebles al que se ve sujeto el establecimiento a asegurar, según la Fiscalía General del Estado (2021, p. 2), el horario más frecuente utilizado por los antisociales es la noche, con un total del 28.8% en cuanto a registros, así mismo, la modalidad de robo con mayor uso es la "estruche" (54%), es decir, se efectúan golpes o llamados a las puertas para verificar si alguien se encuentra dentro del inmueble.

Por lo antes mencionado los días en los que mayormente se lleva a cabo dichos robos son los sábados y domingos, pues en la mayoría de los casos representan a días no laborables, motivo por el que las personas abandonan sus inmuebles, dejándolos prestos a sufrir estos atracos.

La *Ilustración 2-2* representa el plano estructural del centro "Psicológico Infantil PSICOVID", donde, L.M: línea municipal, E.M: eje medianero y las mediciones están expresadas en metros. Además, es importante mencionar que la puerta principal, así como la ventana que limita el interior del establecimiento con la zona publica están fabricados de vidrio.

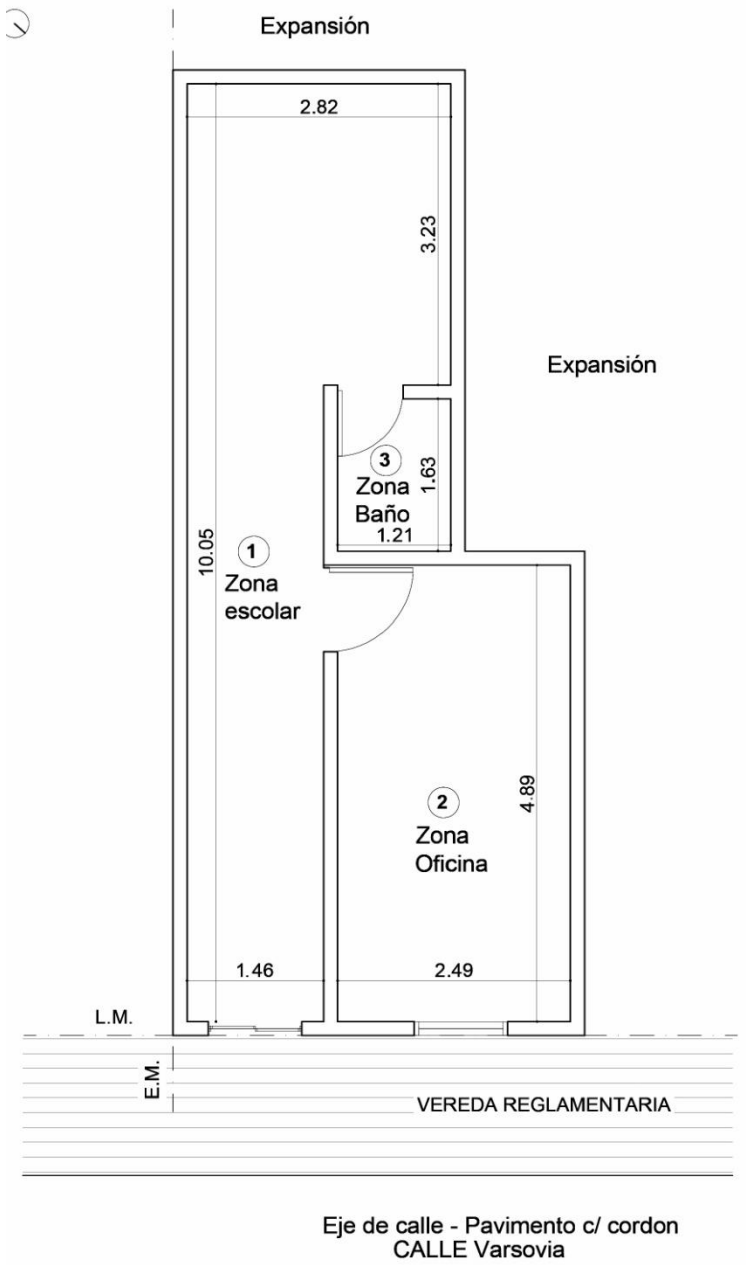


Ilustración 2-2: Plano estructural del centro "Psicológico Infantil PSICOVID"

Realizado por: Chafla, Hernán, 2022

Con base a la *Ilustración 2-2* se establece las diferentes dimensiones respecto a las áreas del establecimiento, en donde, se obtiene un área total de 33.03 m2 ubicada en una sola planta (planta baja), este total se encuentra distribuido en tres zonas; los primeros 18.88 m2 corresponden al área escolar (zona 1), 12.18 m2 corresponden al área de la oficina (zona 2) y 1.97 m2 al área del baño (zona 3).

Además, al hablar de sistemas de seguridad es importante tener en consideración un suministro constante de energía eléctrica el cual permita el funcionamiento del circuito electrónico en cuanto a su alimentación se refiere.

Para ello se tiene en consideración el histórico perteneciente al promedio en horas de la desconexión de energía eléctrica en el Ecuador, producida por cuestiones de fallas o mantenimientos realizados en la red eléctrica. La *Ilustración 3-2*, según el Operador Nacional de Electricidad (CENACE, 2020, pp. 64–65), se muestra las horas de desconexión de energía eléctrica por las cuales se ha sometido el país a través de los años varían entre los rangos de 5.4 y 9.84 horas.

Tomando como datos las horas correspondientes a los últimos años 2019 y 2020, se observa que el promedio de desconexión de suministro eléctrico ronda las 5.62 horas.

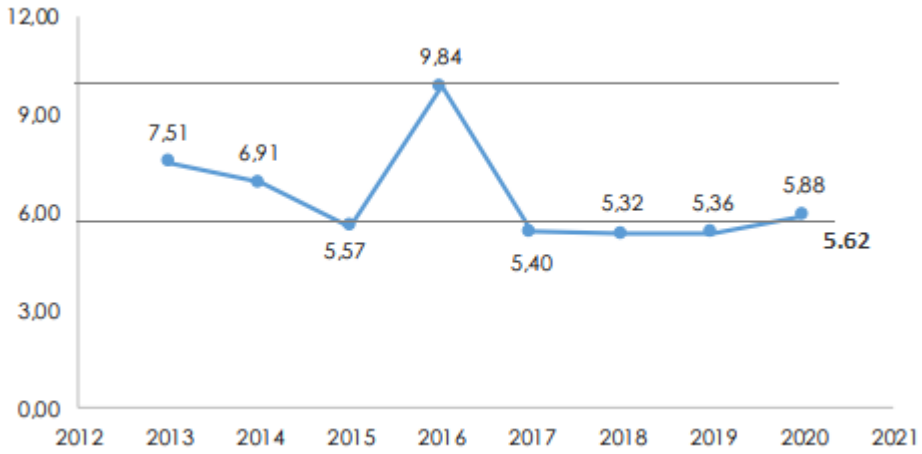


Ilustración 3-2: Horas de desconexión de energía eléctrica en Ecuador

Fuente: (CENACE, 2020, p. 65)

A nivel local, según la Empresa Eléctrica Riobamba S.A. (2022), el tiempo de interrupciones ocurridos específicamente en la ciudad de Riobamba por cuestiones de trabajos programados, fallas o mantenimientos tienen una duración entre 2 a 3 horas, valor que es considerado en el diseño del prototipo de sistema embebido de seguridad.

2.4. Normativas

Según la Norma Técnica Ecuatoriana (2016, p. 7) INEN-IEC 62851-1, traducción de la Norma Internacional, realizada por el Comité Técnico de "Alarmas y Sistemas de Seguridad electrónicos", se plantea que dentro de un sistema de alarma se tiene que considerar: requisitos del sistema, dispositivos de disparo (activación), controlador o unidad local y comunicaciones.

Estos parámetros son requisitos básicos para un sistema de alarma social, la cual permitirá la comunicación visual o vocal entre el sistema de seguridad y la persona/s administradora. Por lo que, según el INEN-IEC 62851-1 se tiene que considerar que:

- Para brindar tranquilidad y asistencia a los usuarios que se encuentran bajo lugares con vigilancia el sistema de seguridad deberá ofrecer el disparo de alarma las 24 horas del día, además tendrá que ser capaz de identificar, transmitir y receptar la señal de alarma.
- Los diferentes números de elementos que componen un sistema de alarma (ver en el apartado de arquitectura) tienen la opción de ser configurados de distintas formas para cumplir con la funcionalidad de brindar seguridad.
- Se tiene que contar con un controlador, el cual será el encargado de transmitir la condición de armado y desarmado de alarma a una CRA (Central Receptora de Alarmas), la misma que puede ser local o con mando a distancia en cuanto al controlador se refiere. La CRA tiene que ser capaz de establecer una comunicación de dos vías dadas entre el usuario y el receptor de alarma (en el caso de existir) quien se encargará de proporcionar asistencia extra a dicho usuario.
- Para algunos sistemas se puede considerar la función de pre- alarma, aunque este apartado no es obligatorio.

Además, se considera otras normativas aplicadas al servicio de seguridad en el Ecuador, orientadas a los procedimientos necesarios para la fundación, funcionamiento, supervisión y control de compañías que prestan servicios de seguridad privada y vigilancia, entre los más relevantes se menciona (Correa, 2008, pp. 1–8):

- Art. 1.- Se considera una compañía de seguridad y vigilancia a aquellas entidades que tengan como objetivo proporcionar servicios de seguridad y vigilancia en cualquiera de las 3 modalidades: móvil, fija e investigación privada. Además, tienen que encontrarse legalmente reconocida y constituida conforme a lo dispuesto en la Ley de Vigilancia y Seguridad.
- Art. 4.- En la modalidad de vigilancia fija las compañías de seguridad son responsable de los lugares de trabajo.
- Art. 5.- En cuanto a la modalidad de vigilancia móvil, se puede ofrecer servicios mediante puestos móviles, transmisión de señales de aviso de alarmas, sistemas de monitoreo con el objetivo de dar protección a usuario o a bienes específicos.
- Art. 19.- Se prohíbe a las compañías de seguridad y vigilancia el hacer uso de frecuencias que son designadas a la fuerza pública, pues el incumplir esta normativa será razón de sanción según lo determina la Ley de Vigilancia y Seguridad Privada.

- Art. 24.- Si se cometiera una infracción administrativa por la empresa de seguridad, así como también por sus miembros operativos y administrativos, se concederá una denuncia ante el Ministerio de Policía y Gobierno.

2.5. Arquitectura

Cumple la función de detallar la ubicación de los diferentes elementos que componen el sistema, entre las arquitecturas básicas están la distribuida y la centralizada (Morón Uche, 2013, p. 10).

La *Ilustración 4-2* representa la arquitectura centralizada de un sistema de seguridad, en ella los elementos como sensores, luces, sirenas (elementos a supervisar), así como los elementos que tendrán que ser controlados, se encuentran ligados a un punto en específico, dicho punto representa el cerebro del sistema, comúnmente se lo utiliza para áreas pequeñas.

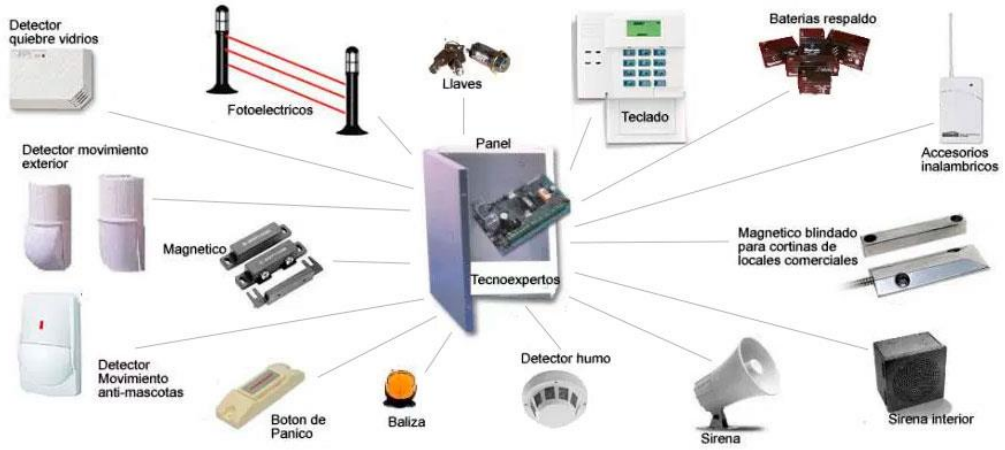


Ilustración 4-2: Arquitectura centralizada de un sistema de seguridad
Fuente: (Grupo Digitec, 2021)

La *Ilustración 5-2* muestra un sistema de seguridad basado en una arquitectura distribuida, dicho sistema se compone por dos módulos de control, modulo maestro y modulo esclavo, el módulo esclavo se encarga de enviar y recibir datos solo cuando el maestro lo solicita. Suelen existir sistemas con arquitectura distribuida referente a la ubicación física mas no a la capacidad de proceso y viceversa.

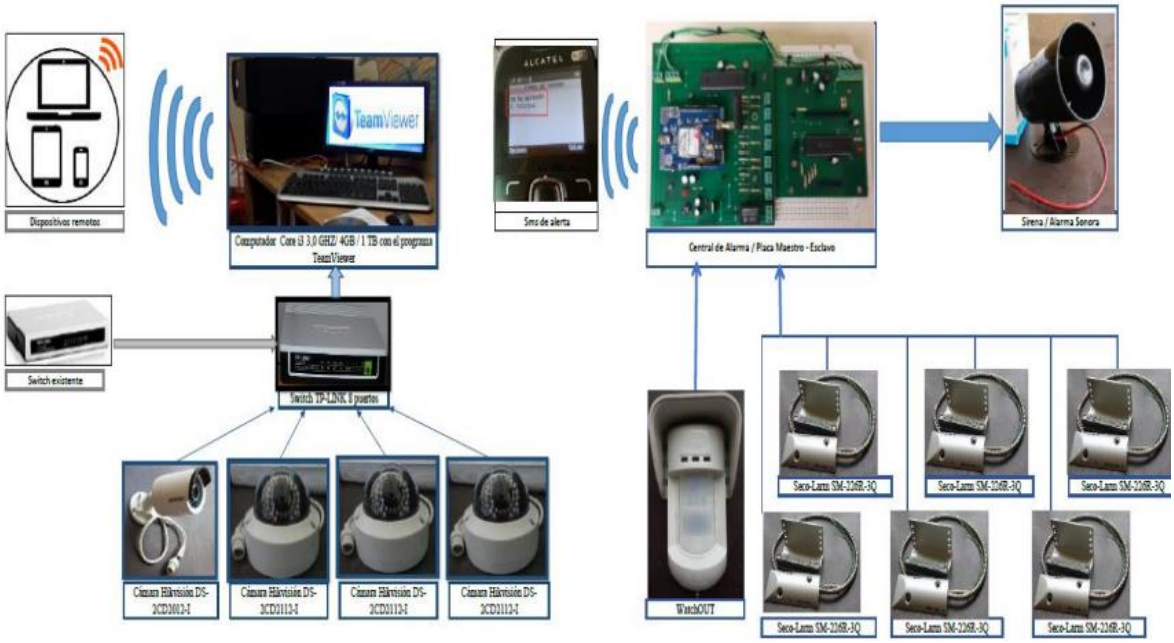


Ilustración 5-2: Arquitectura distribuida de un sistema de seguridad

Fuente: (Aviles and Cobeña, 2015, p. 34)

Componentes. - La *Ilustración 6-2* muestra los componentes que conforman un sistema de alarma social, en el cual se destacan tres grupos: primero aquellos que permiten percibir cualquier cambio o infiltración en cuanto al área supervisada se refiere, conocidos como elemento de adquisición de datos, segundo una unidad de control encargada en procesar los datos recolectados y por medio de los elementos de actuación (tercer grupo) dar respuesta en función a lo programado dentro de dicha unidad de control, conocida también como tarjeta de desarrollo. Dentro de un sistema de seguridad es importante considerar elementos que conformen un circuito de respaldo energético, por ejemplo, una batería eléctrica.

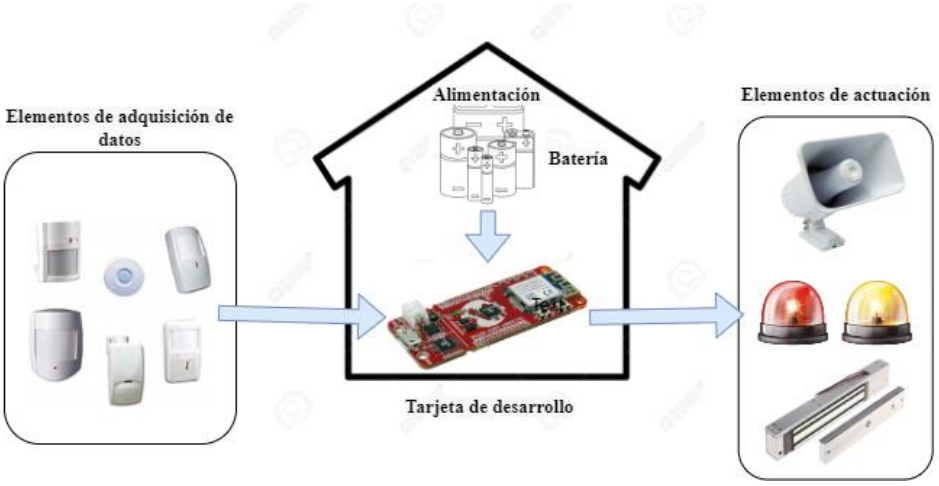


Ilustración 6-2: Componentes que conforman un sistema de seguridad social

Realizado por: Chafla, Hernán, 2022

2.5.1. Elementos de adquisición de datos

Este tipo de sistemas generalmente incluyen componentes de comunicación, vigilancia y detección, en la gran mayoría de casos estos componentes son: sensores, elementos que tienen como propósito pasar una magnitud física a una señal eléctrica (Barrera and Ros, 2016, p. 204), así mismo, a este tipo de sistemas se le suman sirenas, alarmas, focos, entre otros dispositivos utilizados como elementos de actuación, esto con el fin de advertir al administrador de seguridad que el perímetro vigilado ha sido violentado.

Detector de movimiento. - Dispositivos que al estar constituido por elementos emisores y receptores de señales son capaces de detectar el movimiento que se encuentre dentro de su rango de alcance, dicha actividad de detección es representada por un estado de encendido o apagado en su salida. La mayor parte de su campo de aplicación está orientada a sistemas de iluminación y sistemas de seguridad. Gracias a la aplicación en estos sistemas se consigue optimizar el consumo de energía, así como también su eficiencia. El precio de los diferentes detectores de movimiento varía en función a sus características, por ejemplo, existen sensores que cubren ángulos de detección de 110° hasta 360°, así como también la cantidad de distancia que abarcan son mayores unas a otras, la resistividad y grado de protección del sensor es uno de los parámetros importantes a tener en cuenta a la hora que querer adquirirlo, modelo, versión, etc. (Villavicencio, 2018, p. 13).

Detector de sonido. - También conocido como sensor de sonido, a través de sus elementos receptores son capaces de detectar ondas sonoras propagadas en su espectro de trabajo, es decir, son dispositivos capaces de detectar sonido en dependencia a su capacidad de receptar dichas ondas. Existen 3 tipos de sensores cuya diferencia se enfoca en el tipo de salida, entre estos están: con salida audio, salida envolve y salida gate. Se los utiliza principalmente como elementos de sistemas de seguridad, sistemas que incorporan mandos por voz u otras aplicaciones que impliquen la detección de ondas sonoras (Villegas, 2013, pp. 1–2).

Detector infrarrojo. - Son dispositivos optoeléctricos capaces de detectar y medir la radiación electromagnética infrarroja emitida por cuerpos encontrados dentro de su área de visión. La mayoría de estos elementos cuentan con un alto grado de sensibilidad a través del uso de circuitos integrados, son dispositivos que disponen de bajo consumo de energía eléctrica, funcionales, seguros, flexibles en cuanto a la iluminación y sensibilidad, cuentan con ajuste mecánico a los dos sentidos, entre otras características. Sus aplicaciones principales cubren las áreas de seguridad

aérea, seguridad territorial, automovilismo, ciencias médicas, sistemas de seguridad e inclusive uso doméstico (Aguilera, Rosero and Gilces, 2009, pp. 34–37).

Sensor magnético. – Tiene el objetivo de detectar campos magnéticos, producto a ello este tipo de sensores son sensibles a uno o a los dos polos del imán. Dicho de otra forma, este tipo de sensores son capaces de detectar campos magnéticos producidos por corrientes eléctricas o por imanes. Además, algunas de sus características principales es ser un elemento sensible, exacto y preciso. Es por esto que dentro de sus muchas aplicaciones se lo utiliza en sistemas de alarmas (Fernández, 2005, pp. 2–4).

Sensor de vibración. – Pueden ser de aceleración, velocidad o hasta de desplazamiento, cuentan con distintas sensibilidades y cubren un amplio rango para la toma de medidas. Su diseño de construcción establece en su mayoría la precisión y exactitud de las mediciones tomadas, pues en algunos casos se requiere que dicho sensor soporte y trabaje en condiciones bruscas, como bajas y altas temperaturas, lluvia, polvo, etc. (Galindo, 2010, pp. 1–4).

2.5.1.1. Comparativa entre elementos de adquisición de datos

En la *Tabla 3-2* se realiza una comparativa entre las características más relevantes de los elementos de adquisición de datos nombrados anteriormente, para ello se hace referencia al voltaje de alimentación, consumo de corriente, alcance, grados de detección, temperatura de funcionamiento y peso.

Tabla 3-2: Comparativa entre elementos de adquisición de datos

Tipo	Sensor de movimiento	Sensor de sonido	Sensor infrarrojo	Sensor magnético	Sensor de vibración
Alimentación	8.2 - 16 VCC	3.3-5 VCC	3.3 - 5 VCC	10 - 200 VCC	3.3 - 5 VCC
Consumo de corriente	Activo: 10 mA Reposo: 8 mA	5 mA	--	10-100 mA	5-15 mA
Alcance de detección	Hasta 15 metros	Distancia máxima de inducción 0.5 metros	2 – 30 cm	Distancia de activación de 15 -25 mm	Ajustable mediante potenciometro
Grados de detección	110 grados	--	35 grados	--	--
Temperatura de funcionamiento	-10ºC a +50ºC	-40ºC a +85ºC	-40ºC a +170ºC	--	-40ºC a +80ºC
Peso	61g	4g	3.8g	16g	1g

Realizado por: Chafla, Hernán, 2022

Con base a la comparativa expuesta en la *Tabla 3-2* se escoge el sensor de movimiento, pues su rango de alcance (15m) es el más adecuado para cubrir la longitud total del establecimiento (10m pertenecientes a la zona 1 y 4m correspondientes a la zona 2), así también se selecciona el sensor magnético, quien tiene un bajo consumo de corriente, 10mA, su distancia de activación es la más idónea a considerar en cuanto a un cambio o movimiento entre los bordes internos de la puerta principal, indicando la apertura o cierre de la misma.

Finalmente, considerando que la puerta como la ventana principal del establecimiento son de vidrio, se escoge el sensor de vibración quien tiene un consumo de corriente bajo, 5 mA, y un peso mínimo, 1g, elemento que ayudara a sensar los posibles intentos de ingreso forzado.

2.5.2. Elementos de actuación

Dentro de un sistema de seguridad los elementos de actuación son considerados también como elementos disuasorios, su función principal está en el informar a los intrusos que el área está protegida, para ello los elementos mayormente utilizados son:

Alarma audible. -También conocida como sirena, se la puede describir simplemente como un elemento capaz de emitir un sonido a distintos niveles en función a sus decibeles. A lo largo del tiempo el ser humano a relacionado el sonido de este elemento como un mensaje de aviso, alerta y en mayor proporción como un sonido capaz de disuadir el comportamiento de una persona. Es por esto que hoy en día se las utiliza en sistemas de seguridad, donde su activación es señal de alerta de intrusos en el área protegida. Entre las más utilizadas se encuentran aquellas que requieren una fuente de alimentación de 12 VCC, a partir de aquí se tiene una amplia gana en función a sus características, por ejemplo, se encuentra sirenas de 85, 110, 120, 123 dB, etc. Su promedio de respuesta se encuentra alrededor de los 3000 ± 500Hz, corrientes nominales menores a los 30 mA y algunos de ellos contienen elementos adicionales como multivibrador, luz led, protecciones, etc. (12v24vproducts, 2022).

Cerradura magnética. - También conocidas como cerraduras electromagnéticas están compuestas por una placa inducida y un electroimán que al energizarlo crea un flujo magnético que atrae y las une. Existen cerraduras con bloqueo y sin bloqueo, la diferencia radica en el actuar frente a un corte de energía, pues si fuera el caso, las "con bloqueo" permanecen cerradas, mientras las "sin bloqueo" se abren, por ello este primer tipo son recomendadas para puertas que dan acceso a lugares en donde se requiere seguridad (ArgSeguridad, 2021).

Con base a los elementos de actuación antes descritos, se escoge cualquier alarma audible que se encuentre entre el rango de 85 y 120 dB, pues según la ficha de "Señales acústicas de peligro y alarma - R.D. 485/1997, anexo IV.2", dicha sirena deberá emitir una señal sonora superior al del ruido ambiental (siempre y cuando este no sea muy intenso), con un nivel mínimo de 10 dB y máximo de 120 dB, con intervalos de sonido cortos (Arana, Eransus and Vela 2021, pp. 1–2). También se escoge la cerradura magnética de tipo "sin bloqueo", pues en caso de un corte de energía esta permanecería abierta permitiendo al administrador tener acceso a sus pertenencias.

2.5.3. Baterías

Dentro de un sistema de seguridad es imprescindible contar con una constante línea de alimentación eléctrica, por lo que se debe considerar el caso en el que el suministro energético llegase a fallar o saliera de servicio, para suplir esta falencia es necesario tener incorporado un sistema de respaldo en cuanto a la alimentación se refiere, este es un grupo de elementos que se ven involucrados en el sostenimiento de otros equipos mediante el suministro continuo de corriente (Gonzales, 2018, pp. 11–15).

La batería es el elemento principal de un sistema de respaldo energético, su objetivo es brindar suministro de corriente directa a los diferentes equipos a los que se le conecte, su tiempo de duración será inversamente proporcional al consumo eléctrico al que se vea sometido (Alvarado and García, 2012, p. 22). Entre las baterías más utilizadas están:

Li-Po. – Litio y polímero, se conforman por diferentes celdas mayormente utilizadas para proyectos que demandan corrientes mayores a 1A, son recargables, de tamaño y peso pequeños, entre sus aplicaciones se tiene: multirrotores, cámaras, linternas, celulares, drones, etc. (León, 2021).

Ni-Cd. – Níquel-cadmio, son baterías recargables, utilizadas en el campo industrial o de forma doméstica, utilizan hidróxido de níquel como cátodo, cadmio para el ánodo e hidróxido para el electrolito, son utilizadas mayormente para iluminación de respaldo o emergencia, flashes de cámaras, instrumentos electrónicos portátiles, vehículos eléctricos, etc. (Guasch, 1984).

Li-ion. – Ion de litio, compuesta por una o más celdas en configuración serie o paralela, se caracterizan por su carga rápida, duración, densidad de potencia alta, tamaño pequeño, ligera, entre sus campos de aplicación están: vehículos híbridos, eléctricos, cuidado de la salud, aeronaves y celulares (Quintero, Che and Auciello, 2021).

Batería AGM. – Al ser comparada con otras baterías se caracterizan por tener mayor vida útil por motivo de un mínimo desprendimiento se su material activo, mayores valores en cuanto a los arranques en frio. Es una batería a prueba de fugas, derrames, libre de mantenimientos, y diseñada especialmente para ser compatible con sistemas electrónicos sensibles (Coelectrix, 2017).

2.5.3.1. Comparativa entre baterías

En la *Tabla 4-2* se realiza una comparativa respecto a las cuatro baterías citadas anteriormente, pudiendo ser consideradas como elemento principal dentro del sistema de respaldo energético.

Tabla 4-2: Comparativa entre baterías

Parámetro	Li-Po	Ni-Cd	Li-ion	Batería AGM
Energía	100-130 Wh	40-80 Wh	110-160 Wh	168-336 Wh
Tensión por elemento	3.7V	1.25V	3.7V	2 V
Número de ciclos carga	300	2000	3000	1600
Tiempo de carga	1-1.5 horas	10-14 horas	2-4 horas	2-4 horas
Autodescarga por mes	10%	30%	25%	<2%

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 4-2* se escoge la batería de la familia AGM como elemento de respaldo energético, basándose principalmente en el bajo índice de autodescarga que presenta por mes (<2%), pues si el tiempo de inutilización fuese extenso dicha batería aseguraría en mayor porcentaje que el sistema de seguridad continue en funcionamiento en el caso de que la línea principal de energía caiga, así también se escoge esta familia debido al alto rango de energía que es capaz de su ministrar.

2.5.4. Tarjeta de desarrollo

Bajo una perspectiva de ingeniería, una tarjeta de desarrollo es una herramienta utilizada para el diseño, prototipado y construcción de sistemas analógicos o digitales, a través de la cual se estructura y se mejoran los procesos de diseño, trae como ventaja el acortar el tiempo de validación de diseños y cumplir el papel de producto final (González and Silva, 2013, pp. 1–2). Entre las más importantes se destacan:

Arduino. - Es una tarjeta que está basada en un microcontrolador, está compuesta de una interfaz de entrada mediante la cual es posible la conexión de diferentes periféricos, la información obtenida mediante dichos periféricos será trasladada al microcontrolador, el cual al estar

compuesto por circuitos integrados le es posible procesar y grabar la información. Tiene también una interfaz de salida, se encarga principalmente en trasladar a otros periféricos la información que ha sido procesada en el Arduino (Fernández, 2020).

Rasberry Pi. - Es un ordenador pequeño del tamaño de una cartera, capaz de caber en el bolsillo de cualquiera. En esta pequeña tarjeta se encuentra un módulo Wifi, Bluetooth, un procesador de cuatro núcleos y conexiones Ethernet, USB, RAM y HDMI. Tiene el objetivo de fortalecer y estimular en los jóvenes todos aquellos conocimientos básicos de la informática, sin embargo, la tarjeta rompió fronteras al tener un precio económico y al poder ser utilizado para casi cualquier proyecto de la domótica, robótica, etc. Un punto negativo es que Raspberry Foundation tiene el control en cuanto a la creación y fabricación de sus placas, ya que, trabaja con la filosofía de *hardware* propio, cosa que otras plataformas ya no mantienen (Escalante and Vargas, 2019, pp. 1).

FPGA. - Es un conjunto de dispositivos que se basan en matrices de bloques lógicos programables, su característica principal es que puede ser reprogramado para así cambiar su modo de aplicación, es decir, es una tarjeta flexible. Su segunda característica importante es la aceleración, pues la FPGA ayuda a los procesadores a través de aceleraciones vinculadas con la carga y descarga de información a aumentar el rendimiento de un determinado sistema (Robles, 2016, pp. 3–5).

ESP. - Es una familia de tarjetas de desarrollo que comparte el mismo objetivo que otras de microcontroladores, pues se enfocan en acercar a estudiantes, profesionales, especialistas a utilizar su entorno de trabajo mediante la facilitación en la creación de sus proyectos electrónicos. A diferencia de otras familias esta cuenta con un microprocesador de 32 bits, bloques para comunicación USB-Serial y Wifi, bajo consumo energético, varios entornos de código abierto (Arduino y Lua), con bibliotecas creadas para el desarrollo de casi cualquier tipo de proyectos (AV Electronics, 2022).

2.5.4.1. Comparativa entre tarjetas de desarrollo

En la *Tabla 5-2* se realiza una comparativa de las tarjetas de desarrollo que pueden ser consideradas para la realización del proyecto.

Tabla 5-2: Comparativa entre tarjetas de desarrollo

Parámetro	Arduino	Raspberry Pi	FPGA	ESP

Procesador	Atmel AVR	ARM Cortex	Intel Cyclone	Tensilica Xtensa LX3
Voltaje de entrada	5-12 V	Todos los modelos funcionan a 5V	5-9 V	3-5 V
Consumo de energía	19-85 mA	160mA - 1.25A	42-78mA	20-80 mA
Red Incorporada	No	ETH, Wifi	No	Wifi
RAM	8 KB	512 MB - 4 GB	75-1355 KB	96 KB
Almacenamiento	EEPROM (1-4 KB)	Necesita MicroSD	Flash 512 KB -1.6 MB	Flash 1-4 MB
Precio	$10-59	$30-200	$20-80	$8-12
Peso	7-50g	16-50g	23-40g	6.8-20g

Realizado por: Chafla, Hernán, 2022

En función al análisis de la *Tabla 5-2* la tarjeta de desarrollo a seleccionar para el desarrollo físico del presente trabajo de integración curricular es el de la familia ESP debido principalmente al factor económico, siendo la de menor costo al contrastarse con las familias presentadas, así también necesita de un bajo voltaje de alimentación y consumo de corriente (ideal para un sistema de alarma), tiene incorporado Wifi, necesario para establecer comunicación con el usuario a través del uso de una red social y respecto al peso es la tarjeta más liviana en cuanto a las citadas.

2.6. Redes sociales y su frecuencia de uso

Según Salinas Adriana (2021), son aplicaciones y sitios operados a nivel virtual, principalmente se encargan de asociar en grupos a personas que compartan temas de interés, estos pueden estar relacionados con el trabajo, música, parentesco, temas y formas de entretenimiento, etc. Por ello tienen como objetivo el intercambiar información y por ende establecer comunicación entre usuarios. Actualmente las prestaciones que brindan las redes sociales a los usuarios son extensas, por lo que se han vuelto necesarias en el desarrollo de las actividades cotidianas.

Por el surgimiento de nuevas tendencias mundiales cada año, los usuarios se vuelven más exigentes y buscan nuevas aplicaciones que se sean capaces de satisfacer sus requerimientos, como resultado anualmente el top de las redes sociales más utilizadas cambian en función a su frecuencia de uso.

Existen dos categorías de redes sociales: el primero abarca las redes sociales horizontales, su propósito es fortalecer la conexión e interacción entre usuarios, pues no fue creada para ser utilizada por un público en específico, aquí se encuentran Facebook, Twitter, WhatsApp, Telegram, etc. El segundo grupo es conocido como redes sociales verticales, estas se encuentran especializadas en cumplir una sola función de acuerdo a su creación, pueden ser académicas, de

fotografía, video, música, entre otras, un ejemplo a esto es YouTube, LinkedIn, etc. (Guzmán, 2018, p. 4).

Dentro de las redes sociales de carácter horizontal, utilizadas mayormente para uso de mensajería en el año 2022, según Fernández Rosa (2022), se encuentran; WhatsApp con un total de 2000 millones de usuarios activos, Facebook Messenger con 998 millones de usuarios activos y Telegram con 550 millones de usuarios activos.

2.6.1. Comparativa entre redes sociales de mensajería

Debido a que existen varias opciones por las cuales optar como medio de comunicación entre los módulos del prototipo de sistema embebido de seguridad, para una adecuada elección la *Tabla 6-2* muestra la comparativa entre las redes sociales de mensajería más populares.

Tabla 6-2: Comparativa entre redes sociales de mensajería

Parámetro	**WhatsApp**	**Facebook Messenger**	**Telegram**
Disponibilidad para sistemas operativos	Windows, iOS, Android, GNU/Linux.	Windows, iOS, Android, GNU/Linux.	Windows, iOS, Android, GNU/Linux.
Número de usuarios permitidos dentro de un grupo	512	250	200000
Uso obligatorio de tarjeta SIM	Si	No	No
Encontrar usuarios por geolocalización	No	No	Si
Envió de más de un archivo a la vez	Si	Si	No
Control de reenvió de mensajes	No	No	Si
Control de capturas de pantalla	No	No	Si
Eliminación de mensajes sin importar la fecha de envió	No	Si	Si
Creación y uso de chats secretos	No	No	Si
Creación de bots para interactuar con usuarios	No	No	Si

Publicaciones anónimas en grupos públicos	No	No	No

Fuente: (Ramírez, 2021)

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 6-2* se escoge Telegram como red social a utilizar para la visualización y control del prototipo de sistema embebido de seguridad, debido a que es la más adecuada a ser considerada dentro de un sistema de alarma, pues en cuestiones de confidencialidad nos es posible la creación de chats secretos, borrado de cualquier mensaje sin importar el tiempo de su envió y el control del reenvió de mensajes, así como también de capturas de pantalla.

Además, para establecer lazos de comunicación entre Telegram - usuario es posible la creación de aplicaciones de *software* programadas conocidas también como bots, dicha comunicación puede ser de uno a varios, lo que permitiría al sistema de control estar en contacto no solo con el administrador, sino con un grupo selecto de usuarios dispuestos a intervenir en caso de ameritarlo, a su vez dicho grupo admite un número suficientemente grande de miembros (hasta 200000).

2.6.2. Prácticas de seguridad para la utilización de redes sociales

El hacer uso de las redes sociales trae consigo una serie de riesgos que a menudo aumentan conforme pasa el tiempo, tales como: suplantación de identidad, *malware*, uso indebido de contenidos, robo de datos, robo de cuentas, etc. Es muy importante que los diferentes tipos de redes sociales los cuales son utilizados por millones de usuarios y que en consecuencia manejan elevadas cantidades de datos personales tengan incorporados estándares de seguridad de alta calidad, para que de esta forma los usuarios no se sientan posibles victimarios de problemas futuros y hagan uso de los servicios que prestan estas redes de forma tranquila (Guzmán, 2018, p. 7).

Es importante tener en claro un modelo que ayude a reducir riesgos y en la mayoría de los casos evite caer en alguno de estos problemas, por lo que un posible modelo a seguir basa su metodología en tres ideas fundamentales: correcta configuración de perfiles y uso de privacidad, tener en conocimiento las políticas de las redes sociales y la realización de buenas prácticas (Guzmán, 2018, pp. 7–10).

Para el desarrollo del presente trabajo de integración curricular, se considera varios parámetros planteados por los autores: León Rodolfo, Luna Jorge, Schmidt Ileana, Astorga Cristel (2019, pp. 188–209) y Sisalima Jorge (2010, pp. 33–35), los cuales mencionan una serie de recomendaciones que

tienen el objetivo de reducir los riesgos a los que están sujetos todos aquellos que hagan uso de dichas redes, entre las más importantes se tiene:

- Establecer un uso adecuado en cuanto a la administración y contraseñas de usuarios.
- Considerar las políticas y condiciones que normalmente exponen las redes sociales al momento de registro.
- Si la red social es abierta en un ordenador de escritorio o portátil utilizar un *software* de antivirus el cual se encargue de detectar y prevenir el *malware* propagado en estos sitios.
- En caso de que la red social lo permita, hacer uso de petición de contraseña cada vez que se solicite abrir o reestablecer dicha red.
- Tener en consideración los comunicados y avisos que emiten dichas redes a sus usuarios, pues en mayor parte son notificaciones de nuevos inicios de sesión, nuevas políticas de seguridad, privacidad, etc.
- Invertir tiempo para cambiar la configuración que viene por defecto en la red social con el fin de proteger los contenidos e información compartida a través de la red social, así mismo mantener el concepto de privacidad en alto nivel.
- Si la red social lo permite hacer uso de un segundo factor de autenticación.
- Tener en consideración las políticas en cuando a la utilización de imágenes, datos, información, y contenidos a ser compartidos en la red social.
- Toda la información de interés privado mantenerla fuera del alcance de terceros.

CAPÍTULO III

3. MARCO METODOLÓGICO

El presente capítulo cuenta con los siguientes apartados:

3.1. Requerimientos del PSES

Con base a la revisión bibliográfica presentada en el capítulo anterior se pueden definir los diferentes requerimientos de diseñador, así también por medio de una entrevista realizada a la psicóloga Maritza Poma, dueña del centro "Psicológico Infantil -PSICOVID", se definen los diferentes requerimientos de usuario. Los cuales son:

- Asegurar y controlar dos zonas del establecimiento: zona 1 (área escolar, con un total de 18.88 m2) y zona 2 (área de la oficina, con un total de 12.18 m2).
- La comunicación sistema de seguridad- administrador y viceversa, para la visualización y control tiene que ser mediante el uso de Telegram con comunicación vía internet.
- Establecer cuatro módulos de adquisición de datos, un módulo de control y actuación y un módulo de administración, control y visualización de la información.
- El primer módulo de adquisición de datos tendrá que estar compuesto por: un por un módulo NFC- sensor magnético, el segundo por: un sensor de movimiento, el tercero por: un sensor magnético - sensor de vibración y el cuarto por: un sensor de movimiento - sensor de vibración.
- Crear una base de datos en Firebase en donde se almacene los estados de sensores, alarmas y permisos.
- Los módulos de adquisición de datos deberán contar con la capacidad de conectarse a internet para almacenar los estados de sus elementos de sensado dentro de una base de datos.
- El módulo de control y actuación tendrá que establecer comunicación vía internet para la lectura de las variables almacenadas en la base de datos y la interacción con el administrador a través de Telegram.
- Establecer un sistema de control de acceso con tecnología NFC para la zona 2 (área de la oficina).
- Para el sistema de control de acceso se administrarán los permisos de acceso de un solo nivel a los usuarios por medio de una aplicación móvil con comunicación vía internet.
- Enviar a Telegram el historial de ingreso de usuarios a la zona 2 al administrador del PSES.

- Se tiene que poder activar la sirena y dar apertura de la puerta de la zona 2 mediante Telegram.
- Se deberá poder activar o desactivar la alarma en cualquier momento.
- Emitir mensajes de alerta y activar una sirena en caso de que se violara el paso de las zonas aseguradas.
- Implementar un sistema de respaldo de energía eléctrica cuya duración sea o sobrepase 3 horas.
- El sistema tiene que ser modular- escalable.
- Tiene que ser de menor costo en comparación a equipos comerciales de similares características.

3.2. Concepción de la arquitectura general del prototipo

La *Ilustración 1-3* representa la propuesta para el desarrollo del PSES, el cual se basa en el desarrollo de tres módulos fundamentales: adquisición de datos; control y actuación; administración, control y visualización de la información.

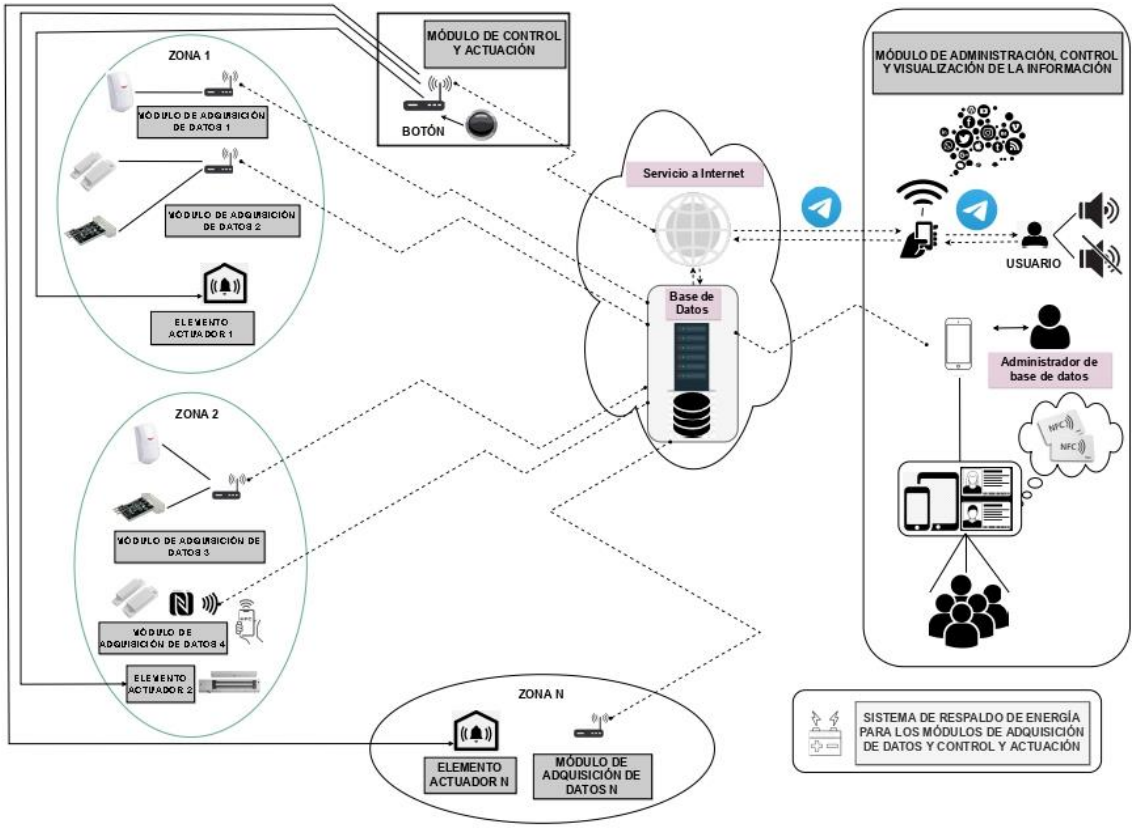


Ilustración 1-3: Arquitectura general del PSES

Realizado por: Chafla, Hernán, 2022

3.2.1. Módulo de adquisición de datos

Está conformado por cuatro módulos, compuestos por todos aquellos dispositivos de sensado ubicados en las dos zonas del establecimiento. La zona 1 correspondiente al área escolar cuenta con dos módulos, los cuales en conjunto tienen tres elementos de adquisición de datos, el primero es un sensor de movimiento el cual cubre los 18.88 m2 (área total de la zona 1) y está encargado de registrar presencia de personas cuando la alarma se encuentre armada, el segundo es un sensor magnético posicionado en los bordes internos de la puerta principal, este elemento se encarga de cambiar de estado cada vez que se detecte la apertura de dicha puerta, el tercer elemento es un sensor de vibración ubicado en la misma puerta principal.

La zona 2 correspondiente al área de la oficina cuenta con dos módulos, los cuales en conjunto tienen cuatro elementos de adquisición de datos, el primero es un sensor de movimiento encargado en sensar 12.18 m2 (área total de la zona 2), el segundo es un lector NFC, encargado de receptar las frecuencias emitidas por tarjetas NFC o por los smartphones de los usuarios, el tercero es un sensor de vibración ubicado en la ventana de esta zona y el cuarto un sensor magnético posicionado en la puerta correspondiente a este lugar.

Estos elementos de adquisición de datos están ligados a varias tarjetas de desarrollo ESP que actúan como procesadores de información, es decir, receptan los datos que les son suministrados, los procesan y los transmiten vía internet a una base de datos creada en *Firebase* para su correspondiente registro.

3.2.2. Módulo de control y actuación

Es el encargado de detectar cambios en los estados de las variables registradas en la base de datos por el módulo de adquisición de datos o por el botón implementado en él y en función a ello emitir diferentes órdenes a los elementos de actuación, como el encendido de la sirena la cual da respuesta a un intento o a una infiltración ocurrida en las zonas supervisadas, y la apertura de la cerradura magnética ubicada en la puerta de acceso a la zona 2, la cual brinda paso únicamente a los usuarios registrados por el administrador. De esta forma se puede decir que este módulo determina el comportamiento del sistema.

Cabe mencionar que los módulos nombrados anteriormente pueden establecer comunicación vía internet con el módulo de administración, control y visualización de información y además cuentan con un sistema de respaldo de energía por si la línea principal de energía falla.

3.2.3. Módulo de administración, control y visualización de la información

A este apartado lo compone un dispositivo móvil (smartphone), el cual establece comunicación vía internet y contiene dos interfaces gráficas: la primera corresponde a la interfaz de Telegram, quien actúa como herramienta de control y visualización de la información, pues a través de ella le es permitido al usuario visualizar los mensajes de alerta de alarma correspondientes a las zonas del establecimiento o los mensajes pertenecientes al historial de acceso de la zona 2, así mismo, por medio de esta primera interfaz nos es posible realizar el control, activando o desactivando la alarma audible, abriendo la puerta de la zona 2, o hasta armando y desarmando el mismo sistema por completo.

La segunda corresponde a la interfaz de la aplicación móvil, quien actúa como herramienta de administración y visualización, pues por medio de ella se observa y se gestiona el proceso de otorgamiento o prohibición de los permisos de acceso de un solo nivel correspondientes a los diferentes usuarios.

3.3. Diseño de la arquitectura de los módulos del PSES

A continuación, se presenta una descripción de los diagramas de bloques correspondientes a los diferentes módulos del PSES.

3.3.1. Módulo de adquisición de datos

La *Ilustración 2-3* representa la estructura por bloques del módulo de adquisición de datos, la misma está conformada por cuatro partes fundamentales: la primera es la etapa de recepción de datos establecida por los bloques de sensado y lector NFC, el segundo es el bloque procesador de información, quien recoge dichos datos, los procesa y a través de la tercera etapa (bloque de transmisión vía internet) los envía a una base de datos para su correspondiente registro. Además, por medio de esta última etapa una vez conectado el módulo a internet se notifica por Telegram su activación

La última etapa está representada por el bloque de alimentación, el cual se encarga de brindar un suministro constante de corriente al módulo perteneciente a este literal, así mismo tiene ligado a él un bloque de respaldo de energía, quien entra en funcionamiento cuando la línea principal de energía falla.

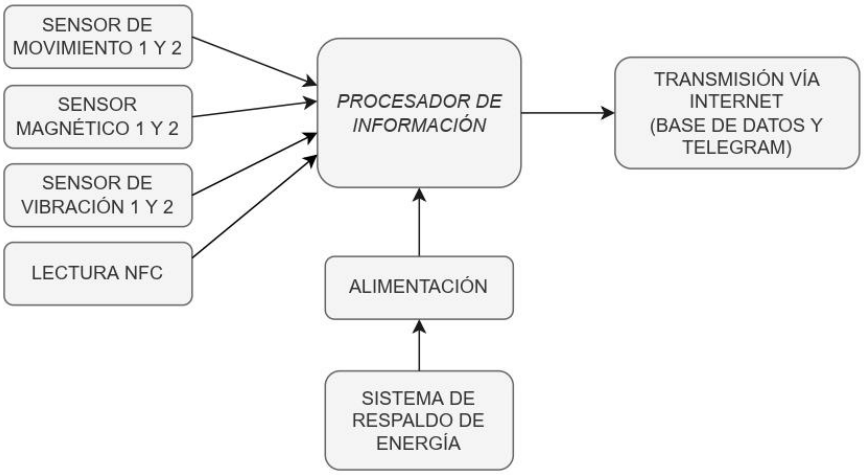


Ilustración 2-3: Diagrama de bloques del módulo de adquisicion de datos

Realizado por: Chafla, Hernán, 2022

3.3.2. Módulo de control y actuación

La *Ilustración 3-3* representa la estructura por bloques del módulo de control y actuación, está conformada por un bloque de comunicación vía internet, a través del cual se interactúa con la base de datos en donde se almacenan los estados correspondientes a las variables registradas, a través del bloque procesador de información se determina qué hacer con los datos que se lean (se determina el comportamiento del sistema), este módulo tiene como efector final elementos de actuación tal como una sirena audible y una cerradura magnética controlados por el bloque de actuadores, y un bloque conformado por un botón el cual da apertura de la puerta desde el interior de la zona.

A esta estructura la conforma también un bloque de comunicación vía internet a través del cual se establece comunicación con la red social Telegram. Finalmente, se integra un bloque de alimentación, el cual tiene el mismo principio de funcionamiento que en el caso del módulo de adquisición de datos.

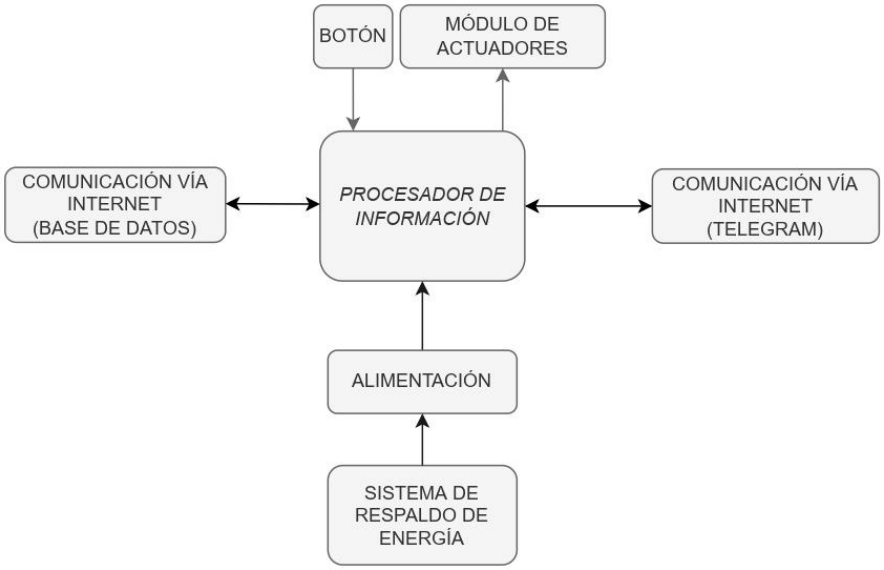


Ilustración 3-3: Diagrama de bloques del módulo de control y actuación

Realizado por: Chafla, Hernán, 2022

3.4. Selección del *hardware* para el PSES

A continuación, se detallan los elementos utilizados para la implementación del prototipo de sistema embebido de seguridad, una descripción y especificaciones técnicas de funcionamiento más importantes.

3.4.1. ESP8266 Wemos D1 mini

Tiene incorporado un procesador de 32 bits, le es posible establecer conectividad Wifi gracias a la incorporación de SoC (System on chip), un chip diseñado para cubrir la necesidad de mantener un mundo conectado. Cuenta con un regulador de voltaje a 3.3V donde dicho voltaje se refleja en los terminales de entradas y salidas (GPIO). Como se muestra en la *Ilustración 4-3* es una tarjeta compacta (35x26x12 mm), en cuanto a sus plataformas de desarrollo soporta varios lenguajes de programación, entre ellos: Arduino, C/C++, Lua (Naylamp Mechatronics, 2021).

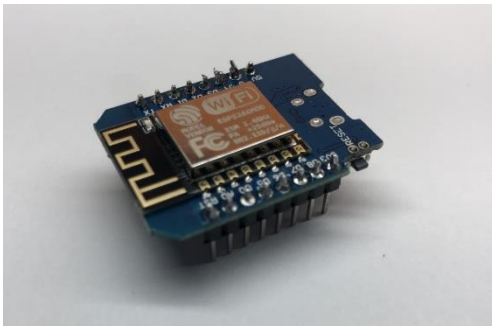


Ilustración 4-3: ESP8266 Wemos D1 mini

Realizado por: Chafla, Hernán, 2022

En la *Tabla 1-3* se describe las especificaciones técnicas de funcionamiento principales de la ESP8266 Wemos D1 mini (Espressif Systems, 2013, pp. 1–23). Para más información véase el Anexo A.

Tabla 1-3: Especificaciones técnicas principales de la ESP8266 Wemos D1 mini

Especificación técnica	Valor
Voltaje de alimentación	5VCC
Consumo de corriente	70mA
Voltaje de Entradas/Salidas	3.3VCC
Frecuencia de reloj	80-160MHz
Terminales digitales	11 (a 3.3V)
Terminales analógicos	1 (de 0-1V)
Conectividad	Wifi Direct- P2P
Módulos	AES, WEP, WAPI, TKIP
Dimensiones	35x26x12 mm
Peso	6 g

Realizado por: Chafla, Hernán, 2022

3.4.2. Sensor magnético MC-38

Es un elemento de tamaño compacto (27x14x8 mm), véase en la *Ilustración 5-3*, este sensor MC-38 consta de un mecanismo NC (normalmente cerrado), producto a esto envía un 1 lógico cuando las dos partes del sensor se encuentran en contacto y un cero lógico cuando no lo están (Unit Electronics, 2019).

Ilustración 5-3: Sensor magnético MC-38

Realizado por: Chafla, Hernán, 2022

En la *Tabla 2-3* se describe las especificaciones técnicas de funcionamiento principales del sensor magnético MC-38 (Synacorp, 2019, pp. 1–2). Para más información véase el Anexo B.

Tabla 2-3: Especificaciones técnicas principales del sensor magnético MC-38

Especificación técnica	Valor
Voltaje de alimentación	5VCC
Corriente máxima	100mA
Potencia nominal	3W
Mecanismo	NC (normalmente cerrado)
Distancia de activación mínima	15 mm
Distancia de activación máxima	25 mm
Dimensiones	27x14x8 mm
Peso	16 g

Realizado por: Chafla, Hernán, 2022

3.4.3. Sensor de movimiento DSC LC-100-PI

Una de las características más importantes de este modelo de sensor es el análisis inteligente de aquellas señales que capta, con el fin de asegurar un sensado confiable, incorpora tecnología Quad (para imagen lineal) lo que ayuda al sistema a ser mucho más preciso en: tamaños corporales, distinción de fondos y a su vez permite contar con la herramienta antimascotas (hasta 25 kg). Además de tener un diseño compacto *Ilustración 6-3*, se puede realizar ajuste a su sensibilidad, conteo de pulsos variables y no requiere de calibración de altura al momento de su instalación (TVC, 2022).

Ilustración 6-3: Sensor de movimiento DSC LC-100-PI

Realizado por: Chafla, Hemán, 2022

En la *Tabla 3-3* se describe las especificaciones técnicas de funcionamiento principales del sensor de movimiento DSC LC-100-PI (DSC, 2013, pp. 1–2). Para más información véase el Anexo C.

Tabla 3-3: Especificaciones técnicas principales del sensor de movimiento DSC LC-100-PI

Especificación técnica	**Valor**
Voltaje de alimentación	9.6-16VCC
Consumo de corriente	12mA (± 5%)
Distancia de sensado	5-15m
Grados de sensado	85º
Método de detección	PIR Quad (4 elementos)
Mecanismo	NC (normalmente cerrado)
Protección RFI	10 V/m más 80%
Frecuencia de operación	80-2000 MHz
Dimensiones	92x62.5x40 mm
Peso	58 g

Realizado por: Chafla, Hernán, 2022

3.4.4. Módulo sensor de vibración Ky-002

Cuenta con dos terminales: el terminal A (TA), es el conductor central compuesto por una resistencia interna de 10KΩ y el terminal B (TB) conformado por un resorte. Al detectar un golpe TA establece contacto con alimentación positiva, mientras que TB toma acción sobre lo ocurrido y cierra el circuito con tierra, esta señal es captada y emitida por el circuito que contiene a este

elemento de sensado, por ello este módulo Ky-002 posee tres terminales (VCC, GND, salida), véase en la *Ilustración 7-3* (Unit Electronics, 2016).

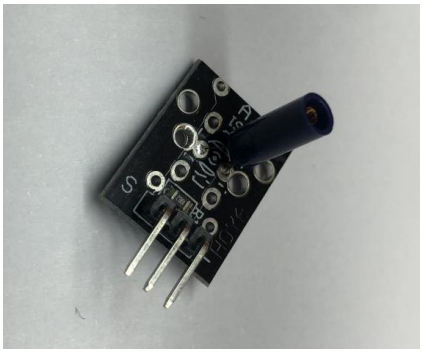


Ilustración 7-3: Módulo sensor de vibración Ky-002

Realizado por: Chafla, Hernán, 2022

En la *Tabla 4-3* se describe las especificaciones técnicas de funcionamiento principales del módulo sensor de vibración Ky-002 (Asuni, 2022, p. 1). Para más información véase el Anexo D.

Tabla 4-3: Especificaciones técnicas principales del módulo sensor de vibración Ky-002

Especificación técnica	Valor
Voltaje de alimentación mínimo	3.3VCC
Voltaje de alimentación máximo	5VCC
Consumo de corriente	5 mA
Señal digital HIGH	No hay detección
Señal digital LOW	Hay detección
Dimensiones	18.5x15 mm
Peso	1 g

Realizado por: Chafla, Hernán, 2022

3.4.5. Módulo RFID/NFC PN532

Tiene compatibilidad con dispositivos y con tarjetas NFC con frecuencia de 13.56MHz, contiene la antena incluida en su propio PCB, como lo muestra la *Ilustración 8-3*, el chip PN532 permite al módulo escribir, leer sobre tags, además establecer comunicación con microcontroladores o con dispositivos móviles que soportan NFC a través de sus tres interfaces de comunicación, como: UART, I2C y SPI. Dicho chip tiene incluido la librería "libnfc" útil para el desarrollo de un sin número de aplicaciones (Naylamp Mechatronics, 2021a).

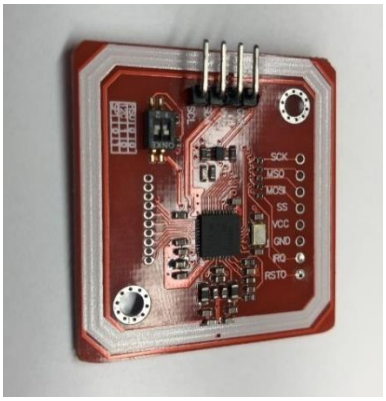


Ilustración 8-3: Módulo RFID/NFC PN532

Realizado por: Chafla, Hernán, 2022

En la *Tabla 5-3* se describe las especificaciones técnicas de funcionamiento principales del módulo RFID/NFC PN532 (NXP B.V, 2017, p. 4). Para más información véase el Anexo E.

Tabla 5-3: Especificaciones técnicas principales del módulo RFID/NFC PN532

Especificación técnica	Valor
Voltaje de alimentación	3.3-5VCC
Consumo de corriente	25 mA
Distancia máxima de lectura	10 cm
Frecuencia de operación	13.56 MHz
Chip	PN532
Interfaz de comunicación	UART, I2C, SPI
Transferencia de datos máxima	10 Mbit/s
Compatible con estándar	NFC: ISO/IEC 18092
Dimensiones	41x43 mm

Realizado por: Chafla, Hernán, 2022

3.4.6. Cerradura magnética ZE-280-5T

Elemento fabricado con una alta tecnología, confiable en el bloqueo y apertura de portones y puertas interiores, la componen dos elementos, véase en la *Ilustración 9-3*, un electroimán y la placa de la cerradura, comúnmente este segundo elemento esta empotrado en la puerta. Para impedir la apertura de dichos elementos ejerce una fuera mayor a los 280 kg (Delta EU, 2022).

Ilustración 9-3: Cerradura magnética ZE-280-5T

Realizado por: Chafla, Hernán, 2022

En la *Tabla 6-3* se describe las especificaciones técnicas de funcionamiento principales de la cerradura magnética ZE-280-5T (DELTA OPTI, 2022, p. 1). Para más información véase el Anexo F.

Tabla 6-3: Especificaciones técnicas principales de la cerradura magnética ZE-280-5T

Especificación técnica	Valor
Voltaje de alimentación mínimo	12VCC
Voltaje de alimentación máximo	24VCC
Consumo de corriente	250-500 mA
Capacidad de carga	280 kg
Retardo ajustable (por precisión)	0-32 segundos
Indicador de salida (para apertura)	NO/NC
Dimensiones	250x47x28 mm (cerradura) 180x38x12 mm (placa de metal)
Peso total	1.73 kg

Realizado por: Chafla, Hernán, 2022

3.4.7. Alarma audible 12V Opalux

Dispositivo electrónico utilizado como elemento de actuación frente a cualquier violación a las zonas aseguradas, también llamado circulina, véase en la *Ilustración 10-3*, emite un mensaje de alerta capaz de disuadir el comportamiento de una persona, este modelo cuenta con un indicador visual led para un aviso de activación más notorio (Delta Enterprises S.A.C, 2022).

Ilustración 10-3: Alarma audible 12V Opalux

Realizado por: Chafla, Hernán, 2022

En la *Tabla 7-3* se describe las especificaciones técnicas de funcionamiento principales de la alarma audible 12V Opalux (Delta Enterprises S.A.C, 2022).

Tabla 7-3: Especificaciones técnicas principales de la alarma audible

Especificación técnica	Valor
Voltaje de alimentación	12VCC
Consumo de corriente	1100 mA
Potencia	25W
Nivel de sonido	90dB
Indicador visual	Luz led
Dimensiones	16.5x10cm

Realizado por: Chafla, Hernán, 2022

3.4.8. Otros elementos

Para la construcción del PSES se hizo uso de otros elementos *hardware*, los cuales forman parte de su arquitectura, entre ellos están:

Convertidor DC-DC MP2307. – Elemento electrónico reductor de tensión, pues proporciona un voltaje de salida menor al de entrada, trabaja de manera constante con una corriente de 1.8A a frecuencia de conmutación aproximada a los 340KHz, tiene incorporado un potenciómetro el cual permite el ajuste de voltaje de salida a pasos de ±25%, véase en la *Ilustración 11-3*. Entre sus características más importantes están: voltaje de entrada 4.75-23VCC, voltaje de salida 1-17VCC,

corriente máxima de salida 3A, temperatura de funcionamiento de -40 a +150ºC, dimensiones 17x11x4mm y peso 3g (MPS, 2006, pp. 1–3).

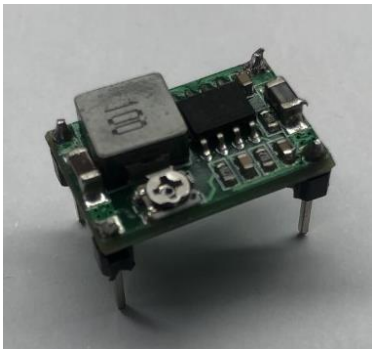


Ilustración 11-3: Convertidor DC-DC MP2307

Realizado por: Chafla, Hernán, 2022

Módulo DFPlayer Mini MP3. – Utilizado como indicador para el control de acceso, pues mediante el llamado y reproducción de sonidos previamente grabados se anuncia si el usuario tiene o no permitido el ingreso a la zona protegida, dicho elemento se muestra en la *Ilustración 12-3*. Entre las características principales de este módulo se encuentran: voltaje de alimentación de 3.2-5VCC, consumo de corriente de 20mA, soporta tarjeta SD de hasta 32G, es posible la creación de hasta 100 carpetas con 255 archivos de audio cada una, formatos MP3-WMA-WAV, ajustable hasta 30 niveles de volumen (AV Electronics, 2020).

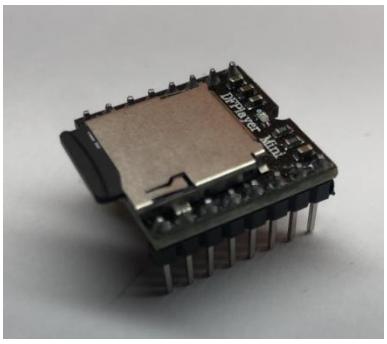


Ilustración 12-3: Módulo DFPlayer Mini MP3

Realizado por: Chafla, Hernán, 2022

Módulo relé de 1 canal. – Capaz de controlar el encendido y el apagado de equipos o dispositivos de alta potencia (hasta 250V a 10A), su canal posee un led indicador y un optoacoplador para el aislamiento eléctrico, véase en la *Ilustración 13-3*. Entre sus características principales están: voltaje de operación 5VCC, consumo de corriente por bobina 90mA, corriente máxima 10A

(normalmente abierta) y 5A (normalmente cerrada), tiempo de acción 5-10ms (Naylamp Mechatronics, 2021c).

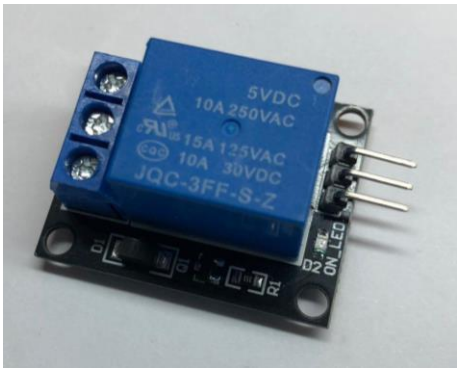


Ilustración 13-3: Módulo relé de 1 canal

Realizado por: Chafla, Hernán, 2022

Fuente de alimentación UHPPOTE. – Fabricado por la empresea UHPPOTE, véase en la *Ilustración 14-3*, entre sus características más importantes se encuentran: voltaje de entrada 100-240VCA, voltaje de salida 12VCC a 5A, en cuanto a cortes de la línea principal de suministro eléctrico está en la capacidad de soportar una batería de respaldo hasta de 12V a 7A y regulación de tiempos de bloqueo de 0-15 segundos (Uhppote, 2020).

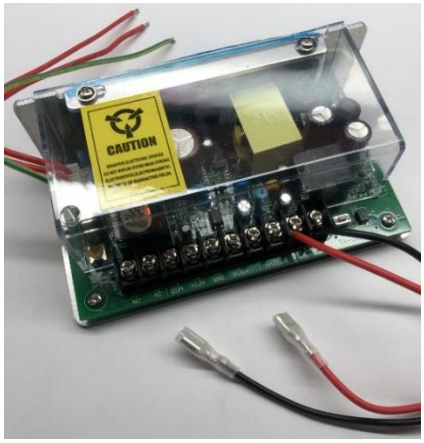


Ilustración 14-3: Fuente de alimentación UHPPOTE

Realizado por: Chafla, Hernán, 2022

3.4.9. Batería para el PSES

Para la selección de la batería, primero se realiza el dimensionamiento respecto al consumo teórico que generan los diferentes elementos hardware del PSES, como lo muestra la *Tabla 8-3*.

Tabla 8-3: Cálculo de consumo de corriente en el PSES

Módulo	Cantidad	Componente	Corriente unitaria (mA)	Corriente total (mA)
Adquisición de datos	4	ESP8266 Wemos D1 mini	70	280
	2	Sensor magnético MC-38	100	200
	2	Sensor de movimiento DSC LC-100-PI	12	24
	2	Sensor de vibración Ky-002	5	10
	1	Módulo RFID/NFC PN532	25	25
	1	Otros elementos	32	32
		TOTAL	571 mA	
Control y actuación	1	ESP8266 Wemos D1 mini	70	70
	1	Cerradura magnética ZE-280-5T	500	500
	1	Alarma audible 12V Opalux	1100	1100
	1	Otros elementos	23	23
TOTAL			1693 mA	
Consumo de corriente total de los módulos			2264 mA	

Realizado por: Chafla, Hernán, 2022

En la *Tabla 8-3*, se observa como resultado un consumo de corriente total de 2264 mA, por lo que es necesario escoger una batería que satisfaga con esta demanda, considerando que los rangos de cortes en la zona van de dos a tres horas, tal como se menciona en el apartado de "Realidad de la zona".

Tomando en cuenta lo antes mencionado se procede a la selección de una batería Rekoser RKE12-7, diseñada para la optimización de su calidad, así como de su vida útil, minimiza su mantenimiento y sus niveles de autodescarga, respecto a su construcción, posee un contenedor y tapa fabricados de ABS, separador de fibra de vidrio, sellador de resina epoxi, válvula de seguridad de caucho, terminal de cobre. Como se observa en la *Ilustración 15-3*, es una batería robusta con dimensiones de 151x65x96mm y peso de 2.1kg (Rekoser, 2022).

Ilustración 15-3: Batería Rekoser RKE12-7

Realizado por: Chafla, Hernán, 2022

En la *Tabla 9-3* se describe las especificaciones técnicas de funcionamiento más importantes de la batería Rekoser RKE12-7 (Rekoser, 2022). Para más información véase el Anexo G.

Tabla 9-3: Especificaciones técnicas de la batería Rekoser RKE12-7

Especificación técnica	**Valor**
Voltaje nominal	12VCC
Corriente máxima de carga	2.1A
Corriente máxima de descarga	105A
Capacidad a 25ºC	7Ah @ 20HR
Resistencia interna	Completamente cargada 25mΩ
Autodescarga	3% por mes a 25ºC
Número de celdas	6
Voltaje de carga a 25ºC	Cycle: 14.6-14.8V (2.1A) Float: 13.6-13.8V
Capacidad afectada a causa de la temperatura	A 40ºC (102%) A 100ºC (100%) A 85ºC (85%) A 65ºC (65%)
Dimensiones	151x65x93 mm (cerradura)
Peso total	2.1 kg

Realizado por: Chafla, Hernán, 2022

Ahora, considerando la siguiente ecuación:

$$h = \frac{(Vb * Ib)}{(Vb * Ic)}$$

Donde:
Vb: voltaje de la batería
Ib: corriente de la batería
Ic: corriente total de consumo
h: duración en horas de la batería

Se obtiene un tiempo de duración igual a 3.091 horas, por lo que dicha batería seleccionada alcanza el rango de tiempo frente a un corte de energía en la zona, por lo que teóricamente satisface con la demanda de corriente que genera el PSES.

3.5. Esquema de conexión del PSES

A continuación, se detallan las conexiones realizadas para: el bloque de alimentación, módulo de adquisición de datos y el módulo de control y actuación.

3.5.1. Esquema de conexión del bloque de alimentación

Está conformado por una fuente de alimentación UHPPOTE, una batería Rekoser RKE12-7 y una bornera de dos terminales, como se muestra en la *Ilustración 16-3*.

- Respecto a la toma eléctrica correspondiente a 110VCA, se conecta la línea de fase al terminal BF y neutro al terminal BN de la fuente de alimentación UHPPOTE, el terminal BT de dicha fuente se conecta a tierra.
- Los terminales de salida positivo (+) y negativo (-) de la batería Rekoser RKE12-7 se conectan a los terminales (+9) y (-10) de la fuente de alimentación UHPPOTE, respectivamente.
- Los terminales (+4) y (-5) correspondientes a la fuente de alimentación UHPPOTE representan las salidas +12VCC y GND, por lo que se conectan a una bornera de 2 terminales, a través de esta salida se brinda suministro eléctrico a todos los elementos que componen el PSES.

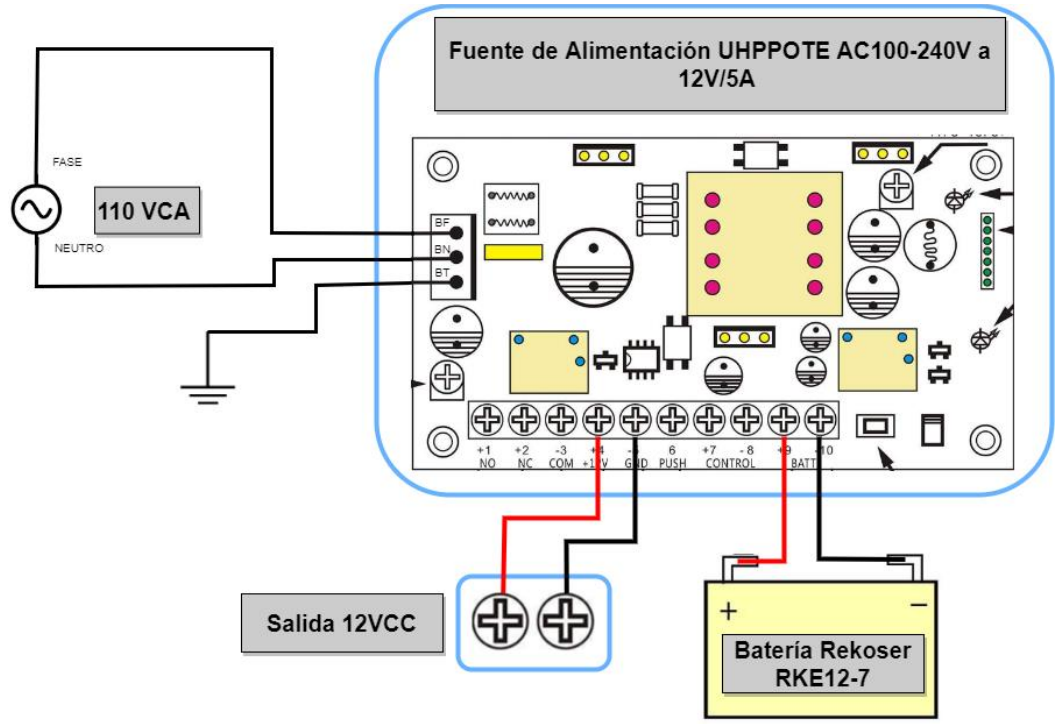


Ilustración 16-3: Esquema de conexión del bloque de alimentación

Realizado por: Chafla, Hernán, 2022

3.5.2. Esquema de conexión del módulo de adquisición de datos

Este apartado está conformado por dos partes, la primera la constituye la adquisición de datos para el control de acceso (módulo 1) y la segunda la adquisición de datos para el sistema de alarma (módulos 2, 3 y 4).

3.5.2.1. Adquisición de datos para el control de acceso

El módulo de adquisición de datos orientado al control de acceso al que también llamaremos módulo de adquisición de datos 1, está compuesto por una tarjeta de desarrollo ESP8266 Wemos D1 Mini, un convertidor DC-DC MP2307, un módulo RFID/NFC PN532, un sensor magnético MC-38, un módulo DFPlayer Mini MP3, un bloque de entradas/ salidas y un bloque de alertas, como se muestra en la *Ilustración 17-3.*

- La salida +12VCC y GND de la fuente de alimentación UHPPOTE se encuentra conectados a los terminales de entrada IN+ (12V) y IN- (GND) del convertidor DC-DC MP2307, respectivamente. El terminal de salida de dicho convertidor OUT+ se conecta a los terminales nombrados como (5V o VCC) de todos los elementos que componen este módulo, y el terminal OUT- del mismo convertidor se conecta a los todos los terminales nombrados

como GND, esta salida de alimentación obtenida (5VCC) sirve para el suministro eléctrico de todos los elementos de este circuito.

- El módulo RFID/NFC PN532 conecta sus terminales de salida SCL y SDA al terminal D1 y D2 de la ESP8266 Wemos D1 Mini, respectivamente.
- El módulo DFPlayer Mini MP3 conecta su salida Tx al terminal D5 y su salida Rx al terminal D6 de la ESP8266 Wemos D1 Mini, además se conectó un altavoz como indicador acústico, donde los terminales SPK1 y SPK2 del módulo DFPlayer Mini MP3 se conecta a la entrada positiva (+) y negativa (-) respectivamente de dicho altavoz.
- El sensor magnético MC-38 conecta su terminal GND con el terminal OUT- del convertidor DC-DC MP2307 y su terminal de salida con el terminal D4 la ESP8266 Wemos D1 Mini.
- Se utilizan tres leds como indicadores, los terminales positivos del led 1, led 2 y led 3 se conecta a los terminales D0, D7 y D8 de la ESP8266 Wemos D1 Mini, respectivamente y los terminales negativos de dichos leds se conectan a tierra (GND).
- El bloque de "Alertas" cuenta con un buzzer el cual emite un sonido cada vez que el módulo RFID/NFC PN532 realiza una lectura, para ello el terminal D3 de la ESP8266 Wemos D1 Mini conecta con la base de un transistor 2N3904, dicho transistor tiene conectado su colector al terminal negativo del buzzer, y su emisor a GND, mientras que el terminal positivo del buzzer se conecta a la alimentación de 5VCC.

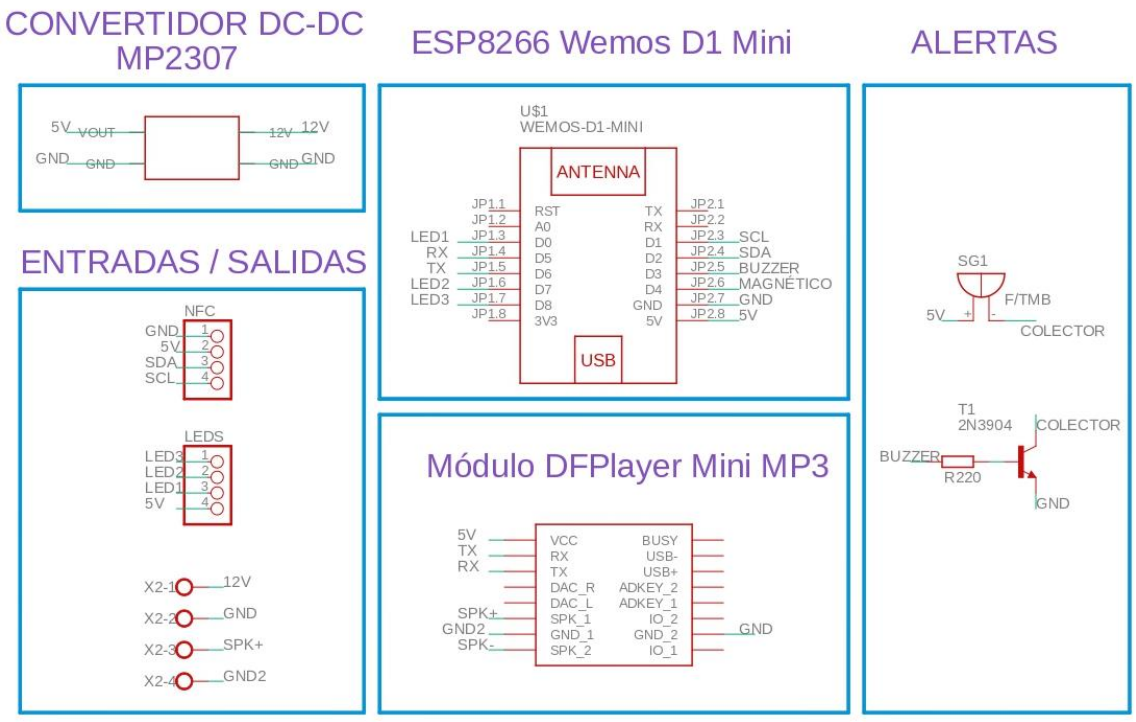


Ilustración 17-3: Adquisición de datos para el control de acceso

Realizado por: Chafla, Hernán, 2022

Como muestra la *Ilustración 18-3*, se realizó el diseño de dicho circuito en PCB para la posterior construcción física del módulo de adquisición de datos para el control de acceso.

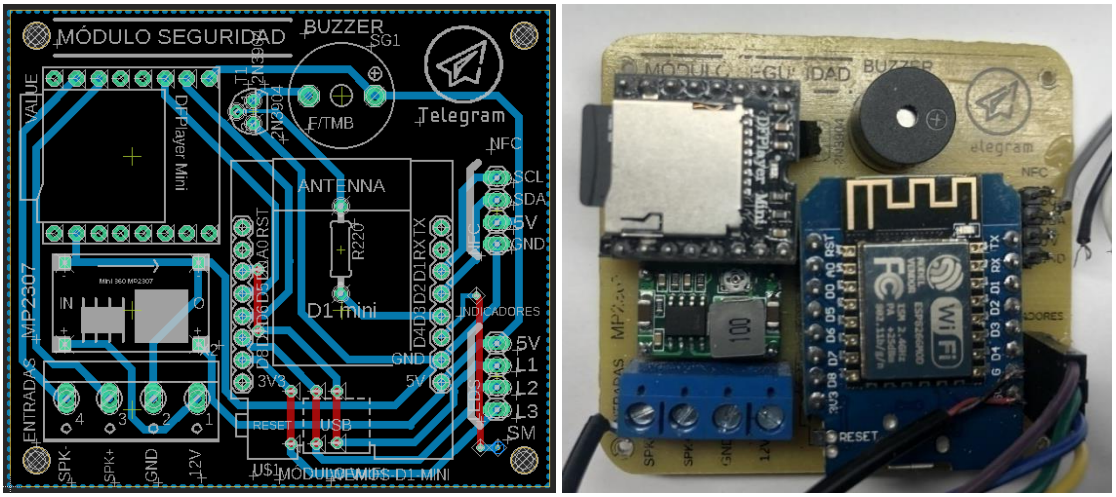


Ilustración 18-3: PCB y construcción del módulo de adquisición de datos para el control de acceso

Realizado por: Chafla, Hernán, 2022

3.5.2.2. Adquisición de datos para el sistema de alarma

Se conforma por los siguientes tres módulos:

a) Módulo de adquisición de datos 2

Está compuesto por una tarjeta de desarrollo ESP8266 Wemos D1 Mini, un convertidor DC-DC MP2307 y un sensor de movimiento DSC LC-100-PI, como se muestra en la *Ilustración 19-3*.

- La salida +12VCC y GND de la fuente de alimentación UHPPOTE se encuentra conectados a los terminales de entrada IN+ (12V) y IN- (GND) del convertidor DC-DC MP2307, respectivamente. El terminal de salida de dicho convertidor OUT+ se conecta al terminal (5V) de la ESP8266 Wemos D1 Mini, y el terminal OUT- del mismo convertidor se conecta a los todos los terminales GND.
- El sensor de movimiento DSC LC-100-PI, con alimentación 12V, conecta su terminal NC (señal) con el terminal "D1" de la ESP8266 Wemos D1 Mini y "D7" se conecta a un led indicador.

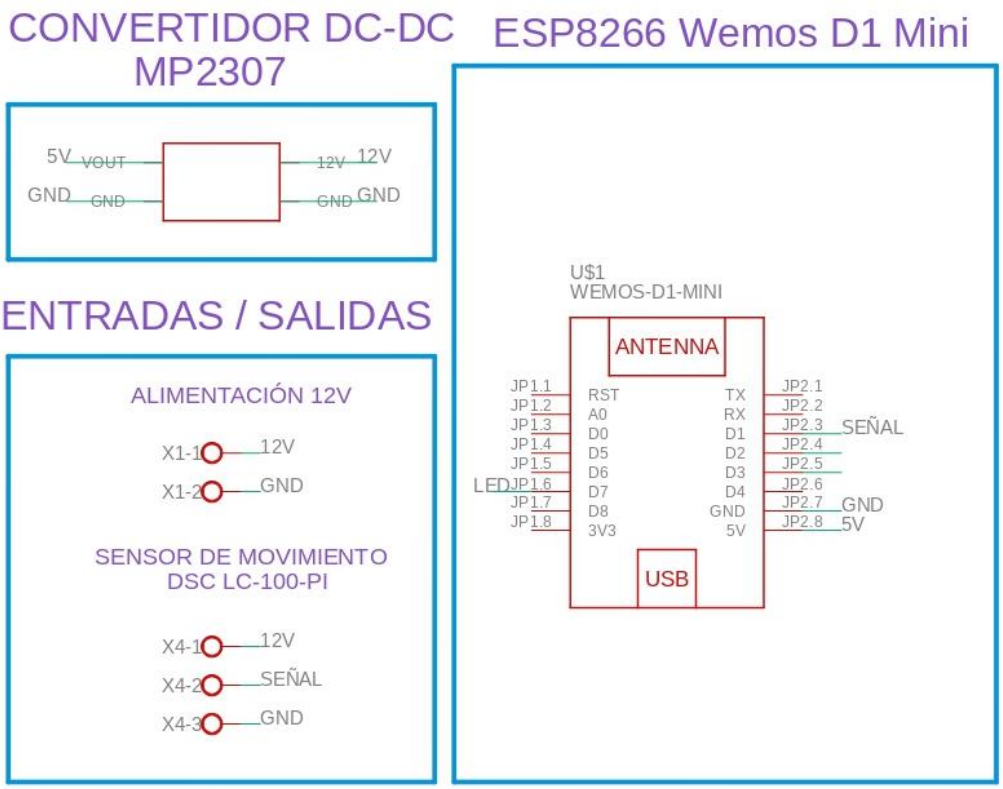


Ilustración 19-3: Módulo de adquisición de datos 2

Realizado por: Chafla, Hernán, 2022

Como lo muestra la *Ilustración 20-3*, se realizó el diseño de dicho circuito en PCB para la posterior construcción física del módulo de adquisición de datos 2 para el sistema de alarma.

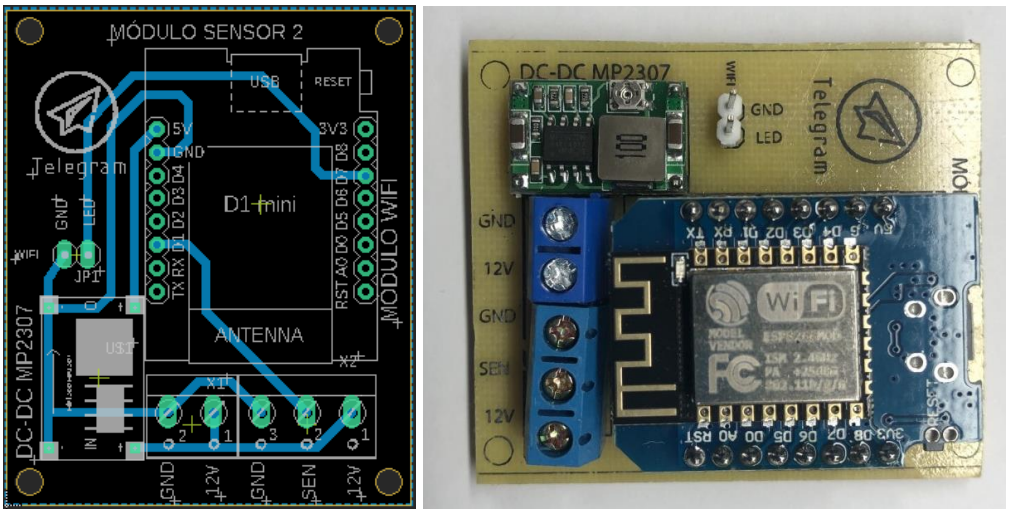


Ilustración 20-3: PCB y construcción del módulo de adquisición de datos 2

Realizado por: Chafla, Hernán, 2022

b) Módulo de adquisición de datos 3

Está compuesto por una tarjeta de desarrollo ESP8266 Wemos D1 Mini, un convertidor DC-DC MP2307, un sensor magnético MC-38 y un sensor de vibración KY-002, como se muestra en la *Ilustración 21-3.*

- La salida +12VCC y GND de la fuente de alimentación UHPPOTE se encuentra conectados a los terminales de entrada IN+ (12V) y IN- (GND) del convertidor DC-DC MP2307, respectivamente. El terminal de salida de dicho convertidor OUT+ se conecta al terminal (5V) de la ESP8266 Wemos D1 Mini, y el terminal OUT- del mismo convertidor se conecta a los todos los terminales GND.
- El sensor de vibración KY-002, con alimentación 5V, conecta su terminal S (golpe) con el terminal D1 de la ESP8266 Wemos D2 Mini.
- El sensor magnético MC-38 conecta su terminal GND con el terminal OUT- (GND) del convertidor DC-DC MP2307 y su terminal de salida con el terminal D1 la ESP8266 Wemos D1 Mini.
- El terminal "D7" de la ESP8266 Wemos D1 Mini se conecta a un led indicador.

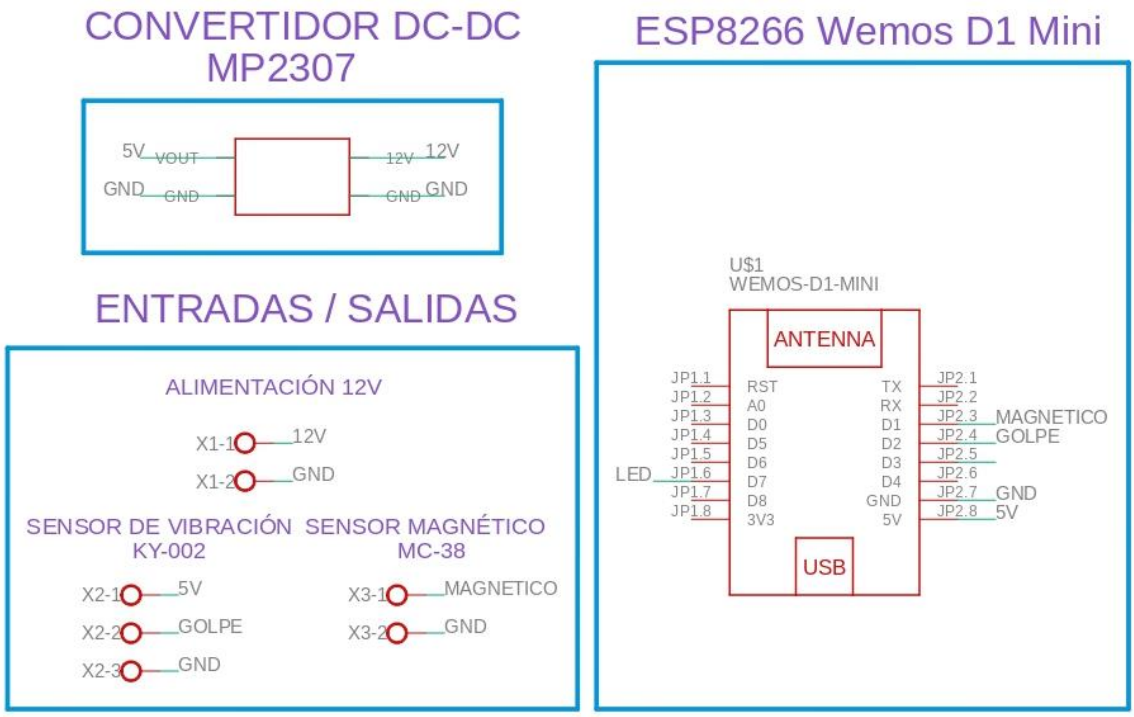


Ilustración 21-3: Módulo de adquisición de datos 3

Realizado por: Chafla, Hernán, 2022

Como lo muestra la *Ilustración 22-3,* se realizó el diseño de dicho circuito en PCB para la posterior construcción física del módulo de adquisición de datos 3 para el sistema de alarma.

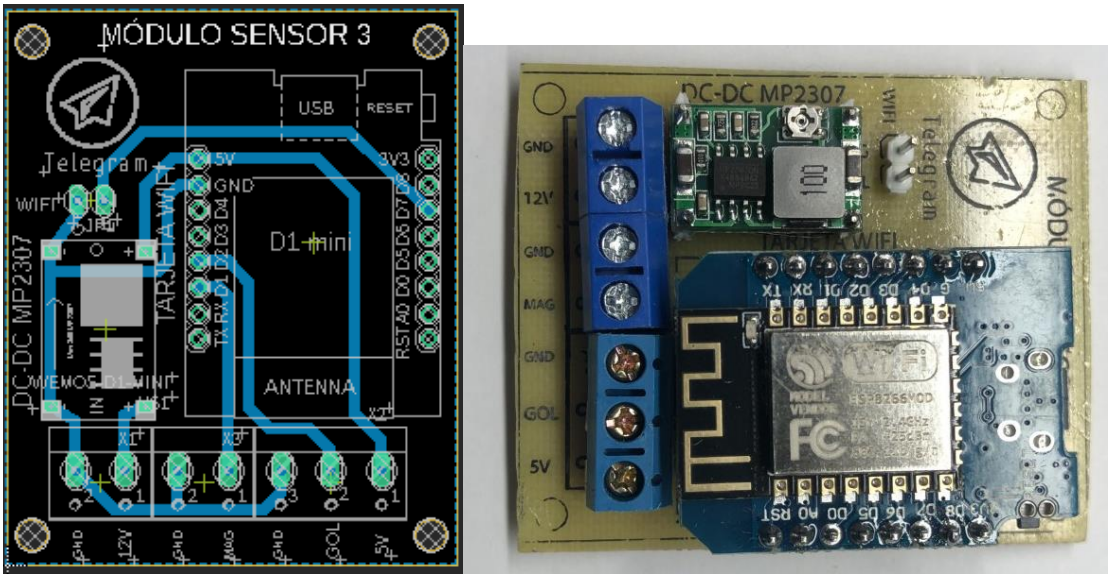


Ilustración 22-3: PCB y construcción del módulo de adquisición de datos 3

Realizado por: Chafla, Hernán, 2022

c) Módulo de adquisición de datos 4

Está compuesto por una tarjeta de desarrollo ESP8266 Wemos D1 Mini, un convertidor DC-DC MP2307, un sensor de movimiento DSC LC-100-PI y un sensor de vibración KY-002 como se muestra en la *Ilustración 23-3.*

- La salida +12VCC y GND de la fuente de alimentación UHPPOTE se encuentra conectados a los terminales de entrada IN+ (12V) y IN- (GND) del convertidor DC-DC MP2307, respectivamente. El terminal de salida de dicho convertidor OUT+ se conecta al terminal (5V) de la ESP8266 Wemos D1 Mini, y el terminal OUT- del mismo convertidor se conecta a los todos los terminales GND.
- El sensor de vibración KY-002, con alimentación 5V, conecta su terminal S (golpe) con el terminal D2 de la ESP8266 Wemos D1 Mini.
- El sensor de movimiento DSC LC-100-PI, con alimentación 12V, conecta su terminal NC (señal) con el terminal D1 de la ESP8266 Wemos D1 Mini.
- El terminal "D7" de la ESP8266 Wemos D1 Mini se conecta a un led indicador.

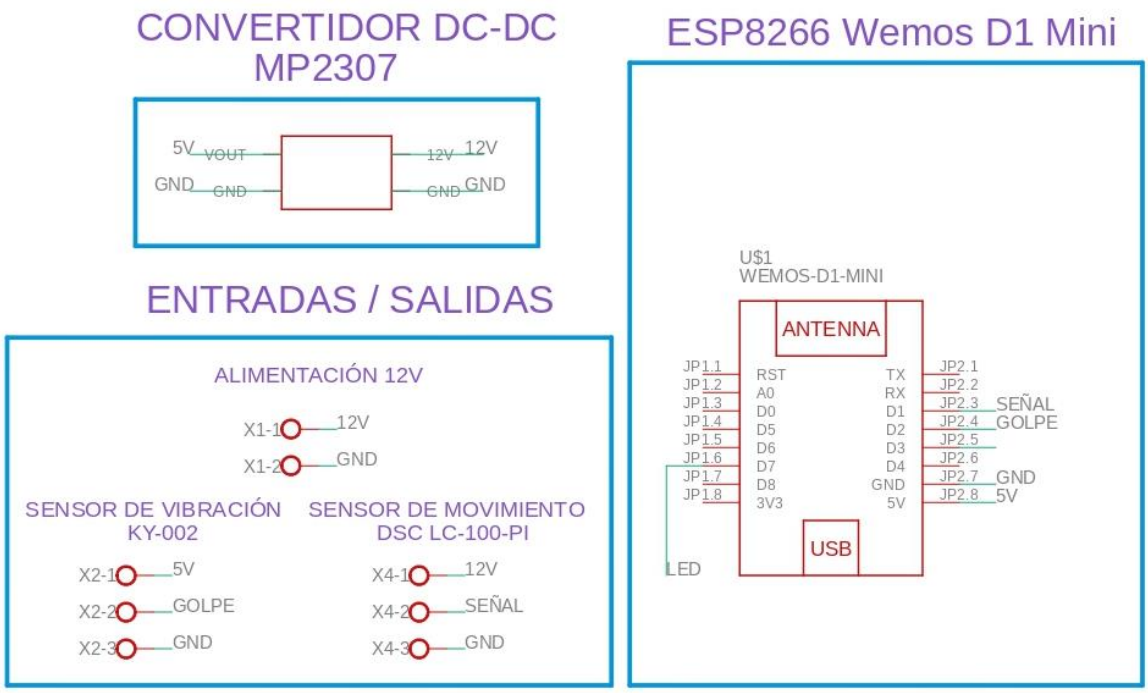


Ilustración 23-3: Módulo de adquisición de datos 4

Realizado por: Chafla, Hemán, 2022

Como lo muestra la *Ilustración 24-3*, se realizó el diseño de dicho circuito en PCB para la posterior construcción física del módulo de adquisición de datos 4 para el sistema de alarma.

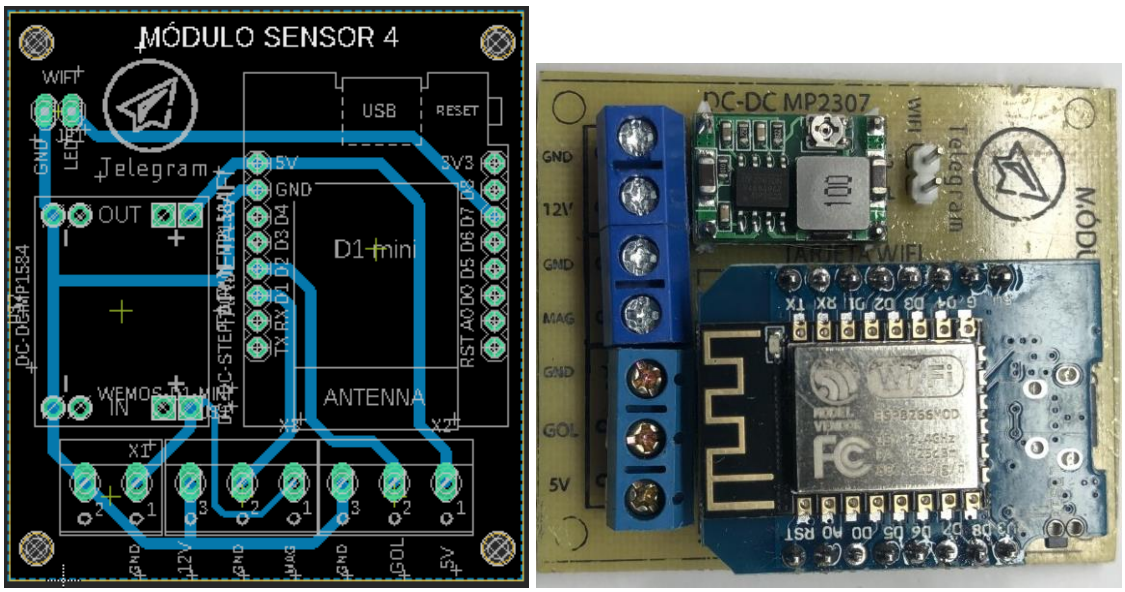


Ilustración 24-3: PCB y construcción del módulo de adquisición de datos 4

Realizado por: Chafla, Hernán, 2022

3.5.3. Esquema de conexión del módulo de control y actuación

El módulo de control y actuación está compuesto por una tarjeta de desarrollo ESP8266 Wemos D1 Mini, un convertidor DC-DC MP2307, un módulo relé, un optoacoplador 4N35 y un bloque de entradas/salidas, como se muestra en la *Ilustración 25-3*.

- La salida +12VCC y GND de la fuente de alimentación UHPPOTE se encuentra conectados a los terminales de entrada IN+ (12V) y IN- (GND) del convertidor DC-DC MP2307, respectivamente. El terminal de salida de dicho convertidor OUT+ se conecta a los terminales nombrados como (5V o VCC) de todos los elementos que componen este módulo, y el terminal OUT- del mismo convertidor se conecta a los todos los terminales nombrados como GND.
- Para la apertura de la puerta se conectó un optoacoplador 4N35 de la siguiente manera: terminal 1 (ánodo) con el terminal D1 de la ESP8266 Wemos D1 Mini, terminal 2 (cátodo) con GND por medio de una resistencia de 330Ω, terminal 5 (colector) con el terminal "PUERTA" del bloque de entradas/salidas (dicho terminal "PUERTA" se conectó con el terminal PUSH de la fuente de alimentación UHPPOTE, mientras que los terminales NC y COM de la misma fuente se conectaron a los terminales IN y GND de la cerradura magnética ZE-280-5T, respectivamente), finalmente el terminal 4 del optoacoplador (emisor) se conectó con GND.
- Para la activación de la alarma audible (sirena) se conectó un relé de la siguiente forma: su terminal IN con el terminal D0 de la ESP8266 Wemos D1 Mini, mientras que sus terminales de salida NO y COM se conectan al terminal positivo (+) y negativo (-) de la alarma audible, respectivamente.
- Para el control de apertura de la puerta desde el interior de la zona asegurada (zona 2) se instaló un pulsador el cual conecta su terminal COM a GND y su terminal NO al terminal D2 de la ESP8266 Wemos D1 Mini.
- Se utilizan tres leds como indicadores, los terminales positivos del led 1, led 2 y led 3 se conecta a los terminales D5, D6 y D7 de la ESP8266 Wemos D1 Mini, respectivamente y los terminales negativos de dichos leds se conectan a tierra (GND).

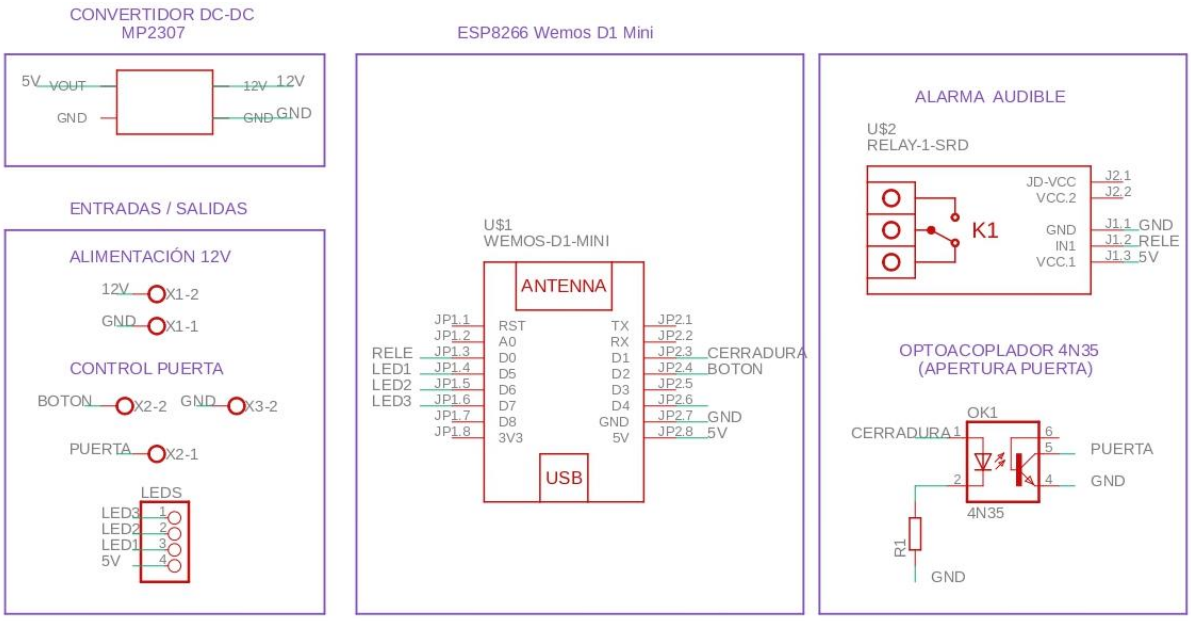


Ilustración 25-3: Esquema de conexión del módulo de control y actuación

Realizado por: Chafla, Hemán, 2022

Como lo muestra la *Ilustración 26-3,* se realizó el diseño de dicho circuito en PCB para la posterior construcción física del módulo de control y actuación.

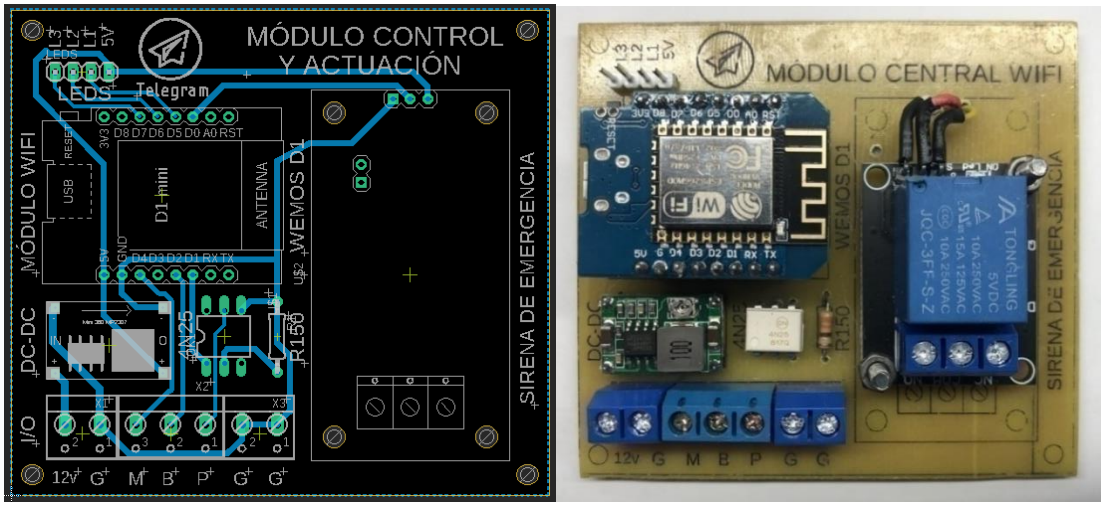


Ilustración 26-3: PCB y construcción del módulo de control y actuación

Realizado por: Chafla, Hernán, 2022

3.6. Diseño del *software* para el PSES

En el siguiente apartado se presenta el *software* de desarrollo escogido para el trabajo en colectivo con los elementos *hardware* antes mencionados, así también se desarrolla los diferentes diagramas de flujo los cuales describen el proceso realizado dentro de Arduino IDE y las

diferentes interfaces gráficas empleadas para el módulo de administración, control y visualización de la información.

3.6.1. Software de desarrollo para el PSES

A continuación, se presentan las diferentes plataformas *software* utilizadas para el desarrollo de los programas encargados de realizar el control, visualización y administración de las diferentes partes que componen el PSES.

Arduino IDE. - Integrated development environment traducido al español como Entorno de desarrollo integrado, compatible para sistemas operativos Windows, Linux o Mac. Es considerado como un programa de aplicación, pues permite la escritura de código, su edición, compilación y depuración. El tener integrado un administrador de bibliotecas permite la abstracción, lo que hace que el entorno de programación sea mucho más compacto y sencillo de utilizar (Arduino, 2018). Para la creación de los diferentes programas (scketh*s*) necesarios para el PSES la versión a utilizar es Arduino IDE 1.8.15 (Softmany, 2022).

EAGLE. – Easily Applicable Graphical Layout Editor traducido al español como Editor de diseño gráfico fácilmente aplicable, compatible para sistemas operativos Windows, Linux o Mac. Utilizado como *software* para diseño electrónico a través del cual es permitido el desarrollo de PCB (placas de circuitos impresos), facilitando el trabajo de los diseñadores mediante la amplia gama de componentes que posee, el conectar sin ningún problema diagramas esquemáticos, enrutamiento automático de PCB y amplio número de bibliotecas incluido. Para la creación de los diferentes diagramas esquemáticos y PCB necesarios para el PSES la versión a utilizar es EAGLE 9.6.2. (Autodesk, 2020).

Android Studio. – Considerado como un entorno de desarrollo integrado, compatible para sistemas operativo Windows, GNU/Linux y macOS. Utilizado para el desarrollo y creación de aplicaciones móviles para Android, pues cuenta con un editor de códigos robusto, sistema de compilación flexible basado en Gradle, emulador incorporado en el mismo *software,* compatibilidad con NDK y C++ y herramientas capaces de ayudar en la identificación de problema de rendimiento, código y compatibilidad. Para el desarrollo de la aplicación móvil utilizada en el sistema de control de acceso para la asignación y bloqueo de permisos de acceso de un solo nivel a los diferentes usuarios la versión a utilizar es Android Studio 11.0.11 (Developers, 2021).

3.6.2. Software requerido para la comunicación del PSES

Para establecer comunicación entre los módulos del PSES, es necesario la creación de una base de datos la cual actúe como intermediaria de la comunicación y la creación de un bot Telegram, tal como se menciona a continuación:

3.6.2.1. Creación de base de datos en Firebase

Es imprescindible la creación de una base de datos la cual se encargue de almacenar los estados de todos los sensores que conforman los módulos de adquisición de datos, estado de los actuadores y direcciones NFC registradas y actuales, esto para una posterior consulta solicitada por el módulo de control y actuación pues en función a ello se basa el actuar del PSES, para ello se utiliza Firebase.

Firebase es una plataforma en la nube creada por Google, la cual cuanta con dos tipos de base de datos no relacionales (NoSQL): Cloud Firestore y Realtime. Para el desarrollo del PSES se hizo uso de una base de datos en tiempo real (Realtime), donde se aprovecha de las siguientes ventajas: los datos que se almacenan son de tipo JSON "formato de intercambio de datos ligero", lo que se traduce a un formato simple de lectura, escritura y generación. La sincronización de datos con sus dispositivos emparejados es inmediata (rango de milisegundos) y automática. El acceso a su interfaz se puede dar desde un computador hasta un dispositivo móvil (Firebase, 2022).

Para su creación se sigue los siguientes pasos: Dirigirse a la página oficial de Firebase, seleccionamos "Ir a la consola", agregar nuevo proyecto, agregamos un nombre de proyecto, confirmamos el uso de Firebase mediante la selección del *check*, habilitamos Google Analytics mediante el *slider* de confirmación, configuramos Google Analytics y seleccionamos "crear proyecto", finalmente seleccionamos y creamos una base de datos en tiempo real y dentro de ella se asignan los nombres y valores de las variables a utilizar, para más detalles véase el Anexo H.

3.6.2.2. Creación de bot Telegram

Para la comunicación entre Telegram y el módulo de control y actuación es necesario tener incorporado en dicha red social un bot el cual se encargue de interactuar con el administrador del PSES para su respectiva supervisión.

Un bot Telegram es considerado como una aplicación de terceros la cual incluye y ofrece una serie de funciones dentro de la misma App de mensajería, por lo cual actúa como una aplicación de *software* cuyo propósito es interactuar con el usuario mediante el chat a través de instrucciones o comandos diferentes el uno al otro, visto de otra manera se lo considera como una herramienta para establecer una comunicación automatizada, la cual esta presta a recibir y enviar información a los dispositivos vinculados a ella (Fernández, 2020a).

Para su creación se sigue los siguientes pasos: Ingresamos a Telegram y buscamos "@BotFather", seleccionamos iniciar, ingresamos el comando "/newbot", ingresamos un nombre para el bot, escogemos un nombre de usuario único para el bot (en este apartado se genera un token indispensable para establecer comunicación con las ESP8266 Wemos D1 mini), reenviamos el último mensaje de respuesta de "@BotFather" al chat de cualquier otro bot del cual se desee copiar sus funciones, finalmente se establece parámetros de seguridad al bot creado, para más detalles véase el Anexo I.

3.6.3. Programas software del PSES

A continuación, se presentan los diferentes programas *software* correspondientes a los módulos de adquisición de datos y al módulo de control y actuación, se detalla también una descripción para los diagramas de flujo que los componen.

3.6.3.1. Programa software del módulo de adquisición de datos

Está conformado por dos partes, la primera la constituye el programa *software* para la adquisición de datos orientado al control de acceso y la segunda el programa *software* para la adquisición de datos orientado al sistema de alarma, por lo cual se tiene:

A) Programa software del módulo de adquisición de datos orientado al control de acceso

La *Ilustración 27-3* representa el diagrama de flujo el cual describe el proceso para la adquisición de datos orientado al control de acceso (módulo 1), el cual se lo describe de la siguiente manera:

Inicialización

- Se definen las siguientes librerías:
  ESP8266WiFi.h. - Habilita acceso y funcionalidades de la red (Arduino, 2022).

WiFiClient.h. - Para enviar solicitudes de conexión a servidores web (Aprendiendo Arduino, 2018).

FirebaseESP8266.h. - Para la comunicación con la base de datos (Mancilla, 2021).

DFRobotDFPlayerMini.h. - Para el funcionamiento del módulo DFPlayer mini MP3 (Electroallweb, 2020).

PN532_I2C.h. - Para el funcionamiento del módulo RFID/NFC PN532 (Xukyo, 2021).

- Se declaran las variables globales que serán utilizadas.
- Declaración de terminales de entrada para su conexión con el sensor magnético 1 y terminales de salida para su conexión a dos indicadores led y un buzzer.
- Inicialización del módulo NFC a través de la habilitación de sus terminales de comunicación SCL y SDA.
- Inicialización del módulo DFPlayer mini MP3 a través de la habilitación de sus terminales de comunicación RX y TX.
- Establecimiento de parámetros para la comunicación con Firebase mediante el llamado a su anfitrión y su respectiva autenticación.
- Activación del led indicador 1, como muestra que la tarjeta de desarrollo se encuentra encendida.
- Inicialización y conexión de la ESP8266 Wemos D1 mini a internet.

Ciclo de repetición

- Se pregunta si la ESP8266 Wemos D1 mini no está conectada a internet, de ser así se realiza un nuevo intento de conexión, caso contrario se procede a la lectura de datos NFC.
- Se pregunta si la lectura NFC actual es diferente a la anterior, de ser así envía el dato leído a Firebase para su correspondiente registro, caso contrario consulta las direcciones NFC registradas en la base de datos (Firebase).
- Se pregunta si la lectura NFC actual es igual a una dirección registrada en la base de datos, de ser así el módulo MP3 reproduce un sonido de bienvenida, se enciende un indicador led 2 y se cambia el estado de la variable "cerradura" creada en la base de datos a "ON".
- Si la lectura NFC realizada no es igual a una dirección registrada se pregunta si la App solicita un nuevo registro de usuario, de ser así envía la dirección del nuevo usuario a la base de datos para su posterior registro.
- Si la App no solicita un nuevo registro de usuario se pregunta si la lectura NFC actual es igual a una dirección bloqueada, de ser así el módulo MP3 reproduce un sonido de "bloqueo", caso contrario el módulo MP3 reproduce un sonido de "usuario inexistente".

- Se lee el estado del sensor magnético, posterior a esto se pregunta si el sensor magnético se activó, si cumple, se envía el estado de dicho sensor a la base de datos (Firebase) para su posterior registro, caso contrario regresa al inicio del ciclo de repetición.

El programa realizado en Arduino IDE 1.8.15 se encuentra adjunto en el Anexo J.

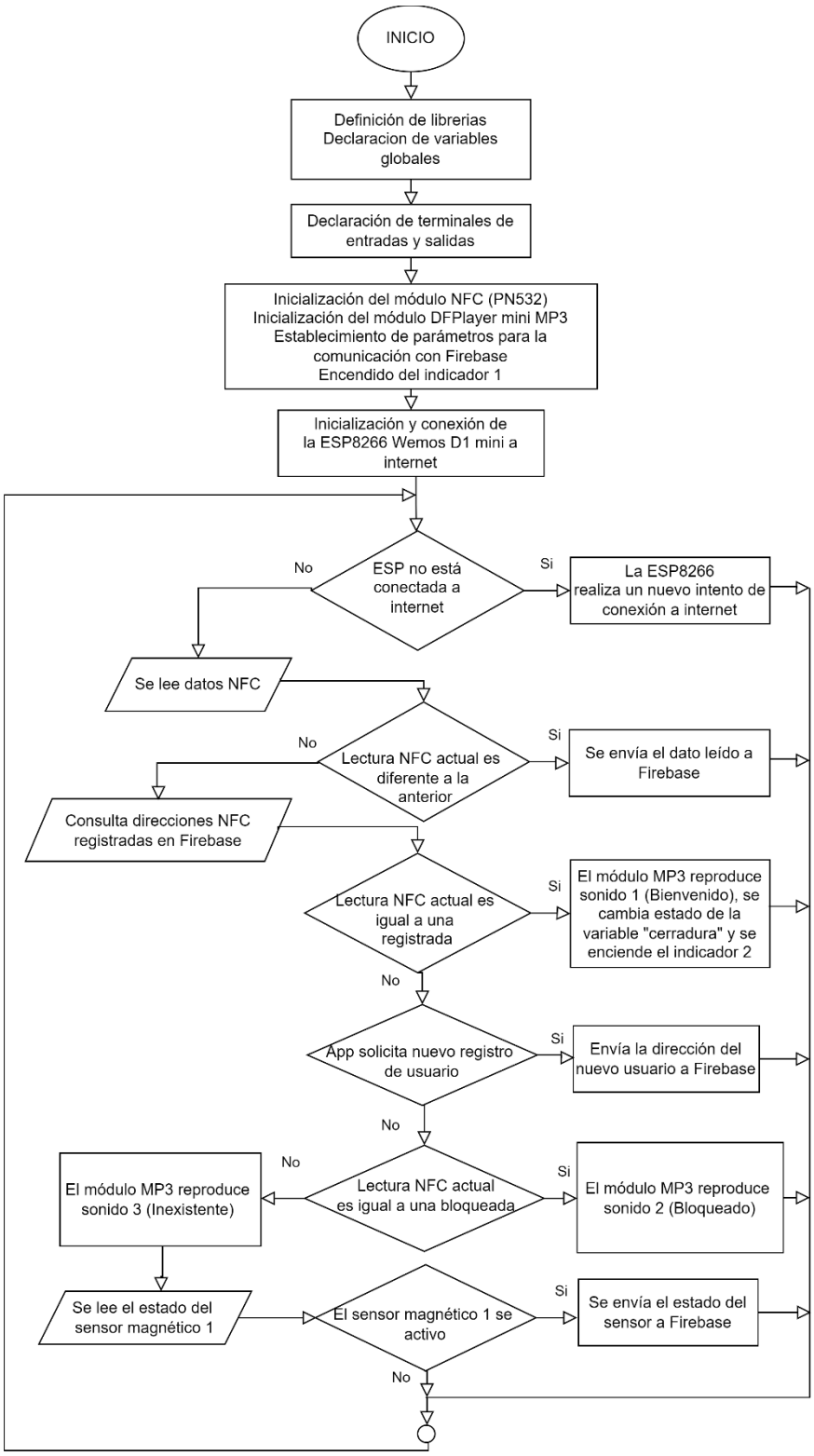


Ilustración 27-3: Diagrama de flujo del módulo de adquisición de datos orientado al control de acceso

Realizado por: Chafla, Hernán, 2022

B) Programas software para la adquisición de datos orientado al sistema de alarma

Se conforma por los siguientes tres ítems:

1) Programa software para el módulo de adquisición de datos 2

La *Ilustración 28-3* representa el diagrama de flujo el cual describe el proceso del módulo de adquisición de datos 2 orientado al sistema de alarma, el cual se lo describe de la siguiente manera:

Inicialización

- Se definen las siguientes librerías:

  ESP8266WiFi.h. - Habilita acceso y funcionalidades de la red (Arduino, 2022).

  WiFiClient.h. - Para enviar solicitudes de conexión a servidores web (Aprendiendo Arduino, 2018).

  FirebaseESP8266.h. - Para la comunicación con la base de datos (Mancilla, 2021).
- Se declaran las variables globales que serán utilizadas.
- Declaración de terminal de entrada para su conexión con el sensor de movimiento 1 y salidas para la activación de los dos indicadores led.
- Establecimiento de parámetros para la comunicación con Firebase mediante el llamado a su anfitrión y su respectiva autenticación.
- Activación del led indicador 1, como muestra que la tarjeta de desarrollo se encuentra encendida.
- Inicialización y conexión de la ESP8266 Wemos D1 mini a internet.

Ciclo de repetición

- Se pregunta si la ESP8266 Wemos D1 mini está conectada a internet, de ser así enciende el led indicador 2, notifica a Telegram que el módulo se encuentra listo y después se procede a la siguiente comparación, caso contrario realiza un nuevo intento de conexión a internet.
- Se pregunta si el sistema de alarma esta activado, de ser así procede a la lectura del estado del sensor de movimiento 1.
- Se pregunta si el sensor de movimiento 1 se activó, si lo está, se envía el estado de dicho sensor a la base de datos (Firebase) para su correspondiente registro, caso contrario regresa al inicio del ciclo de repetición.

El programa realizado en Arduino IDE 1.8.15 se encuentra adjunto en el Anexo K.

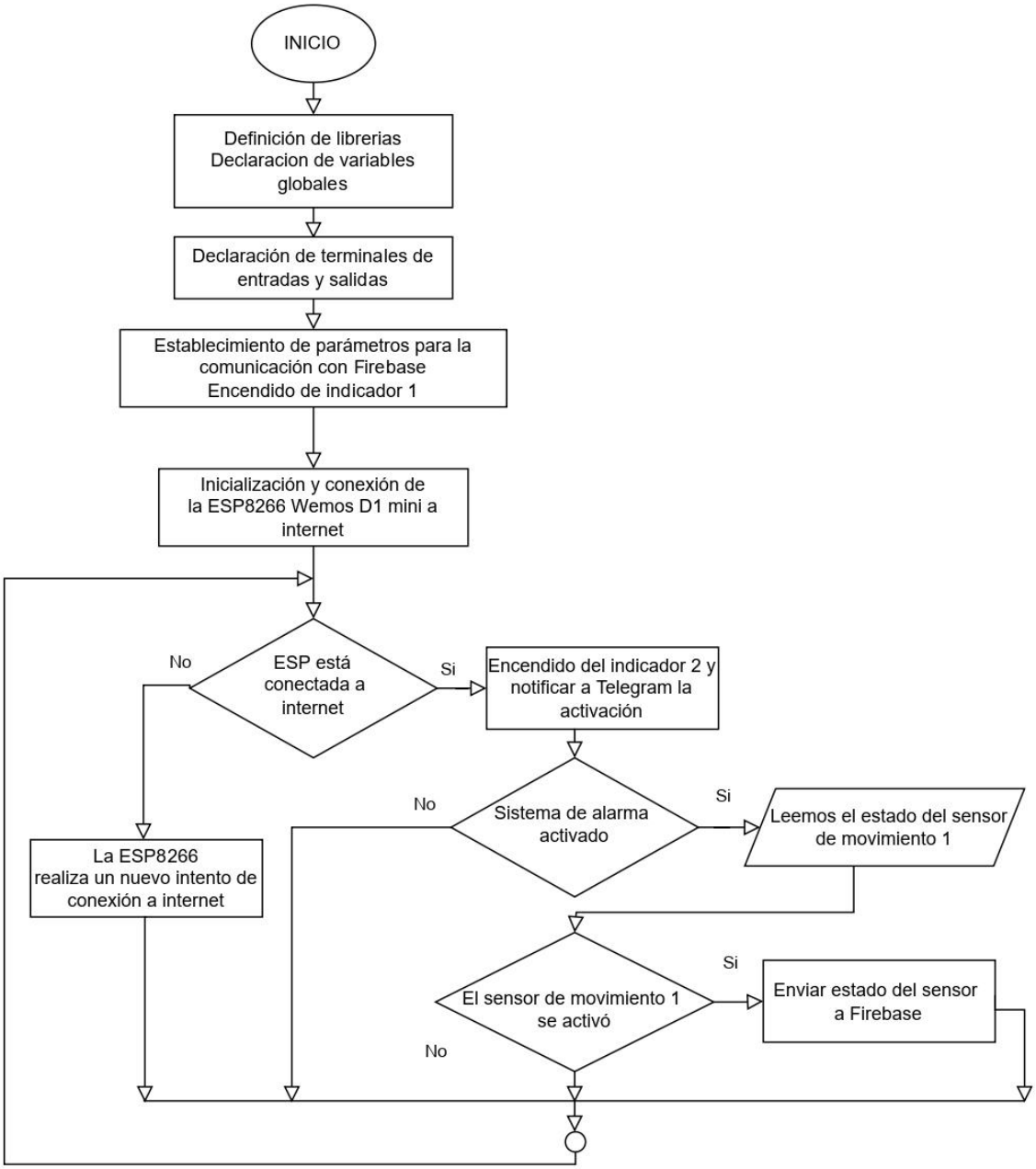


Ilustración 28-3: Diagrama de flujo para el módulo de adquisición de datos 2

Realizado por: Chafla, Hernán, 2022

2) Programa software para el módulo de adquisición de datos 3

La *Ilustración 29-3* representa el diagrama de flujo el cual describe el proceso del módulo de adquisición de datos 3 orientado al sistema de alarma, el cual se lo describe de la siguiente manera:

Inicialización

- Se definen las siguientes librerías:

ESP8266WiFi.h. - Habilita acceso y funcionalidades de la red (Arduino, 2022).

WiFiClient.h. - Para enviar solicitudes de conexión a servidores web (Aprendiendo Arduino, 2018).

FirebaseESP8266.h. - Para la comunicación con la base de datos (Mancilla, 2021).

- Se declaran las variables globales que serán utilizadas.
- Declaración de terminal de entrada para su conexión con el sensor de vibración 1 y el sensor magnético 2 y terminales de salida para su conexión con los dos indicadores led.
- Establecimiento de parámetros para la comunicación con Firebase mediante el llamado a su anfitrión y su respectiva autenticación.
- Activación del led indicador 1, como muestra que la tarjeta de desarrollo se encuentra encendida.
- Inicialización y conexión de la ESP8266 Wemos D1 mini a internet.

Ciclo de repetición

- Se pregunta si la ESP8266 Wemos D1 mini está conectada a internet, de ser así enciende el led indicador 2, notifica a Telegram que el módulo se encuentra listo y después se procede a la siguiente comparación, caso contrario realiza un nuevo intento de conexión a internet.
- Se pregunta si el sistema de alarma esta activado, de ser así procede a la lectura del estado del sensor de vibración 1 y magnético 2.
- Se pregunta si el sensor de vibración o si el sensor magnético se encuentra activado**,** si cumple con cualquiera de estas condiciones, se envía el estado de dichos sensores a la base de datos (Firebase) para su posterior registro, caso contrario regresa al inicio del ciclo de repetición.

El programa realizado en Arduino IDE 1.8.15 se encuentra adjunto en el Anexo L.

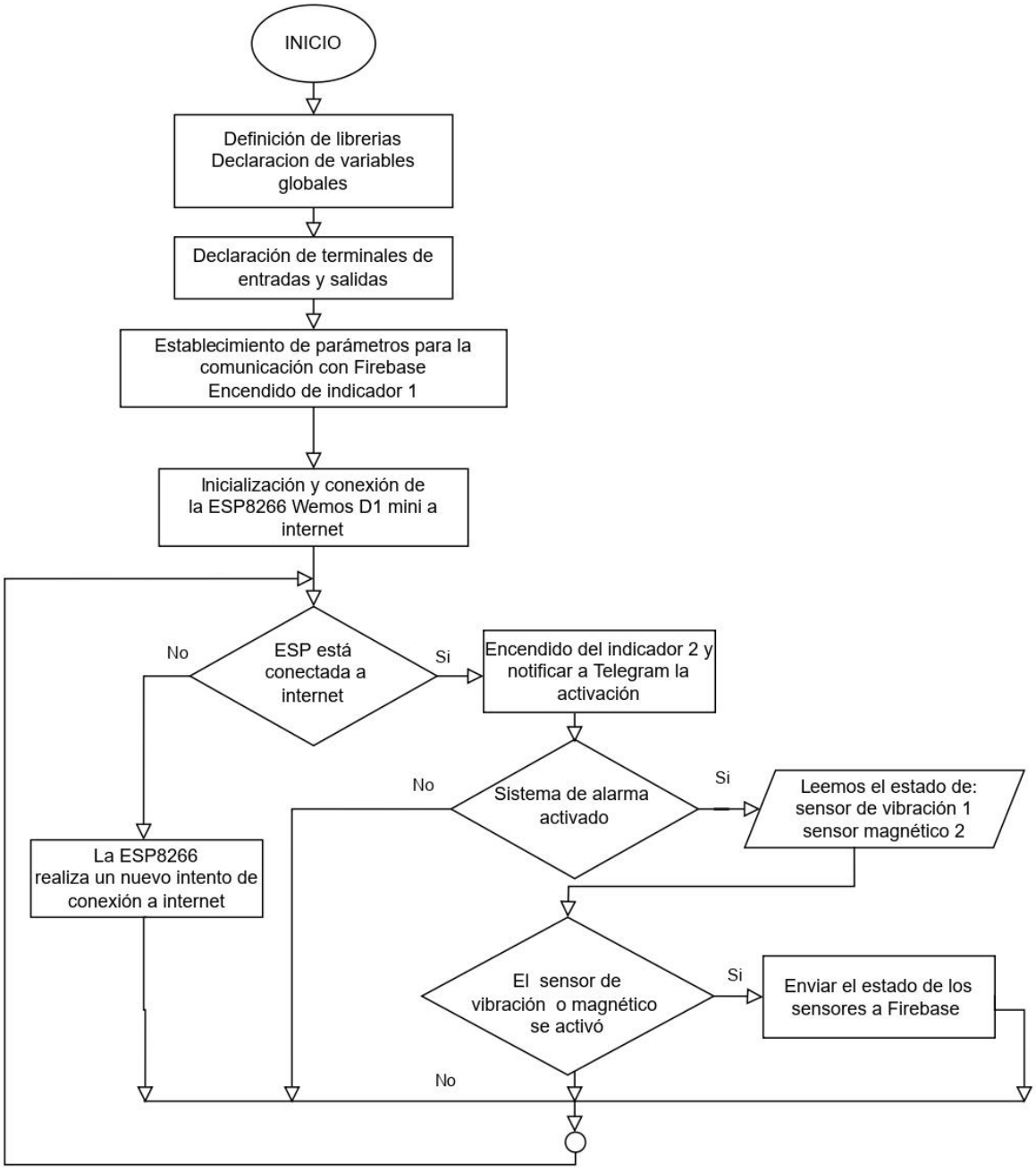


Ilustración 29-3: Diagrama de flujo para el módulo de adquisición de datos 3

Realizado por: Chafla, Hernán, 2022

3) Programa software para el módulo de adquisición de datos 4

La *Ilustración 30-3* representa el diagrama de flujo el cual describe el proceso del módulo de adquisición de datos 4 orientado al sistema de alarma, el cual se lo describe de la siguiente manera:

Inicialización

- Se definen las siguientes librerías:

  ESP8266WiFi.h. - Habilita acceso y funcionalidades de la red (Arduino, 2022).

  WiFiClient.h. - Para enviar solicitudes de conexión a servidores web (Aprendiendo Arduino, 2018).

  FirebaseESP8266.h. - Para la comunicación con la base de datos (Mancilla, 2021).
- Se declaran las variables globales que serán utilizadas.
- Declaración de terminales de entrada para su conexión con el sensor de vibración 2 y el sensor de movimiento 2 y terminales de salida para su conexión con los 2 indicadores led.
- Establecimiento de parámetros para la comunicación con Firebase mediante el llamado a su anfitrión y su respectiva autenticación.
- Activación del led indicador 1, como muestra que la tarjeta de desarrollo se encuentra encendida.
- Inicialización y conexión de la ESP8266 Wemos D1 mini a internet.

Ciclo de repetición

- Se pregunta si la ESP8266 Wemos D1 mini está conectada a internet, de ser así enciende el led indicador 2, notifica a Telegram que el módulo se encuentra listo y después se procede a la siguiente comparación, caso contrario realiza un nuevo intento de conexión a internet.
- Se pregunta si el sistema de alarma esta activado, de ser así procede a la lectura del estado del sensor de vibración 2 y sensor de movimiento 2.
- Se pregunta si el sensor de vibración 2 o si el sensor de movimiento 2 se activaron, si cumple con cualquiera de estas condiciones, se envía el estado de dichos sensores a la base de datos (Firebase) para su posterior registro, caso contrario regresa al inicio del ciclo de repetición.

El programa realizado en Arduino IDE 1.8.15 se encuentra adjunto en el Anexo M.

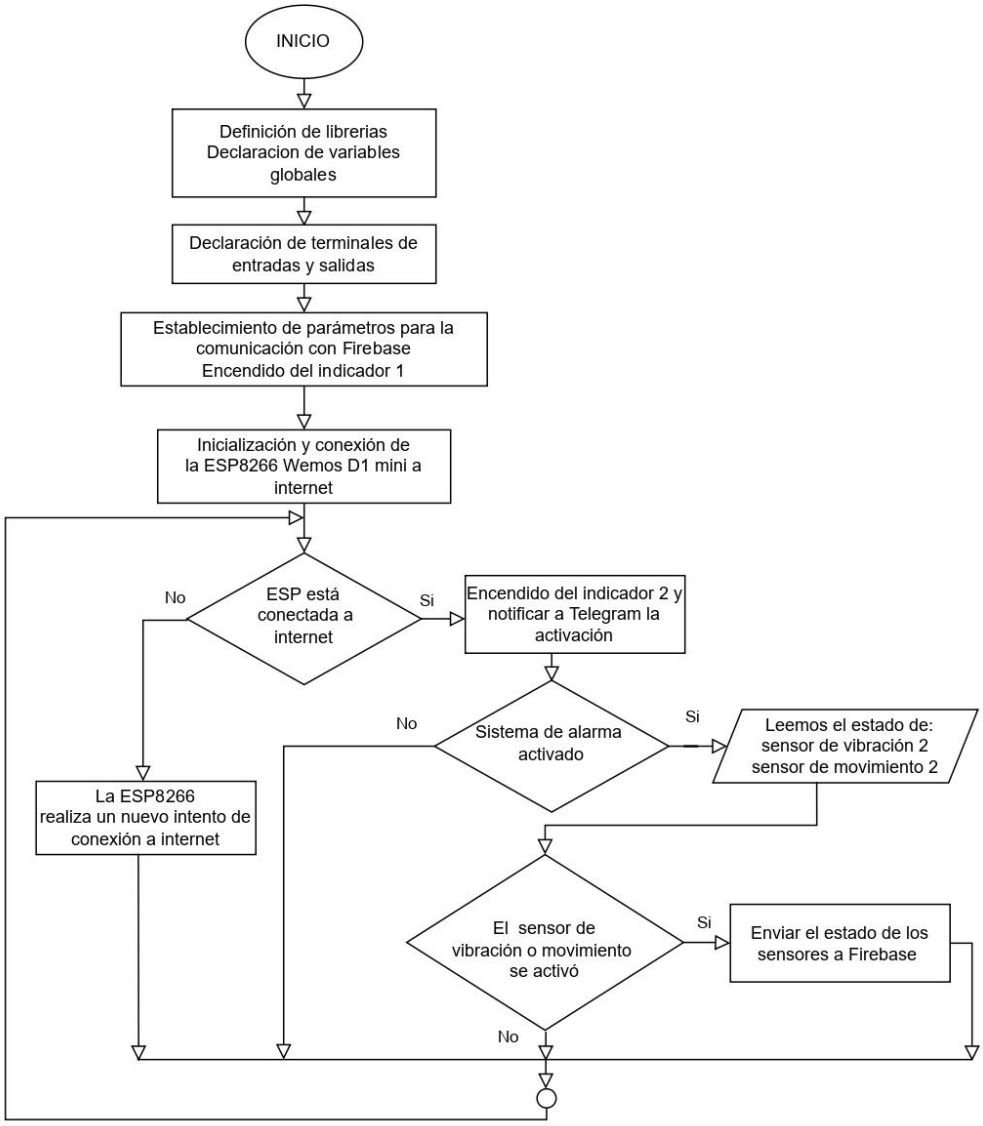


Ilustración 30-3: Diagrama de flujo para el módulo de adquisición de datos 4

Realizado por: Chafla, Hernán, 2022

3.6.3.2. Programas software del módulo de control y actuación

La *Ilustración 31-3* representa el diagrama de flujo el cual describe el proceso para el módulo de control y actuación, el programa se lo describe de la siguiente manera:

Inicialización

- Se definen las siguientes librerías:

  ESP8266WiFi.h. - Habilita acceso y funcionalidades de la red (Arduino, 2022).

  WiFiClient.h. - Para enviar solicitudes de conexión a servidores web (Aprendiendo Arduino, 2018).

FirebaseESP8266.h. - Para la comunicación con la base de datos (Mancilla, 2021).

CTBot.h. - Para la utilización e interacción con bots de Telegram (Arduino, 2022a).

- Se declaran las variables globales que serán utilizadas.
- Se declaran los terminales de salidas para su posterior conexión con la alarma audible, cerradura magnética y tres indicadores led. Y terminales de entrada para su conexión con el botón.
- Establecimiento de parámetros para la comunicación con Firebase mediante el llamado a su anfitrión y su respectiva autenticación.
- Establecimiento de parámetros para la comunicación con Telegram mediante el llamado al bot creado, la interacción con dicho bot se lo realiza a través del ingreso de un nombre y su token respectivo.
- Inicialización y conexión de la ESP8266 Wemos D1 mini a internet.

Ciclo de repetición

- Se pregunta si la ESP8266 Wemos D1 mini está conectada a internet, de ser así procede a recibir datos de Telegram, caso contrario realiza un nuevo intento de conexión a internet.
- Se recibe datos desde Telegram, posterior a ello se pregunta si se recibió la orden de activar el sistema de alarma desde Telegram, de ser así se consulta a Firebase los estados de los sensores.
- Se pregunta si existe algún cambio de los estados de los sensores consultados, de ser así se envía un mensaje de alerta a Telegram y dentro del establecimiento se enciente el elemento actuador "alarma audible".
- Si desde Telegram no se recibió la orden de activar el sistema de alarma, se pregunta ahora, si se solicita la activación del elemento actuador "alarma audible", de ser así se lo enciende, caso contrario se procede a su inactivación.
- Se pregunta si el estado de la variable "cerradura" creada en la base de datos se encuentra en estado "ON", de ser así abre la puerta y enciende el led indicador 1.
- Si el estado de la variable "cerradura" creada en la base de datos no está en "ON", se pregunta si se solicita acceso a la misma zona mediante un comando enviado desde Telegram, de ser así procede a la activación de la cerradura magnética para la apertura de la puerta y el encendido del led indicador 2.
- En el caso de que no se solicite acceso a la zona 2 mediante petición de Telegram, se pregunta si se solicita acceso a partir de pulsar el botón, de ser así procede a la activación de la cerradura magnética para la apertura de la puerta y el encendido del led indicador 3, caso contrario regresa al inicio del ciclo de repetición.

El programa realizado en Arduino IDE 1.8.15 se encuentra adjunto en el Anexo N.

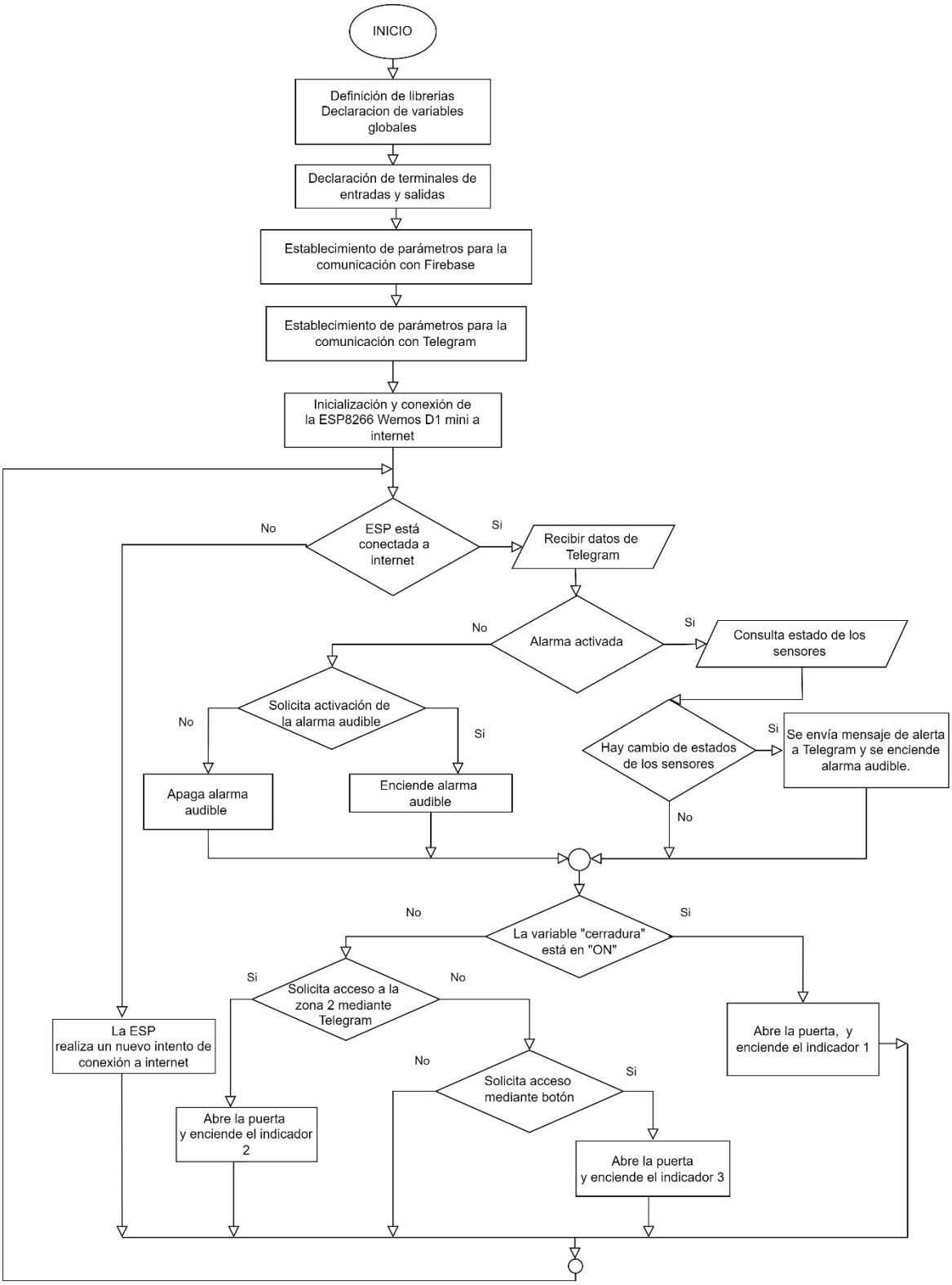


Ilustración 31-3: Diagrama de flujo del módulo de control y actuación

Realizado por: Chafla, Hernán, 2022

3.7. Interfaces gráficas del módulo de administración, control y visualización de la información

Lo compone un dispositivo móvil (smartphone), el cual contiene dos interfaces gráficas: la primera corresponde a la interfaz de Telegram, quien actúa como herramienta de control y visualización de la información y la segunda a la interfaz de la aplicación móvil orientada al control de acceso, actuando como herramienta de administración y visualización de la información.

3.7.1. Interfaz de control y visualización de la información -Telegram

Actúa como herramienta de control y visualización de la información, pues a través de ella le es permitido al usuario visualizar mediante un chat grupal de Telegram los mensajes de alerta de alarma correspondientes a las zonas del establecimiento, o los mensajes pertenecientes al historial de acceso de la zona 2.

Por medio de esta primera interfaz nos es posible realizar el control del sistema de alarma. Los integrantes que conforman el grupo de Telegram son selección del administrador, y tendrán control sobre el PSES mediante el envió de instrucciones o comandos en forma de mensajes de texto. La *Ilustración 32-3* muestra un ejemplo de mensajes de pruebas enviados por el PSES a la interfaz de Telegram.

Ilustración 32-3: Mensajes del PSES enviados a Telegram

Realizado por: Chafla, Hernán, 2022

3.7.2. Software para el dispositivo móvil

El PSES cuenta con una aplicación para dispositivos móviles Android orientada al control de acceso, desarrollada en el software Android Studio 11.0.11, cuyo objetivo es ser utilizada como herramienta de administración y visualización, pues por medio de ella se observa y se gestiona el proceso de otorgamiento o prohibición de los permisos de acceso de un solo nivel correspondientes a los diferentes usuarios. La información respecto a la programación realizada para el desarrollo de la aplicación se muestra en el Anexo O. La aplicación móvil cuenta con una interfaz intuitiva para el usuario y está constituida por las siguientes ventanas:

La *Ilustración 33-3* presenta el menú principal de la App móvil, a través del cual el administrador puede solicitar la lista de usuarios registrados en la base de datos por medio del botón "Iniciar Sesión" una vez se haya ingresado las credenciales de correo electrónico y contraseña, o puede añadir un nuevo usuario por medio del botón "Regístrate".

Ilustración 33-3: Ventana principal de la aplicación móvil

Realizado por: Chafla, Hernán, 2022

La *Ilustración 34-3* presenta los menús utilizados para el registro de un nuevo usuario dentro de la base de datos. Una vez ingresada la información correspondiente en los cuatro campos de texto del primer menú se hace una solicitud a la base de datos para un nuevo registro, posteriormente en el segundo menú se agrega la información personal del usuario y por medio del botón

"Obtener" se genera la dirección única de la tarjeta o smartphone que solicita el registro de su dirección NFC. Finalmente, mediante el botón "Actualizar datos" se guarda y actualiza la base de datos con la nueva información.

Ilustración 34-3: Ventanas para el registro de un nuevo usuario NFC

Realizado por: Chafla, Hernán, 2022

La *Ilustración 35-3* representa las ventanas en donde se muestra la lista de usuarios registrados una vez se haya ingresado las credenciales de inicio de sesión (*Ilustración 33-3*). Mediante la selección de cualquier usuario de la lista se produce su bloqueo, significando la no autorización de su ingreso a la zona protegida.

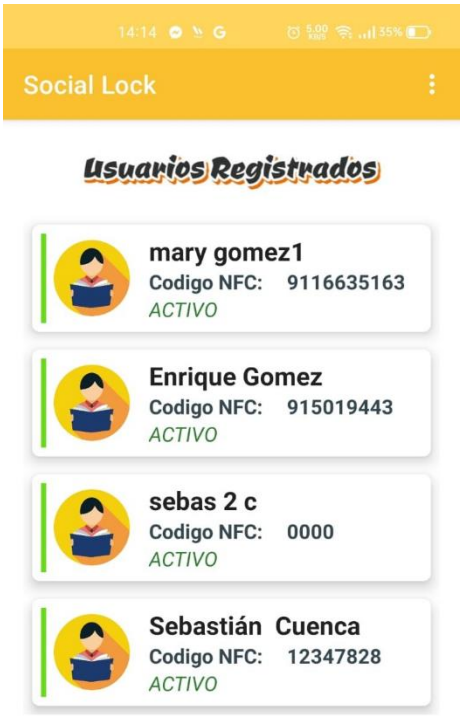


Ilustración 35-3: Ventana con usuarios registrados en Firebase

Realizado por: Chafla, Hemán, 2022

3.8. Diseño estructural del prototipo

Está conformado por dos partes: la carcasa que cubre el módulo de adquisición de datos orientado al control de acceso (módulo 1) y la carcasa que cubre el módulo de adquisición de datos orientado al sistema de alarma (módulo 2, 3 y 4), tal como se muestra a continuación:

3.8.1. Estructura para el módulo de adquisición de datos orientado al control de acceso

La *Ilustración 36-3* muestra el diseño de la estructura correspondiente a este literal, realizado en SolidWorks 2020 SP1.0 para su posterior construcción física utilizando impresión 3D, tomando como material de impresión el termoplástico PLA (ácido poliláctico) pues es un material flexible, fácil de manejar, inodoro, manipulable post-impresión, y resistente.

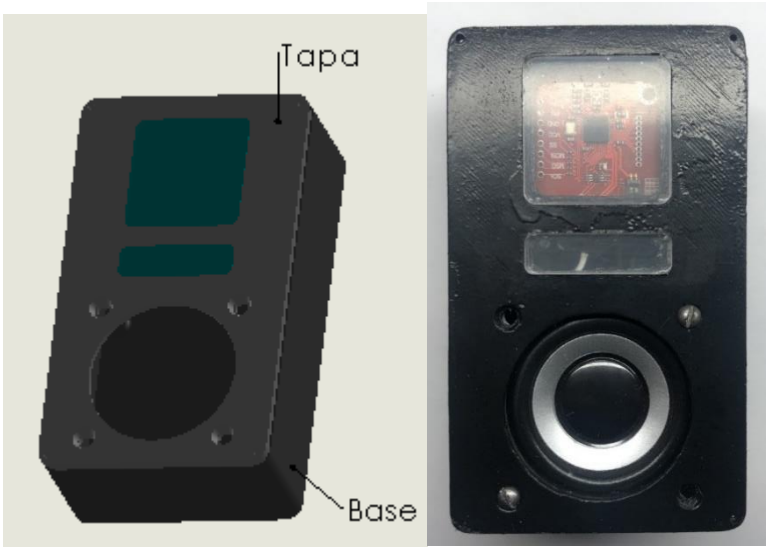


Ilustración 36-3: Estructura para el módulo de adquisición de datos 1

Realizado por: Chafla, Hernán, 2022

La *Ilustración 37-3* muestra las partes del plano más importantes pertenecientes a la estructura para el módulo de adquisición de datos 1, para ver el plano completo dirigirse al Anexo K.

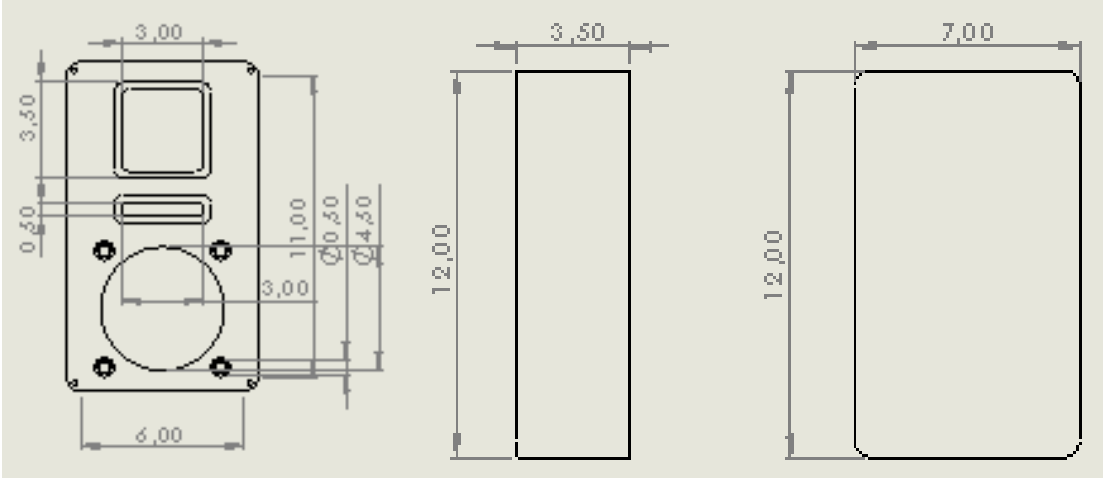


Ilustración 37-3: Parte del plano estructural del módulo de adquisición de datos 1

Realizado por: Chafla, Hernán, 2022

La *Tabla 10-3* resume las medidas más importantes expresadas en centímetros pertenecientes a la estructura del módulo de adquisición de datos 1.

Tabla 10-3: Medidas más importantes para la estructura del módulo de adquisición de datos 1

Ítem	Medida
Alto	12 cm
Ancho	7 cm
Profundidad	3.5 cm
Dimensión para lectura NFC	3.5X3.5 cm

Realizado por: Chafla, Hernán, 2022

3.8.2. Estructura para el módulo de adquisición de datos orientado al sistema de alarma

La *Ilustración 38-3* muestra el diseño de la estructura correspondiente para los módulos de adquisición de datos 2, 3 y 4 por individual, realizado en SolidWorks 2020 SP1.0 para su posterior construcción física utilizando impresión 3D, tomando como material de impresión el termoplástico PLA (ácido poliláctico) pues es un material flexible, fácil de manejar, inodoro, manipulable post-impresión, y resistente.

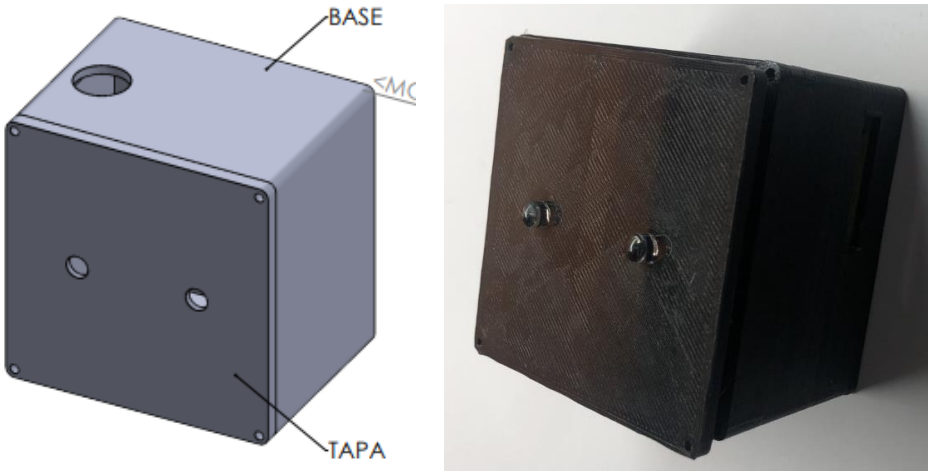


Ilustración 38-3: Estructura para los módulo de adquisición de datos 2, 3 y 4

Realizado por: Chafla, Hernán, 2022

La *Ilustración 39-3* muestra las partes del plano más importantes pertenecientes a la estructura para los módulos de adquisición de datos 2, 3 y 4 para ver el plano completo dirigirse al Anexo L.

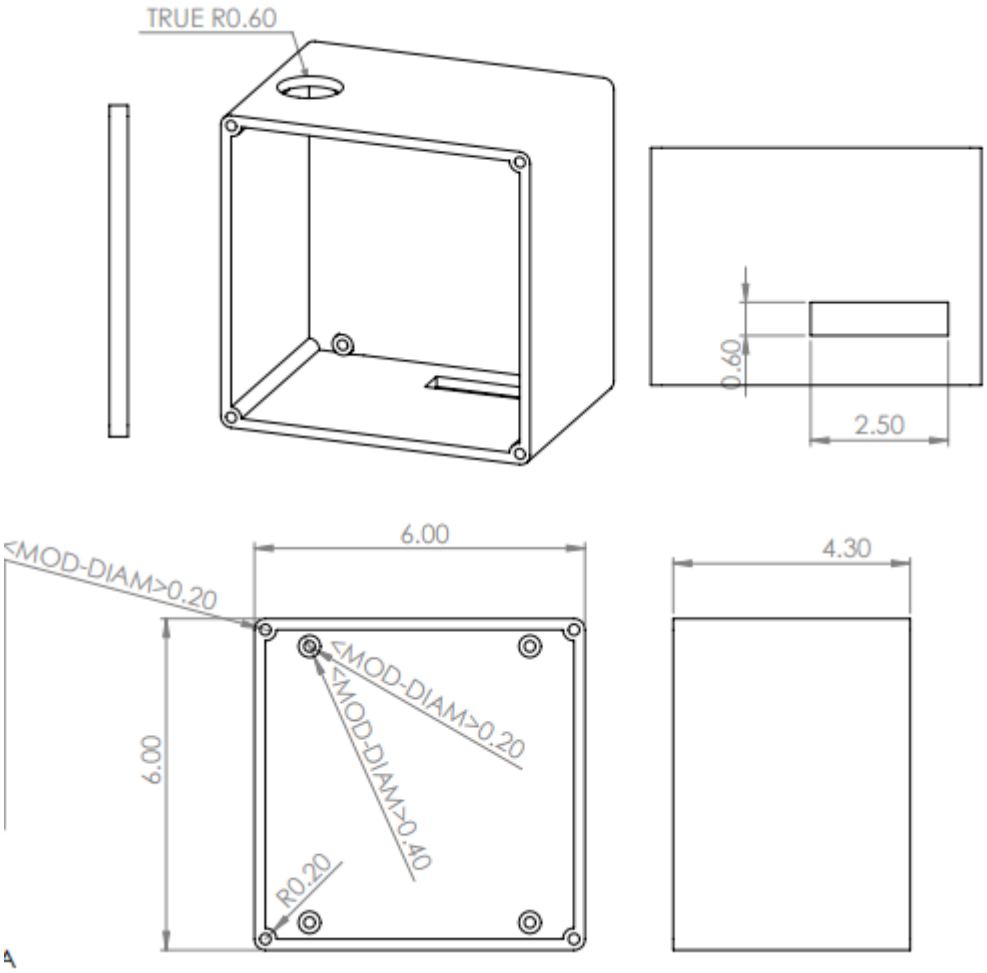


Ilustración 39-3: Parte del plano estructural de los módulo de adquisición de datos 2, 3 y 4

Realizado por: Chafla, Hernán, 2022

La *Tabla 11-3* resume las medidas más importantes expresadas en centímetros pertenecientes a la estructura del módulo de adquisición de datos 2, 3 y 4.

Tabla 11-3: Medidas más importantes para la estructura del módulo de adquisición de datos 2, 3 y 4

Ítem	Medida
Alto	6 cm
Ancho	6 cm
Profundidad	4.3 cm
Diámetro del orificio para la unión tapa-base	0.2 cm
Radio de orificio para pin de carga	0.6 cm

Realizado por: Chafla, Hernán, 2022

CAPÍTULO IV

4. MARCO DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En el siguiente capítulo se realiza diferentes tipos de pruebas orientados a los módulos que componen la concepción de la arquitectura general del PSES, tal como, módulos de adquisición de datos, módulo de control- actuación, módulo de administración- control y visualización de la información. Se los puede observar en la *Ilustración 1-4.*

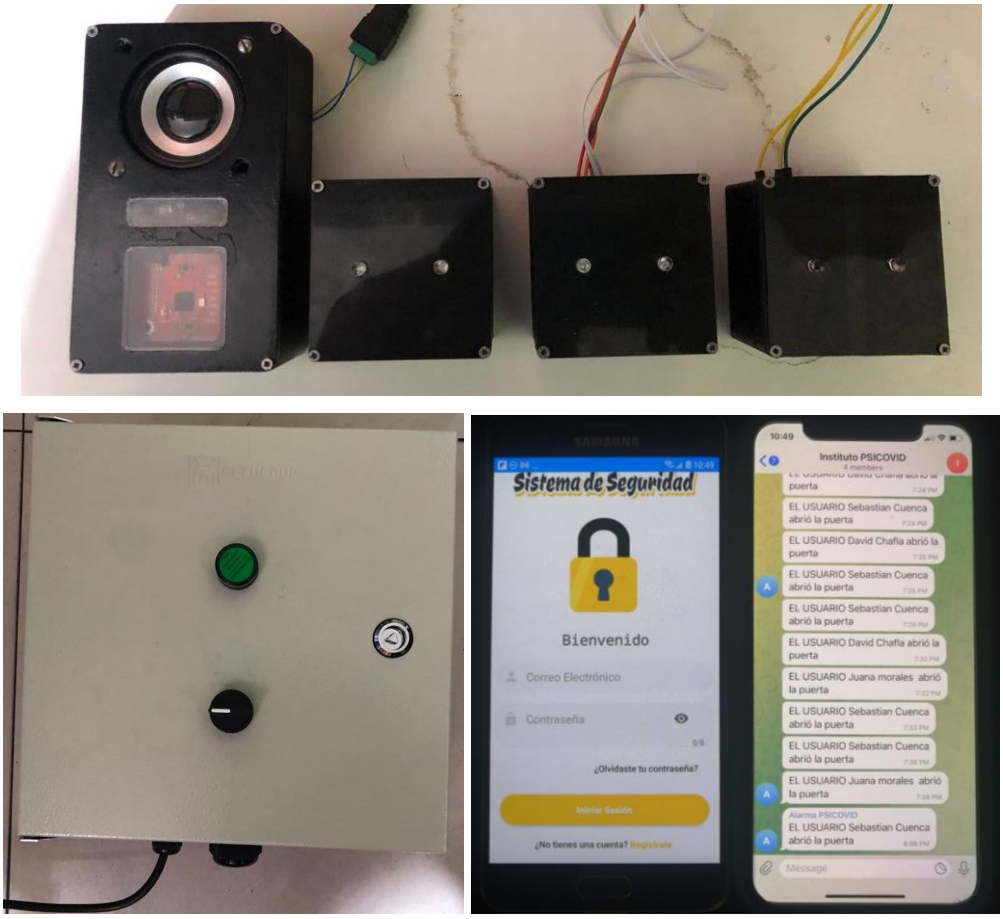


Ilustración 1-4: Módulos que componen la arquitectura general del PSES

Realizado por: Chafla, Hernán, 2022

Tomando en cuenta el primer criterio planteado por varios autores (Fisher, Stoeckel and Laing, 1951, p. 59) para definir un tamaño de muestra, el cual menciona que se tiene que considerar los recursos disponibles para la recolección de estas, pues con base a ello se establece el máximo de muestras. Por lo que la recomendación que comparten es tomar siempre el mayor número, pues la lógica indica que mientras más grande sea este valor menor será el error conseguido.

Así también los autores plantean que el tamaño de muestra tiene que ser el suficiente como para probar si estadísticamente las diferencias entre proporciones son significativas. Por lo que, con base al criterio antes mencionado, dentro de este capítulo, tomando en cuenta el tiempo disponible para la elaboración del proyecto de integración curricular, para las validaciones por medio del cálculo de error relativo se considera tomar un total de 30 muestras recogidas en un lapso de 3 días.

Para encontrar el valor correspondiente a este error primero se necesita hallar el error absoluto, pues a través de él se cuantifica la desviación existente en una medida en términos absolutos respecto al supuesto valor "verdadero", por lo que el resultado obtenido determina la sensibilidad del aparato medido (Posadas, 2022, p. 4).

Sin embargo, en esta ocasión es necesario encontrar la importancia relativa de la medida perteneciente a la desviación hallada mediante el error absoluto, pues se desconoce el error característico de los elementos de sensado, para ello se hace uso del error relativo, utilizado como criterio de calidad.

Para la interpretación de los resultados obtenidos mediante el cálculo del (Er), dos autores opinan lo siguiente: El valor obtenido al hallar el Er se lo puede clasificar en tres rangos, Er menor a 1%, entre el 5% al 10% y superior al 10%, asignando un resultado experimental bueno, aceptable y poco confiable, respectivamente (Santo and Lecumberry, 2005, pp. 14–15).

Por otro lado, según Senar (1999, p. 54), se considera a la repetibilidad como una medida estadística perteneciente a la consistencia entre un grupo de medidas repetidas bajo un mismo escenario. El número de muestras tomadas para las pruebas de repetibilidad dentro de este capítulo es de 10, en consideración a la cifra utilizada por otros autores en sus trabajos de investigación (Portuondo and Portuondo, 2010, p. 120).

Posteriormente se calcula el coeficiente de variación (CV), el cual para varios investigadores es considerado como indicador de confiabilidad y calidad a la que está sujeto el experimento (Ruiz 2010, p. 149–150). Producto a ello muchos científicos lo utilizan para rechazar o aceptar la validez del experimento al que se lo aplique (Bowman, 2001, pp. 137–139). El CV toma valores relativos en el rango de 0 y 1, aun que dichos valores también pueden ser representados porcentualmente.

Para su interpretación, si el CV es próximo a 0 (0%) quiere decir que la muestra es compacta por lo que existe poca variabilidad de datos, si el CV supera a 0.3 (30%) se traduce a que su media es

poco representativa, finalmente, si el valor del CV tiende a 1 (100%) significa que los datos son muy dispersos por lo que su media pierde confiabilidad (Requena, 2016).

La evidencia correspondiente a las pruebas realizadas para este capítulo se encuentra adjuntas en el Anexo R.

4.1. Caracterización de los módulos de adquisición de datos

En este apartado se realizan pruebas orientadas a los elementos de sensado que conforman a los módulos de adquisición de datos 1, 2, 3 y 4, con el objetivo de determinar la sensibilidad por medio del cálculo y obtención del error absoluto, calidad a través del error relativo (Er), confiabilidad y calidad del elemento al que se le aplique la prueba mediante el coeficiente de variación (CV) tras realizar un análisis de repetibilidad.

4.1.1. Validación de los elementos de sensado del módulo de adquisición de datos 1

A continuación, se realizan pruebas para la validación de los elementos de sensado que componen el módulo de adquisición de datos 1.

Validación del sensor magnético 1 MC-38. - Se lo realiza mediante pruebas orientadas a las características técnicas que presenta este elemento de sensado, con el objetivo de determinar el criterio de calidad de dicho sensor magnético 1.

Para ello, se establece el valor perteneciente a la distancia mínima de activación del sensor según su hoja de datos y con ayuda de un equipo patrón, en este caso un flexómetro, se toman muestras correspondientes a las distancias de disparo, véase en la *Tabla 1-4*, finalmente se calcula el error absoluto y error relativo para un posterior análisis de resultados.

Tabla 1-4: Validación del sensor magnético 1 MC-38

N.º de muestra	Distancia de activación mínima			
	Valor según hoja de datos (mm)	Flexómetro (mm)	Error absoluto	Error relativo (%)
1	15	16	-1	6.25
2	15	15	0	0

3	15	16	-1	6.25
4	15	14	1	7.14
5	15	15	0	0
6	15	16	-1	6.25
7	15	16	-1	6.25
8	15	15	0	0
9	15	16	-1	6.25
10	15	16	-1	6.25
11	15	15	0	0
12	15	16	-1	6.25
13	15	14	1	7.14
14	15	15	0	0
15	15	15	0	0
16	15	16	-1	6.25
17	15	16	-1	6.25
18	15	16	-1	6.25
19	15	14	1	7.14
20	15	16	-1	6.25
21	15	16	-1	6.25
22	15	15	0	0
23	15	15	0	0
24	15	15	0	0
25	15	16	-1	6.25
26	15	16	-1	6.25
27	15	16	-1	6.25
28	15	15	0	0
29	15	14	1	7.14
30	15	15	0	0

Realizado por: Chafla, Hernán, 2022

En la *Tabla 1-4* se observa que como resultado de la validación del sensor magnético 1 MC-38 en cuanto a su distancia mínima de activación el Er máximo encontrado es de 7.14%, por lo que, según definición de autores, al encontrarse el valor en el rango de 5%<Er <10%, significa que se obtuvo un resultado experimental con criterio de calidad aceptable.

Repetibilidad de lecturas NFC para el control de acceso. – El objetivo de esta prueba es determinar la confiabilidad y calidad del módulo RFID/ NFC PN532 mediante el cálculo del coeficiente de variación (CV) tras realizar un análisis de repetibilidad.

Para ello, se toma una tarjeta NFC registrada y se procede a la lectura de ella mediante dicho módulo, considerando que cada lectura se la realiza sobre el mismo individuo y entorno, para un

registro cuantitativo una respuesta correcta del módulo se la considera como "1", caso contrario se la representa con un "0".

Posteriormente se toman dos usuarios, ambos están registrados en la base de datos, *Ilustración 2-4*, sin embargo, el primero de ellos se encuentra en estado "activo" lo que quiere decir que cuenta con permiso para el acceso a la zona protegida, mientras que el segundo usuario se encuentra en estado "inactivo" (bloqueado) por lo que el sistema deberá negar su solicitud de ingreso a la zona.

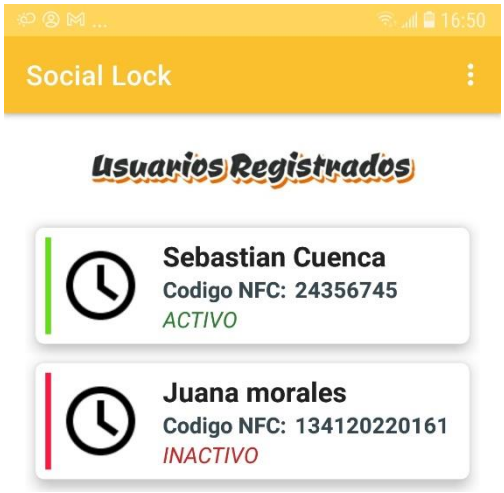


Ilustración 2-4: Usuarios registrados para el control de acceso

Realizado por: Chafla, Hernán, 2022

En la *Tabla 2-4* se observa la prueba de repetibilidad realizada para un usuario en estado activo.

Tabla 2-4: Repetibilidad de lecturas NFC para un estado activo

Número de muestra	Parámetros				
	Fecha/hora	Nombre de usuario	Código NFC	Estado (Registrado)	Respuesta en tiempo real
1	25/6/2022 14:46:00	Sebastián Cuenca	24356745	Activo	1
2	25/6/2022 14:46:10	Sebastián Cuenca	24356745	Activo	1
3	25/6/2022 14:46:20	Sebastián Cuenca	24356745	Activo	1
4	25/6/2022 14:46:30	Sebastián Cuenca	24356745	Activo	1
5	25/6/2022 14:46:40	Sebastián Cuenca	24356745	Activo	1
6	25/6/2022 14:46:50	Sebastián Cuenca	24356745	Activo	1
7	25/6/2022 14:47:00	Sebastián Cuenca	24356745	Activo	1
8	25/6/2022 14:47:10	Sebastián Cuenca	24356745	Activo	1
9	25/6/2022 14:47:20	Sebastián Cuenca	24356745	Activo	1

10	25/6/2022 14:47:30	Sebastián Cuenca	24356745	Activo	1
		Media			1
		Desviación estándar (σ)			0
		Coeficiente de variación (CV)			0%

Realizado por: Chafla, Hernán, 2022

En la *Tabla 3-4* se observa la prueba de repetibilidad realizada para un usuario en estado inactivo.

Tabla 3-4: Repetibilidad de lecturas NFC para un estado inactivo

Número de muestra	**Parámetros**				
	Fecha/hora	**Nombre de usuario**	**Código NFC**	**Estado (Registrado)**	**Respuesta en tiempo real**
1	25/6/2022 14:48:00	Juana Morales	12347828	Inactivo	1
2	25/6/2022 14:48:10	Juana Morales	12347828	Inactivo	1
3	25/6/2022 14:48:20	Juana Morales	12347828	Inactivo	1
4	25/6/2022 14:48:30	Juana Morales	12347828	Inactivo	1
5	25/6/2022 14:48:40	Juana Morales	12347828	Inactivo	1
6	25/6/2022 14:48:50	Juana Morales	12347828	Inactivo	1
7	25/6/2022 14:49:00	Juana Morales	12347828	Inactivo	1
8	25/6/2022 14:49:10	Juana Morales	12347828	Inactivo	1
9	25/6/2022 14:49:20	Juana Morales	12347828	Inactivo	1
10	25/6/2022 14:49:30	Juana Morales	12347828	Inactivo	1
		Media			1
		Desviación estándar (σ)			0
		Coeficiente de variación (CV)			0%

Realizado por: Chafla, Hernán, 2022

De la *Tabla 2-4* y la *Tabla 3-4* se obtiene un mismo resultado del coeficiente de variación CV=0%, por lo que, según definición de autores al ser el CV igual a 0% significa que se tiene muestras compactas, por lo que no existe variabilidad de datos.

Producto a ello se dice que las lecturas NFC realizadas por el módulo son lecturas estables, haciendo que el comportamiento de dicho elemento de adquisición de datos sea confiable y de calidad.

4.1.2. Validación de los elementos de sensado del módulo de adquisición de datos 2

A continuación, se realizan pruebas para la validación de los elementos de sensado que componen el módulo de adquisición de datos 2.

Validación del sensor de movimiento 1 DSC LC-100-PI. - Se lo realiza mediante pruebas orientadas a las características técnicas que presenta este elemento de sensado, con el objetivo de determinar el criterio de calidad de dicho sensor de movimiento 1, para ello, se plantean los valores pertenecientes a la distancia mínima y grados máximos de detección del sensor según su hoja de datos.

Posteriormente, se calibra de forma física el sensor a su menor distancia de detección y con ayuda de equipos patrones como el flexómetro y graduador, se toman medidas correspondientes a distancias y ángulos de disparo respectivamente, véase en la *Tabla 4-4*, finalmente se calcula el error absoluto y error relativo para un posterior análisis de resultados.

Tabla 4-4: Validación del sensor de movimiento 1 DSC LC-100-PI

N.º de muestra	Distancia de detección				Grados de detección			
	Valor calibrado (m)	Flexómetro (m)	Error absoluto	Error relativo (%)	Valor calibrado (°)	Graduador (°)	Error absoluto	Error relativo (%)
1	5	5.03	-0.03	0.6	85	83	2	2.41
2	5	5.02	-0.02	0.4	85	82	3	3.66
3	5	5.02	-0.02	0.4	85	82	3	3.66
4	5	5.03	-0.03	0.6	85	84.5	0.5	0.59
5	5	5.01	-0.01	0.2	85	84.5	0.5	0.59
6	5	4.99	0.01	0.2	85	84.5	0.5	0.59
7	5	5.01	-0.01	0.2	85	84.5	0.5	0.59
8	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
9	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
10	5	4.98	0.02	0.4	85	86.5	-1.5	1.73
11	5	5	0	0	85	84.5	0.5	0.59
12	5	5.02	-0.02	0.4	85	83	2	2.41
13	5	5.01	-0.01	0.2	85	83	2	2.41
14	5	5.02	-0.02	0.4	85	82	3	3.66
15	5	5.02	-0.02	0.4	85	82	3	3.66
16	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
17	5	5.01	-0.01	0.2	85	86.5	-1.5	1.73
18	5	5.01	-0.01	0.2	85	82	3	3.66
19	5	5.01	-0.01	0.2	85	84.5	0.5	0.59
20	5	5	0	0	85	86.5	-1.5	1.73
21	5	5.01	-0.01	0.2	85	86.5	-1.5	1.73
22	5	5.01	-0.01	0.2	85	86.5	-1.5	1.73
23	5	5	0	0	85	83	2	2.41

24	5	5.02	-0.02	0.4	85	83	2	2.41
25	5	5.01	-0.01	0.2	85	83	2	2.41
26	5	5.01	-0.01	0.2	85	84.5	0.5	0.59
27	5	4.99	0.01	0.2	85	84.5	0.5	0.59
28	5	5.02	-0.02	0.4	85	87.5	-2.5	2.86
29	5	5.02	-0.02	0.4	85	87.5	-2.5	2.86
30	5	5.01	-0.01	0.2	85	87.5	-2.5	2.86

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 4-4*, se determina que como resultado de la validación del sensor de movimiento 1 DSC LC-100-PI en cuanto a su distancia mínima de activación el Er máximo es de 0.6%, mientras en cuanto a sus grados de detección el Er máximo es de 3.66%.

Por lo que, según definición de autores, al encontrarse el primer valor en el rango de Er <1% y el segundo en 1%<Er <5%, significa que se obtuvo un resultado experimental con criterio de calidad bueno, y un resultado experimental con criterio de calidad entre bueno y aceptable, respectivamente.

4.1.3. Validación de los elementos de sensado del módulo de adquisición de datos 3

A continuación, se realizan pruebas para la validación de los elementos de sensado que componen el módulo de adquisición de datos 3.

Validación del sensor magnético 2 MC-38. - Se lo realiza mediante pruebas orientadas a las características técnicas que presenta este elemento de sensado, con el objetivo de determinar el criterio de calidad de dicho sensor magnético 2.

Para ello, se establece el valor perteneciente a la distancia mínima de activación del sensor según su hoja de datos y con ayuda de un equipo patrón, en este caso un flexómetro, se toman muestras correspondientes a las distancias de disparo, véase en la *Tabla 5-4*, finalmente se calcula el error absoluto y error relativo para un posterior análisis de resultados.

Tabla 5-4: Validación del sensor magnético 2 MC-38

N.º de muestra	**Distancia de activación mínima**			
	Valor según hoja	**Flexómetro (mm)**	**Error absoluto**	**Error relativo (%)**

	de datos (mm)			
1	15	16	-1	6.25
2	15	16	-1	6.25
3	15	16	-1	6.25
4	15	15	0	0
5	15	16	-1	6.25
6	15	16	-1	6.25
7	15	15	0	0
8	15	15	0	0
9	15	16	-1	6.25
10	15	16	-1	6.25
11	15	16	-1	6.25
12	15	16	-1	6.25
13	15	14	1	7.14
14	15	16	-1	6.25
15	15	15	0	0
16	15	16	-1	6.25
17	15	16	-1	6.25
18	15	16	-1	6.25
19	15	16	-1	6.25
20	15	16	-1	6.25
21	15	16	-1	6.25
22	15	15	0	0
23	15	16	-1	6.25
24	15	16	-1	6.25
25	15	16	-1	6.25
26	15	16	-1	6.25
27	15	16	-1	6.25
28	15	16	-1	6.25
29	15	14	1	7.14
30	15	15	0	0

Realizado por: Chafla, Hernán, 2022

En la *Tabla 5-4* se observa que como resultado de la validación del sensor magnético 2 MC-38 en cuanto a su distancia mínima de activación el Er máximo encontrado es de 7.14%, por lo que, según definición de autores, al encontrarse el valor en el rango de 5%<Er <10%, significa que se obtuvo un resultado experimental con criterio de calidad aceptable.

4.1.4. Validación de los elementos de sensado del módulo de adquisición de datos 4

A continuación, se realizan pruebas para la validación de los elementos de sensado que componen el módulo de adquisición de datos 4.

Validación del sensor de movimiento 2 DSC LC-100-PI. - Se lo realiza mediante pruebas orientadas a las características técnicas que presenta este elemento de sensado, con el objetivo de determinar el criterio de calidad de dicho sensor de movimiento 2, para ello, se plantean los valores pertenecientes a la distancia mínima y grados máximos de detección del sensor según su hoja de datos.

Posteriormente, se calibra de forma física el sensor a su menor distancia de detección y con ayuda de equipos patrones como el flexómetro y graduador, se toman medidas correspondientes a distancias y ángulos de disparo respectivamente, véase en la *Tabla 6-4*, finalmente se calcula el error absoluto y error relativo para un posterior análisis de resultados.

Tabla 6-4: Validación del sensor de movimiento 2 DSC LC-100-PI

N.º de muestra	Distancia de detección				Grados de detección			
	Valor calibrado (m)	Flexómetro (m)	Error absoluto	Error relativo (%)	Valor calibrado (°)	Graduador (°)	Error absoluto	Error relativo (%)
1	5	5.05	-0.05	0.99	85	87	-2	2.3
2	5	5.04	-0.04	0.79	85	87	-2	2.3
3	5	5.04	-0.04	0.79	85	86	-1	1.16
4	5	5.04	-0.04	0.79	85	86	-1	1.16
5	5	5.01	-0.01	0.2	85	86	-1	1.16
6	5	4.99	0.01	0.2	85	89	-4	4.49
7	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
8	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
9	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
10	5	5	0	0	85	88	-3	3.41
11	5	5	0	0	85	88	-3	3.41
12	5	5.02	-0.02	0.4	85	88	-3	3.41
13	5	5.02	-0.02	0.4	85	88	-3	3.41
14	5	5.02	-0.02	0.4	85	87	-2	2.3
15	5	5.02	-0.02	0.4	85	90	-5	5.56
16	5	5.01	-0.01	0.2	85	87	-2	2.3
17	5	5.01	-0.01	0.2	85	87	-2	2.3
18	5	5.04	-0.04	0.79	85	87	-2	2.3
19	5	5.04	-0.04	0.79	85	86	-1	1.16
20	5	5	0	0	85	86	-1	1.16

21	5	5.01	-0.01	0.2	85	86	-1	1.16
22	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
23	5	5.02	-0.02	0.4	85	86.5	-1.5	1.73
24	5	5.02	-0.02	0.4	85	88	-3	3.41
25	5	5.02	-0.02	0.4	85	88	-3	3.41
26	5	5.03	-0.03	0.6	85	88	-3	3.41
27	5	5.03	-0.03	0.6	85	87.5	-2.5	2.86
28	5	5.03	-0.03	0.6	85	87.5	-2.5	2.86
29	5	5.02	-0.02	0.4	85	87.5	-2.5	2.86
30	5	5.02	-0.02	0.4	85	88	-3	3.41

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 6-4*, se determina que como resultado de la validación del sensor de movimiento 2 DSC LC-100-PI en cuanto a su distancia mínima de activación el Er máximo es de 0.99%, mientras en cuanto a sus grados de detección el Er máximo es de 5.56%.

Por lo que, según definición de autores, al encontrarse el primer valor en el rango de Er <1% y el segundo en 5%<Er <10%, significa que se obtuvo un resultado experimental con criterio de calidad bueno, y un resultado experimental con criterio de calidad aceptable, respectivamente.

4.2. Caracterización del módulo de control y actuación

En el siguiente apartado se realiza pruebas de repetibilidad en la comunicación del módulo de control y actuación y los módulos de adquisición de datos 1, 2, 3 y 4, además se plantea pruebas orientadas a la activación de la cerradura magnética desde el interior de la zona protegida.

4.2.1. Repetibilidad en la comunicación entre el módulo de control y actuación y los módulos de adquisición de datos

Para cuantificar las muestras registradas en las pruebas correspondientes a esta sección, una correcta comunicación entre módulos tras la activación de los sensores en un primer intento se la considera como "1", caso contrario se la representa con un "0". Con esto se plantea:

Comunicación entre el módulo de control y actuación -módulo de adquisición de datos 1. - El objetivo de esta prueba es determinar la confiabilidad y calidad de la comunicación entre estos módulos mediante el cálculo del coeficiente de variación (CV) tras realizar un análisis de repetibilidad.

Para ello, se activó el sensor magnético 1, posteriormente se visualiza en la pantalla serial de Arduino la variable enviada desde el módulo de adquisición de datos 1 al módulo de control y actuación utilizando Firebase como intermediario de la comunicación, finalmente se observan los mensajes de alerta en Telegram indicando la activación del sensor, véase en la *Ilustración 3-4.*

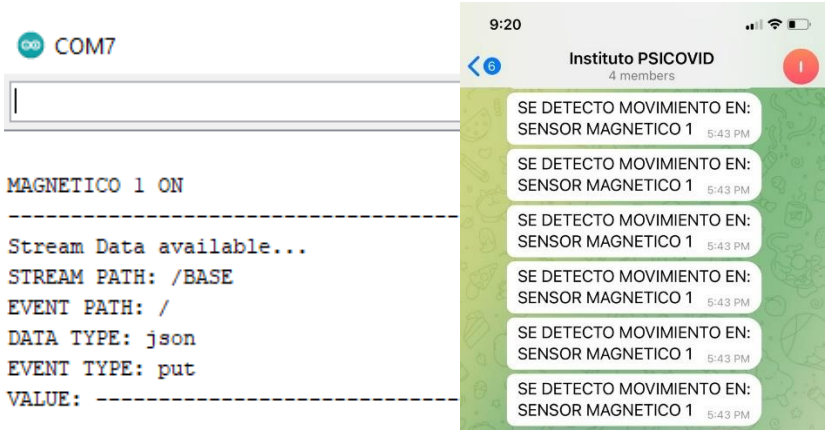


Ilustración 3-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha)

Realizado por: Chafla, Hernán, 2022

La prueba de repetibilidad realizada se observa en la *Tabla 7-4.*

Tabla 7-4: Comunicación entre el módulo de control y actuación- módulo de adquisición de datos 1

Número de muestra	Parámetros (Sensor magnético 1)		
	Fecha/hora	N.º de intento de activación	Respuesta en tiempo real
1	29/6/2022 17:43:00	1	1
2	29/6/2022 17:43:10	1	1
3	29/6/2022 17:43:20	1	1
4	29/6/2022 17:43:30	1	1
5	29/6/2022 17:43:40	1	1
6	29/6/2022 17:43:50	1	1
7	29/6/2022 17:44:00	1	1
8	29/6/2022 17:44:10	1	1
9	29/6/2022 17:44:20	1	1
10	29/6/2022 17:44:30	1	1
Media			1
Desviación estándar (σ)			0
Coeficiente de variación (CV)			0%

Realizado por: Chafla, Hernán, 2022

De la *Tabla 7-4* se obtiene un coeficiente de variación CV=0%, por lo que, según definición de autores al ser el CV igual a 0% significa que se tiene muestras compactas, por lo que no existe variabilidad de datos, teniendo así valores estables. Producto a ello se dice que la comunicación entre el módulo de adquisición de datos 1 y el módulo de control y actuación es confiable y de calidad.

Comunicación entre el módulo de control y actuación -módulo de adquisición de datos 2. – El objetivo de esta prueba es determinar la confiabilidad y calidad de la comunicación entre estos módulos mediante el cálculo del coeficiente de variación (CV) tras realizar un análisis de repetibilidad.

Para ello, se activó el sensor de movimiento 1, posteriormente se visualiza en la pantalla serial de Arduino la variable enviada desde el módulo de adquisición de datos 2 al módulo de control y actuación utilizando Firebase como intermediario de la comunicación, finalmente se observan los mensajes de alerta en Telegram indicando la activación del sensor, véase en la *Ilustración 4-4.*

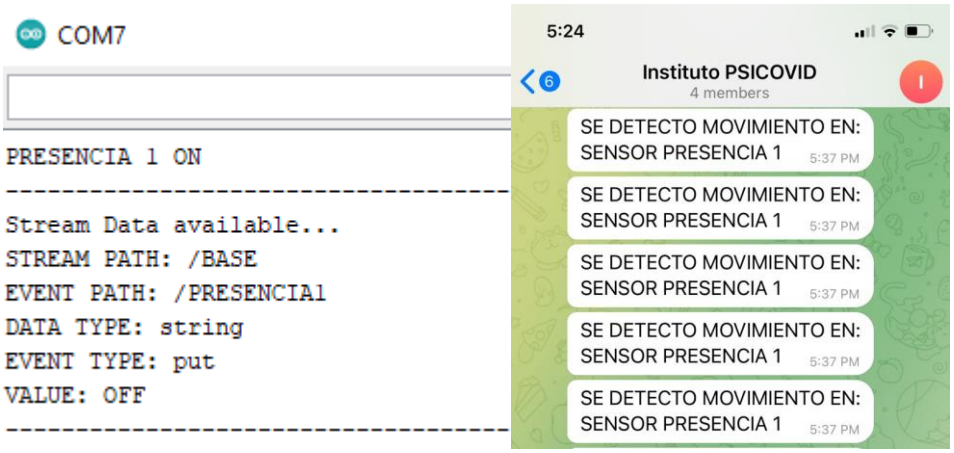


Ilustración 4-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha)

Realizado por: Chafla, Hernán, 2022

La prueba de repetibilidad realizada se observa en la *Tabla 8-4.*

Tabla 8-4: Comunicación entre el módulo de control y actuación- módulo de adquisición de datos 2

Número de muestra	Parámetros (Sensor de movimiento 1)		
	Fecha/hora	N.º de intento de activación	Respuesta en tiempo real

1	29/6/2022 17:37:06	1	1
2	29/6/2022 17:37:12	1	1
3	29/6/2022 17:37:18	1	1
4	29/6/2022 17:37:24	1	1
5	29/6/2022 17:37:30	1	1
6	29/6/2022 17:37:36	1	1
7	29/6/2022 17:37:42	1	1
8	29/6/2022 17:37:48	1	1
9	29/6/2022 17:37:54	1	1
10	29/6/2022 17:38:00	1	1
Media			1
Desviación estándar (σ)			0
Coeficiente de variación (CV)			0%

Realizado por: Chafla, Hernán, 2022

De la *Tabla 8-4* se obtiene un coeficiente de variación CV=0%, por lo que, según definición de autores al ser el CV igual a 0% significa que se tiene muestras compactas, por lo que no existe variabilidad de datos, teniendo así valores estables. Producto a ello se dice que la comunicación entre el módulo de adquisición de datos 2 y el módulo de control y actuación es confiable y de calidad.

Comunicación entre el módulo de control y actuación -módulo de adquisición de datos 3. - El objetivo de esta prueba es determinar la confiabilidad y calidad de la comunicación entre estos módulos mediante el cálculo del coeficiente de variación (CV) tras realizar un análisis de repetibilidad.

Para ello, se activó el sensor de vibración 1 y el sensor magnético 2, posteriormente se visualiza en la pantalla serial de Arduino la variable enviada desde el módulo de adquisición de datos 3 al módulo de control y actuación utilizando Firebase como intermediario de la comunicación, finalmente se observan los mensajes de alerta en Telegram indicando la activación del sensor, véase en la *Ilustración 5-4*.

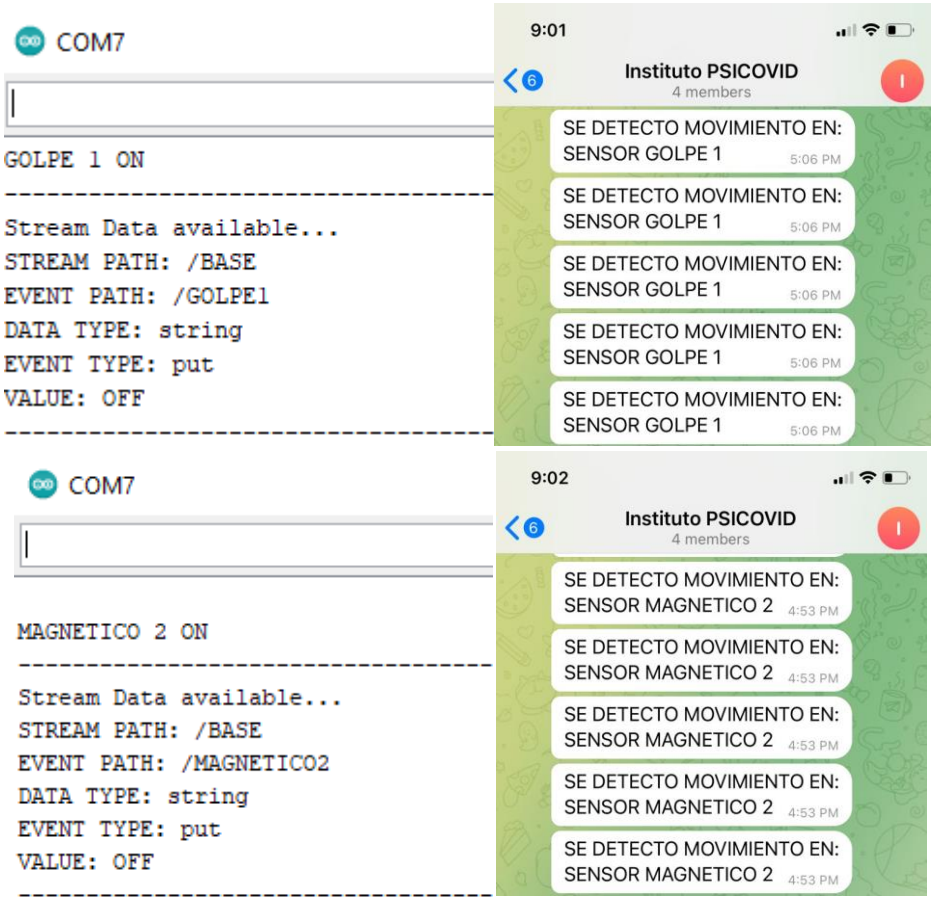


Ilustración 5-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha)

Realizado por: Chafla, Hernán, 2022

La prueba de repetibilidad realizada se observa en la *Tabla 9-4.*

Tabla 9-4: Comunicación entre el módulo de control y actuación- módulo de adquisición de datos 3

N.º de muestra	Parámetros (Sensor de vibración 1)			Parámetros (Sensor magnético 2)		
	Fecha/hora	N.º de intento de activación	Respuesta en tiempo real	Fecha/hora	N.º de intento de activación	Respuesta en tiempo real
1	29/6/2022 17:06:06	1	1	29/6/2022 16:53:00	1	1
2	29/6/2022 17:06:12	1	1	29/6/2022 16:53:06	1	1
3	29/6/2022 17:06:18	1	1	29/6/2022 16:53:12	1	1
4	29/6/2022 17:06:24	1	1	29/6/2022 16:53:18	1	1
5	29/6/2022 17:06:30	1	1	29/6/2022 16:53:24	1	1
6	29/6/2022 17:06:36	1	1	29/6/2022 16:53:30	1	1
7	29/6/2022 17:06:42	1	1	29/6/2022 16:53:36	1	1

8	29/6/2022 17:06:48	1	1	29/6/2022 16:53:42	1	1
9	29/6/2022 17:06:54	1	1	29/6/2022 16:53:48	1	1
10	29/6/2022 17:09:00	3	0	29/6/2022 16:53:54	1	1
Media			0,9			1
Desviación estándar (σ)			0,09			0
Coeficiente de variación (CV)			10%			0%

Realizado por: Chafla, Hernán, 2022

De la *Tabla 9-4* se obtiene un coeficiente de variación CV=10% a causa del sensor de vibración 1 y un CV=0% por el sensor magnético 2.

Por lo que, según definición de autores al no superar el 30% y ser próximos al 0% significa que se tiene muestras compactas, produciendo poca variabilidad de datos, teniendo así valores estables. Producto a ello se dice que la comunicación entre el módulo de adquisición de datos 3 y el módulo de control y actuación es confiable y de calidad.

Comunicación entre el módulo de control y actuación -módulo de adquisición de datos 4. - El objetivo de esta prueba es determinar la confiabilidad y calidad de la comunicación entre estos módulos mediante el cálculo del coeficiente de variación (CV) tras realizar un análisis de repetibilidad.

Para ello, se activó el sensor de movimiento 2 y el sensor de vibración 2, posteriormente se visualiza en la pantalla serial de Arduino la variable enviada desde el módulo de adquisición de datos 4 al módulo de control y actuación utilizando Firebase como intermediario de la comunicación, finalmente se observan los mensajes de alerta en Telegram indicando la activación de los sensores, véase en la *Ilustración 6-4.*

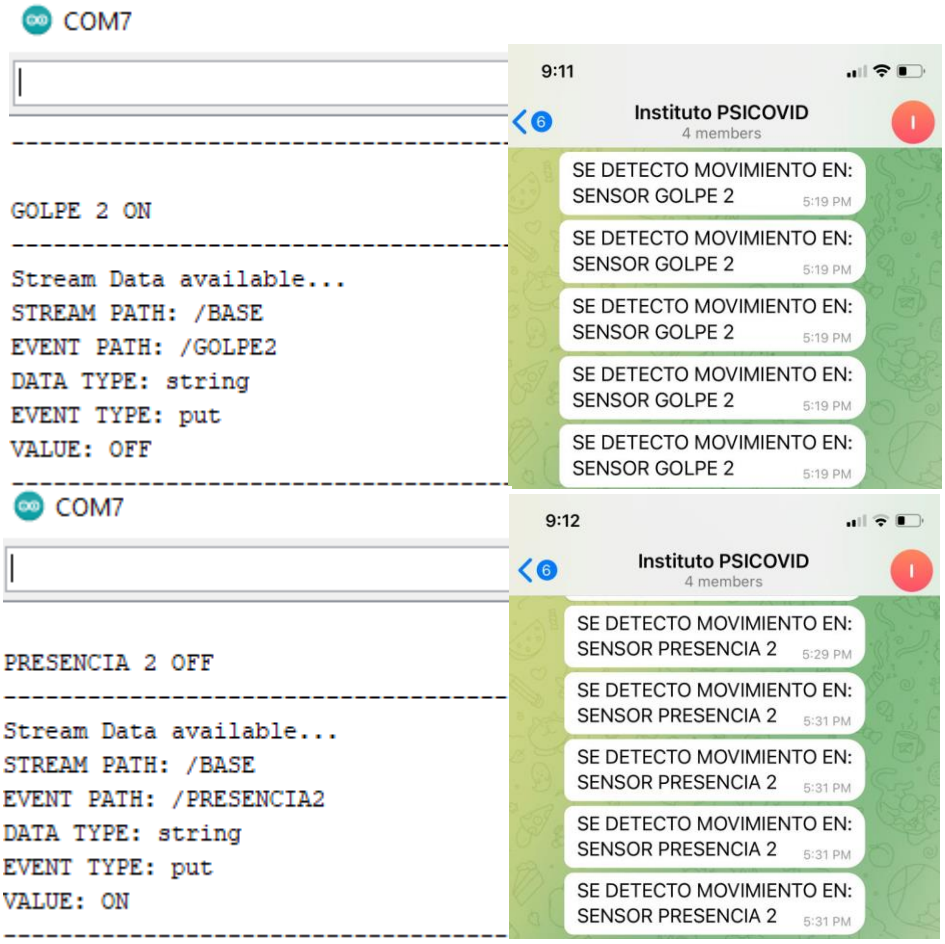


Ilustración 6-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha)

Realizado por: Chafla, Hernán, 2022

La prueba de repetibilidad realizada se observa en la *Tabla 10-4.*

Tabla 10-4: Comunicación entre el módulo de control y actuación-módulo de adquisición de datos 4

N.º de muestra	Parámetros (Sensor de vibración 2)			Parámetros (Sensor de movimiento 2)		
	Fecha/hora	N.º de intento de activación	Respuesta en tiempo real	Fecha/hora	N.º de intento de activación	Respuesta en tiempo real
1	29/6/2022 17:19:10	1	1	29/6/2022 17:31:00	1	1
2	29/6/2022 17:19:20	1	1	29/6/2022 17:31:06	1	1
3	29/6/2022 17:19:30	1	1	29/6/2022 17:31:12	1	1
4	29/6/2022 17:19:40	1	1	29/6/2022 17:31:18	1	1
5	29/6/2022 17:19:50	2	0	29/6/2022 17:31:24	1	1
6	29/6/2022 17:20:00	1	1	29/6/2022 17:31:30	1	1

7	29/6/2022 17:20:10	1	1	29/6/2022 17:31:36	1	1
8	29/6/2022 17:20:20	1	1	29/6/2022 17:31:42	1	1
9	29/6/2022 17:20:30	1	1	29/6/2022 17:31:48	1	1
10	29/6/2022 17:20:40	1	1	29/6/2022 17:31:54	1	1
Media			0,9			1
Desviación estándar (σ)			0,09			0
Coeficiente de variación (CV)			10%			0%

Realizado por: Chafla, Hernán, 2022

De la *Tabla 10-4* se obtiene un coeficiente de variación CV=10% a causa del sensor de vibración 2 y un CV=0% por el sensor de movimiento 2.

Por lo que, según definición de autores al no superar el 30% y ser próximos al 0% significa que se tiene muestras compactas, produciendo poca variabilidad de datos, teniendo así valores estables. Producto a ello se dice que la comunicación entre el módulo de adquisición de datos 4 y el módulo de control y actuación es confiable y de calidad.

4.2.2. Repetibilidad en la activación de la cerradura magnética

El objetivo de esta prueba es determinar la confiabilidad y calidad de la activación de la cerradura magnética desde el interior de la zona 2 mediante el cálculo del coeficiente de variación (CV) tras realizar un análisis de repetibilidad.

Para ello, se presiona el botón ligado al módulo de control y actuación el cual da apertura a la zona protegida, posteriormente se visualiza en la pantalla serial de Arduino del módulo de control y actuación el cambio de estado de la variable correspondiente, véase *Ilustración 7-4.*

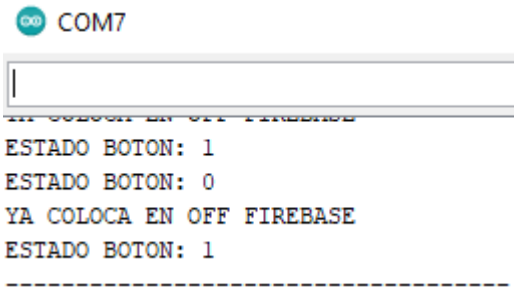


Ilustración 7-4: Pantalla serial de arduino del módulo de control y actuación

Realizado por: Chafla, Hernán, 2022

Como se observa en la *Tabla 11-4*, para cuantificar las muestras registradas en esta prueba, una correcta activación de la cerradura magnética tras presionar el botón en un primer intento se lo considera como "1", caso contrario se lo representa con un "0".

Tabla 11-4: Repetibilidad en la activación de la cerradura magnética

N.º de muestra	Parámetros (botón)		
	Fecha/hora	N.º de intento de activación	Respuesta en tiempo real
1	29/6/2022 17:53:49	1	1
2	29/6/2022 17:53:56	1	1
3	29/6/2022 17:54:03	1	1
4	29/6/2022 17:54:10	1	1
5	29/6/2022 17:54:17	1	1
6	29/6/2022 17:54:24	1	1
7	29/6/2022 17:54:31	1	1
8	29/6/2022 17:54:38	1	1
9	29/6/2022 17:54:45	1	1
10	29/6/2022 17:54:52	1	1
Media			1
Desviación estándar (σ)			0
Coeficiente de variación (CV)			0%

Realizado por: Chafla, Hernán, 2022

De la *Tabla 11-4* se obtiene un coeficiente de variación CV=0%, por lo que, según definición de autores al ser el CV igual a 0% significa que se tiene muestras compactas, por lo que no existe variabilidad de datos, teniendo así valores estables. Producto a ello se dice que la activación de la cerradura magnética desde el interior de la zona 2 es confiable y de calidad.

4.3. Caracterización del módulo de administración, control y visualización de la información

En este apartado se plantea pruebas orientadas a la transmisión de la información para el control del PSES y pruebas de registro de usuarios para el control de acceso.

4.3.1. Pruebas de transmisión de la información para el control del PSES

El objetivo de esta prueba es determinar la integridad de la información entre Telegram y el módulo de control y actuación, es decir, que lo transmitido desde Telegram sea lo recibido en el módulo de control y actuación.

Para ello, se envió los mensajes "/alarma_on", "/alarma_off" los cuales activan y desactivan el sistema de alarma del PSES, respectivamente, con un total de 10 muestras para cada comando como si de una prueba de repetibilidad se tratara, el mismo procedimiento se lo realizó con el comando "/sirena_on", "/sirena_off" para el control del elemento actuador alarma audible y el comando "/abrir" para la apertura de la puerta de la zona 2.

En la *Ilustración 8-4*, *Ilustración 9-4* e *Ilustración 10-4* se visualizan los mensajes enviados desde Telegram y los recibidos en el módulo de control y actuación a partir de utilizar la pantalla serial de Arduino (ítem "text").

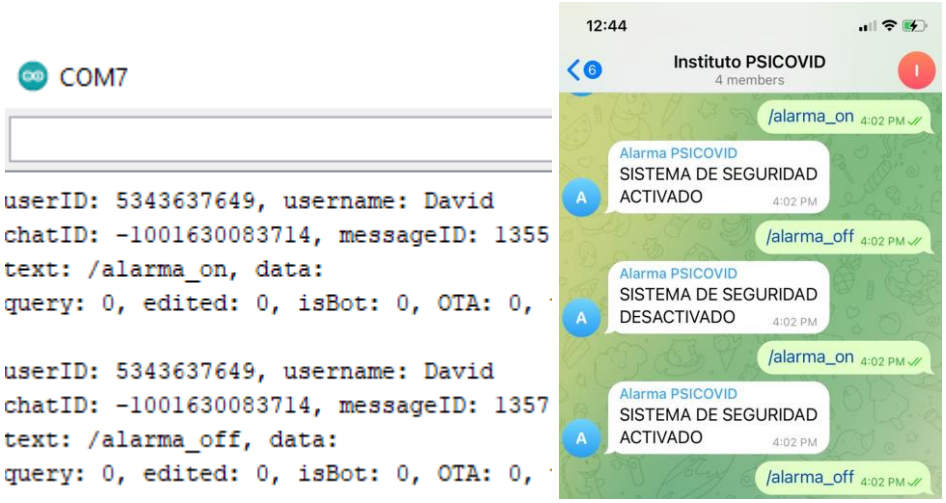


Ilustración 8-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha), para el comando "/alarma_on", "/alarma_off"

Realizado por: Chafla, Hernán, 2022

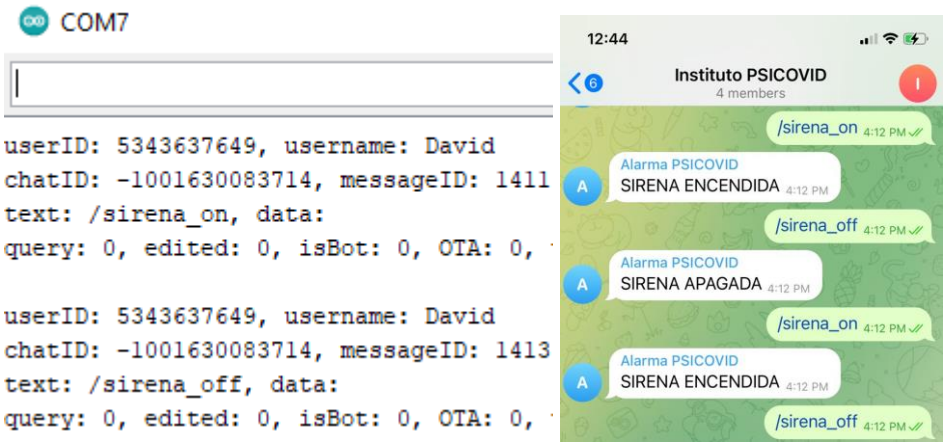


Ilustración 9-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha), para el comando "/sirana_on", "/sirena_off"

Realizado por: Chafla, Hernán, 2022

Ilustración 10-4: Pantalla serial de arduino (izquierda), mensajes de alerta en Telegram (derecha), para el comando "/abrir"

Realizado por: Chafla, Hernán, 2022

La prueba realizada en este apartado se observa en la *Tabla 12-4*.

Tabla 12-4: Pruebas de transmisión de la información para el control del PSES

N.º de muestra	Sistema de alarma		Alarma audible		Cerradura magnética	
	Mensaje enviado (Telegram)	Mensaje recibido	Mensaje enviado (Telegram)	Mensaje recibido	Mensaje enviado (Telegram)	Mensaje recibido
1	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
2	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
3	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
4	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
5	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
6	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
7	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
8	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
9	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
10	/alarma_on	/alarma_on	/sirena_on	/sirena_on	/abrir	/abrir
11	/alarma_off	/alarma_off	/sirena_off	/sirena_off		
12	/alarma_off	/alarma_off	/sirena_off	/sirena_off		
13	/alarma_off	/alarma_off	/sirena_off	/sirena_off		
14	/alarma_off	/alarma_off	/sirena_off	/sirena_off		
15	/alarma_off	/alarma_off	/sirena_off	/sirena_off		
16	/alarma_off	/alarma_off	/sirena_off	/sirena_off		
17	/alarma_off	/alarma_off	/sirena_off	/sirena_off		

18	/alarma_off	/alarma_off	/sirena_off	/sirena_off
19	/alarma_off	/alarma_off	/sirena_off	/sirena_off
20	/alarma_off	/alarma_off	/sirena_off	/sirena_off

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 12-4*, tras aplicar la técnica de observación se establece que existe integridad de la información en todos los mensajes enviados desde Telegram hacia el módulo de control y actuación para la activación y desactivación del sistema de alarma, alarma audible y apertura de la puerta en la zona 2.

4.3.2. Prueba de registro de usuarios para el control de acceso

El objetivo de esta prueba es determinar la integridad de la información entre la aplicación móvil y la base de datos, es decir, la información ingresada en los diferentes campos solicitados por la App para el registro de usuarios tiene que ser la misma información almacenada en Firebase.

El procedimiento a seguir es el siguiente: dentro de la aplicación se escoge la opción "Regístrate", posteriormente el administrador del PSES tendrá que llenar los campos solicitados en las diferentes ventanas de la App con la información del nuevo usuario, tal como se observa en la *Ilustración 11-4.*

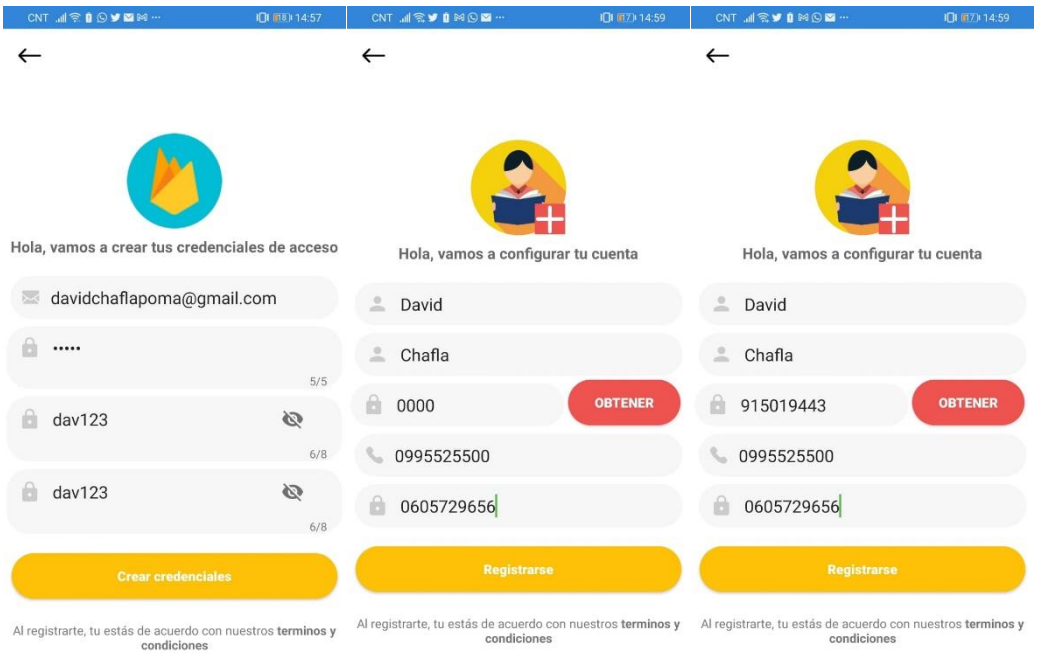


Ilustración 11-4: Ventanas que conforman la aplicación móvil para el control de acceso

Realizado por: Chafla, Hernán, 2022

Al presionar el botón “obtener” es importante acercar la tarjeta o dispositivo NFC que se desee añadir al módulo de adquisición de datos 1 para su correspondiente lectura, véase en la *Ilustración 12-4*.

Ilustración 12-4: Lectura de tarjeta NFC para su registro

Realizado por: Chafla, Hernán, 2022

Como se observa en la *Ilustración 13-4*, una vez registrado el nuevo usuario se procede a abrir la base de datos para visualizar la información que se almaceno en ella.

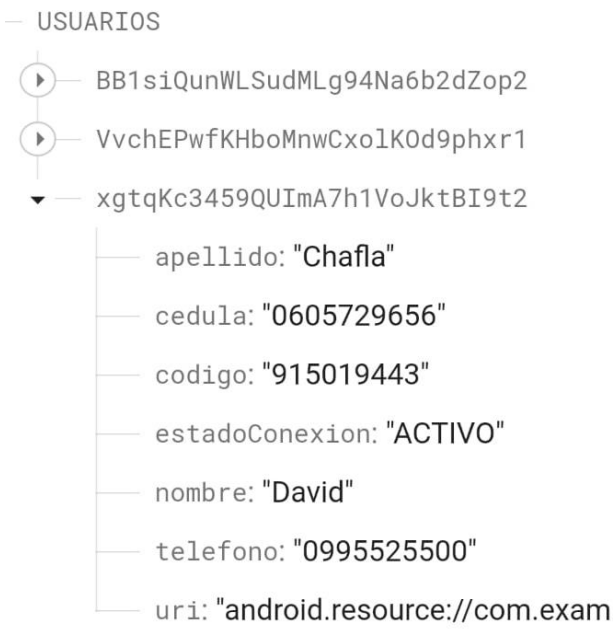


Ilustración 13-4: Informacion registrada en Firebase

Realizado por: Chafla, Hernán, 2022

Con base a la *Ilustración 11-4* y la *Ilustración 13-4*, tras aplicar la técnica de observación se establece que existe integridad de la información entre lo ingresado en los diferentes campos de la aplicación móvil y lo registrado en la base de datos respectiva.

4.4. Caracterización de la comunicación para los módulos de PSES

El objetivo de esta prueba es determinar la distancia de comunicación máxima que alcanzan los módulos de adquisición de datos 1, 2, 3 y 4 y el módulo de control y actuación respecto al router con frecuencia de 2.4GHz.

Para ello al contar cada módulo con un mismo modelo de tarjeta de desarrollo (ESP8266 Wemos D1 mini) se evalúa de manera general la transmisión de datos con línea de vista y con interferencia, para lo cual se escoge y se ubica un módulo de adquisición de datos en un área cercana al centro "Psicológico infantil- PSICOVID", estableciendo tramos hasta cuando se presenten problemas de trasmisión de datos. Para la medición de las longitudes se empleó Google Earth.

La *Ilustración 14-4* representa el alcance de comunicación con interferencia, donde, el router se encuentra ubicado en el interior del establecimiento (punto A) y el módulo de prueba se encuentra ubicado en su exterior (punto B).

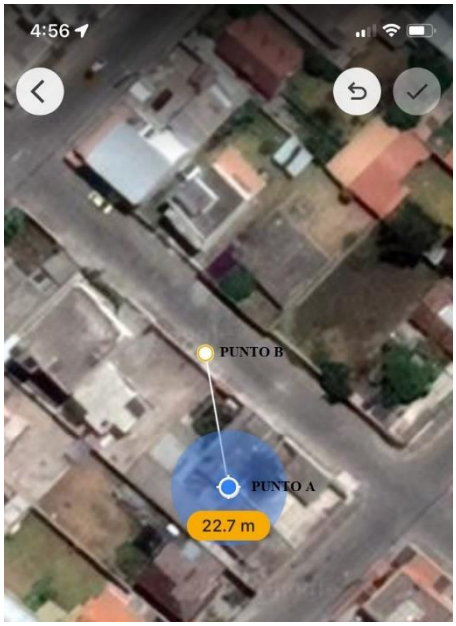


Ilustración 14-4: Alcance de comunicación con interferencia

Realizado por: Chafla, Hernán, 2022

La *Ilustración 15-4* representa el alcance de comunicación con línea de vista, en donde el router se encuentra ubicado en el exterior del establecimiento (punto A) al igual que el módulo de prueba (punto B).

Ilustración 15-4: Alcance de comunicación con línea de vista

Realizado por: Chafla, Hernán, 2022

Una vez habiendo realizado varias pruebas de alcance de comunicación máxima entre los diferentes módulos del PSES y el router, con y sin línea de vista, es posible establecer el nivel de recepción de datos en función a la distancia, el cual se lo categoriza de la siguiente manera:

En cuanto a la comunicación con línea de vista, "alto" 0 < distancias ≤ 35 (metros) presenta comunicación estable, con retardos de hasta 2 segundos, "medio" 35< distancias ≤ 41.9 (metros) presenta pequeños problemas de comunicación con auto recuperación de señal de red y retardos de hasta 3 segundos, "nulo" distancias >41.9 (metros) no se establece comunicación alguna entre emisor-receptor, véase en la *Ilustración 16-4.*

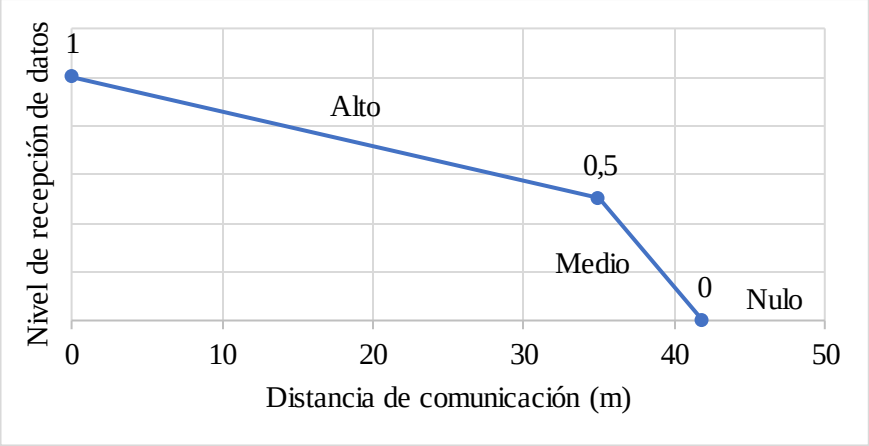


Ilustración 16-4: Nivel de recepción de datos en función a la distancia, con linea de vista.

Realizado por: Chafla, Hernán, 2022

En cuanto a la comunicación con interferencia, "alto" 0 < distancias ≤ 19 (metros) presenta comunicación estable, con retardos de hasta 3 segundos, "medio" 19< distancias ≤ 22.7 (metros) presenta pequeños problemas de comunicación con auto recuperación de señal de red y retardos de hasta 4 segundos, "nulo" distancias >22.7 (metros) no se establece comunicación alguna entre emisor-receptor, véase en la *Ilustración 17-4.*

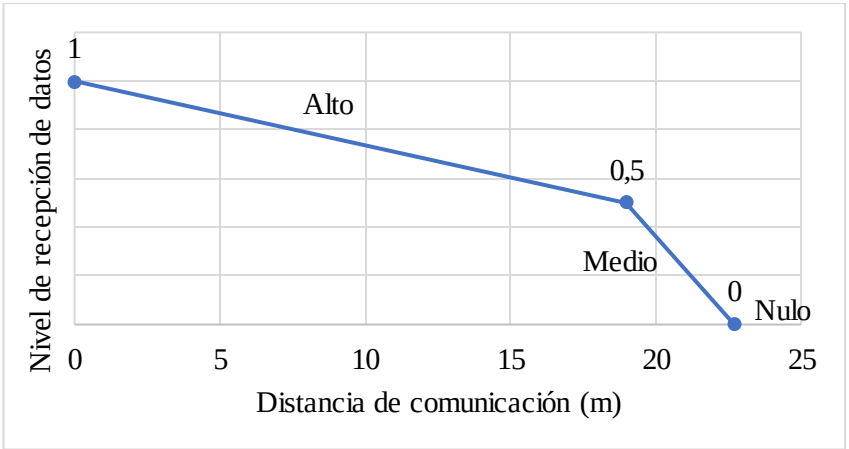


Ilustración 17-4: Nivel de recepción de datos en función a la distancia, con interferencia.

Realizado por: Chafla, Hernán, 2022

Con base a la *Ilustración 16-4* y la *Ilustración 17-4*, se establece que la distancia de comunicación máxima entre los módulos del PSES y el router, para un nivel de comunicación "alto" con retardos de tiempo entre 2 y 3 segundos es de 35m con línea de vista y 19m con interferencia, respectivamente.

4.5. Pruebas de la alimentación del PSES

En este apartado se realizan pruebas del consumo energético del PSES y la estimación de carga/descarga de la batería Rekoser RKE12-7.

4.5.1. Consumo energético del PSES

El objetivo de esta prueba es determinar el consumo de energía real que tiene el PSES en estado activo e inactivo.

Consumo energético en estado inactivo. - Para este literal con ayuda de un multímetro se mide por individual el consumo de cada módulo que conforma el PSES habiendo desarmado la alarma en un paso anterior, posteriormente se suma los valores registrados en las mediciones obteniendo así el consumo de corriente total.

Consumo energético en estado activo. - Para este literal tras armar el sistema de alarma con ayuda de un multímetro se mide por individual el consumo de cada módulo activando los elementos sensores y actuadores respectivos, con la intención de captar el pico máximo de consumo de corriente de cada uno de ellos, posteriormente se suma los valores registrados obteniendo así el consumo de corriente total.

En la Tabla *13-4* se presenta los resultados obtenidos tras realizar las mediciones de consumo energético para un estado activo e inactivo.

Tabla 13-4: Consumo de corriente del PSES para un estado activo e inactivo.

Módulo	Estado inactivo (mA)	Estado activo (mA)
Adquisición de datos 1	82.5	109.3
Adquisición de datos 2	37.6	64.5
Adquisición de datos 3	39.1	59.5
Adquisición de datos 4	45.7	51
Control y actuación- bloque de alimentación	60	220
Total	264.9	504.3

Realizado por: Chafla, Hernán, 2022

Con base a la Tabla 13-4, se observa que el consumo de energía real del PSES para un estado inactivo es de 264.9 mA y para un estado activo es de 504.3 mA, siendo menor con un 88.3% y un 77.72%, respectivamente, comparado con el consumo calculado de forma teórica.

4.5.2. Estimación de la carga y descarga de la batería

El objetivo de esta prueba es determinar el tiempo de carga y de duración de la batería frente a un corte de energía eléctrica en la línea principal.

Tiempo de carga y descarga de la batería Rekoser RKE12-7. - Como primer paso se procedió a descargar dicha batería en su totalidad, después se conecta la batería al suministro eléctrico y se cronometra el tiempo que demora hasta que llegue a un voltaje de 13.6 V, valor especificado en su hoja de datos, véase en la *Ilustración 18-4.*

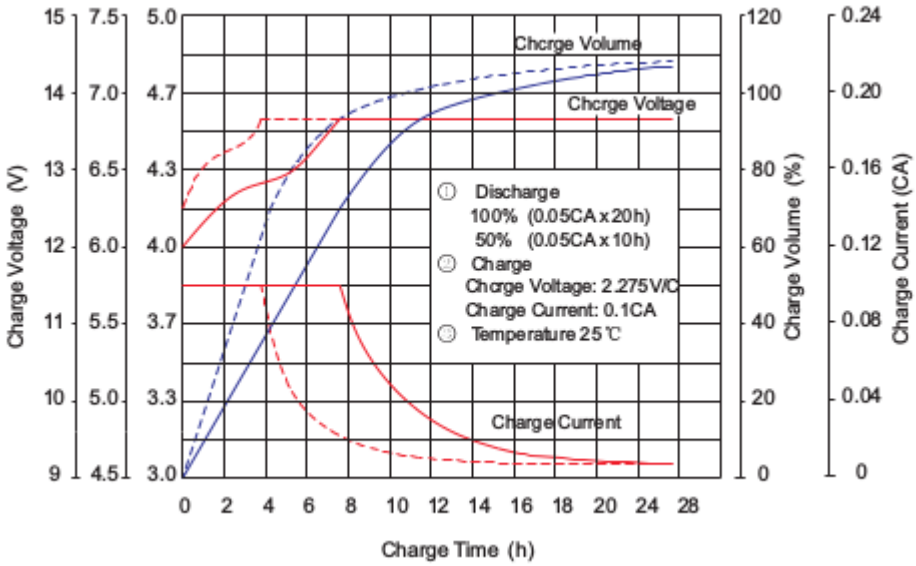


Ilustración 18-4: Caracteristica de descarga de la batería Rekoser 12V7Ah

Fuente: (Rekoser, 2022)

El tiempo de carga registrado en este procedimiento fue de 3.75 horas, valor que se aproxima al expuesto teóricamente en las especificaciones técnicas de la batería.

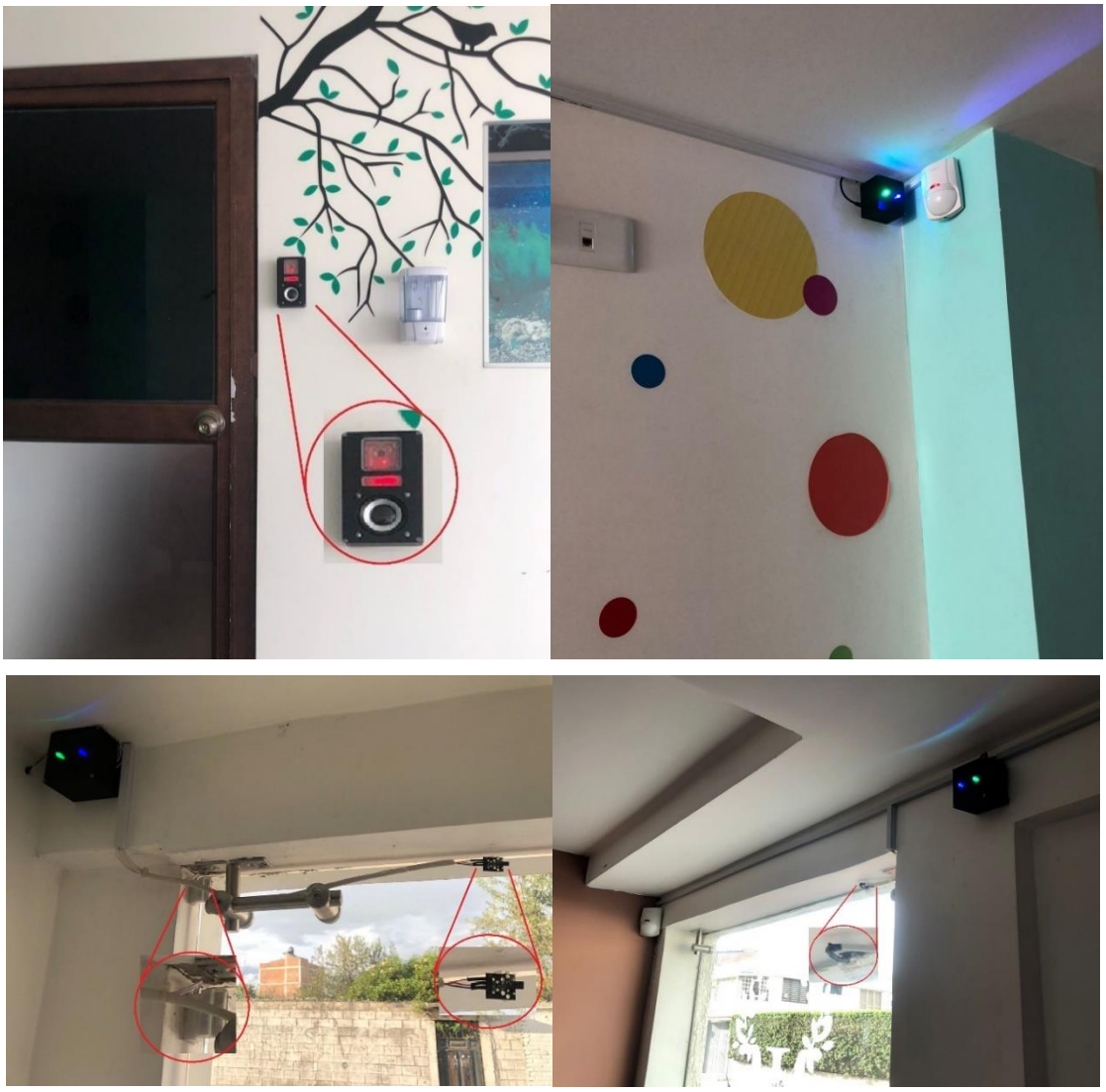
Finalmente, para determinar el tiempo de duración o descarga de la batería se hace uso de la ecuación 1 citada en el capítulo 3.

Reemplazando los resultados obtenidos de la *Tabla 13-4* en la ecuación 1, se tiene un tiempo de duración igual a 13.88 horas para un consumo en estado activo, y una duración de 26.43 horas

para un consumo en estado inactivo, por lo que la duración de dicha batería satisface el tiempo de corte de energía en la zona el cual se encuentra en el rango de 2 a 3 horas (Empresa Eléctrica Riobamba S.A., 2022).

4.6. Funcionamiento general del PSES

Una vez habiendo realizado la caracterización de cada módulo que conforma el PSES de manera individual, así como pruebas de integridad de información, distancias de comunicación, alimentación y demás, como siguiente paso se procedió a la implementación del sistema completo dentro de las instalaciones del centro "Psicológico Infantil PSICOVID", véase en la *Ilustración 19-4*.



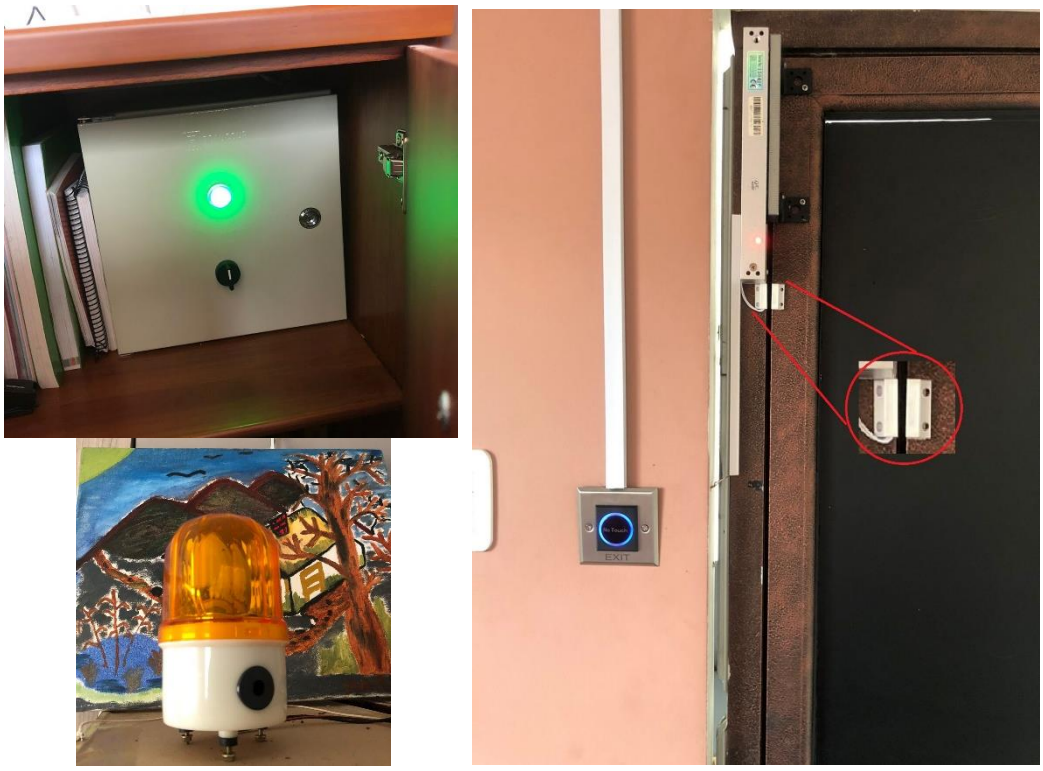


Ilustración 19-4: Implementación del PSES dentro de las instalaciones del centro "Psicológico Infantil PSICOVID".

Realizado por: Chafla, Hernán, 2022

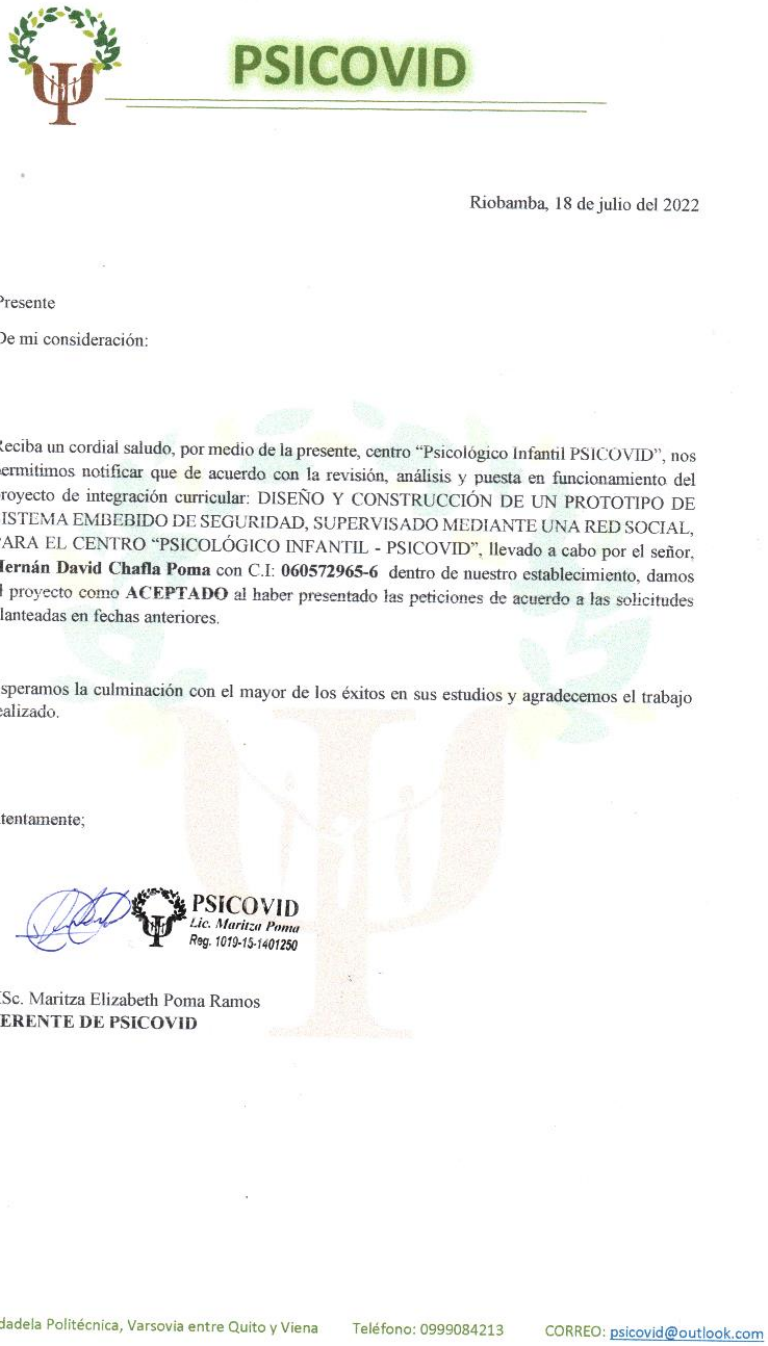
Posteriormente, encontrándose el PSES ensamblado en su totalidad se realizaron pruebas orientadas al control del sistema en conjunto mediante Telegram, para ello:

En repetidas ocasiones se armó el sistema de alarma y se lo activo de tal forma que cada elemento de adquisición de datos por individual, incorporado en su respectivo módulo, fuese el responsable de la acción realizada, las respuestas a cada una de estas pruebas resultaron ser favorables, reportando alertas y tomando acción de lo sucedido.

Para el control de acceso se tomaron tarjetas registradas, no registradas y bloqueadas, continuamente se realizaron lecturas constantes para observar el comportamiento del sistema, al finalizar se pudo comprobar que la apertura de la puerta únicamente se dio a los usuarios con tarjetas registradas, tal y como debía suceder.

Continuamente se realizaron pruebas de: activación directa de la alarma audible, administración de usuarios mediante la aplicación móvil, apertura de la puerta desde Telegram y desde el interior de la zona por medio del botón, teniendo resultados adecuados por cada prueba aplicada.

Finalmente, una vez culminado con el proceso que conlleva este apartado se procedió a realizar la entrega del PSES a la psicóloga Maritza Poma, dueña del centro "Psicológico Infantil - PSICOVID", quien dio constancia al correcto funcionamiento del proyecto de integración curricular elaborado, por tanto, como evidencia a ello en la *Ilustración 20-4* se adjunta la carta recibida que valida lo mencionado.



PSICOVID

Riobamba, 18 de julio del 2022

Presente

De mi consideración:

Reciba un cordial saludo, por medio de la presente, centro "Psicológico Infantil PSICOVID", nos permitimos notificar que de acuerdo con la revisión, análisis y puesta en funcionamiento del proyecto de integración curricular: DISEÑO Y CONSTRUCCIÓN DE UN PROTOTIPO DE SISTEMA EMBEBIDO DE SEGURIDAD, SUPERVISADO MEDIANTE UNA RED SOCIAL, PARA EL CENTRO "PSICOLÓGICO INFANTIL - PSICOVID", llevado a cabo por el señor, **Hernán David Chafla Poma** con C.I: **060572965-6** dentro de nuestro establecimiento, damos al proyecto como **ACEPTADO** al haber presentado las peticiones de acuerdo a las solicitudes planteadas en fechas anteriores.

Esperamos la culminación con el mayor de los éxitos en sus estudios y agradecemos el trabajo realizado.

Atentamente;

PSICOVID
Lic. Maritza Poma
Reg. 1019-15-1401250

MSc. Maritza Elizabeth Poma Ramos
GERENTE DE PSICOVID

DIRECIÓN: Ciudadela Politécnica, Varsovia entre Quito y Viena Teléfono: 0999084213 CORREO: psicovid@outlook.com

Ilustración 20-4: Certificado de aceptación del proyecto de integración curricular emitido por el centro "Psicológico Infantil -PSICOVID"

Realizado por: Chafla, Hernán, 2022

4.7. Análisis económico para la construcción del PSES

En la *Tabla 14-4* se presenta el costo total requerido para la construcción del PSES, para ello se hace mención a los costos unitarios pertenecientes a cada elemento necesario para la construcción del mismo y la cantidad requerida de dichos elementos. Los costos expuestos a continuación corresponden a su adquisición dentro de Ecuador.

Tabla 14-4: Análisis económico para la construcción del PSES

Módulo	Cantidad	Componente	Costo unitario (USD)	Costo total (USD)
Adquisición de datos (1-4)	4	ESP8266 Wemos D1 mini	$ 8.00	$ 32.00
	2	Sensor magnético MC-38	$ 1.50	$ 3.00
	2	Sensor de movimiento DSC LC-100-PI	$ 12.40	$ 24.80
	2	Sensor de vibración Ky-002	$ 2.50	$ 5.00
	1	Módulo RFID/NFC PN532	$ 11.95	$ 11.95
	4	Convertidor DC-DC MP2307	$ 1.00	$ 4.00
	1	Módulo DFPlayer Mini MP3	$ 4.00	$ 4.00
	4	Impresión 3D del diseño estructural	$ 20.00	$ 80.00
	1	Otros elementos	$ 10.00	$ 10.00
	TOTAL		$	174.75
Control y actuación	1	ESP8266 Wemos D1 mini	$ 8.00	$ 8.00
	1	Cerradura magnética ZE-280-5T	$ 38.50	$ 38.50
	1	Alarma audible 12V Opalux	$ 10.00	$ 10.00
	1	Módulo relé	$ 2.00	$ 2.00
	1	Convertidor DC-DC MP2307	$ 1.00	$ 1.00
	1	Estructura	$ 19.00	$ 19.00
	1	Otros elementos	$ 23.00	$ 23.00
	TOTAL		$	101.50
Bloque de alimentación	1	Batería Rekoser RKE12-7	$ 17.00	$ 17.00
	1	Fuente de alimentación UHPPOTE	$ 27.50	$ 27.50
	TOTAL		$	44.50
Costo- tiempo de ingeniería (30%)			$	96.23
COSTO TOTAL DEL PSES			$	416.98

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 14-4*, se determina que el costo total de construcción del PSES es de $416.98, del cual se desglosa los siguientes porcentajes de costos de construcción: el 41.91% para la implementación de los 4 módulos de adquisición de datos, el 24.34% para el módulo de control

y actuación, el 10.67% para el bloque de alimentación y el 23.08% del tiempo de ingeniería empleado para la construcción de estos.

Sin embargo, con lo antes mencionado se deduce que el costo para la construcción de los 4 módulos de adquisición de datos es de $174.75, por lo que, si se analiza de forma individual son los que requieren de menor inversión económica para su construcción, al ser un sistema escalable esto resulta ser beneficioso, pues al expandirse el establecimiento lo que estrictamente se tiene que añadir son más de estos módulos, el número dependerá del área y zonas que se desee proteger.

4.7.1. Comparativa con un sistema comercial

En este apartado se realiza la comparativa del PSES con dos sistemas de similares características e iguales funciones: el primero orientado al sistema de alarma comercializado por la empresa Laarcom (Laarcom, 2022) y el segundo un sistema de control de acceso comercializado por la empresa Anviz (Anviz, 2022).

Para el sistema de alarma se realizó una cotización por medio de la página web oficial de la empresa, seleccionando como parámetros las características del lugar en donde se desea la implementación, tales como, tipo de establecimiento (oficina), número de ventanas (una), número de puertas (dos), y número de ambientes del interior (dos).

Para el control de acceso se indago en la página web de la empresa hasta encontrar el sistema que más se asemeje al incorporado en el PSES. Unificando las principales características de los dos sistemas antes mencionados, se realizó la comparativa correspondiente la cual puede ser vista en la *Tabla 15-4*.

Tabla 15-4: Comparativa entre las características del PSES y un sistema comercial

Característica	PSES	Sistema comercial
	Sistema de alarma	
N.º de zonas a asegurar	2	2
Voltaje de alimentación	5 y 12 (V)	16 (V)
Batería	7A	4A
N.º de detectores de movimiento	2	2
N.º de contactos magnéticos	2	3
N.º de sensores de vibración	2	0
Potencia de sirena	25W	20W

Monitoreo	Telegram	App Laarcom Smart
	Control de acceso	
N.º de zonas a asegurar	1	1
Voltaje de alimentación	12V	12V
Modos de identificación	NFC	RFID, huella
Distancia de lectura máxima	10 cm	2.2 cm
Registro de usuarios	Aplicación móvil	RS485 y mini USB
Dimensiones	12x7x3.5(cm)	14.5x5.5x3.7(cm)
COSTO TOTAL	$ 416.98	$ 545.51

Realizado por: Chafla, Hernán, 2022

Con base a la *Tabla 15-4* se observa que el costo del PSES es 23.56% más económico que dispositivos comerciales. Los voltajes de operación son menores en relación con el sistema comercial, encontrándose en los 5 y 12V & 12 y 16V, respectivamente. Además de destacar algunos beneficios extras con los cuales cuenta el PSES, tales como, mayor capacidad de batería, sensores de vibración, potencia de sirena, dimensiones y tipo de monitoreo utilizado.

CONCLUSIONES

- Se diseñó y construyó un prototipo de sistema embebido de seguridad para el centro Psicológico Infantil Psicovid el cual es monitoreado y controlado mediante el uso de Telegram. Tiene incorporado dos sistemas de seguridad, el primero orientado a un sistema de alarma el cual cumple con la norma Ecuatoriana INEN-IEC 62851-1 y el segundo orientado al control de acceso basado en tecnología NFC.
- El prototipo de sistema embebido de seguridad basa su operabilidad en el desarrollo de tres módulos: adquisición de datos, control y actuación, administración - control y visualización de la información los cuales cumplen con funciones específicas. Se recurrió a que cada uno de dichos módulos utilice tecnología Wifi como puerta de acceso a internet, obteniendo un alcance de comunicación de 35m con línea de vista y 19m con interferencia, incorporándose retardos de tiempo entre 2 y 3 segundos.
- Se determinó que el error relativo (Er) máximo dado por los dos sensores magnéticos es de 7.14%, por lo que, la adquisición de datos realizada por dichos elementos de sensado tienen como resultado experimental un criterio de calidad aceptable.
- Con base a las pruebas realizadas a los dos sensores de movimiento se determinó un Er máximo en cuando a su distancia de activación de 0.6% y 0.99% y en cuanto a sus grados de detección 3.66% y 5.56%, respectivamente. Por lo que, la adquisición de datos realizada por el primer elemento de sensado tienen como resultado experimental un criterio de calidad entre bueno y aceptable. Mientras la adquisición de datos realizada por el segundo elemento de sensado tienen como resultado experimental un criterio de calidad aceptable.
- Mediante las pruebas de repetibilidad aplicadas a los sensores de vibración, se encontró un coeficiente de variación (CV) igual al 10%, por lo que se establece que el trabajo que cumplen dichos sensores es confiable y de calidad.
- Tras realizar pruebas de repetibilidad orientadas a: lecturas del módulo NFC, comunicación entre el módulo de control y actuación con los módulos de adquisición de datos (sin contar los sensores de vibración) y la activación de la cerradura magnética a partir de un botón, se obtuvo un CV=0% significando estabilidad de datos y haciendo que su comportamiento sea confiable y de calidad.
- Por medio de pruebas de integridad de la información tras aplicar la técnica de la observación orientadas al control del prototipo mediante Telegram y el registro de usuarios mediante la aplicación móvil, se determinó que no existen perdida de datos en ninguna ocasión.
- En cuanto a la alimentación se constató que el PSES tienen un consumo energético real en estado activo de 504.3 mA y en estado inactivo de 264.9 mA, respectivamente siendo menor

con un 77.72% y un 88.3% al consumo calculado de forma teórica. Producto a ello se determinó que si la batería entra en funcionamiento tendría una duración de 13.88 horas para el estado activo y de 23.43 horas para el estado inactivo.

- Una vez habiendo realizado el análisis económico necesario para la construcción del PSES se determinó un costo total de $416.98 siendo un 23.56% más económico que dispositivos comerciales de similares características.

RECOMENDACIONES

- Aumentar el tiempo de pruebas para la validación de los diferentes módulos que componen el PSES, pues tal vez el tiempo empleado en el presente trabajo de integración curricular no es el suficiente.
- Para tener control sobre la activación del sensor de vibración se sugiere utilizar una placa de circuito SW-420 la cual trabaje en conjunto con un sistema de visión artificial para la identificación de una falsa señal de alarma y un verdadero intento de robo.
- Incorporar un sistema de alimentación renovable para cada módulo por individual el cual pueda ser monitoreado por medio de la misma red social, con el fin de tener control sobre el mismo y evitar que el PSES quede inutilizado con la caída de la línea principal de energía en paralelo a la de respaldo.
- Implementar un sistema de control de acceso el cual considere la jerarquía de empleados dentro de un establecimiento, es decir considerando un nivel de permisos. Teniendo en cuenta visión artificial en conjunto a NFC para un doble factor de autenticación de identidad.
- Se sugiere realizar estudios para la implementación de un sistema de cámaras de seguridad a las que se pueda acceder en tiempo real mediante una video llamada o la petición de captura de imágenes solicitada desde Telegram.
- Para futuras investigaciones, en el caso de los sensores magnéticos, sensor de vibración y módulo de lectura para el control de acceso, se recomienda incrustarlos en el interior de las estructuras que se van a monitorear.
- Utilizar equipos patrones de mejor precisión para la caracterización de los sensores que conforman a los módulos de adquisición de datos.

BIBLIOGRAFÍA

12V24VPRODUCTS, 2022. Análisis de las 15 mejores sirenas de 12 V del mundo. [en línea]. [Consulta: 1 May 2022]. Disponible en: https://www.12v24vproducts.org/es/sirena-12-voltios.

AGUAYO, L., 2018. *Implementación de un sistema de alarma mediante la plataforma arduino a través de telefonía móvil en el decanato de la facultad de ciencias técnicas* [en línea]. Proyecto de investigación. Manabí: Universidad Estatal del Sur de Manabí. [Consulta: 11 January 2022]. Disponible en: http://repositorio.unesum.edu.ec/bitstream/53000/1505/1/UNESUM-ECU-REDES-2018-29.pdf.

AGUILERA, H., ROSERO, G. and GILCES, A., 2009. Prototipo de funcionamiento de sensor infrarrojo de seguridad en una dobladora hidráulica de la mecánica industrial. *Journal of Business and entrepreneurial* [en línea], pp. 33–45. [Consulta: 1 June 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/7888297.pdf.

ALVARADO, G. and GARCÍA, A., 2012. *Estudio de sistemas de respaldo de energía eléctrica para cuarto de telecomunicaciones en la finca limoncito* [en línea]. Tesis. Guayaquil: Universidad Católica de Santiago de Guayaquil. [Consulta: 19 May 2022]. Disponible en: http://repositorio.ucsg.edu.ec/bitstream/3317/8547/1/T-UCSG-PRE-TEC-ITEL-215.pdf.

ANVIZ, 2022. Kit completo de control de acceso. [en línea]. [Consulta: 2 July 2022]. Disponible en: https://www.todoelectronica.com/kit-completo-de-control-de-acceso-que-no-incluye-cerradura-electronica-p-99314.html.

APRENDIENDO ARDUINO, 2018. Etiqueta: WiFiClient. [en línea]. [Consulta: 10 June 2022]. Disponible en: https://www.aprendiendoarduino.com/tag/wificlient/.

ARANA, M., ERANSUS, J. and VELA, A., 2021. Señales acústicas de peligro y alarma. [en línea]. Pamplona: [Consulta: 2 May 2022]. Disponible en: https://www.navarra.es/NR/rdonlyres/EF1224A4-E797-4B30-9ED7-E04C53A3F829/146320/FTP1SeAcusticas.pdf.

ARDUINO, 2018. What is Arduino? [en línea]. [Consulta: 9 June 2022]. Disponible en: https://www.arduino.cc/en/Guide/Introduction.

ARDUINO, 2022a. CTBot. [en línea], [Consulta: 11 June 2022]. Disponible en: https://www.arduino.cc/reference/en/libraries/ctbot/.

ARDUINO, 2022b. Libraries WiFi. [en línea]. [Consulta: 10 June 2022]. Disponible en: https://www.arduino.cc/reference/en/libraries/wifi/.

ARGSEGURIDAD, 2021. Cerraduras electromagnéticas. [en línea]. [Consulta: 1 June 2022]. Disponible en: https://www.argseguridad.com/blog/cerraduras-electromagneticas/.

ASUNI, N., 2022. Modulo sensor de vibración KY-002 para Arduino. [en línea]. [Consulta: 6 June 2022]. Disponible en: http://www.electronicapty.com/modulo-sensor-de-vibracion-ky-002-para-arduino-detail?tmpl=component&format=pdf.

AUTODESK, 2020. What is EAGLE? [en línea]. [Consulta: 9 June 2022]. Disponible en: https://www.autodesk.com/products/eagle/overview?term=1-YEAR&tab=subscription#!

AV ELECTRONICS, 2020. Módulo DFPlayer Mini MP3 Player. [en línea]. [Consulta: 7 June 2022]. Disponible en: https://avelectronics.cc/producto/modulo-dfplayer-mini-mp3-player/.

AV ELECTRONICS, 2022. WeMos D1 mini ESP8266. [en línea]. [Consulta: 26 April 2022]. Disponible en: https://avelectronics.cc/producto/wemos-d1-mini-esp8266/.

AVILES, A. and COBEÑA, C., 2015. *Diseño e implementación de un sistema de seguridad a través de cámaras, sensores y alarma, monitorizado y controlado telemétricamente para el centro de acogida "patio mi pana" perteneciente a la fundación proyecto salesiano* [en línea]. Tesis. Guayaquil: Universidad Politécnica Salesiana. [Consulta: 11 January 2022]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/10401/1/UPS-GT001444.pdf.

BARRERA, Ó. and ROS, J., 2016. *Sistemas eléctricos y de seguridad y confortabilidad* [en línea]. 2. Madrid: Paraninfo. [Consulta: 28 May 2022]. Disponible en: https://books.google.es/books?hl=es&lr=&id=6Xo3DAAAQBAJ&oi=fnd&pg=PP1&dq=componentes+sistemas+de+seguridad&ots=ZTDatyGkMQ&sig=drOS5ys2Emw-rdPqLCVBIQ2YTho#v=onepage&q&f=false.

BONE, V., 2019. *Prototipo de un sistema monitores de video para la seguridad de viviendas, con comunicación a dispositivos de tecnología celular y alimentados por paneles solares* [en línea]. Tesis. Riobamba: Escuela Superior Politécnica de Chimborazo. [Consulta: 5 January 2022]. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/13498/1/98T00265.pdf.

BOWMAN, D., 2001. CONTEMPORARY ISSUES Common Use of the CV: A Statistical Aberration in Crop Performance Trials. *The Journal of Cotton Science* [en línea], vol. 5, pp. 137–141. [Consulta: 2 July 2022]. Disponible en: https://www.cotton.org/journal/2001-05/2/upload/jcs05-137.pdf.

CARBONELL, M., 2020. Domótica para el control de seguridad. [en línea]. [Consulta: 5 January 2022]. Disponible en: https://www.hogarsense.es/domotica/seguridad-domotica.

CARIGNANO, M.F., 2022. NFC (Near Field Communication). *Instituto Universitario Aeronáutico* [en línea], pp. 1–22. [Consulta: 25 May 2022]. Disponible en: https://rdu.iua.edu.ar/bitstream/123456789/462/1/TFI_ESE_Maria_Fernanda_Carignano.pdf.

CASTAÑO, D. and ALONSO, J., 2019. *Sistema de reconocimiento facial para control de acceso a viviendas* [en línea]. Tesis. Bogotá: Universidad Católica de Colombia. [Consulta: 7 January 2022]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20grado.pdf.

CASTELLANOS, J., 2000. Las empresas de seguridad privada y las amenazas a la seguridad. *Ponencia preparada para el VI Seminario sobre Investigación y Educación en Estudios de Seguridad y Defensa* [en línea]. Santiago de Chile: s.n., pp. 1–16. [Consulta: 4 January 2022]. Disponible en: https://www.resdal.org/producciones-miembros/redes-03-castellanos.pdf.

CENACE, 2020. Informe anual 2020. [en línea]. Ecuador: [Consulta: 26 May 2022]. Disponible en: http://www.cenace.gob.ec/wp-content/uploads/downloads/2021/04/Informe-Anual-CENACE-2020-Parte-1.pdf.

CHAMARRO IGLESIA, A., 2007. Las comisiones de garantías de la videovigilancia. *Revista de Derecho Político* [en línea], pp. 211–246. [Consulta: 5 January 2022]. Disponible en: https://revistas.uned.es/index.php/derechopolitico/article/view/9015/8608.

CHANG, D. and LOZANO, A., 2013. *Desarrollo e implementación de un sistema para el control e inventario continuo, utilizando tecnologìa RFID, para la biblioteca de la UPS sede Guayaquil* [en línea]. Tesis. Guayaquil: Universidad Politécnica Salesiana. [Consulta: 23 May 2022]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/5521/1/UPS-GT000510.pdf.

CHOLAN, Y. and VARAS, G., 2017. *Diseño de un sistema de seguridad para viviendas utilizando un microcontrolador PIC16F877A* [en línea]. Tesis. Lima: Universidad de Ciencias y Humanidades. [Consulta: 6 January 2022]. Disponible en: https://repositorio.uch.edu.pe/bitstream/handle/20.500.12872/165/Cholan_YB_Varas_GP_TIEL_2017.pdf?sequence=1&isAllowed=y.

COELECTRIX, 2017. Batería AGM. [en línea]. [Consulta: 31 May 2022]. Disponible en: https://coelectrix.com/bateria-agm.

COLCHA, A., 2020. El wi-fi de los espacios públicos de Riobamba ya se restableció. [en línea]. [Consulta: 2 January 2022]. Disponible en: https://www.laprensa.com.ec/wi-fi-publico-riobamba/.

COLOMER, J., MELÉNDEZ, J. and AYZA, J., 2022. *Sistemas de Supervisión* [en línea]. S.l.: s.n. [Consulta: 18 July 2022]. Disponible en: https://intranet.ceautomatica.es/sites/default/files/upload/10/files/sistemas%20de%20supervision.pdf.

CORREA, R., 2008. *Reglamento a la ley de vigilancia y seguridad* [en línea]. 28 August 2008. Ecuador: s.n. [Consulta: 4 January 2022]. Decreto Ejecutivo 1181. Disponible en: https://www.gob.ec/sites/default/files/regulations/2018-10/REGLAMENTO%20A%20LA%20LEY%20DE%20VIGILANCIA%20Y%20SEGURIDAD.pdf.

DELTA ENTERPRISES S.A.C, 2022. Circulinas. [en línea]. [Consulta: 7 June 2022]. Disponible en: http://www.deltanegocios.com/circulinas.htm.

DELTA EU, 2022. Cerradura electromagnética ZE-280-5T. [en línea]. [Consulta: 6 June 2022]. Disponible en: https://shopdelta.eu/cerradura-electromagnetica-ze-280-5t_l6_p14137.html.

DELTA OPTI, 2022. Cerradura electromagnética ZE-280-5T. [en línea]. [Consulta: 6 June 2022]. Disponible en: https://shopdelta.eu/ajax.php?page=shop/flypage_pdf&category_id=1003&product_id=14137.

DEVELOPERS, 2021. Introducción a Android Studio. [en línea]. [Consulta: 9 June 2022]. Disponible en: https://developer.android.com/studio/intro?hl=es-419.

DSC, 2013. Detector PIR digital inmune a mascotas LC-100-PI. [en línea]. [Consulta: 6 June 2022]. Disponible en: https://tvc.mx/media/128982/Ficha-de-tecnica-LC100.pdf.

ECU-911, 2020. Rendición de cuentas 2020. [en línea]. S.l.: [Consulta: 5 January 2022]. Disponible en: https://www.ecu911.gob.ec/wp-content/uploads/2021/04/Informe-Rendicion-Cuentas_2020-CZ3.pdf.

EL COMERCIO, 2021. Barrios de Quito invierten en tecnología para mejorar la seguridad. [en línea]. [Consulta: 3 January 2022]. Disponible en: https://www.elcomercio.com/actualidad/gda/quito-barrios-delincuencia-seguridad-asaltos.html.

ELECTROALLWEB, 2020. Modulo DFPlayer mini reproductor mp3 para arduino. [en línea]. [Consulta: 27 May 2022]. Disponible en: https://www.electroallweb.com/index.php/2020/07/22/modulo-dfplayer-mini-reproductor-mp3-tutorial-completo/.

EMPRESA ELÉCTRICA RIOBAMBA S.A., 2022. Interrupciones Programadas. [en línea]. [Consulta: 27 May 2022]. Disponible en: http://www.eersa.com.ec/site/noticias-3/.

ENSACO, 2022. Domótica y sistemas de seguridad inteligentes en casas y empresas. [en línea]. [Consulta: 2 January 2022]. Disponible en: https://www.ensaco.es/domotica-y-sistemas-de-seguridad-inteligentes-en-casas-y-empresas/.

ENVIOSSMS, 2021. Planes y precios de envíos masivos de SMS. [en línea]. [Consulta: 2 January 2022]. Disponible en: https://ec.enviossms.com/precios.

ESCALANTE, D. and VARGAS, D., 2019. Raspberry pi: la tecnología reducida en placa. *Universidad Santiago de Cali* [en línea], pp. 1–19. [Consulta: 4 June 2022]. Disponible en:

https://repository.usc.edu.co/bitstream/handle/20.500.12421/4250/RASPBERRY%20PI.pdf?sequence=3&isAllowed=y#:~:text=La%20Raspberry%20Pi%20es%20un,acceso%20a%20la%20tecnolog%C3%ADa%20inform%C3%A1tica.

ESPRESSIF SYSTEMS, 2013. Espressif smart connectivity platform: ESP8266. [en línea]. [Consulta: 5 June 2022]. Disponible en: https://www.elecrow.com/download/ESP8266_Specifications_English.pdf.

FERNÁNDEZ, G., 2005. *Sensores magnéticos e inductivos* [en línea]. Tesis. Pachuca: Universidad Autónoma del Estado de Hidalgo. [Consulta: 1 June 2022]. Disponible en: https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Sensores%20magneticos.pdf.

FERNÁNDEZ, R., 2022. Redes sociales con mayor número de usuarios activos a nivel mundial en enero de 2022. [en línea]. [Consulta: 22 May 2022]. Disponible en: https://es.statista.com/estadisticas/600712/ranking-mundial-de-redes-sociales-por-numero-de-usuarios/.

FERNÁNDEZ, Y., 2020a. Bots de Telegram. [en línea]. [Consulta: 9 June 2022]. Disponible en: https://www.xataka.com/basics/bots-telegram-que-como-funcionan-recomendados-para-empezar.

FERNÁNDEZ, Y., 2020b. Qué es Arduino, cómo funciona y qué puedes hacer con uno. [en línea]. [Consulta: 19 January 2022]. Disponible en: https://www.xataka.com/basics/que-arduino-como-funciona-que-puedes-hacer-uno.

FIREBASE, 2022. Make your app the best it can be. [en línea]. [Consulta: 9 June 2022]. Disponible en: https://firebase.google.com/?hl=es-419&gclid=Cj0KCQjw-daUBhCIARIsALbkjSaBAi-ur6kG3jp9tiTR7zIloKsh-QX-Oew01mnIbUekbo8_sv0d20saAobkEALw_wcB&gclsrc=aw.ds.

FISCALÍA GENERAL DEL ESTADO, 2021. Las cifras de robos. [en línea]. [Consulta: 2 January 2022]. Disponible en: https://www.fiscalia.gob.ec/estadisticas-de-robos/.

FISHER, A., STOECKEL, J. and LAING, J., 1951. *Manual para el diseño de investigación operativa en planificación familiar* [en línea]. 2. México, D.F.: The Population Council. [Consulta: 7 July 2022]. Disponible en: Manual para el diseño de investigacion operativa en planificacion familiar.

GAIBOR, K. and LOOR, F., 2018. *Diseñar un sistema de alarma inalámbrico de bajo costo para la protección de viviendas tipo, en sectores de bajos recursos económicos de la ciudad de Guayaquil* [en línea]. Tesis. Guayaquil: Universidad de Guayaquil. [Consulta: 13 January 2022]. Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/32554/1/B-CINT-PTG-N.294%20%20Gaibor%20Carrillo%20Karina%20Dolores%20.%20Loor%20Mor%c3%a1n%20Fernando%20Antonio.pdf.

GALINDO, G., 2010. *Construcción y validación de un sensor de vibraciones usando un sistema micro-electro-mecánico* [en línea]. Tesis. Valdivia: Universidad Austral de Chile. [Consulta: 2 May 2022]. Disponible en: http://cybertesis.uach.cl/tesis/uach/2010/bmfcig158c/doc/bmfcig158c.pdf.

GALINDO, J. and GAMBOA, S., 2016. *Control de acceso a archivos y carpetas a través del reconocimiento facial* [en línea]. Tesis. Bogotá: Universidad Autónoma de Colombia. [Consulta: 8 January 2022]. Disponible en: http://www.fuac.edu.co/recursos_web/documentos/ing.sistemas/ojs/index.php/UACSIS/article/view/27.

GONZALES, D., 2018. *Diseño de un sistema de respaldo de energía eléctrica* [en línea]. Tesis. Chiclayo: Universidad César Vallejo. [Consulta: 17 May 2022]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/25911/Gonzales_SDA.pdf?sequence=1&isAllowed=y.

GONZÁLEZ, G. and SILVA, F., 2013. Diseño e implementación de una Tarjeta de Desarrollo con profundización en desarrollo de aplicación de touch sensing. *LACCEI* [en línea], pp. 1–10. [Consulta: 31 May 2022]. Disponible en: http://laccei.org/LACCEI2013-Cancun/RefereedPapers/RP157.pdf.

GRUPO DIGITEC, 2021. Alarmas de Robo. [en línea]. [Consulta: 4 January 2022]. Disponible en: https://www.grupodigitec.co.cr/soluciones/alarmas-de-robo.

GUAÑA, J. and LEMA, J., 2013. *Análisis de los servicios que ofertan las empresas de seguridad en la ciudad de Riobamba y diseño de un sistema estratégico de servicios innovadores para generar ventajas competitivas en la Empresa de Seguridad S.O.S período 2012* [en línea]. Tesis. Riobamba: Escuela Superior Politécnica de Chimborazo. [Consulta: 8 January 2022]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/9973.

GUASCH, J.F., 1984. *Baterías de Ni-Cd, uso y mantenimiento* [en línea]. 1984. S.l.: s.n. [Consulta: 26 May 2022]. NTP 104. Disponible en: https://www.insst.es/documents/94886/326801/ntp_104.pdf/9f51800b-4e02-400d-92c4-0e55d6221f4a.

GUZMÁN, C., 2018. Seguridad aplicada en la utilización de redes sociales. *Universidad Piloto de Colombia* [en línea], pp. 1–11. [Consulta: 17 July 2022]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6951/Seguridad%20Aplicada%20en%20Sitios%20de%20Redes%20Sociales.pdf?sequence=1.

HERRERA, J., PÉREZ, P. and MARCIANO, M., 2009. Tecnología RFID aplicada al control de accesos. *Polibits* [en línea], pp. 57–62. [Consulta: 21 May 2022]. Disponible en: http://www.scielo.org.mx/pdf/poli/n40/n40a9.pdf.

IBARRA, J. and PAREDES, K., 2018. Neural Networks for acces control based on face recognition usinhg. *Revista PUCE* [en línea], pp. 281–295. [Consulta: 19 May 2022]. Disponible en: http://www.revistapuce.edu.ec/index.php/revpuce/article/view/140/242.

INEC, 2021a. Indicadores de tecnología de la información y comunicación. [en línea]. S.l.: [Consulta: 27 May 2022]. Disponible en: https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2020/202012_Boletin_Multiproposito_Tics.pdf.

INEC, 2021b. Justicia y crimen. [en línea]. [Consulta: 2 January 2022]. Disponible en: https://www.ecuadorencifras.gob.ec/justicia-y-crimen/.

INEN, 2016. *Alarmas y sistemas de seguridad electrónicos - sistemas de alarma social* [en línea]. April 2016. Ecuador: s.n. [Consulta: 27 May 2022]. IEC 62851-1:2014, IDT. Disponible en: https://www.normalizacion.gob.ec/buzon/normas/62851-1-IEC.pdf.

JIMÉNEZ ORNELAS, R.A., 2005. La delincuencia juvenil: fenómeno de la sociedad actual. [en línea], pp. 216–261. [Consulta: 1 January 2022]. Disponible en: http://www.scielo.org.mx/pdf/pp/v11n43/v11n43a9.pdf.

JOHNSON CONTROLS, 2019. Qué es un control de acceso y cuáles son sus beneficios. [en línea]. [Consulta: 6 January 2022]. Disponible en: https://blog.johnsoncontrols.es/consejos/que-es-control-acceso-y-cuales-son-beneficios/.

LA PRENSA CHIMBORAZO, 2021a. Casas han sido robadas en Riobamba. [en línea]. [Consulta: 5 January 2022]. Disponible en: https://www.laprensa.com.ec/182-viviendas-han-sido-robadas/.

LA PRENSA CHIMBORAZO, 2021b. Top 5 de los barrios más peligrosos de Riobamba. [en línea]. [Consulta: 2 January 2022]. Disponible en: https://www.laprensa.com.ec/top-5-de-los-mas-peligrosos/.

LAARCOM, 2022. Cotiza tu alarma. [en línea]. [Consulta: 5 July 2022]. Disponible en: https://www.laarcom.com/cotizar-sistema-de-alarmas.

LAGE, 2019. Cuáles son los sistemas de seguridad para empresas. [en línea]. [Consulta: 3 January 2022]. Disponible en: https://www.lage.com.mx/blog/sistemas-de-seguridad-en-una-empresa.

LEÓN, F., 2021. Baterías LiPo. [en línea]. [Consulta: 16 May 2022]. Disponible en: https://dynamoelectronics.com/baterias-lipo-caracteristicas-y-cuidados/.

MANCILLA, A., 2021. FIREBASE — ESP8266. [en línea]. [Consulta: 10 June 2022]. Disponible en: https://www.electroallweb.com/index.php/2020/07/22/modulo-dfplayer-mini-reproductor-mp3-tutorial-completo/.

MORÓN UCHE, R., 2013. *Sistema de seguridad para la supervisión de vivienda mediante microcontrolador PIC y red sms* [en línea]. S.l.: Universidad Zaragoza. [Consulta: 27 May 2022]. Disponible en: https://zaguan.unizar.es/record/11904/files/TAZ-PFC-2013-443.pdf.

MPS, 2006. Datasheet MP2307 monolithic power systems. [en línea]. [Consulta: 7 June 2022]. Disponible en: https://pdf1.alldatasheet.com/datasheet-pdf/view/189147/MPS/MP2307.html.

NAYLAMP MECHATRONICS, 2021a. Módulo lector RFIF/NFC 13.56 MHz PN532. [en línea]. [Consulta: 6 June 2022]. Disponible en: https://naylampmechatronics.com/rfid-nfc/182-modulo-lector-rfid-nfc-1356mhz-pn532.html.

NAYLAMP MECHATRONICS, 2021b. Módulo lector RFIF/NFC PN532. [en línea]. [Consulta: 4 June 2022]. Disponible en: https://naylampmechatronics.com/rfid-nfc/182-modulo-lector-rfid-nfc-1356mhz-pn532.html.

NAYLAMP MECHATRONICS, 2021c. Módulo relay 2CH 5VDC. [en línea]. [Consulta: 7 June 2022]. Disponible en: https://naylampmechatronics.com/drivers/31-modulo-relay-2-canales-5vdc.html.

NXP B.V., 2017. Near fiel communication (NFC) controller. [en línea]. [Consulta: 5 June 2022]. Disponible en: https://www.nxp.com/docs/en/nxp/data-sheets/PN532_C1.pdf.

PALOMINO, B.R., 2022. ¿Cómo afecta la tecnología en la sociedad? [en línea]. [Consulta: 3 January 2022]. Disponible en: http://www.cusur.udg.mx/es/sites/default/files/adjuntos/como_afecta_la_tecnologia_a_la_sociedad_02.pdf.

PNUD, 2022. Programa de las naciones unidas para el desarrollo. [en línea]. [Consulta: 3 January 2022]. Disponible en: https://www.undp.org/es/content/ecuador/es/home/sustainable-development-goals/goal-9-industry-innovation-and-infrastructure.

PORTUONDO, Y. and PORTUONDO, J., 2010. LA REPETIBILIDAD Y REPRODUCIBILIDAD EN EL ASEGURAMIENTO DE LA CALIDAD DE LOS PROCESOS DE MEDICIÓN. *Tecnología Química* [en línea], vol. XXX, pp. 117–121. ISSN 0041-8420. Disponible en: https://www.redalyc.org/articulo.oa?id=445543770014.

POSADAS, A., 2022. *Determinación de errores y tratamiento de datos* [en línea]. 2022. Almería: Universidad de Almería. [Consulta: 7 July 2022]. Disponible en: https://w3.ual.es/~aposadas/TeoriaErrores.pdf.

QUINTERO, V., CHE, O. and AUCIELLO, O., 2021. Baterías de Ion litio: características y aplicaciones. *Revista de I+D Tecnológico* [en línea], [Consulta: 28 May 2022]. Disponible en: http://portal.amelica.org/ameli/jatsRepo/339/3392002003/html/index.html.

RAMÍREZ, I., 2021. WhatsApp, Telegram, Signal o Messenger. [en línea]. [Consulta: 20 May 2022]. Disponible en: https://www.xatakandroid.com/listas/whatsapp-telegram-signal-messenger-comparativa-a-fondo-aplicaciones-mensajeria-para-movil.

REKOSER, 2022. 12V 7Ah Batería AGM para uso general. [en línea]. [Consulta: 8 June 2022]. Disponible en: https://rekoser.com/es/batteries/agm/rke12-7/.

REQUENA, B., 2016. Coeficiente de variación de Pearson. [en línea]. [Consulta: 30 June 2022]. Disponible en: https://www.universoformulas.com/estadistica/descriptiva/coeficiente-variacion-pearson/#:~:text=El%20coeficiente%20de%20variaci%C3%B3n%20toma,y%20la%20media%20pierde%20confiabilidad.

RIVAS, J. and VELAZQUEZ, C., 2011. *Implementación de sistema de seguridad con video-vigilancia y software libre* [en línea]. México, D.F.: Instituto Politécnico Nacional. [Consulta: 15 January 2022]. Disponible en: https://tesis.ipn.mx/jspui/bitstream/123456789/11622/1/3.pdf.

ROBLES, B., 2016. *Principios del FPGA y aplicaciones en el control de procesos industriales* [en línea]. Tesis. San Salvador: Universidad de el Salvador. [Consulta: 14 January 2022]. Disponible en: https://ri.ues.edu.sv/id/eprint/9862/1/Principios%20del%20FPGA%20y%20aplicaciones%20en%20el%20control%20de%20procesos%20industriales.pdf.

RODRÍGUEZ, A., 2009. *Análisis y descripción de identificación por radio frecuencia: Tecnología, aplicaciones, seguridad y privacidad* [en línea]. Tesis. Mexico D.F.: Instituto Politécnico Nacional. [Consulta: 24 May 2022]. Disponible en: https://tesis.ipn.mx/bitstream/handle/123456789/5441/C2.302.pdf?sequence=1&isAllowed=y.

RODRÍGUEZ, N. and CARRIÓN, S., 2016. *Diseño de un prototipo basado en la tecnología RFID para el monitoreo de equipos digitales* [en línea]. Tesis. Bogotá: Universidad Libre. [Consulta: 25 May 2022]. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/10814/RFID.pdf.

RUIZ, J., 2010. Eficiencia relativa y calidad de los experimentos de fertilización en el cultivo de caña de azúcar. [en línea], vol. 28, pp. 149–154. [Consulta: 4 July 2022]. Disponible en: https://www.researchgate.net/publication/317439783_Eficiencia_relativa_y_calidad_de_los_experimentos_de_fertilizacion_en_el_cultivo_de_cana_de_azucar.

SALINAS, A., 2021. Redes sociales más usadas en el mundo 2021: TOP 10. [en línea]. [Consulta: 4 January 2022]. Disponible en: https://mott.marketing/redes-sociales-mas-usadas-en-el-mundo-top-10/.

SANTO, M. and LECUMBERRY, G., 2005. *El proceso de medición, análisis y comunicación de datos experimentales* [en línea]. Río Cuarto: s.n. [Consulta: 6 July 2022]. Disponible en: https://www.unrc.edu.ar/unrc/digtal/El_proceso_de_med.pdf.

SCHMIDT-FONSECA, I., LEÓN-ANCHÍA, R., ASTORGA-AGUILAR, C. and LUNA-ANGULO, J.M., 2019. RIESGOS Y MEDIDAS PREVENTIVAS SOBRE USO DE REDES SOCIALES POR PARTE DEL ESTUDIANTADO QUE CURSA EDUCACIÓN SECUNDARIA EN EL DISTRITO DE HORQUETAS, SARAPIQUÍ, HEREDIA, COSTA RICA. *InterSedes* [en línea], vol. 20, no. 42, pp. 186–207. [Consulta: 16 May 2022]. ISSN 2215-2458. DOI 10.15517/isucr.v20i42.41850. Disponible en: https://www.redalyc.org/journal/666/66666205008/html/.

SEGUÍ MORENO, J., 2012. Practical applications of NFC. *3ciencias* [en línea], pp. 1–9. [Consulta: 25 May 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4817327.pdf.

SENAR, J.C., 1999. La medición de la Repetibilidad y el error de medida. [en línea], pp. 53–64. [Consulta: 1 July 2022]. Disponible en: http://www.bcn.cat/museuciencies_fitxers/imatges/FitxerContingut1201.pdf.

SHOPNFC, 2022. Teléfonos y tablets compatibles con las etiquetas NFC. [en línea]. [Consulta: 26 May 2022]. Disponible en: https://www.shopnfc.com/es/content/7-telefonos-y-tabletas-compatibles-con-etiquetas-nfc.

SISALIMA, J., 2010. *Seguridad de Redes Sociales* [en línea]. Loja: Universidad Técnica Particular de Loja. [Consulta: 12 May 2022]. Disponible en: https://dspace.utpl.edu.ec/bitstream/123456789/1439/3/Sisalima_Granda_Jorge_Omar.pdf.

SOFTMANY, 2022. Arduino. [en línea]. [Consulta: 17 June 2022]. Disponible en: https://softmany.com/es/arduino/.

SYNACORP, 2019. Door & window magnetic sensor switch for Arduino / IOT / alarm system. [en línea]. [Consulta: 1 June 2022]. Disponible en: https://blogmasterwalkershop.com.br/arquivos/datasheet/Datasheet%20MC-38.pdf.

TVC, 2022. DSC LC100PI, detector de movimiento. [en línea]. [Consulta: 3 June 2022]. Disponible en: https://tvc.mx/products/29913/dsc-lc100pi-detector-de-movimiento-infrarrojo-cableado-ant.

UHPPOTE, 2020. UHPPOTE AC100-240V a 12V/5A fuente de alimentación. [en línea]. [Consulta: 8 June 2022]. Disponible en: https://www.amazon.com/-/es/UHPPOTE-AC100-240V-Alimentaci%C3%B3n-Soporte-respaldo/dp/B07K6DCNPR#productDetails.

UNIT ELECTRONICS, 2016. Sensor vibración módulo KY-002. [en línea]. [Consulta: 6 June 2022]. Disponible en: https://uelectronics.com/producto/modulo-ky-002-sensor-vibracion/.

UNIT ELECTRONICS, 2019. Sensor magnético MC-38. [en línea]. [Consulta: 1 June 2022]. Disponible en: https://uelectronics.com/producto/sensor-magnetico-mc-38/.

VARGAS, A., 2013. *Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida* [en línea]. Tesis. Bogotá: Universidad Militar Nueva Granada. [Consulta: 19 May 2022]. Disponible en: https://sistemamid.com/panel/uploads/biblioteca/2015-03-22_12-17-54117600.pdf.

VÉRTICE S.L, 2011. *Videovigilancia: CCTV usando videos IP* [en línea]. Vértice. Málaga: s.n. [Consulta: 5 January 2022]. Disponible en: https://books.google.es/books?hl=es&lr=&id=xb3mzBE-yIoC&oi=fnd&pg=PA1&dq=videovigilancia&ots=IayL4cVF-G&sig=CchMpkrvatRTLDZn8gWpYcMl-Lc#v=onepage&q=videovigilancia&f=false.

VILLAVICENCIO, M., 2018. *Uso de sensores de movimiento para el ahorro de energía eléctrica en el alumbrado público de la calle galo plaza en el cantón Tosagua* [en línea]. Tesis. Manabí: Universidad Laica "Eloy Alfaro" de Manabí. [Consulta: 31 May 2022]. Disponible en: https://repositorio.uleam.edu.ec/bitstream/123456789/2108/1/ULEAM-IEL-0049.pdf.

VILLEGAS, A., 2013. *Diseño de un detector de sonidos de motosierra con bajo consumo energético* [en línea]. Tesis. Cartago: Instituto Tecnológico de Costa Rica. [Consulta: 31

May 2022]. Disponible en: https://repositoriotec.tec.ac.cr/bitstream/handle/2238/3057/Proyecto%20Detector%20de%20sonidos%20de%20motosierra%20de%20bajo%20consumo%20energ%c3%a9tico.pdf?sequence=1&isAllowed=y.

WE ARE SOCIAL, 2021. Digital 2021 global overview report. [en línea]. [Consulta: 2 January 2022]. Disponible en: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/.

XUKYO, 2021. Uso del lector RFID PN532 con Arduino. [en línea]. [Consulta: 11 June 2022]. Disponible en: https://www.aranacorp.com/es/uso-del-lector-rfid-pn532-con-arduino/.

ANEXOS

ANEXO A: Hoja de datos de la ESP8266 Wemos D1 Mini

7.2 RF Performance

The following are measured under room temperature conditions with 3.3V and 1.1V power supplies.

Description	Min	Typical	Max	Unit
Input frequency	2412		2484	MHz
Input impedance		50		Ω
Input reflection			-10	dB
Output power of PA for 72.2Mbps	14	15	16	dBm
Output power of PA for 11b mode	17.5	18.5	19.5	dBm
Sensitivity				
CCK, 1Mbps		-98		dBm
CCK, 11Mbps		-91		dBm
6Mbps (1/2 BPSK)		-93		dBm
54Mbps (3/4 64-QAM)		-75		dBm
HT20, MCS7 (65Mbps, 72.2Mbps)		-71		dBm
Adjacent Channel Rejection				
OFDM, 6Mbps		37		dB
OFDM, 54Mbps		21		dB
HT20, MCS0		37		dB
HT20, MCS7		20		dB

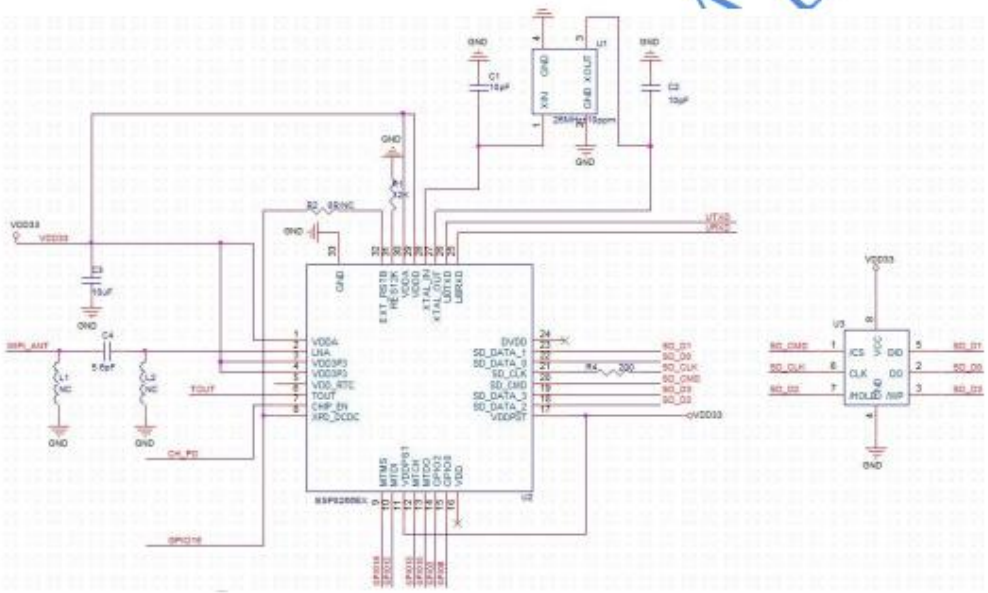
Optional hold functionality can be built into the IO if requested. When the IO is not driven by the internal or external circuitry, the hold functionality can be used to hold the state to the last used state.

The hold functionality introduces some positive feedback into the pad. Hence, the external driver that drives the pad must be stronger than the positive feedback. The required drive strength is however small – in the range of 5uA.

Parameter	Symbol	Min	Max	Unit
Input low voltage	V_{IL}	-0.3	0.25×VIO	V
Input high voltage	V_{IH}	0.75×VIO	3.6	V
Input leakage current	I_{IL}		50	nA
Output low voltage	V_{OL}		0.1×VIO	V
Output high voltage	V_{OH}	0.8×VIO		V
Input pin capacitance	C_{pad}		2	pF
VDDIO	V_{IO}	1.7	3.6	V
Maximum drive capability	I_{MAX}		12	mA
Temperature	T_{amb}	-20	100	°C

All digital IO pins are protected from over-voltage with a snap-back circuit connected between the pad and ground. The snap-back voltage is typically about 6V, and the holding voltage is 5.8V. This provides protection from over-voltages and ESD. The output devices are also protected from reversed voltages with diodes.

4 Application Diagram



ANEXO B: Hoja de datos del sensor magnético MC-38

Door & Window Magnetic Sensor Switch for Arduino / IOT / Alarm System

MC-38 Wired Door Window Sensor | Magnetic Switch | Home Alarm System, Recess able style (which means they can be "set into" for example: a door or window). The MC38 can be wired to your door, or window, any where you want a magnetic sensor to alarm when opened.

Metal shield anti-fire ABS, the alarm sounds when the magnets separated. No external power supply is required-- simply connect to wired or wireless alarm control panel GND and N.C ports directly!

SPECIFICATIONS:

- Connecting Mode: N.C.
- Rated current: 100mA
- Rated voltage: 200VDC
- Operating distance: more than 15mm, less than 25mm
- Rated power: 3W
- Dimension: 28x15x0.9cm
- Cable Length: 30.5cm ± 12mm
- Switch output: normally closed (switch and magnet are together when the switch is closed)

FEATURES:

- Easy installation Reliable performance
- Good characteristic of abrasion-proof
- Best Choice for you to protect family

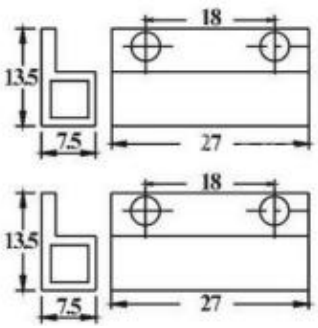
APPLICATION:

- Easy installation Reliable performance
- Good characteristic of abrasion-proof
- Best Choice for you to protect family
- There are two types of reed switches: "normally open" reed switches and "normally closed" reed switches.
- The metal reeds on a normally open switch stay open when there is no magnet near the switch. In the presence of a magnetic field, the contacts of a normally-open reed switch will close. A normally-closed reed switch is closed when it is not near a magnet; as a magnet is brought close to it, a normally-closed switch will open

PIN-OUTS:

The switch is non polar, so you can plug in the wires in any way.

DIMENSIONS (MM):



ANEXO C: Hoja de datos del sensor de movimiento DSC LC-100-PI

DSC
De Tyco Security Products

Detector PIR digital inmune a mascotas
LC-100-PI

Características que hacen la diferencia:

- Contacto de alarma Forma 'A' y pulsador de sabotaje
- Análisis digital de señal
- Diseño estético de bajo perfil
- Presentado en plástico ABS para protección contra impactos
- Excepcional inmunidad a luz blanca
- Inmunidad a mascotas de hasta 25 Kg (55 lbs)
- Tecnología Quad Linear Imaging para un análisis detallado de las dimensiones de los cuerpos y diferenciación de fondos y mascotas
- Compacto diseño electrónico avanzado basado en ASIC para instalaciones residenciales
- Conteo de pulsos regulable
- Ajuste de sensibilidad del PIR
- Altura de montaje libre de calibración
- Disponible en cajas de 6 unidades (LC-100-PI-6PK)

Ya sea una instalación residencial o comercial, los dispositivos de detección de la serie LC preparan para lo inesperado a los sistemas de seguridad brindando protección para cada ambiente, rincón y pasillo.

El LC-100-PI combina efectivamente desempeño con precio competitivo. El detector presenta análisis inteligente de señal para una detección confiable, inmunidad a mascotas de hasta 55 libras (25 kg) y diseño de bajo perfil que se adapta a cualquier decorado.

Protección confiable

El procesamiento avanzado basado en ASIC brinda una detección superior y a la vez rechazo a falsas alarmas ayudando a mantener seguros a personas y bienes. La tecnología Quad Linear Imaging permite un análisis preciso de las dimensiones de los cuerpos y diferenciación de fondos y mascotas.

Procesamiento digital de señal

Una efectiva detección de movimiento depende de la habilidad del sensor para identificar intrusos y proveer una verdadera resistencia a falsas alarmas. La serie LC de dispositivos de detección ubica intrusos con exactitud gracias a su procesamiento digital de la señal. La información digital es analizada con mayor precisión usando software y no está sujeta a degradación de la señal causada por amplificación, ruido, distorsión o recorte de la señal.

Inmunidad a mascotas

Los sensores de alta precisión tienen la capacidad de brindar detección de calidad y al mismo tiempo ignorar mascotas de hasta 25 Kg (55 lb) de peso.

Rápida y fácil instalación

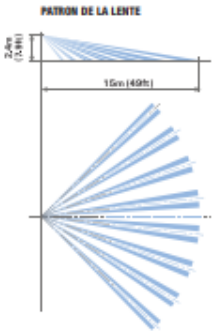
Una vez que el detector ha sido instalado a la altura de montaje recomendada, los instaladores simplemente deben realizar una breve prueba de detección (prueba de caminar), efectuar los ajustes necesarios y la unidad quedará lista para funcionar. Los LEDs altamente visibles pueden verse a simple vista y ayudan al instalador a determinar el rango de detección desde cualquier distancia o ángulo dentro del patrón de cobertura.

Ubicación del detector

Cuando elija una ubicación para el detector asegúrese de considerar lo siguiente:

- No oriente el detector hacia superficies reflectivas
- Evite ubicaciones expuestas a corrientes de aire directas
- No ubique el detector en lugares con luz solar directa o reflejada
- No lo ubique cerca de grandes obstrucciones que puedan limitar su área de cobertura

Patrón de cobertura



Calibración del rango de detección

El rango de detección del detector de movimiento es graduable desde 16' a 49' (5 m a 15 m). Posee un potenciómetro que puede girarse en sentido horario o antihorario para aumentar o disminuir respectivamente el rango. Para un óptimo funcionamiento, el rango debe ser calibrado para cubrir en forma efectiva las dimensiones del área a proteger.

Especificaciones

Dimensiones	(92 mm x 62.5 mm x 40 mm) 3.62" x 2.46" x 1.57"
Peso	58 g (2.04 oz)
Método de detección	PIR Quad (Cuatro elementos)
Entrada de alimentación	9.6 a 16 VCC
Consumo de corriente (en reposo)	8 mA (± 5%)
Consumo de corriente (activo)	12 mA (± 5%)
Interruptor antisabotaje:	
Valores nominales de contactos	0.1 Amper @ 28 VCC
Protección RFI	10 V/m más 80% AM de 80 a 2000 MHz

ANEXO D: Hoja de datos del sensor de vibración KY-002

Modulo Sensor de Vibracion KY-002 para Arduino

Codigo: **110932**

Descripción

Este módulo permitirá detectar de forma fácil, rápida y precisa vibración producida en el lugar en el cual este se encuentre, posee un sensor el cual tiene la capacidad de detectar las diversas vibraciones producidas en un ambiente,por ello lo puedes anclar literalmente a cualquier cosa y saber cuándo esta se mueve o se golpea. este módulo es compatible con Arduino o con cualquier Microcontrolador que posea un pin de 5 Volts.

Este módulo sensor de vibraciones funciona como un Switch, al detectar una vibración cierra un circuito lo que genera que el usuario pueda detectar los movimientos.

Especificaciones:

- Voltaje de funcionamiento: 3.3V ~ 5V
- interruptor digital salida (0 / 1)
- Material: PCB
- Dimensiones: 2.4x1.5x0.9

ANEXO E: Hoja de datos del módulo RFID/NFC PN532

PN532/C1

Near Field Communication (NFC) controller

Rev. 3.6 — 28 November 2017 Product data sheet
115436 COMPANY PUBLIC

1. General description

The PN532 is a highly integrated transceiver module for contactless communication at 13.56 MHz based on the 80C51 microcontroller core. It supports 6 different operating modes:

- ISO/IEC 14443A/MIFARE Reader/Writer
- FeliCa Reader/Writer
- ISO/IEC 14443B Reader/Writer
- ISO/IEC 14443A/MIFARE Card MIFARE Classic 1K or MIFARE Classic 4K card emulation mode
- FeliCa Card emulation
- ISO/IEC 18092, ECMA 340 Peer-to-Peer

The PN532 implements a demodulator and decoder for signals from ISO/IEC 14443A/MIFARE compatible cards and transponders. The PN532 handles the complete ISO/IEC 14443A framing and error detection (Parity & CRC).

The PN532 supports MIFARE Classic 1K or MIFARE Classic 4K card emulation mode. The PN532 supports contactless communication using MIFARE Higher transfer speeds up to 424 kbit/s in both directions.

The PN532 can demodulate and decode FeliCa coded signals. The PN532 handles the FeliCa framing and error detection. The PN532 supports contactless communication using FeliCa Higher transfer speeds up to 424 kbit/s in both directions.

The PN532 supports layers 2 and 3 of the ISO/IEC 14443 B Reader/Writer communication scheme, except anticollision. This must be implemented in firmware as well as upper layers.

In card emulation mode, the PN532 is able to answer to a Reader/Writer command either according to the FeliCa or ISO/IEC 14443A/MIFARE card interface scheme. The PN532 generates the load modulation signals, either from its transmitter or from the LOADMOD pin driving an external active circuit. A complete secure card functionality is only possible in combination with a secure IC using the NFC-WI/S^{2}C interface.

Compliant to ECMA 340 and ISO/IEC 18092 NFCIP-1 Passive and Active communication modes, the PN532 offers the possibility to communicate to another NFCIP-1 compliant device, at transfer speeds up to 424 kbit/s.The PN532 handles the complete NFCIP-1 framing and error detection.

The PN532 transceiver can be connected to an external antenna for Reader/Writer or Card/PICC modes, without any additional active component.

3. Applications

- Mobile and portable devices
- Consumer applications

4. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{BAT}	battery supply voltage			2.7	-	5.5	V
ICV_{DD}	LDO output voltage	V_{BAT} > 3.4 V V_{SS} = 0 V	[1]	2.7	3	3.4	V
PV_{DD}	Supply voltage for host interface	V_{SS} = 0 V		1.6	-	3.6	V
SV_{DD}	Output voltage for secure IC interface	V_{SS} = 0 V (SV_{DD} Switch Enabled)		DV_{DD} -0.5	-	DV_{DD}	V
I_{HPD}	Hard-Power-Down current consumption	V_{BAT} = 5 V		-	-	2	µA
I_{SPD}	Soft-Power-Down current consumption	V_{BAT} = 5 V, RF level detector on		-	-	45	µA
I_{DVDD}	Digital supply current	V_{BAT} = 5 V, SV_{DD} switch off	[3]	-	25	-	mA
I_{SVDD}	SV_{DD} load current	V_{BAT} = 5 V, SV_{DD} switch on		-	-	30	mA
I_{AVDD}	Analog supply current	V_{BAT} = 5 V		-	6	-	mA
I_{TVDD}	Transmitter supply current	During RF transmission, V_{BAT} = 5 V		-	60[3]	150[4]	mA
P_{tot}	Continuous total power dissipation	T_{amb} = -30 to +85 °C	[2]	-	-	0.5	W
T_{amb}	ambient temperature			-30	-	+85	°C

[1] DV_{DD}, AV_{DD} and TV_{DD} must always be at the same supply voltage
[2] The total current consumption depends on the firmware version (different internal IC clock speed)
[3] With an antenna tuned at 50 Ω at 13.56 MHz
[4] The antenna should be tuned not to exceed this current limit (the detuning effect when coupling with another device must be taken into account)

ANEXO F: Hoja de datos de la cerradura magnética ZE-280-5T

Código: ZE.280.5T

CERRADURA ELECTROMAGNÉTICA **ZE-280-5T**

Neto: 37.72 EUR Bruto: 46.40 EUR

Cerradura electromagnética simple superficial. Con un diseño simple y la moderna tecnología de fabricación, es un dispositivo fiable para bloquear las puertas y los portones. Para forzar la entrada cerrada por la cerradura, debe usar la fuerza de > 280 kg. Funciona de una manera reversible - está abierta en ausencia de la tensión de alimentación. La cerradura está constituida por dos elementos: el electroimán (normalmente montado en el bastidor) y la placa de la cerradura (normalmente montada en la puerta). El funcionamiento libre de errores de la cerradura es un resultado de la falta de elementos mecánicos que después de un cierto tiempo están sujetos a daños. El dispositivo está diseñado para su uso en interiores.

ESPECIFICACIONES

Capacidad de carga:	280 kg
Voltaje nominal:	12 V DC / 24 V DC
Consumo de energía:	500 mA / 250 mA
Algunas características:	• Indicación LED; • Salida NO/NC para indicar la apertura de la puerta; • Retardo ajustable de cierre de la cerradura : 0 s ... 32 s - Ajuste con potenciómetro de precisión
Peso:	1.73 kg (total)
Dimensiones:	• 250 x 47 x 28 mm (CERRADURA ELECTROMAGNÉTICA) • 180 x 38 x 12 mm (placa de metal)
Garantía:	2 años

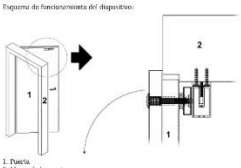
PRESENTACIÓN

Vista interior:

El retardo de la alimentación de la cerradura se puede ajustar con el potenciómetro en el rango de 0 ... 32s

Dimensiones:

Esquema de funcionamiento del dispositivo:



1. Puerta
2. Marco de la puerta

Debe prestarse atención a las almohadillas de goma montadas entre la puerta y el elemento móvil de la cerradura. Estas almohadillas garantizan el correcto montaje de los elementos de la cerradura cuando la puerta está cerrada.

Incluido:

DELTA-OPTI Monika Matysiak; https://www.delta.poznan.pl
POL; 60-713 Poznań; Graniczna 10
e-mail: delta-opti@delta.poznan.pl; tel: +(48) 61 864 69 60

DELTA-OPTI Monika Matysiak; https://www.delta.poznan.pl
POL; 60-713 Poznań; Graniczna 10
e-mail: delta-opti@delta.poznan.pl; tel: +(48) 61 864 69 60

ANEXO G: Hoja de datos de la batería Rekoser RKE12-7

REKOSER

RKE12-7

12V7Ah @ 20HR

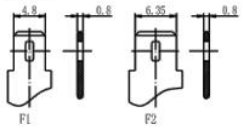
Rekoser AGM Battery for General Purpose

AGM Battery. Rekoser stationary series, general use, has been specially designed to optimize its life and quality, minimizing maintenance and maximizing self discharge of their properties for longer storage. RKE series is ideal for security and alarm systems, UPS systems,emergency light systems and other small backup applications.

ISO9001 ISO14001 CE

Complied standards
- IEC 60896-21/22
- JIS C8704
- GB/T19639

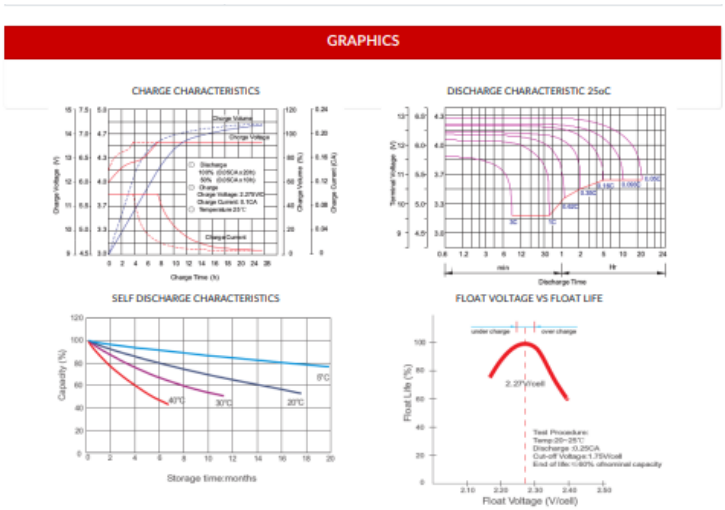
Terminal



SPECIFICATIONS				
Nominal Voltage	12V			
Capacity (25°C)	7Ah @ 20HR			
Internal Resistance	Fully Charged 25 m Ω			
Self Discharge	3% of capacity declined per month at 25°C			
Cell number	6 cells			
Capacity Affected by Temperature	102% (40°C)	100% (25°C)	85% (0°C)	65% (-15°C)
Charge Voltage (25°C)	Cycle - 14.6-14.8V (-30mV/C), max. Current 2.1A		Float - 13.6-13.8V (-20mV/C)	
Max. Charge Current	2.1A			
Max. Discharge Current	105A			

DIMENSIONS AND WEIGHT	
Dimensions (mm)	151x65x93(99)
Weight (kgs)	2.1

CONSTRUCTION	
Component	Raw Material
Positive	Lead dioxide
Negative	Lead

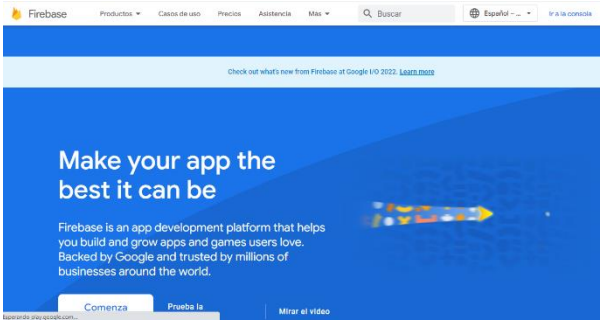


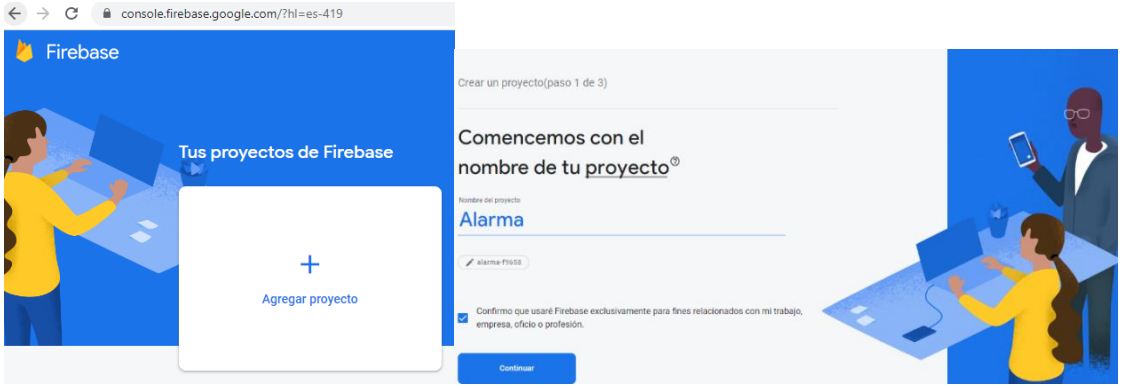
Negative	Lead
Container	ABS (Flame Retardant Optional)
Cover	ABS (Flame Retardant Optional)
Sealant	Epoxy Resin
Safety Valve	Rubber
Terminal	Copper
Separator	Fibre Glass
Electrolyte	Sulphuric acid

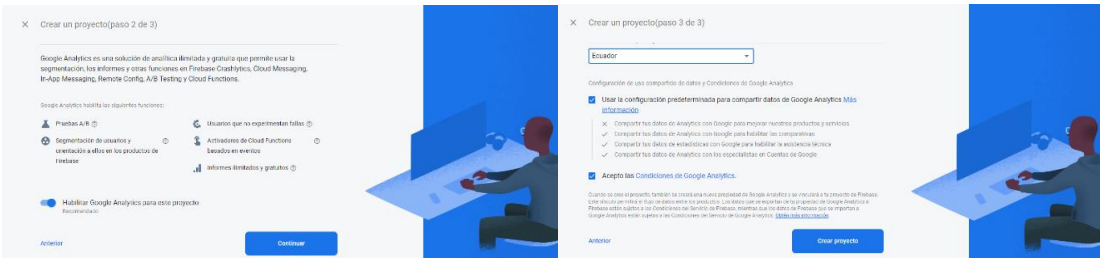
CONSTANT DISCHARGE RATINGS (A, W) AT 25°C

F.V / Time	5MIN		10MIN		15MIN		30MIN		1HR		3HR		5HR		10HR		20HR	
11.10 V	17.5A	32.9W	13.7A	26.0W	11.6A	22.2W	7.13A	13.7W	4.25A	8.24W	1.84A	3.62W	1.19A	2.3W	0.65A	1.29W	0.33A	0.67W
10.80 V	19.8A	36.6W	14.5A	27.3W	11.9A	22.5W	7.28A	13.9W	4.31A	8.28W	1.86A	3.63W	1.2A	2.35W	0.66A	1.3W	0.34A	0.68W
10.50 V	22.1A	40.3W	15.4A	28.5W	12.2A	22.8W	7.41A	14.0W	4.4A	8.38W	1.89A	3.65W	1.21A	2.36W	0.67A	1.31W	0.35A	0.69W
10.20 V	24.2A	43.7W	16.1A	29.5W	12.5A	23.2W	7.58A	14.2W	4.48A	8.46W	1.91A	3.66W	1.23A	2.37W	0.68A	1.32W	0.36A	0.7W
10.02 V	26.1A	46.5W	16.8A	30.5W	12.8A	23.6W	7.71A	14.3W	4.55A	8.53W	1.93A	3.67W	1.24A	2.38W	0.69A	1.33W	0.36A	0.71W
9.60 V	28.1A	49.4W	17.4A	31.3W	13.3A	24.2W	7.9A	14.6W	4.61A	8.59W	1.95A	3.68W	1.26A	2.4W	0.7A	1.34W	0.37A	0.72W

ANEXO H: Creación de base de datos en Firebase

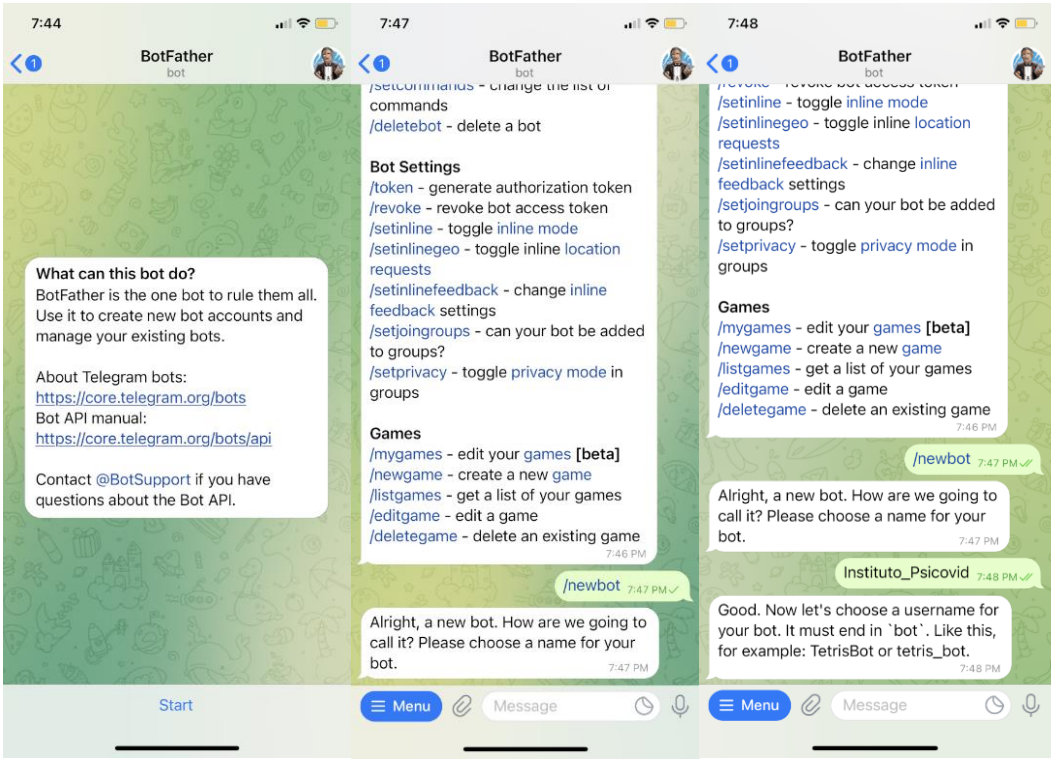


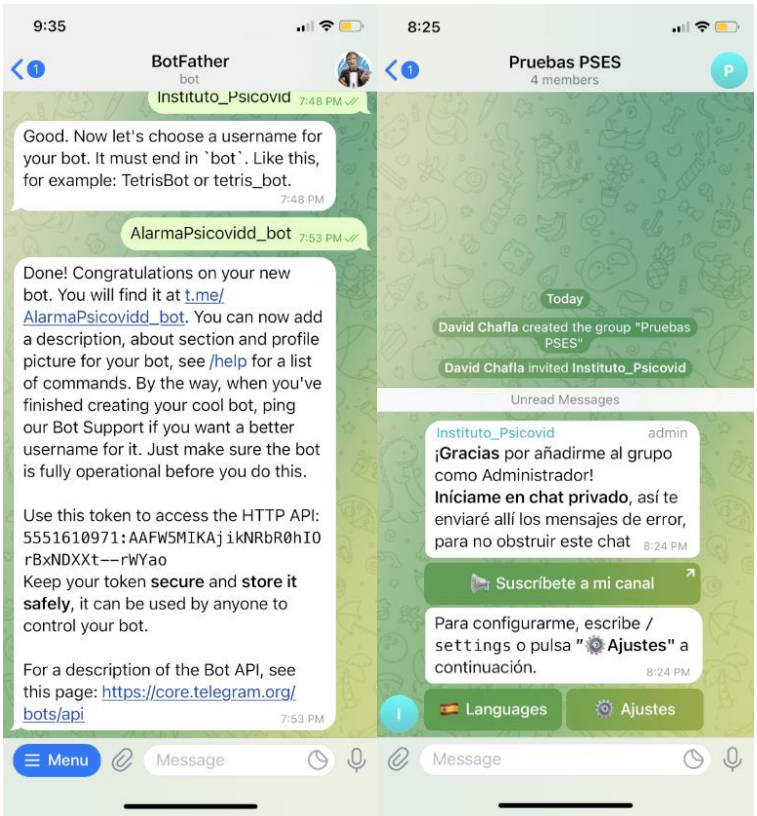



Crear un proyecto(paso 2 de 3)
Google Analytics es una solución de analítica ilimitada y gratuita que permite usar la segmentación, los informes y otras funciones en Firebase Crashlytics, Cloud Messaging, In-App Messaging, Remote Config, A/B Testing y Cloud Functions.
Habilitar Google Analytics para este proyecto
Anterior
Continuar
Crear un proyecto(paso 3 de 3)
Ecuador
Usar la configuración predeterminada para compartir datos de Google Analytics
Acepto las Condiciones de Google Analytics.
Anterior
Crear proyecto


https://alarma-428b3-default-rtdb.firebase
BASE
ALARMA: "APAGADA"
CERRADURA: "OFF"
GOLPE1: "OFF"
GOLPE2: "OFF"
MAGNETICO1: "ON"
MAGNETICO2: "OFF"
NFC: "915019443"
NOMBRE: ""
PRESENCIA1: "OFF"
PRESENCIA2: "OFF"
SIRENA: "OFF"
USUARIOS
USUARIOS
BB1siQunWLSudMLg94Na6b2dZop2
VvchEPwfKHboMnwCxolKOd9phxr1
xgtqKc3459QUImA7h1VoJktBI9t2
apellido: "Chafla"
cedula: "0605729656"
codigo: "915019443"
estadoConexion: "ACTIVO"
nombre: "David"
telefono: "0995525500"
uri: "android.resource://com.exam

ANEXO I: Creación de bot Telegram





ANEXO J: Programa en Arduino IDE para el módulo de adquisición de datos 1

```
#include "DFRobotDFPlayerMini.h"   //Libreria mp3
#include "SoftwareSerial.h"


// NFC
#include <Wire.h>                  //I2C library
#include <PN532_I2C.h>             //Libreria NFC para conexión I2C
#include "PN532.h"                 //Libreria NFC
#include <NfcAdapter.h>            //Libreria NFC

PN532_I2C pn532i2c(Wire);                     //Crea objeto del NFC
PN532 nfc(pn532i2c);



// TELEGRAM
#define BOT_TOKEN "5214361087:AAFrVH2pbWC-R_DVrh-8GPr2CdWYRAkpTzQ"
#include <FastBot.h>
FastBot bot(BOT_TOKEN);
#define CHAT_ID "-1001630083714"


#if defined(ESP32)
#include <WiFi.h>
#include <FirebaseESP32.h>
#elif defined(ESP8266)
#include <ESP8266WiFi.h>
#include <FirebaseESP8266.h>
#endif

// Provide the RTDB payload printing info and other helper functions.
#include <addons/RTDBHelper.h>

/* 1. Define the WiFi credentials */
#define WIFI_SSID "RED WIFI PSICOVID"
#define WIFI_PASSWORD "12345678"

/* 2. Define the RTDB URL */
#define DATABASE_URL "alarma-428b3-default-rtdb.firebaseio.com"
//<databaseName>.firebaseio.com or
<databaseName>.<region>.firebasedatabase.app

/* 3. Define the Firebase Data object */
FirebaseData fbdo;
FirebaseData stream;

/* 4, Define the FirebaseAuth data for authentication data */
FirebaseAuth auth;

/* Define the FirebaseConfig data for config data */
FirebaseConfig config;


DFRobotDFPlayerMini myDFPlayer;

SoftwareSerial mySoftwareSerial(D5, D6); // RX, TX

#define buzzer D8
#define verde  D4
#define azul   D0

  .

   size_t numChild = sizeof(childPath) / sizeof(childPath[0]);

   for (size_t i = 0; i < numChild; i++)
   {
     if (stream.get(childPath[i]))
     {

       if (stream.type.equals("json"))
         {


           if (stream.dataPath.indexOf("USUARIOS") > 0) {

               String valorCortado = String(stream.dataPath);
               valorCortado =  valorCortado.substring(10,
valorCortado.length());

               list_ID[contadorlista3] = valorCortado;
               contadorlista3++;

               Serial.println("dato cortado: " + valorCortado);

             }
         }
       if (stream.dataPath.equals("/USUARIOS")) {


         if (stream.type.equals("json"))
         {


           boolean existeID = false;

           FirebaseJson json = stream.value ;

           size_t len = json.iteratorBegin();
           FirebaseJson::IteratorValue value;
           for (size_t i = 0; i < len; i++)
           {

               value = json.valueAt(i);

               if (value.key != "apellido" && value.key != "cedula" &&
value.key != "codigo" && value.key != "estadoConexion" && value.key !=
"nombre" && value.key != "telefono" && value.key != "uri") {


                   if (value.key.length() > 0) {

                     for (size_t i = 0; i < tamano; i++)
                     {

                       if (list_ID[i] == value.key) {

                         existeID = true;
                         break;
                       }
```

```
#define rojo   D7


boolean registro = false;   // true registra, false lee para puerta

String tarjetaActual;
String tarjetaSiguiente;


/*
    FIREBASE
*/
boolean inicioNFC = false;

const int tamano = 15;
String list_ID[tamano];
String list_NFC[tamano];// guarda todos los id registrados
String list_ENABLE[tamano];// si el usuario tiene acceso o no

String list_NOMBRE[tamano];// si el usuario tiene acceso o no
String list_APELLIDO[tamano];// si el usuario tiene acceso o no


String stringActual;
String stringSiguiente;


String nombreUsuario;


int contadorlista1 = 0;
int contadorlista2 = 0;
int contadorlista3 = 0;
int contadorlista4 = 0;
int contadorlista5 = 0;


boolean estadoPuerta = false;
boolean estadoNombre = false;

boolean estadoAlarma = false;

int contadorConsulta = 0;


unsigned long previousMillis = 0;        // will store last time LED
was updated

// constants won't change:
const long interval = 1500;           // interval at which to blink
(milliseconds)


String parentPath = "/BASE";
String childPath[2] = {"/DISPOSITIVOS", "/USUARIOS"};



// Global function that handles stream data
void streamCallback(MultiPathStreamData stream)


                     if (!existeID) {
                       list_ID[contadorlista3] = value.key;
                       contadorlista3++;
                     }
                   }

               }


                   if (!existeID) {


       if (value.key.equals("codigo")) {

         list_NFC[contadorlista1] = value.value.substring(1,
value.value.length()-1);
         contadorlista1++;

       }

       if (value.key.equals("estadoConexion")) {

         list_ENABLE[contadorlista2] = value.value.substring(1,
value.value.length()-1);
         contadorlista2++;

       }

       if (value.key.equals("nombre")) {

         list_NOMBRE[contadorlista4] = value.value.substring(1,
value.value.length()-1);
         contadorlista4++;

       }


       if (value.key.equals("apellido")) {

         list_APELLIDO[contadorlista5] = value.value.substring(1,
value.value.length()-1);
         contadorlista5++;

       }

     }


               Serial.printf("%d, Type: %s, Name: %s, Value: %s\n", i,
value.type == FirebaseJson::JSON_OBJECT ? "object" : "array",
value.key.c_str(), value.value.c_str());
           }
```

ANEXO K: Programa en Arduino IDE para el módulo de adquisición de datos 2

```
// TELEGRAM
#define BOT_TOKEN "5214361087:AAFrVH2pbWC-R_DVrh-8GPr2CdWYRAkpTzQ"
#include <FastBot.h>
FastBot bot(BOT_TOKEN);
#define CHAT_ID "-1001630083714"



#if defined(ESP32)
#include <WiFi.h>
#include <FirebaseESP32.h>
#elif defined(ESP8266)
#include <ESP8266WiFi.h>
#include <FirebaseESP8266.h>
#endif

// Provide the RTDB payload printing info and other helper functions.
#include <addons/RTDBHelper.h>

/* 1. Define the WiFi credentials */
#define WIFI_SSID "RED WIFI PSICOVID"
#define WIFI_PASSWORD "12345678"

/* 2. Define the RTDB URL */
#define DATABASE_URL "alarma-428b3-default-rtdb.firebaseio.com"
//<databaseName>.firebaseio.com or
<databaseName>.<region>.firebasedatabase.app

/* 3. Define the Firebase Data object */
FirebaseData fbdo;
FirebaseData stream;

/* 4, Define the FirebaseAuth data for authentication data */
FirebaseAuth auth;

/* Define the FirebaseConfig data for config data */
FirebaseConfig config;

#define presencia D1
#define ledwifi   D7


boolean estadoAlarma = false;

boolean estadoPresencia          = false;
boolean estadoPresenciaSiguiente = false;



  // Global function that handles stream data
void streamCallback(StreamData data)
{

  Serial.printf("sream path, %s\nevent path, %s\ndata type, %s\nevent
type, %s\n\n",
                data.streamPath().c_str(),
                data.dataPath().c_str(),
                data.dataType().c_str(),
                data.eventType().c_str());
  printResult(data); // see addons/RTDBHelper.h

Serial.println();

pinMode(presencia, INPUT_PULLUP);
pinMode(ledwifi, OUTPUT);

digitalWrite(ledwifi, LOW);


WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  Serial.print("Connecting to Wi-Fi");
  while (WiFi.status() != WL_CONNECTED)
  {
      Serial.print(".");
      delay(300);
  }
  Serial.println();
  Serial.print("Connected with IP: ");
  Serial.println(WiFi.localIP());
  Serial.println();

  Serial.printf("Firebase Client v%s\n\n", FIREBASE_CLIENT_VERSION);

  /* Assign the certificate file (optional) */
  // config.cert.file = "/cert.cer";
  // config.cert.file_storage = StorageType::FLASH;

  /* Assign the database URL(required) */
  config.database_url = DATABASE_URL;

  config.signer.test_mode = true;

  /**
   Set the database rules to allow public read and write.

     {
        "rules": {
            ".read": true,
            ".write": true
        }
      }

  */

  Firebase.reconnectWiFi(true);

  /* Initialize the library with the Firebase authen and config */
  Firebase.begin(&config, &auth);



  Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/PRESENCIA1",
"OFF");


  // Recommend for ESP8266 stream, adjust the buffer size to match
your stream data size
  #if defined(ESP8266)
    stream.setBSSLBufferSize(2048 /* Rx in bytes, 512 - 16384 */,
512 /* Tx in bytes, 512 - 16384 */);
  #endif
  Serial.println();

  Serial.printf("Received stream payload size: %d (Max. %d)\n\n",
data.payloadLength(), data.maxPayloadLength());


  if(data.dataPath() ==  "/ALARMA"){

     if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

        if(data.to<String>() =="APAGADA"){

          estadoAlarma = false;
          Serial.println("ALARMA APAGADA");

          Serial.printf("SET GOLPE1... %s\n",
Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/PRESENCIA1", "OFF")
? "ok" : fbdo.errorReason().c_str());

        }


        if(data.to<String>() =="ENCENDIDA"){

          estadoAlarma = true;
          Serial.println("ALARMA ENCENDIDA");

        }

      }
    }



  }

  // Global function that notifies when stream connection lost
  // The library will resume the stream connection automatically
  void streamTimeoutCallback(bool timeout)
  {
    if(timeout){
      // Stream timeout occurred
      Serial.println("Stream timeout, resume streaming...");
    }

    if (!stream.httpConnected()){
      Serial.printf("error code: %d, reason: %s\n\n", stream.httpCode(),
stream.errorReason().c_str());
    }

  }



  void setup() {

    Serial.begin(115200);


  if (!Firebase.beginStream(stream, "/BASE/DISPOSITIVOS"))
  {
    // Could not begin stream connection, then print out the error
detail
    Serial.println(stream.errorReason());
  }

  Firebase.setStreamCallback(stream, streamCallback,
streamTimeoutCallback);


   bot.setChatID(CHAT_ID);
   bot.sendMessage("NODO SENSOR 2 LISTO");

//myBot.sendMessage(-1001630083714, "MODULO CENTRAL WiFi
LISTO");    // el numero -1001630083714 es el id del grupo

Serial.println("LISTOOOO");

}



void loop() {

  if (WiFi.status() != WL_CONNECTED) {

    digitalWrite(ledwifi, LOW);

  }

  else
  {

    digitalWrite(ledwifi, HIGH);

    estadoPresencia = digitalRead(presencia);

 if(estadoAlarma){


    if (estadoPresenciaSiguiente != estadoPresencia) {

      estadoPresenciaSiguiente = estadoPresencia;

      if (estadoPresenciaSiguiente) {
            Serial.printf("SET PRESENCIA1... %s\n",
Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/PRESENCIA1", "ON") ?
"ok" : fbdo.errorReason().c_str());

      }
```

ANEXO L: Programa en Arduino IDE para el módulo de adquisición de datos 3

```
void setup() {

  Serial.begin(115200);
  Serial.println();

  pinMode(magnetico, INPUT_PULLUP);
  pinMode(golpe, INPUT);
  pinMode(ledwifi, OUTPUT);

  digitalWrite(ledwifi, LOW);



  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
    Serial.print("Connecting to Wi-Fi");
    while (WiFi.status() != WL_CONNECTED)
    {
        Serial.print(".");
        delay(300);
    }
    Serial.println();
    Serial.print("Connected with IP: ");
    Serial.println(WiFi.localIP());
    Serial.println();

    Serial.printf("Firebase Client v%s\n\n\n", FIREBASE_CLIENT_VERSION);

    /* Assign the certificate file (optional) */
    // config.cert.file = "/cert.cer";
    // config.cert.file_storage = StorageType::FLASH;

    /* Assign the database URL(required) */
    config.database_url = DATABASE_URL;

    config.signer.test_mode = true;

    /**
     Set the database rules to allow public read and write.

        {
          "rules": {
              ".read": true,
              ".write": true
          }
        }

    */

    Firebase.reconnectWiFi(true);

    /* Initialize the library with the Firebase authen and config */
    Firebase.begin(&config, &auth);



                  data.dataPath().c_str(),
                  data.dataType().c_str(),
                  data.eventType().c_str());
    printResult(data); // see addons/RTDBHelper.h
    Serial.println();

    Serial.printf("Received stream payload size: %d (Max. %d)\n\n",
  data.payloadLength(), data.maxPayloadLength());


    if(data.dataPath() ==  "/ALARMA"){

        if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

            if(data.to<String>() =="APAGADA"){

              estadoAlarma = false;
              Serial.println("ALARMA APAGADA");

              Serial.printf("SET GOLPE1... %s\n",
  Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/GOLPE1", "OFF") ?
  "ok" : fbdo.errorReason().c_str());
              Serial.printf("SET MAGNETICO2... %s\n",
  Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/MAGNETICO2", "OFF")
  ? "ok" : fbdo.errorReason().c_str());

            }


            if(data.to<String>() =="ENCENDIDA"){

              estadoAlarma = true;
              Serial.println("ALARMA ENCENDIDA");

            }

        }
      }



  }

  // Global function that notifies when stream connection lost
  // The library will resume the stream connection automatically
  void streamTimeoutCallback(bool timeout)
  {
    if(timeout){
      // Stream timeout occurred
      Serial.println("Stream timeout, resume streaming...");
    }

    if (!stream.httpConnected()){
      Serial.printf("error code: %d, reason: %s\n\n", stream.httpCode(),
  stream.errorReason().c_str());
    }
```

```
// TELEGRAM
#define BOT_TOKEN "5214361087:AAFrVH2pbWC-R_DVrh-8GFr2CdWYRAkpTzQ"
#include <FastBot.h>
FastBot bot(BOT_TOKEN);
#define CHAT_ID "-1001630083714"



#if defined(ESP32)
#include <WiFi.h>
#include <FirebaseESP32.h>
#elif defined(ESP8266)
#include <ESP8266WiFi.h>
#include <FirebaseESP8266.h>
#endif

// Provide the RTDB payload printing info and other helper functions.
#include <addons/RTDBHelper.h>

/* 1. Define the WiFi credentials */
/* 1. Define the WiFi credentials */
#define WIFI_SSID "RED WIFI PSICOVID"
#define WIFI_PASSWORD "12345678"

/* 2. Define the RTDB URL */
#define DATABASE_URL "alarma-428b3-default-rtdb.firebaseio.com"
//<databaseName>.firebaseio.com or
<databaseName>.<region>.firebasedatabase.app

/* 3. Define the Firebase Data object */
FirebaseData fbdo;
FirebaseData stream;

/* 4, Define the FirebaseAuth data for authentication data */
FirebaseAuth auth;

/* Define the FirebaseConfig data for config data */
FirebaseConfig config;

#define magnetico D1  // EN LA PLACA REAL COLOCA D1
#define golpe     D2
#define ledwifi   D7


boolean estadoAlarma = false;

boolean estadoMagnetico          = false;
boolean estadoMagneticoSiguiente = false;
boolean estadoGolpe              = false;
boolean estadoGolpeSiguiente     = false;



  // Global function that handles stream data
void streamCallback(StreamData data)
{

  Serial.printf("sream path, %s\nevent path, %s\ndata type, %s\nevent
type, %s\n\n\n",
                data.streamPath().c_str(),



    Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/MAGNETICO2",
"OFF");
    Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/GOLPE1", "OFF");


    // Recommend for ESP8266 stream, adjust the buffer size to match
your stream data size
    #if defined(ESP8266)
      stream.setBSSLBufferSize(2048 /* Rx in bytes, 512 - 16384 */,
512 /* Tx in bytes, 512 - 16384 */);
    #endif


    if (!Firebase.beginStream(stream, "/BASE/DISPOSITIVOS"))
    {
      // Could not begin stream connection, then print out the error
detail
      Serial.println(stream.errorReason());
    }

    Firebase.setStreamCallback(stream, streamCallback,
streamTimeoutCallback);


     bot.setChatID(CHAT_ID);
     bot.sendMessage("NODO SENSOR 1 LISTO");

  //myBot.sendMessage(-1001630083714, "MODULO CENTRAL WiFi
LISTO");    // el numero -1001630083714 es el id del grupo

  Serial.println("LISTOOOO");

}



void loop() {

  if (WiFi.status() != WL_CONNECTED) {

    digitalWrite(ledwifi, LOW);

  }

  else
  {

    digitalWrite(ledwifi, HIGH);

    estadoMagnetico = digitalRead(magnetico);
    estadoGolpe = digitalRead(golpe);


    if(estadoAlarma){


      if (estadoMagneticoSiguiente != estadoMagnetico) {

      estadoMagneticoSiguiente = estadoMagnetico;

      if (estadoMagneticoSiguiente) {
```

ANEXO M: Programa en Arduino IDE para el módulo de adquisición de datos 4

```
// TELEGRAM
#define BOT_TOKEN "5214361087:AAFrVH2pbWC-R_DVrh-8GPr2CdWYRAkpTzQ"
#include <FastBot.h>
FastBot bot(BOT_TOKEN);
#define CHAT_ID "-1001630083714"



#if defined(ESP32)
#include <WiFi.h>
#include <FirebaseESP32.h>
#elif defined(ESP8266)
#include <ESP8266WiFi.h>
#include <FirebaseESP8266.h>
#endif

// Provide the RTDB payload printing info and other helper functions.
#include <addons/RTDBHelper.h>

/* 1. Define the WiFi credentials */
#define WIFI_SSID "RED WIFI PSICOVID"
#define WIFI_PASSWORD "12345678"


/* 2. Define the RTDB URL */
#define DATABASE_URL "alarma-428b3-default-rtdb.firebaseio.com"
//<databaseName>.firebaseio.com or
<databaseName>.<region>.firebasedatabase.app

/* 3. Define the Firebase Data object */
FirebaseData fbdo;
FirebaseData stream;

/* 4, Define the FirebaseAuth data for authentication data */
FirebaseAuth auth;

/* Define the FirebaseConfig data for config data */
FirebaseConfig config;

#define presencia D1
#define golpe     D2
#define ledwifi   D7


boolean estadoAlarma = false;

boolean estadoPresencia          = false;
boolean estadoPresenciaSiguiente = false;
boolean estadoGolpe              = false;
boolean estadoGolpeSiguiente     = false;




  // Global function that handles stream data
void streamCallback(StreamData data)
{

  Serial.printf("sream path, %s\nevent path, %s\ndata type, %s\nevent
type, %s\n\n",


   void setup() {

    Serial.begin(115200);
    Serial.println();

    pinMode(presencia, INPUT_PULLUP);
    pinMode(golpe, INPUT_PULLUP);
    pinMode(ledwifi, OUTPUT);

    digitalWrite(ledwifi, LOW);



   WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
      Serial.print("Connecting to Wi-Fi");
      while (WiFi.status() != WL_CONNECTED)
      {
          Serial.print(".");
          delay(300);
      }
      Serial.println();
      Serial.print("Connected with IP: ");
      Serial.println(WiFi.localIP());
      Serial.println();

      Serial.printf("Firebase Client v%s\n\n", FIREBASE_CLIENT_VERSION);

      /* Assign the certificate file (optional) */
      // config.cert.file = "/cert.cer";
      // config.cert.file_storage = StorageType::FLASH;

      /* Assign the database URL(required) */
      config.database_url = DATABASE_URL;

      config.signer.test_mode = true;

      /**
       Set the database rules to allow public read and write.

          {
            "rules": {
                ".read": true,
                ".write": true
            }
          }

      */

      Firebase.reconnectWiFi(true);

      /* Initialize the library with the Firebase authen and config */
      Firebase.begin(&config, &auth);
                data.streamPath().c_str(),
                data.dataPath().c_str(),
                data.dataType().c_str(),
                data.eventType().c_str());
  printResult(data); // see addons/RTDBHelper.h
  Serial.println();

  Serial.printf("Received stream payload size: %d (Max. %d)\n\n",
data.payloadLength(), data.maxPayloadLength());


  if(data.dataPath() ==  "/ALARMA"){

     if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

         if(data.to<String>() =="APAGADA"){

          estadoAlarma = false;
          Serial.println("ALARMA APAGADA");

          Serial.printf("SET GOLPE2... %s\n",
Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/GOLPE2", "OFF") ?
"ok" : fbdo.errorReason().c_str());
          Serial.printf("SET PRESENCIA2... %s\n",
Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/PRESENCIA2", "OFF")
? "ok" : fbdo.errorReason().c_str());

        }


        if(data.to<String>() =="ENCENDIDA"){

          estadoAlarma = true;
          Serial.println("ALARMA ENCENDIDA");

        }

      }
    }



}

// Global function that notifies when stream connection lost
// The library will resume the stream connection automatically
void streamTimeoutCallback(bool timeout)
{
  if(timeout){
    // Stream timeout occurred
    Serial.println("Stream timeout, resume streaming...");
  }

  if (!stream.httpConnected()){
    Serial.printf("error code: %d, reason: %s\n\n", stream.httpCode(),
stream.errorReason().c_str());
  }


}


      Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/PRESENCIA2",
  "OFF");
      Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/GOLPE2", "OFF");


      // Recommend for ESP8266 stream, adjust the buffer size to match
  your stream data size
      #if defined(ESP8266)
        stream.setBSSLBufferSize(2048 /* Rx in bytes, 512 - 16384 */,
  512 /* Tx in bytes, 512 - 16384 */);
      #endif


      if (!Firebase.beginStream(stream, "/BASE/DISPOSITIVOS"))
      {
        // Could not begin stream connection, then print out the error
  detail
        Serial.println(stream.errorReason());
      }

      Firebase.setStreamCallback(stream, streamCallback,
  streamTimeoutCallback);


       bot.setChatID(CHAT_ID);
       bot.sendMessage("NODO SENSOR 3 LISTO");

    //myBot.sendMessage(-1001630083714, "MODULO CENTRAL WiFi
  LISTO");    // el numero -1001630083714 es el id del grupo

    Serial.println("LISTOOOO");

  }


  void loop() {

    if (WiFi.status() != WL_CONNECTED) {

      digitalWrite(ledwifi, LOW);

    }

    else
    {

      digitalWrite(ledwifi, HIGH);


      estadoPresencia = digitalRead(presencia);
      estadoGolpe = digitalRead(golpe);


    if(estadoAlarma){

       if (estadoPresenciaSiguiente != estadoPresencia) {

        estadoPresenciaSiguiente = estadoPresencia;
```

ANEXO N: Programa en Arduino IDE para el módulo de control y actuación

```
// TELEGRAM
#define BOT_TOKEN "5214361087:AAFrVH2pbWC-R_DVrh-8GPr2CdWYRAkpTzQ"
#include <FastBot.h>
FastBot bot(BOT_TOKEN);
#define CHAT_ID "-1001630083714"



#if defined(ESP32)
#include <WiFi.h>
#include <FirebaseESP32.h>
#elif defined(ESP8266)
#include <ESP8266WiFi.h>
#include <FirebaseESP8266.h>
#endif

// Provide the RTDB payload printing info and other helper functions.
#include <addons/RTDBHelper.h>

/* 1. Define the WiFi credentials */
#define WIFI_SSID "RED WIFI PSICOVID"
#define WIFI_PASSWORD "12345678"

/* 2. Define the RTDB URL */
#define DATABASE_URL "alarma-428b3-default-rtdb.firebaseio.com"
//<databaseName>.firebaseio.com or
<databaseName>.<region>.firebasedatabase.app

/* 3. Define the Firebase Data object */
FirebaseData fbdo;
FirebaseData stream;

/* 4, Define the FirebaseAuth data for authentication data */
FirebaseAuth auth;

/* Define the FirebaseConfig data for config data */
FirebaseConfig config;

unsigned long dataMillis = 0;
int count = 0;

volatile bool dataChanged = false;

#define sirena     D0
#define cerradura  D1
#define boton      D4
#define magnetico  D2

boolean estadoBoton              = false;
boolean estadoBotonSiguiente     = false;
boolean estadoAlarma             = false;
boolean estadoMagnetico          = false;
boolean estadoMagneticoSiguiente = false;
boolean estadoCerradura          = false;
boolean estadoCerraduraSiguiente = false;
boolean evento                   = false;


unsigned long previousMillis = 0;        // will store last time LED
was updated


              if(data.to<String>() =="OFF"){
               Serial.println("MAGNETICO 1 OFF");
              }
            }
          }

           if(data.dataPath() ==  "/MAGNETICO2"){

           if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

               if(data.to<String>() =="ON"){
                evento = true;

                Serial.println("MAGNETICO 2 ON");
                bot.sendMessage("SE DETECTO MOVIMIENTO EN: SENSOR MAGNETICO
      2");

              }

               if(data.to<String>() =="OFF"){
                Serial.println("MAGNETICO 2 OFF");
              }
            }
          }


           if(data.dataPath() ==  "/GOLPE1"){

           if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

               if(data.to<String>() =="ON"){
                evento = true;

                Serial.println("GOLPE 1 ON");
                bot.sendMessage("SE DETECTO MOVIMIENTO EN: SENSOR GOLPE
      1");

              }

               if(data.to<String>() =="OFF"){
                Serial.println("GOLPE 1 OFF");
              }
            }
          }

          if(data.dataPath() ==  "/GOLPE2"){

           if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

               if(data.to<String>() =="ON"){
                evento = true;

                Serial.println("GOLPE 2 ON");
                bot.sendMessage("SE DETECTO MOVIMIENTO EN: SENSOR GOLPE
      2");

              }
```

```
// constants won't change:
const long interval = 1200;           // interval at which to blink
(milliseconds)



  // Global function that handles stream data
void streamCallback(StreamData data)
{

  Serial.printf("sream path, %s\nevent path, %s\ndata type, %s\nevent
type, %s\n\n",
                data.streamPath().c_str(),
                data.dataPath().c_str(),
                data.dataType().c_str(),
                data.eventType().c_str());
  printResult(data); // see addons/RTDBHelper.h
  Serial.println();

  Serial.printf("Received stream payload size: %d (Max. %d)\n\n",
data.payloadLength(), data.maxPayloadLength());


  if(data.dataPath() ==  "/CERRADURA"){

     if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

         if(data.to<String>() =="ON"){
          Serial.println("ABRI LA PUERTA");

          digitalWrite(cerradura, HIGH);
          delay(1000);
          digitalWrite(cerradura, LOW);

          Serial.printf("SET CERRADURA... %s\n",
Firebase.setStringAsync(fbdo, "/BASE/DISPOSITIVOS/CERRADURA", "OFF") ?
"ok" : fbdo.errorReason().c_str());

        }

      }
    }



    if(data.dataPath() ==  "/MAGNETICO1"){

    if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

        if(data.to<String>() =="ON"){

         evento = true;

         Serial.println("MAGNETICO 1 ON");
         bot.sendMessage("SE DETECTO MOVIMIENTO EN: SENSOR MAGNETICO
1");
       }


         if(data.to<String>() =="OFF"){
          Serial.println("GOLPE 2 OFF");
         }
       }
     }


    if(data.dataPath() ==  "/PRESENCIA1"){

     if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

         if(data.to<String>() =="ON"){

          evento = true;

          Serial.println("PRESENCIA 1 ON");
          bot.sendMessage("SE DETECTO MOVIMIENTO EN: SENSOR PRESENCIA
1");

         }

         if(data.to<String>() =="OFF"){
          Serial.println("PRESENCIA 1 OFF");
         }
       }
     }


     if(data.dataPath() ==  "/PRESENCIA2"){

     if (data.dataTypeEnum() == fb_esp_rtdb_data_type_string){

         if(data.to<String>() =="ON"){
          evento = true;

          Serial.println("PRESENCIA 2 ON");
          bot.sendMessage("SE DETECTO MOVIMIENTO EN: SENSOR PRESENCIA
2");

         }

         if(data.to<String>() =="OFF"){
          Serial.println("PRESENCIA 2 OFF");
         }
       }
     }

  dataChanged = true;

}

// Global function that notifies when stream connection lost
// The library will resume the stream connection automatically
void streamTimeoutCallback(bool timeout)
{
  if(timeout){
    // Stream timeout occurred
    Serial.println("Stream timeout, resume streaming...");
  }
```

ANEXO O: Programación realizada para el desarrollo de la App móvil orientada al control de acceso

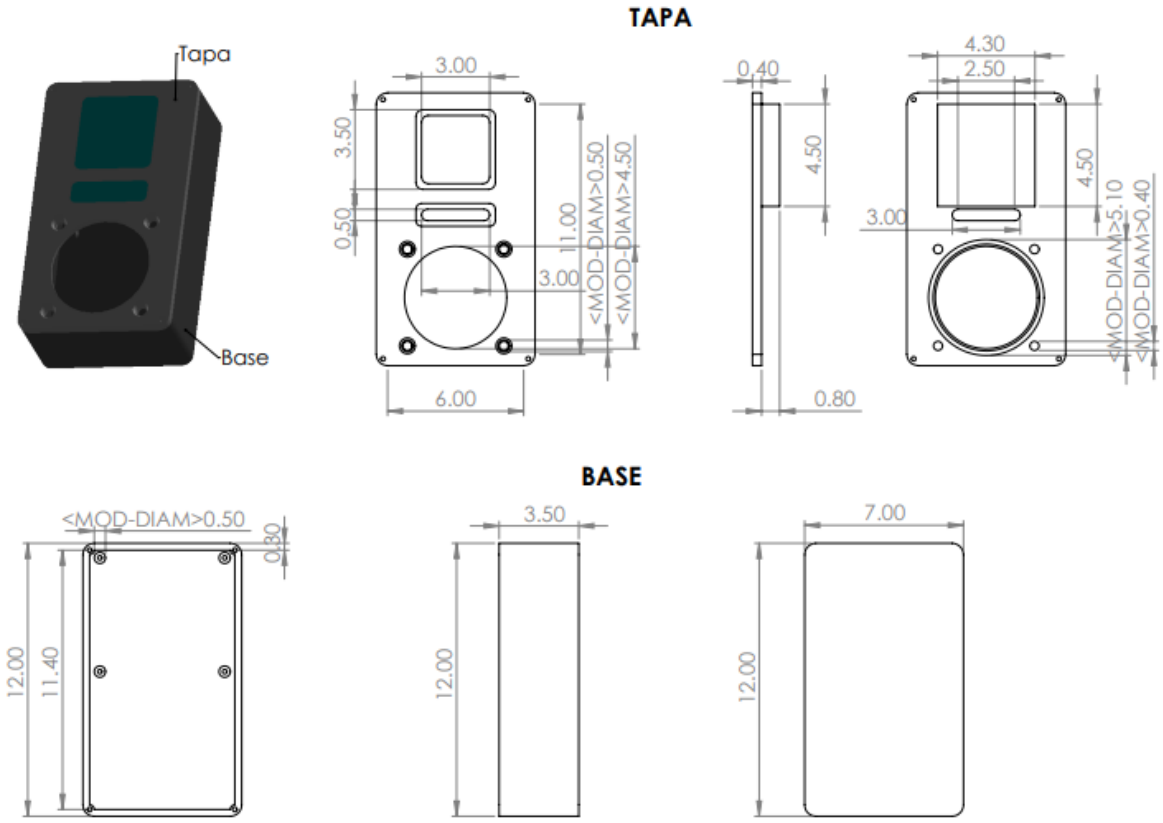
```
<?xml version="1.0" encoding="utf-8"?>
<RelativeLayout
xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:padding="16dp"
    tools:context=".intro">


    <ImageView
        android:id="@+id/titulo1"
        android:layout_width="300dp"
        android:layout_height="55dp"
        android:layout_centerHorizontal="true"
        android:background="@drawable/tituloletras"
        android:paddingLeft="8dp"
        android:paddingEnd="8dp"></ImageView>

    <View
        android:id="@+id/view1"
        android:layout_width="match_parent"
        android:layout_height="5dp"
        android:background="@color/purple_700"
        android:layout_below="@+id/titulo1"
        android:layout_marginTop="5dp">
    </View>


    <LinearLayout
        android:id="@+id/linear1"
        android:layout_width="match_parent"
        android:layout_height="100dp"
        android:orientation="horizontal"
        android:layout_below="@id/view1"
        android:layout_centerHorizontal="true"
        >


        <ImageView
            android:layout_width="100dp"
            android:layout_height="100dp"
            android:layout_weight="1"
            app:srcCompat="@drawable/msello"
            tools:ignore="ContentDescription" />

        <ImageView
            android:layout_width="100dp"
            android:layout_height="100dp"
            android:layout_weight="1"
            app:srcCompat="@drawable/sellocelectronica"
            tools:ignore="ContentDescription" />


    </LinearLayout>


    <com.airbnb.lottie.LottieAnimationView

        android:id="@+id/animation_view"
```

```
package com.example.appnfc;
import android.content.Intent;
import android.os.Build;
import android.os.Bundle;
import android.speech.tts.TextToSpeech;
import android.view.WindowManager;
import androidx.annotation.RequiresApi;
import androidx.appcompat.app.AppCompatActivity;
import java.util.Locale;
import java.util.Timer;
import java.util.TimerTask;
public class intro extends AppCompatActivity {

    private static final long SPLASH_TIME=4500;
    TextToSpeech tts;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_intro);


getWindow().setFlags(WindowManager.LayoutParams.FLAG_FULLSCREEN,
WindowManager.LayoutParams.FLAG_FULLSCREEN);

        tts = new TextToSpeech(getApplicationContext(), new
TextToSpeech.OnInitListener() {
            @RequiresApi(api = Build.VERSION_CODES.LOLLIPOP)
            @Override
            public void onInit(int status) {
                if (status != TextToSpeech.ERROR) {
                    Locale locSpanish = new Locale("spa", "MEX");
                    tts.setLanguage(locSpanish);
                    tts.speak("Sistema de seguridad con redes
sociales", TextToSpeech.QUEUE_FLUSH, null, null);
                }
            }
        });


        TimerTask task= new TimerTask() {
            @Override
            public void run() {
                startActivity(new Intent(intro.this, login.class));
                finish();
            }
        };
        Timer timer=new Timer();
        timer.schedule(task,SPLASH_TIME);
    }
```

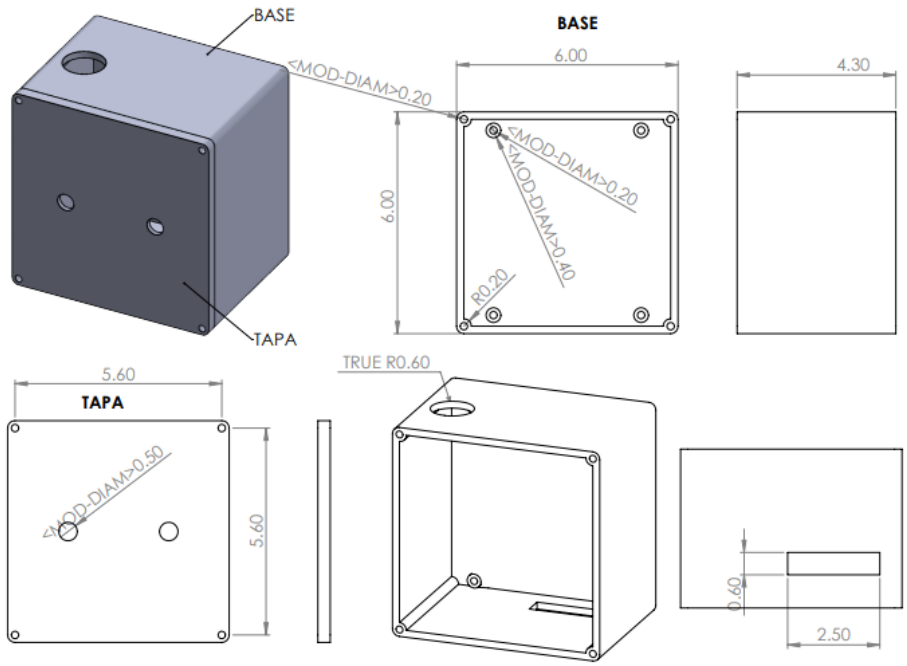
```
<?xml version="1.0" encoding="utf-8"?>
<RelativeLayout
xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:background="@color/md_grey_100"
    tools:context=".activityPerfil"
    >

    <androidx.appcompat.widget.Toolbar
        android:id="@+id/toolbar"
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:background="@android:color/transparent"

app:navigationIcon="@drawable/ic_back"></androidx.appcompat.widget.Too
lbar>

    <RelativeLayout
        android:id="@+id/relativeCuenta"
        android:layout_width="match_parent"
        android:layout_height="match_parent"
        android:layout_below="@+id/toolbar"
        >


        <ScrollView
            android:layout_width="match_parent"
            android:layout_height="match_parent"
            android:orientation="vertical"
            android:fillViewport="true"
            android:fitsSystemWindows="true"
            >


            <RelativeLayout
                android:layout_width="match_parent"
                android:layout_height="match_parent"

                >


                <View
                    android:layout_width="match_parent"
                    android:layout_height="200dp"
                    android:background="@color/md_red_400" />



                <TextView
                    android:layout_width="wrap_content"
                    android:layout_height="wrap_content"
                    android:layout_marginTop="20dp"
                    android:layout_marginLeft="20dp"
                    android:textColor="@color/white"
                    android:textSize="30dp"
                    android:text="CUENTA"
                    android:layout_gravity="center_horizontal"
```

```
package com.example.appnfc;


import android.Manifest;
import android.app.ActivityManager;
import android.app.AlertDialog;
import android.app.ProgressDialog;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.DialogInterface;
import android.content.Intent;
import android.content.IntentFilter;
import android.content.SharedPreferences;
import android.content.pm.PackageManager;
import android.graphics.Bitmap;
import android.graphics.Matrix;
import android.media.MediaPlayer;
import android.net.ConnectivityManager;
import android.net.NetworkInfo;
import android.net.Uri;
import android.os.Build;
import android.os.Bundle;
import android.provider.MediaStore;
import android.text.TextUtils;
import android.util.Base64;
import android.util.Log;
import android.view.Menu;
import android.view.MenuItem;
import android.view.View;
import android.widget.Button;
import android.widget.ImageView;
import android.widget.RelativeLayout;
import android.widget.TextView;
import android.widget.Toast;


import androidx.annotation.Nullable;
import androidx.appcompat.app.AppCompatActivity;
import androidx.core.app.ActivityCompat;


import com.bumptech.glide.Glide;
import
com.google.android.material.bottomnavigation.BottomNavigationView;
import com.google.android.material.textfield.TextInputEditText;
import com.google.firebase.auth.FirebaseAuth;
import com.google.firebase.auth.FirebaseUser;
import com.google.firebase.database.DataSnapshot;
import com.google.firebase.database.DatabaseError;
import com.google.firebase.database.DatabaseReference;
import com.google.firebase.database.FirebaseDatabase;
import com.google.firebase.database.ValueEventListener;
import com.google.firebase.database.annotations.NotNull;
import com.google.firebase.storage.FirebaseStorage;
import com.google.firebase.storage.StorageReference;


import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.util.HashMap;
import java.util.Map;


import de.hdodenhof.circleimageview.CircleImageView;
```

ANEXO P: Plano estructural del módulo de adquisición de datos orientado al control de acceso

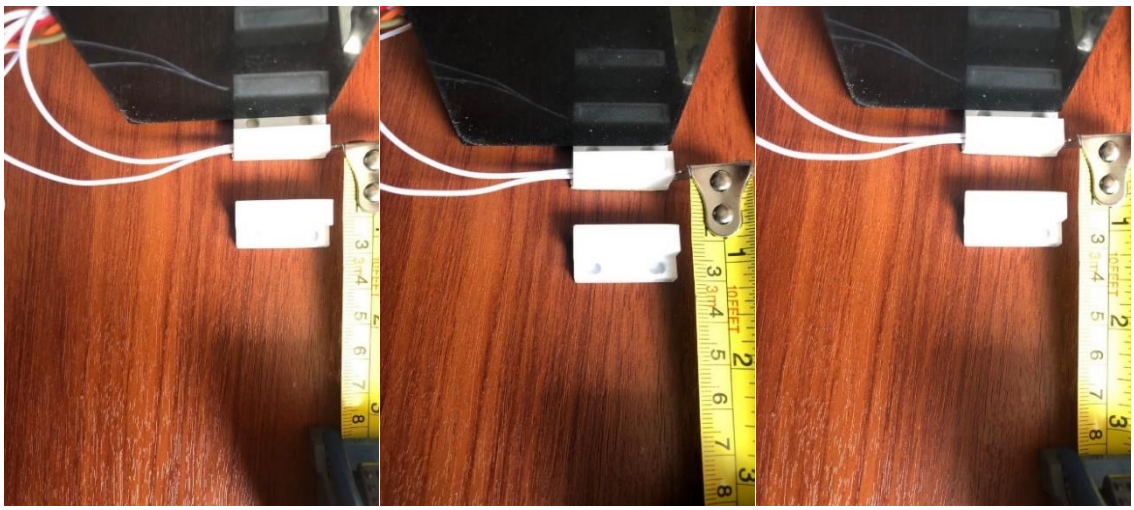


ANEXO Q: Plano estructural del módulo de adquisición de datos orientado al sistema de alarma

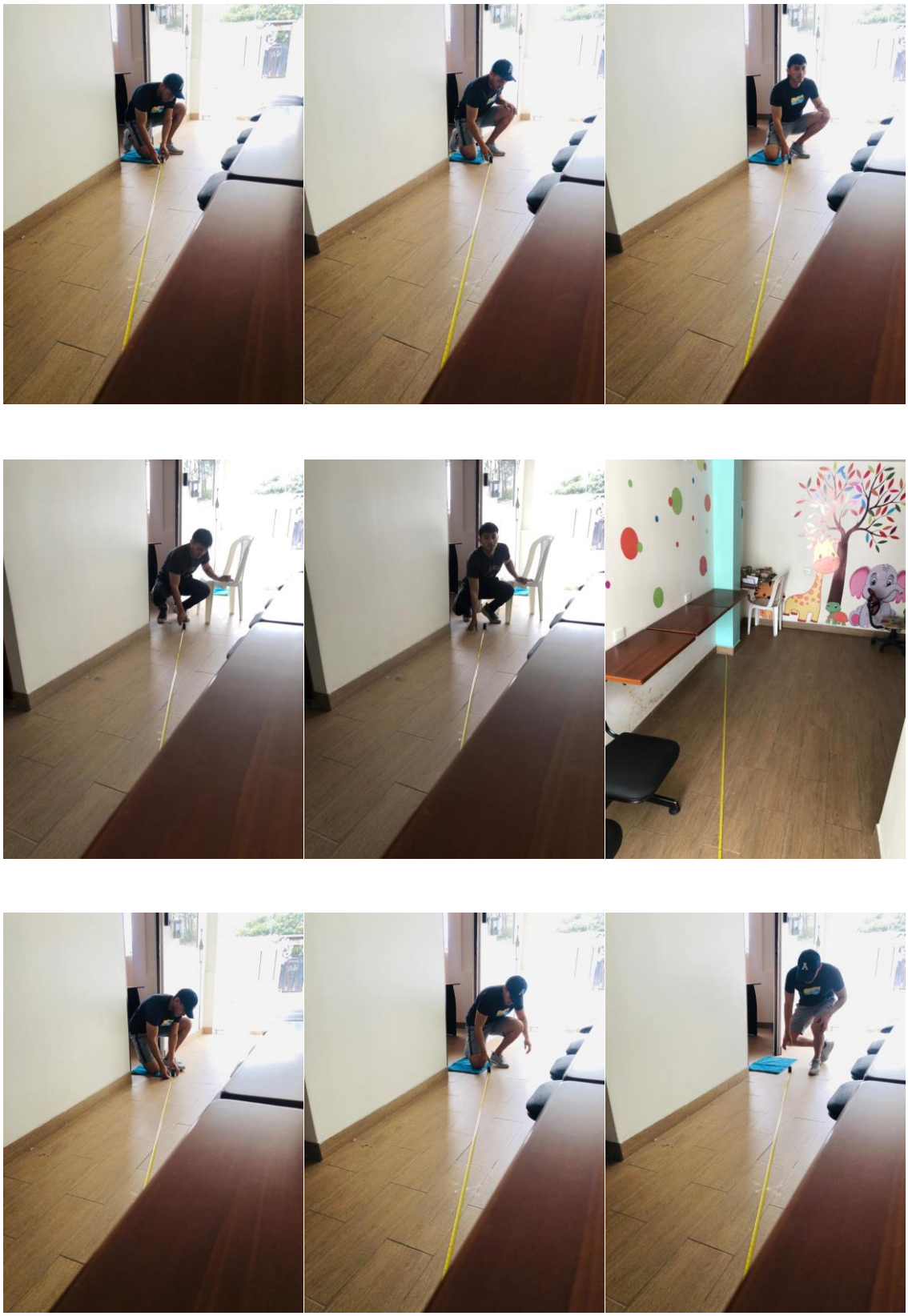


ANEXO R: Evidencia del marco de análisis e interpretación de resultados

Pruebas de distancia de activación para los sensores magnéticos 1 y 2.



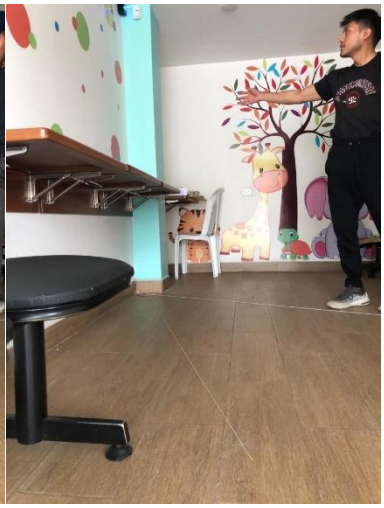
Pruebas al sensor de movimiento 1, respecto a su distancia mínima de detección.



Pruebas al sensor de movimiento 1, respecto a su ángulo de detección.

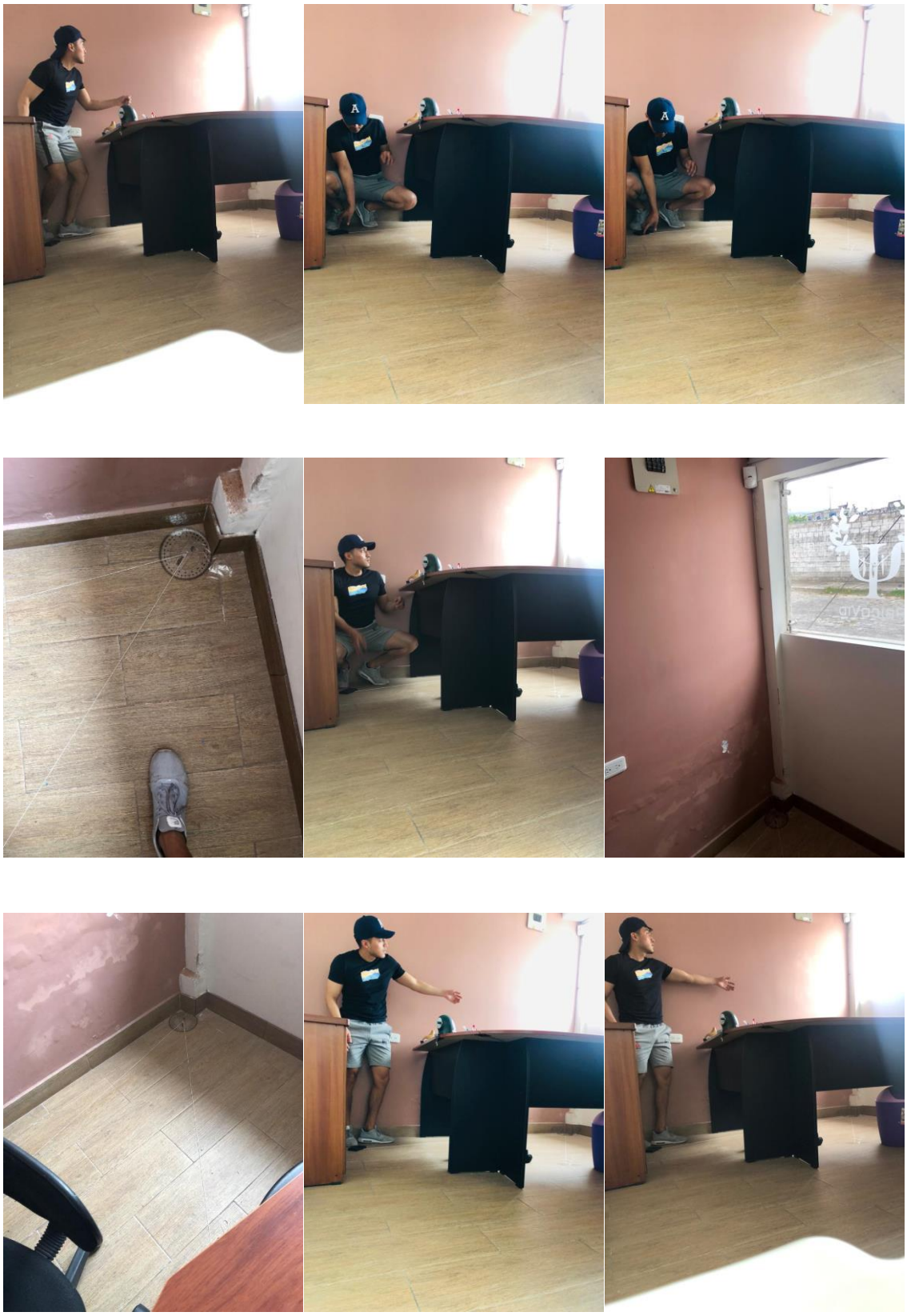




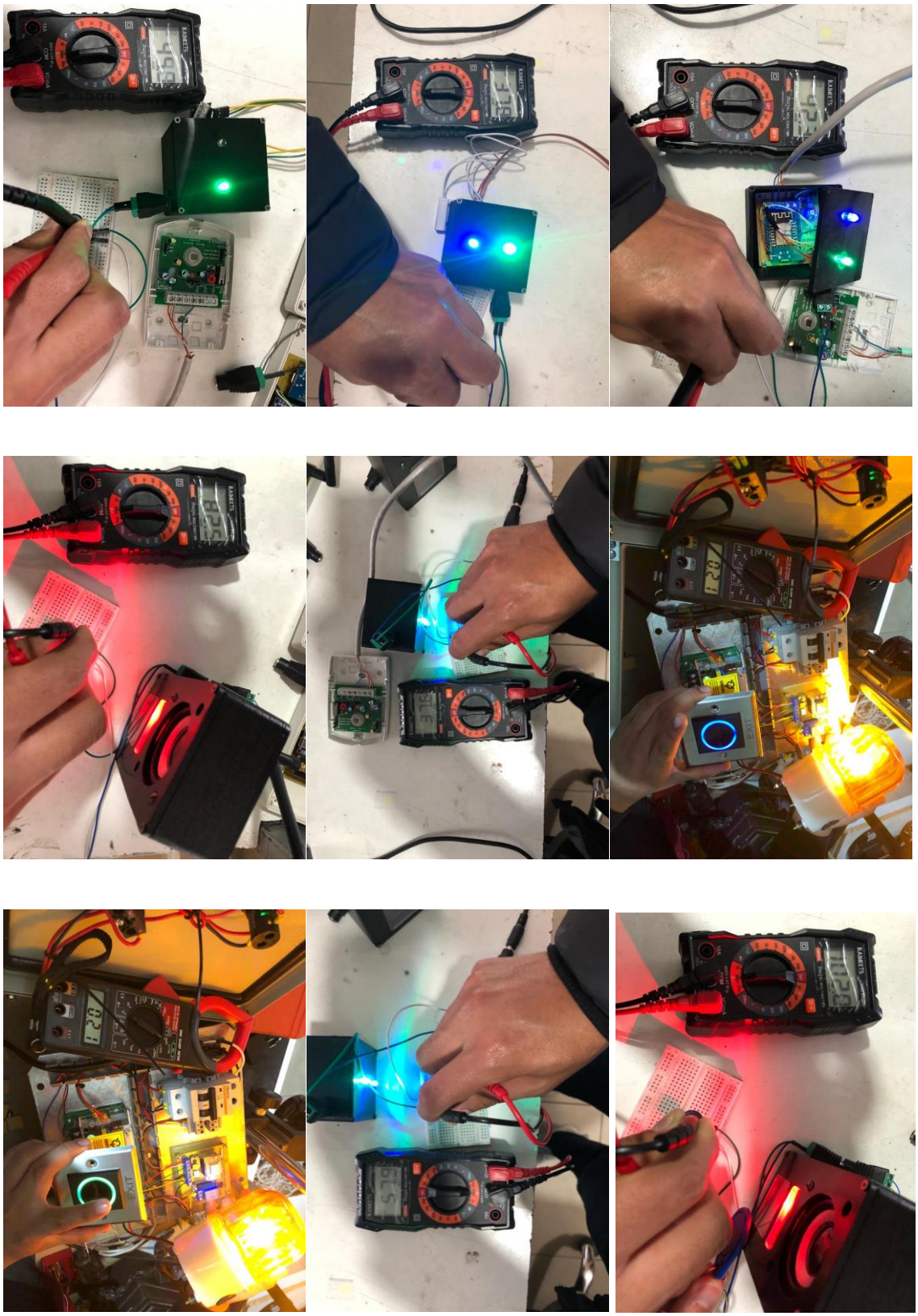

Pruebas al sensor de movimiento 2, respecto a su distancia mínima de detección.

Pruebas al sensor de movimiento 2, respecto a sus grados de detección.

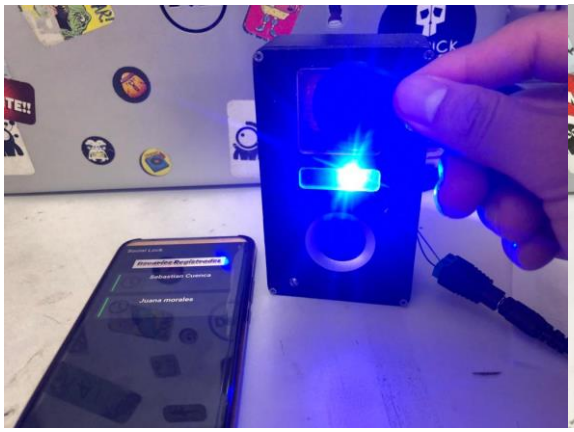


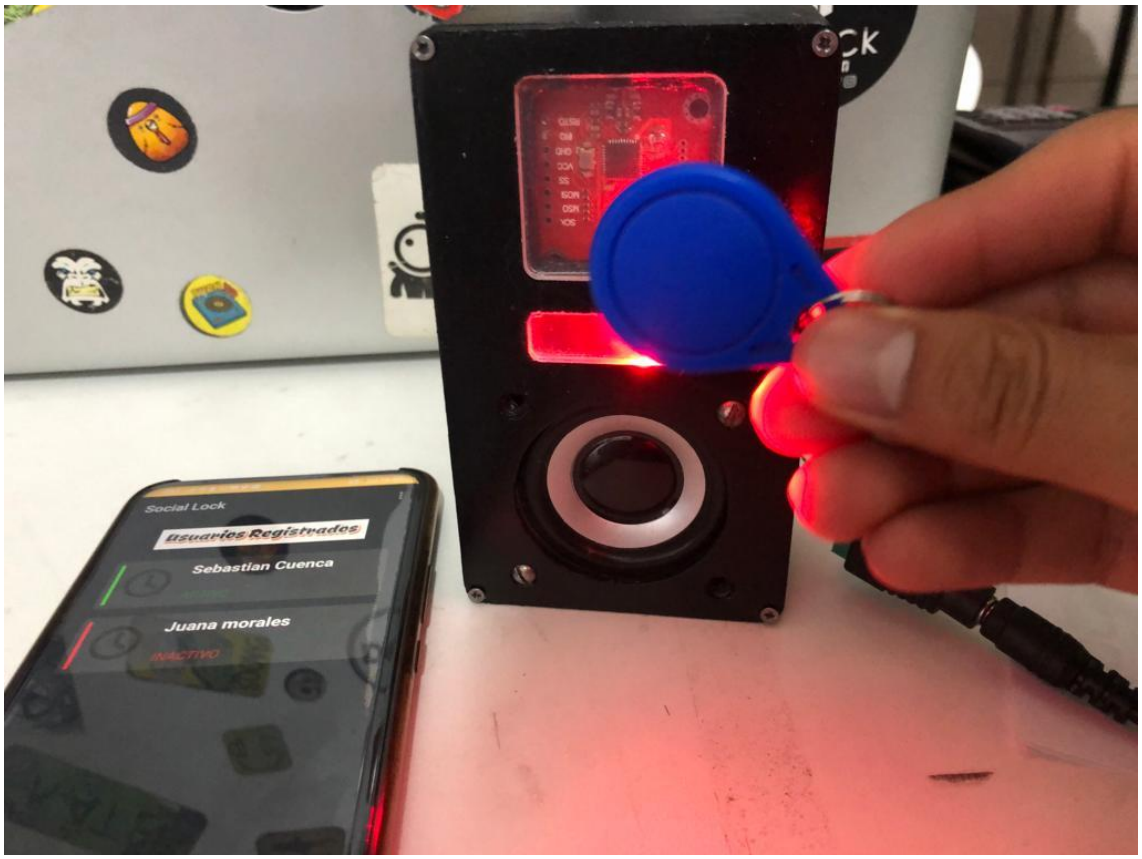
Pruebas activación de los sensores de vibración 1 y 2.

Pruebas de consumo de corriente.



Pruebas de lecturas NFC y registro de usuarios para el control de acceso.





ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 19 / 10 / 2022

INFORMACIÓN DE LOS AUTORES
Nombres – Apellidos: HERNÁN DAVID CHAFLA POMA
INFORMACIÓN INSTITUCIONAL
Facultad: INFORMÁTICA Y ELECTRÓNICA
Carrera: ELECTRÓNICA Y AUTOMATIZACIÓN
Título a optar: INGENIERO EN ELECTRÓNICA Y AUTOMATIZACIÓN
f. Analista de Biblioteca responsable: Ing. Fernanda Arévalo M.