UCC UNIVERSIDAD CATÓLICA DE CÓRDOBA JESUITAS | Sistema de Bibliotecas

PRODUCCIÓN ACADÉMICA

Galmes, Francisco

Misa López, Carolina

Centralización del sistema de alarmas de seguridad de la Universidad Católica de Córdoba

Tesis para la obtención del título de grado de Ingeniero Electrónico y en Sistemas

Director: Castagnola, Juan Luis

Documento disponible para su consulta y descarga en Biblioteca Digital - Producción Académica, repositorio institucional de la Universidad Católica de Córdoba, gestionado por el Sistema de Bibliotecas de la UCC.

Esta obra está bajo una licencia de Creative Commons Reconocimiento-No Comercial-Sin Obra Derivada 4.0 Internacional.

UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

TRABAJO FINAL

INGENIERÍA ELECTRÓNICA
INGENIERÍA EN SISTEMAS

"Centralización del sistema de alarmas de seguridad de la Universidad Católica de Córdoba"

AUTORES:
Galmes, Francisco
Misa López, Carolina

TUTORES:
Dr. Ing. Castagnola, Juan Luis
Ing. Carreño, Ignacio
Ing. Porrini, Federico

Córdoba - Argentina
2022

AGRADECIMIENTOS

Luego de un largo camino lleno de aprendizajes tanto en lo técnico como en lo personal, al ver el resultado obtenido en este trabajo solamente se nos ocurre una palabra ¡Gracias!

Gracias a nuestros tutores, Dr. Ing. Juan Luis Castagnola, Ing. Ignacio Carreño e Ing, Federico Porrini, por su inestimable coordinación y continuo apoyo durante el desarrollo de este trabajo haciendo de este una tarea no sólo formativa, sino también interesante y enriquecedora para nuestro futuro.

Gracias a nuestras familias, hermanos y padres, por su apoyo incondicional en todos nuestros proyectos y metas que nos hemos propuesto, por su acompañamiento en todo momento el cual nos ha llenado de fuerza de energía animándonos a crecer como personas y como profesionales.

Gracias a cada uno de nuestros amigos y compañeros, por estar presentes en cada uno de nuestros pasos siendo el soporte que nos motiva a seguir adelante con nuestros objetivos.

Gracias infinitas a todos ustedes y, por supuesto, a Dios por ponerlos en nuestro camino.

RESUMEN

Durante los últimos años, la Argentina ha atravesado una creciente preocupación pública por el problema de la inseguridad, significando un estado de inquietud constante en todos los sectores sociales. La Universidad Católica de Córdoba no está exenta a esta problemática por los numerosos establecimientos y espacios de gran extensión haciendo que su supervisión sea dificultosa. La presente propuesta busca desarrollar un sistema integral que vincule y complemente el sistema de seguridad actual. Mediante la construcción de un producto mínimo viable, se propone una aplicación web que visibiliza los datos del estado de las alarmas en tiempo real, recolectados por los módulos de hardware, para la rápida actuación del equipo de seguridad frente a un intento de intrusión.

Palabras claves: seguridad, alarmas, aplicación web, intrusión.

ABSTRACT

During the last few years, Argentina has experienced a growing public concern about the problem of insecurity, which has caused a constant state of anxiousness in every social sector. The Catholic University of Cordoba is exposed to this problem due to the numerous establishments and spaces of great extension, making their supervision difficult. This proposal aims to develop an integral system that links and complements the current security system. Through the building of a minimum viable product, we propose a web application that displays the real-time status data of the alarms, recorded by the hardware modules, for a faster action of the security team in case of an intrusion attempt.

Key words: security, alarm, web application, intrusion.

CONTENIDO

GLOSARIO **10**

INTRODUCCIÓN **13**

PLANTEAMIENTO DE LA PROBLEMÁTICA **15**

OBJETIVOS **17**

Objetivo general **17**

Objetivos específicos **17**

METODOLOGÍA **18**

MARCO TEÓRICO **20**

Internet de las cosas (IoT - Internet of things) **20**

Sistemas de seguridad **21**

Componentes 21

Sistemas de seguridad de intrusión 23

Prestadores de sistemas de alarmas monitoreadas 23

Protocolo de comunicación **25**

Seguridad del protocolo MQTT 29

QoS (Quality of Service) 30

Microcontrolador **30**

Sensores y componentes electrónicos **33**

Sensores PIR 35

Servidor web **37**

Cron Jobs **42**

Base de datos **43**

ANÁLISIS Y DISEÑO DE LA SOLUCIÓN **44**

Relevamiento y análisis de requerimientos **44**

Especificaciones de caso de uso 46

Diseño de la base de datos **55**

Modelo entidad relación. 55

Descripción de las entidades del sistema 57

Modelo relacional de datos 63

Diseño de interfaces de usuario **65**

DESARROLLO DE LA PROPUESTA **66**

Descripción general de la solución **66**

Arquitectura 66

Seguridad 67

Análisis Funcional 68

Hardware 71

Controlador 74

Aplicación Web 75

IMPACTO ECONÓMICO **83**

Estructura de costos **83**

POSIBILIDADES DE CRECIMIENTO DEL PRODUCTO **86**

CONCLUSIÓN **88**

ANEXO I **89**

Propuesta alternativa **89**

BIBLIOGRAFÍA **92**

LISTA DE FIGURAS

Figura 1. Etapas del proyecto 18
Figura 2. Sistema de seguridad aplicado a grandes organizaciones. 20
Figura 3. Componentes de un sistema de seguridad. 22
Figura 4. Arquitectura de sistema con MQTT. 26
Figura 5. Conexión MQTT. 27
Figura 6. Método de suscripción del protocolo. 27
Figura 7. Envío de información en MQTT. 27
Figura 8. Suscripción al broker central. 28
Figura 9. Composición del mensaje del protocolo. 29
Figura 10. Microcontrolador NodeMCU ESP8266. 31
Figura 11. Descripción GPIO placa de desarrollo 32
Figura 12. Descripción de la ESP 01 y sus GPIO. 33
Figura 13. Módulo ZMPTB101B. 34
Figura 14. Módulo lectura de batería. 34
Figura 15. Módulo regulador de voltaje. 35
Figura 16. Modelo comercial del sensor PIR. 35
Figura 17. Radiación infrarroja y comparación de lentes. 37
Figura 18. Representación Raspberry Pi con sus GPIO. 38
Figura 19. Logo PHP. 38
Figura 20. Gráfico comparativo de frameworks. 39
Figura 21. Logo de Laravel. 40
Figura 22. Arquitectura MVC. 41
Figura 23. Infraestructura del software. 42
Figura 24. Estructura de un cron job. 42
Figura 25. Logo MariaDB. 43
Figura 26. Diagrama de caso de uso de la propuesta. 45
Figura 27. Modelo entidad - relación. 56
Figura 28. Entidad USERS. 57
Figura 29. Entidad ROLES. 58
Figura 30. Entidad BUILDINGS. 58
Figura 31. Entidad USERS_BUILDINGS. 59

Figura 32. Entidad ALARMS. 59
Figura 33. Entidad ACCOUNTABLE_PEOPLE. 60
Figura 34. Entidad ACCOUNTABLE_PEOPLE_ALARMS 60
Figura 35. Entidad COMPONENTS. 61
Figura 36. Entidad COMPONENT_TYPES. 62
Figura 37. Entidad LOGS. 62
Figura 38. Modelo relacional de datos. 64
Figura 39. Logotipo de la Universidad. 65
Figura 40. Colores institucionales de la universidad. 65
Figura 41. Arquitectura general del sistema. 67
Figura 42. Caso práctico: sistema de alarmas de la Facultad de Ingeniería. 69
Figura 43. Representación del envío de información. 70
Figura 44. Payload lectura de tensión eléctrica. 70
Figura 45. Payload lectura de batería. 70
Figura 46. Payload de detección de movimiento por los sensores PIR. 71
Figura 47. Módulo de lectura de voltaje de red. 72
Figura 48. Módulo de lectura de batería. 73
Figura 49. Módulo de detección del estado del sensor PIR. 74
Figura 50. Flujo de información de los módulos. 75
Figura 51. Ingreso a la plataforma. 76
Figura 52. Pantalla principal, notificaciones. 77
Figura 53. Modal de ingreso de observaciones. 77
Figura 54. Lista de usuarios. 78
Figura 55. Formulario de dada de alta de usuarios. 78
Figura 56. Lista de alarmas. 79
Figura 57. Modal de descarga de reportes. 79
Figura 58. Modal de descarga de reportes con el selector de rango de fechas. 80
Figura 59. Reporte histórico, archivo .xlsx. 80
Figura 60. Formulario de dada de alta de una alarma. 81
Figura 61. Panel de control. 82
Figura 62. Módulo de botón activación 90
Figura 63. Flujo de información y arquitectura de los módulos. 90
Figura 64. Arquitectura del sistema. 91

LISTA DE TABLAS

Tabla 1. Comparación de MariaDB y MySQL. 43
Tabla 2. Matriz de permisos de los usuarios. 46
Tabla 3. Descripción del caso de uso “Ingresar a la plataforma”. 46
Tabla 4. Descripción del flujo normal del caso de uso “Ingreso a la plataforma”. 46
Tabla 5. Descripción del flujo alterno del caso de uso “Ingresar a la plataforma”. ... 47
Tabla 6. Descripción del caso de uso “Dar de alta un usuario”. 47
Tabla 7. Descripción del flujo normal del caso de uso “Dar de alta un usuario”. 47
Tabla 8. Descripción del flujo alterno del caso de uso “Dar de alta un usuario”. 48
Tabla 9. Descripción del caso de uso “Modificar los datos de un usuario”. 48
Tabla 10. Descripción del flujo normal del caso de uso “Modificar los datos de un usuario”. 48
Tabla 11. : Descripción del flujo alterno del caso de uso “Modificar los datos de un usuario”. 49
Tabla 12. Descripción del caso de uso “Dar de baja un usuario”. 49
Tabla 13. Descripción del flujo normal del caso de uso “Dar de baja un usuario”. ... 49
Tabla 14. Descripción del flujo alterno del caso de uso “Dar de baja un usuario”. ... 49
Tabla 15. Descripción del caso de uso “Dar de alta una alarma”. 50
Tabla 16. Descripción del flujo normal del caso de uso “Dar de alta una alarma”.... 50
Tabla 17. Descripción del flujo alterno del caso de uso “Dar de alta una alarma”.... 50
Tabla 18. Descripción del caso de uso “Modificar los datos de una alarma”..... 51
Tabla 19. Descripción del flujo normal del caso de uso “Modificar los datos de una alarma”. 51
Tabla 20. Descripción del flujo alterno del caso de uso “Modificar los datos de una alarma”. 51
Tabla 21. Descripción del caso de uso “Dar de baja una alarma”. 52
Tabla 22. Descripción del flujo normal del caso de uso “Dar de baja una alarma”... 52
Tabla 23. Descripción del flujo alterno del caso de uso “Dar de baja una alarma”... 52
Tabla 24. Descripción del caso de uso “Ver el estado de la alarma”. 52
Tabla 25. Descripción del flujo normal del caso de uso “Ver el estado de la alarma”. 53
Tabla 26. Descripción del flujo alterno del caso de uso “Ver el estado de la alarma”.

..... 53
Tabla 27. Descripción del caso de uso “Descargar reporte de eventos de la alarma”. 53
Tabla 28. Descripción del flujo normal del caso de uso “Descargar reporte de eventos de la alarma”. 53
Tabla 29. Descripción del flujo alterno del caso de uso “Descargar reporte de eventos de la alarma”. 54
Tabla 30. Descripción del caso de uso “Configurar el estado de las alarmas”. 54
Tabla 31. Descripción del flujo normal del caso de uso “Configurar el estado de las alarmas”. 54
Tabla 32. Descripción del flujo alterno del caso de uso “Configurar el estado de las alarmas”. 54
Tabla 33. Casos de uso del hardware. 55
Tabla 34. Descripción de los tipos. 57
Tabla 35. Descripción entidad USERS. 57
Tabla 36. Descripción entidad ROLES. 58
Tabla 37. Descripción entidad BUILDINGS. 58
Tabla 38. Descripción entidad USERS_BUILDINGS. 59
Tabla 39. Descripción entidad ALARMS. 59
Tabla 40. Descripción entidad ACCOUNTABLE_PEOPLE. 60
Tabla 41. Descripción entidad ACCOUNTABLE_PEOPLE_ALARMS. 61
Tabla 42. Descripción entidad COMPONENTS. 61
Tabla 43. Descripción entidad COMPONENTS_TYPES. 62
Tabla 44. Descripción entidad LOGS. 63
Tabla 45. Análisis de costos de recursos humanos. 83
Tabla 46. Costo de elementos físicos. 84
Tabla 47. Resumen del costo del desarrollo. 84

GLOSARIO

Alarma: mecanismo de advertencia audible, visual, etc., sobre la proximidad de un peligro.

Análisis Funcional: técnica que se utiliza para identificar las competencias, capacidades y alcance del desarrollo propuesto.

Aplicación Web: programa que se codifica en un lenguaje interpretable por los navegadores web.

Arquitectura Informática: diseño conceptual y estructural operacional de un sistema de computadoras.

Atributo: especificación que define una propiedad de un elemento.

Base de datos: herramienta que permite recopilar, almacenar y organizar gran cantidad datos que pueden ser consultados rápidamente de acuerdo a las características deseadas.

Caso de uso: descripción de una acción o actividad.

Controlador: componente informático que le permite al sistema operativo y un dispositivo comunicarse entre sí.

Entidades: representación de un objeto o concepto del mundo real que se describe en una base de datos.

GPIO: es un pin genérico en un chip, cuyo comportamiento (incluyendo si es un pin de entrada o salida) se puede controlar (programar) por el usuario en tiempo de ejecución.

Guardia: persona encargada de las funciones de vigilancia y cuidado de un establecimiento o predio.

Hardware: conjunto de componentes tangibles, físicas de un sistema informático.

Interfaces: unión que se establece entre dos dispositivos o sistemas independientes para establecer una comunicación y funcionar de forma conjunta.

Intrusión: acción de introducirse indebida o ilegalmente en una propiedad.

Lenguaje de programación: estructura con base sintáctica y semántica que definen instrucciones a un programa informático.

Metodologías ágiles: herramientas que permiten adaptar la forma de trabajo a las condiciones del proyecto, consiguiendo flexibilidad e inmediatez en la respuesta para amoldar el proyecto y su desarrollo a las circunstancias específicas del entorno.

Microcontrolador: circuito integrado programable con la capacidad de ejecutar las órdenes y tareas grabadas en su memoria.

Modal: ventanas informáticas que se activan cuando el usuario presiona un botón particular.

Notificación: alerta que informa al usuario sobre un evento.

Protocolo de comunicación: conjunto de reglas de restricción y procedimientos entre dos o más entidades que definen el intercambio de información para lograr la comunicación entre ellos.

Radiación Infrarroja: tipo de radiación electromagnética cuya longitud de onda es mayor que la de la luz visible pero menor que la de microondas.

Rol: conjunto de permisos que posee un usuario en el sistema.

Seguridad: característica de algo donde no se registran peligros, daños ni riesgo.

Sensor: dispositivo destinado a la detección de acciones o estímulos externos que requieren respuesta en consecuencia.

Señal: es una notificación asíncrona enviada a un sistema para informarle de un evento.

Servidor: computadora que provee servicios a los demás ordenadores que forman parte de su red.

Sistema informático: conjunto de elementos físicos y lógicos que permiten almacenar y procesar información.

Software: programa informático compuesto de instrucciones y reglas que permiten ejecutar distintas tareas en una computadora.

Usuarios: persona que usa ordinariamente algo. En el ámbito de la informática, un usuario es quien interactúa con el sistema informático con un objetivo particular.

INTRODUCCIÓN

En un mundo globalizado donde la presencia de la Ciencia y la Tecnología forman parte en todo momento del desarrollo de nuestras vidas es posible que no seamos conscientes de la magnitud de participación que tienen. Al referirnos a “tecnologías” seguramente pensamos en elementos con los que interactuamos todos los días: celular, computadoras y otros, pero la Ciencia y la Tecnología están presentes en ellos y en más, estos son instrumentos de transformación en nuestra sociedad.

La ingeniería como facultad de una persona de aplicar sus conocimientos experiencias, ideas y recursos (humanos y materiales) con el fin de realizar proyectos o generar desarrollos, estructuras, modelos que permitan satisfacer las necesidades y mejorar la calidad de vida del ser humano, es el resultado de la combinación de la Ciencia como herramienta que permite a la Ingeniería crear y operar Tecnología.

De esta manera, el avance referido a las tecnologías de información y comunicación en las últimas décadas ha permitido que los ingenieros desarrollen, organicen y actualicen los sistemas de información y ayuden a las distintas empresas a innovar tecnológicamente su forma de transmitir y controlar su información de manera óptima, confiable y precisa.

La seguridad en hogares y empresas es uno de los bienes más preciados en la actualidad, es por ello que la industria de sistemas de monitoreo y seguridad ha sido uno de los ámbitos destacados en la aplicación de la tecnología para modernizar sus productos y servicios. Por ejemplo, el desarrollo de aplicaciones informáticas que permiten monitorear en vivo desde cualquier lugar y accionar por medio de un solo clic, alertando al proveedor de seguridad para que reaccione de inmediato, ha sido una de las principales soluciones elegidas por grandes y pequeños consumidores.

En las siguientes páginas, se expone el diseño y desarrollo de un producto a medida para la Universidad Católica de Córdoba organizado en cuatro etapas:

Primera etapa: Se presenta la problemática y el diagnóstico de la misma.

Segunda etapa: En base al relevamiento de requerimientos se presenta el modelado de la propuesta del sistema y la definición de los aspectos metodológicos para su construcción.

Tercera etapa: Se desarrolla la propuesta en pos de cumplir los objetivos y especificaciones definidas en la segunda etapa.

Cuarta etapa: Se analizan futuras actualizaciones del producto.

PLANTEAMIENTO DE LA PROBLEMÁTICA

En los últimos tiempos, la inseguridad en la República Argentina se ha convertido en un tema central en las conversaciones cotidianas y en los medios de comunicación. Así, la preocupación de los ciudadanos al sentirse vulnerables los lleva a tomar medidas orientadas a la prevención y protección frente a los delitos. Dichas acciones son implementadas principalmente en el hogar mediante el uso de sistemas anti-intrusión, o simplemente llamadas alarmas, y sistemas de cámaras de seguridad.

La Universidad Católica de Córdoba (UCC), fundada en el año 1956, es una universidad argentina situada en la ciudad de Córdoba. Esta cuenta con tres sedes para sus unidades académicas:

- Sede Campus, ubicada camino a Alta Gracia: donde se encuentra el Rectorado y las facultades de Derecho y Ciencias Sociales, Arquitectura, Ciencias Económicas y de Administración, Ciencia Política y Relaciones Internacionales, Ciencias Químicas, Agropecuarias e Ingeniería. Además, en él se encuentra el Hospital Veterinario, el Jardín Botánico Gaspar Suárez S.J., diversos laboratorios para las Facultades de Ciencias Químicas y Agropecuarias y la biblioteca Jean Sonet sj., así como el centro de Investigación en Biología Molecular de la Facultad de Medicina y el CONICET.

- Sede Centro: donde desarrollan su actividad académica las Facultades de Filosofía y Humanidades, Teología, Educación y el ICDA.

- La sede de Barrio General Paz donde se encuentra la Facultad de Ciencias de la Salud.

En cada una de estas se encuentran múltiples alarmas individuales instaladas en los distintos edificios con un sistema de notificación sonoro exterior para casos de irrupción durante su activación. Frente a esta disposición y configuración del sistema de seguridad se encuentra un gran inconveniente: el lapso de tiempo entre dicha notificación y la actuación del personal de seguridad para verificar la situación. Así

mismo al tener una gran cantidad de sensores y espacios es compleja la identificación de cuál fue el que activó la alarma y por consiguiente la bocina sonora. El sistema de seguridad actual se encuentra en funcionamiento, pero presenta muchas falencias en cuestión de tiempos de respuesta.

Es por ello que en el siguiente trabajo se desarrollará e implementará un sistema en el cual, mediante el uso de conceptos de domótica, se notifique en tiempo real sobre el incidente ocurrido, seguido de la información necesaria para actuar en consecuencia y así disminuir y optimizar el tiempo de reacción.

OBJETIVOS

Objetivo general

El objetivo principal del proyecto es reducir el tiempo de reacción del personal de seguridad frente a irrupciones en cualquiera de sus espacios y establecimientos dejando trazabilidad de cada evento relacionado a las alarmas de la Universidad Católica de Córdoba.

Objetivos específicos

- Complementar las carreras de Ingeniería en Sistemas e Ingeniería Electrónica en la aplicación de conceptos del campo de la domótica.

- Alertar al personal de seguridad sobre irrupciones en cualquier sitio de la Universidad e incidentes de las alarmas en tiempo real.

- Informar el plan de acción frente a un imprevisto de las alarmas.

- Registrar la actividad de los guardias al momento en el que es alertado.

METODOLOGÍA

La metodología consiste en un conjunto de métodos, tareas, habilidades y conocimientos utilizados para alcanzar los objetivos planteados. En la disciplina de gestión de proyectos se plantean numerosas propuestas metodológicas que van desde las más tradicionales, centrándose específicamente en el control de los procesos, estableciendo cada una de las tareas involucradas, los artefactos que se producirán y las herramientas que se emplearán. Estas han demostrado su efectividad en un gran número de proyectos, sin embargo, en los últimos tiempos estas han significado un costo alto por la complejidad que le agrega al proceso y la dedicación exclusiva de un equipo para su seguimiento.

Las metodologías ágiles como propuesta que se centra en el factor humano, en la colaboración con el cliente y el desarrollo incremental del producto con pequeñas iteraciones, han demostrado su efectividad al reducir drásticamente los tiempos de desarrollo manteniendo una alta calidad. A la hora de indagar sobre los requerimientos del cliente y diseñar las soluciones que se adapten a estos se puede adoptar métodos como el conocido Design Thinking, centrado en las personas entendiendo su contexto y a encontrar soluciones a problemas complejos con viabilidad técnica y económica. A continuación (figura 1), se presenta un gráfico que resume las etapas que propone el método en cuestión:

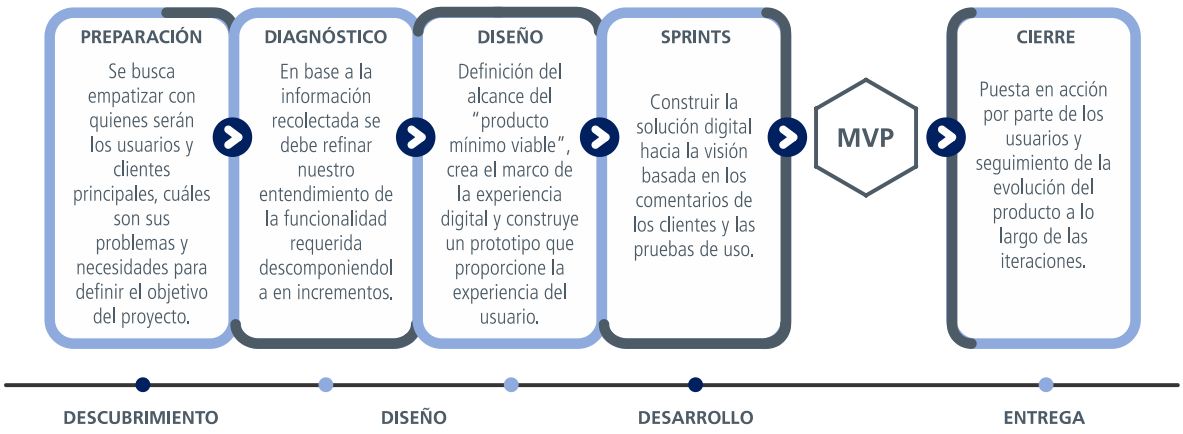

Figura 1. Etapas del proyecto

El término MVP (del inglés Minimum Viable Product) hace referencia a productos con características básicas pero suficientes para agregar valor al negocio y a las necesidades iniciales del cliente y, al mismo tiempo, proporcionar retroalimentación para el desarrollo futuro. Es considerado como una estrategia de mejora continua ya que se enfoca en lograr el más completo entendimiento de las necesidades y deseos del usuario final permitiendo detectar errores u omisiones en la etapa temprana del proyecto para corregirlo para validarlo nuevamente al concluir el próximo sprint[1].

En las próximas páginas se desarrollará el proceso de construcción del MVP con el fin de centralizar las notificaciones del sistema de alarmas de la Universidad Católica de Córdoba en una página web a la cual tendrá acceso el personal de seguridad y las secretarías de las unidades académicas siguiendo cada uno de los pasos anteriormente mencionados.

[1] Sprint. Cada uno de los ciclos o iteraciones por los que pasa el producto durante el desarrollo del proyecto ágil.

MARCO TEÓRICO

Internet de las cosas (IoT - Internet of things)

En el último tiempo Internet ha evolucionado de una manera que jamás se hubiera imaginado. Desde su humilde comienzo como Advanced Research Projects Agency Network (ARPANET) en 1969, en la actualidad se estima que Internet interconecta 50.000 millones de dispositivos, proporcionando conexiones globales que hacen posible que exista la navegación web, las redes sociales y los dispositivos móviles inteligentes.

Internet de las cosas, también conocido por sus siglas en inglés “IoT”, es un concepto que ha surgido en esta era de la interconexión de la población mundial y será el disparador del diseño del presente proyecto. Podríamos definirlo como la red de objetos o dispositivos inteligentes que comparten los datos recolectados por los sensores conectándose a otro dispositivo de transición para enviarlos a la nube para ser analizados.

Si bien las aplicaciones de este campo son infinitas, ya que pueden ser implementados tanto en la vida cotidiana como en el entorno empresarial e industrial, nos enfocaremos en definir a la domótica como disparador de las próximas páginas. La domótica consiste en el uso de la tecnología para la automatización de procesos en viviendas y edificios, como por ejemplo los dispositivos controlados por voz a los que se les solicita la reproducción de música desde un repositorio en internet e incluso, como en nuestro caso, los sistemas de seguridad que se conectan a la red para el aviso de intrusiones en un hogar.

Figura 2. Sistema de seguridad aplicado a grandes organizaciones.

De esta manera, el crecimiento de los índices de inseguridad y el avance de la tecnología ha dado lugar a que los propietarios comiencen a sumergirse en los kits de seguridad eligiendo el más conveniente a la medida de sus necesidades y presupuesto. El internet de las cosas ha hecho que sea más cómodo y sencillo la instalación de sistemas de seguridad inteligentes proporcionando un seguimiento en línea seguro, controlable e incluso personalizado en tiempo real, y además la posibilidad de control y mantenimiento remoto de los dispositivos.

Sistemas de seguridad

Para entender con mayor profundidad el concepto que estudiaremos, realizaremos una exposición sobre el término “alarma”. La palabra alarma tiene su origen del vocablo italiano “allarme” que significa “el arma”, grito que se daba por presencia del enemigo. Es por ello que el término alarma puede definirse como toda señal o aviso diseñado para activarse como respuesta a un evento para advertir sobre la proximidad de peligro.

De esta manera, se ha logrado definir a los sistemas de alarmas como un conjunto de elementos de seguridad de tipo pasivo, ya que su fin no es evitar una situación de fuga de gas, incendios o intrusión, sino más bien advertir sobre estos para actuar y disminuir los daños producidos.

Componentes

Al analizar un sistema debemos hacer hincapié en los componentes que hacen posible lograr su objetivo. A continuación, describiremos cada uno de ellos en cuanto a sus funciones:

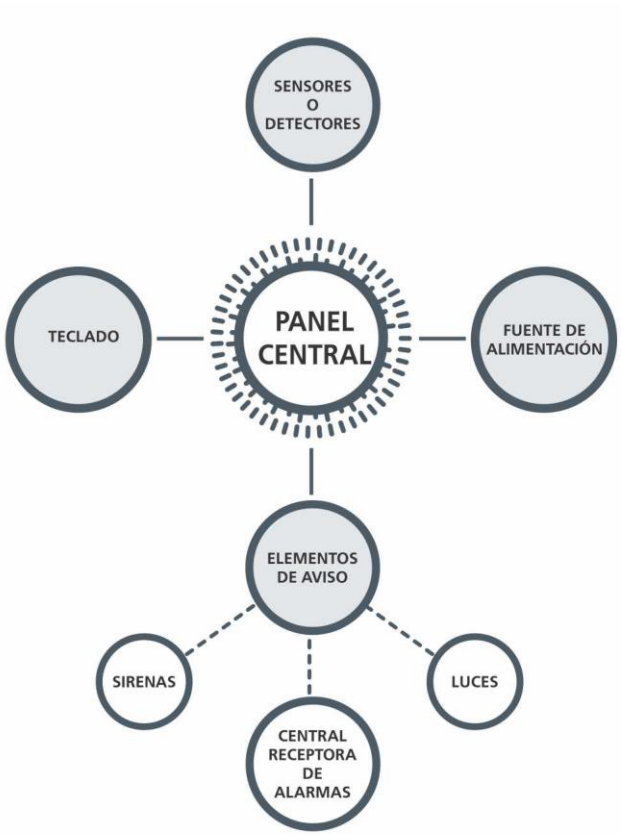

Figura 3. Componentes de un sistema de seguridad.

- **Central procesadora** (o panel de control) es el módulo en la cual se albergan la placa base, la fuente y la memoria central. En ella se reciben las señales emitidas por los sensores y, en consecuencia, dispara la alarma comunicándose con el servicio de monitoreo.

- **Teclado** es donde los usuarios configuran el panel de control ingresando los códigos preestablecidos para activar o desactivar el sistema. Además, pueden encontrarse botones específicos para funciones de emergencia para situaciones médicas, de intrusión, fuego, etc.

- **Sirena exterior** con autonomía propia, es decir que pueden funcionar aún si se produce un corte de suministro eléctrico o si pierde comunicación con la central procesadora.

- **Detectores** como sensores que detectan los cambios de temperatura, movimiento y humedad. Estos son quienes disparan las alarmas al detectar algún cambio en esas variables.

Sistemas de seguridad de intrusión

Una vez familiarizados con los conceptos generales de sistemas de seguridad, estamos en condiciones de ahondar sobre uno específico que será recurrente de aquí en más: los sistemas de alarmas de intrusión o robo. Conceptualizamos a un sistema de alarma contra robo e intrusión como aquel que es instalado en determinada área del edificio para proteger perímetros designados detectando cualquier intrusión o acto de vandalismo. Es decir, este sistema detecta la presencia del individuo intentando acceder a la zona protegida mediante sensores infrarrojos o detectores de puertas y ventanas y se activa alertando al servicio de seguridad sobre el incidente.

Así, al momento de desarrollar un sistema de este tipo debemos considerar algunos puntos que hacen a su utilidad:

- El sistema de protección debe considerarse suficientemente seguro para evitar que alguien pueda manipularlo con fines ajenos a este. No se debe alterar la integridad del sistema bajo ninguna circunstancia ya que derivaría en una situación de riesgo para la empresa o vivienda.

- Deben considerarse situaciones por fallas por corriente eléctrica que pudieran ocasionar pérdidas de información.

- Debe establecerse una serie de protocolos y procedimientos como respuesta del sistema de monitoreo de cualquier señal. Cualquier situación debe ser reportada al servicio de seguridad dedicado al tratamiento de estos problemas.

Prestadores de sistemas de alarmas monitoreadas

Expertos denominan al periodo de la actualidad como la “Cuarta revolución industrial” caracterizada por la fusión de distintas tecnologías de manufactura y desarrollo en pos de la desintegración de las fronteras entre lo físico, digital y biológico, con la tendencia de automatización e intercambio de datos en campos de sistemas ciber físicos, el Internet de las cosas y la computación en la nube. De esta manera, la digitalización de la industria y los servicios se traslada a todos los sectores,

construyendo compañías ágiles que se enfocan en mejorar sus productos y servicios para un público más digital.

Un claro ejemplo es aquellas que ofrecen sistemas de alarmas monitoreadas donde un conjunto de dispositivos electrónicos distribuidos estratégicamente dentro de un edificio o vivienda envían información a una central de monitoreo para la seguridad de los individuos que lo habitan. En el mercado cordobés se presentan sistemas de seguridad con esta tecnología, entre ellas se encuentran prestigiosos nombres como ADT alarmas, X-28 alarmas y 24hs Security, así como también empresas en auge como Alarmas Verisure.

En primer lugar, la prestigiosa empresa de alarmas y seguridad ADT ya con 24 años en el mercado argentino y más de 50 en España se destaca por ser una de las más avanzadas en el campo aplicando la tecnología como parte de sus productos de seguridad interactiva. Ofrece desde Geo-servicios con los cuales puedes activar tu sistema de seguridad a distancia hasta monitoreo de video inteligencia 24/7. En el último periodo desarrollaron una plataforma denominada Interactive Security en donde se puede encontrar todas las facilidades y herramientas del sistema de seguridad en una aplicación móvil.

En el caso de X- 28 alarmas, con sus 37 años en el mercado local, propone un abanico completo de soluciones en cuanto a seguridad. Entre ellos se encuentra la capacidad de tener una detección anticipada, protección de puertas y ventanas con tecnología de última generación y comunicaciones inalámbricas en grandes rangos físicos. Así mismo tiene un sistema de seguridad integral de protección contra incendios y gases, con los detectores de presencia de gas y monóxido de carbono se le puede agregar una cuota extra de seguridad al hogar. Además, cabe destacar que, al igual que ADT, ha desarrollado una aplicación móvil para tener todas las herramientas y novedades al alcance de la mano.

Entre las grandes opciones y con mucha trayectoria también se encuentra 24hs Security, ya con 28 años de experiencia en el mercado local destaca frente a sus competidores por los bajos costos de instalación y mantenimiento. Ofrece soluciones similares adaptando su servicio a la última tecnología disponible.

Por último, mencionar a empresas en auge como alarmas Verisure, donde se puede visualizar que su gran foco y dedicación está en el desarrollo tecnológico, lo que la destaca frente a sus competidores es el desarrollo de su potente aplicación web que brinda información con un alto grado de precisión.

Como los productos y servicios que ofrecen son muy similares, a la hora de elegir debemos analizar los factores más importantes, entre ellos el presupuesto que tenemos, nivel de seguridad y alcance de la misma y nivel de servicio. Todas estas opciones se encuentran en el mercado local y pueden ser de gran utilidad para la seguridad de una vivienda, oficina u hogar, pero cuando se trata de una organización o compañía como la Universidad se encuentran algunas limitaciones debido a que los clientes presentan requerimientos particulares que son complejos de adaptar a una estructura tan estandarizada. En estos casos los desarrollos particulares cumplen mejor con las exigencias, especificaciones y expectativas del usuario, ya que el proyecto en su totalidad se realiza a la medida de lo solicitado por el cliente.

Protocolo de comunicación

Para desarrollar la logística en un entorno de Internet de las cosas, son necesarias diversas tecnologías que hagan realidad la comunicación entre dispositivos de manera eficaz y eficiente. Para su vinculación se utilizan diversos protocolos de comunicación siendo estas normas aceptadas como válidas al momento de perturbar la radiofrecuencia y enviar señales. Algunos muy populares son HTTP, MQTT y Web Socket. Basados en la necesidad de un protocolo con máxima seguridad y velocidad de transmisión se seleccionó el renombrado MQTT.

MQTT (Message Queue Telemetry Transport) es un protocolo de comunicación M2M (machine-to-machine) de tipo cola de mensajes. Este es un protocolo controlado por eventos, esto quiere decir que no hay transmisión de datos periódica o continua y por ende, se mantiene el volumen de transmisión al mínimo, evitando el envío excesivo de información no relevante.

La lógica radica en un servicio de mensajería push con patrón publicador/suscriptor (sub-pub). En la arquitectura de este protocolo múltiples clientes

se conectan con un servidor central único denominado broker, logrando así recolectar y vincular numerosos puntos de información. Su funcionamiento puede ser descrito de la siguiente manera, los clientes son los encargados en iniciar la conexión con el broker con el protocolo TCP/IP (esta conexión se mantiene abierta hasta que el cliente la finaliza).

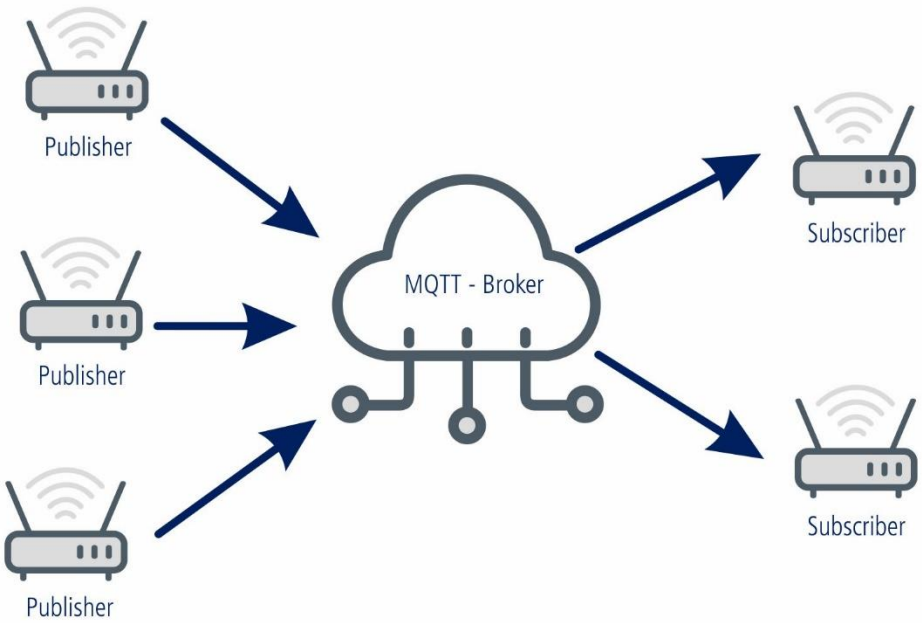

Figura 4. Arquitectura de sistema con MQTT.

Para ser aún más claros y poder visualizar la simplicidad del protocolo, se puede resumir el proceso de conexión y verificación del mismo en 2 pasos. Esto se observa en la figura 5.

1. El cliente envía un mensaje connect que contiene la información, como por ejemplo el nombre de usuario, contraseña, identificación del cliente, entre otras.

2. El broker responde con un mensaje connack, que brinda el estado de la conexión. Puede ser aceptada, rechazada o tener diversos estados.

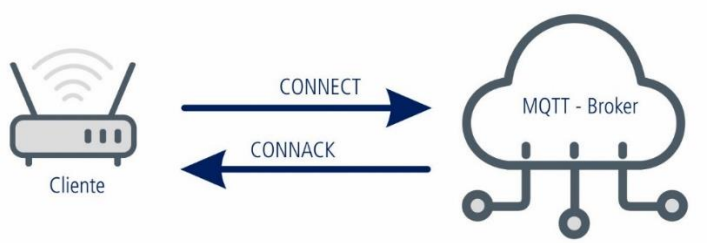

Figura 5. Conexión MQTT.

En pos de darle un orden y jerarquía a su estructura, MQTT propone temáticas a las cuales los clientes deben suscribirse para publicar un mensaje. Estas temáticas son denominadas topic.

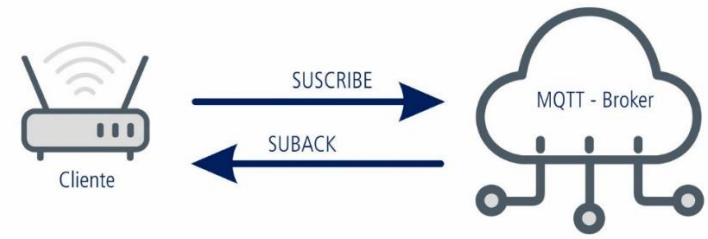

Figura 6. Método de suscripción del protocolo.

La conexión de los clientes con el servidor central que es denominado broker se realiza a través de un mensaje denominado publicación, en su idioma original publish. Estos mensajes contienen un paquete definido como payload, es decir el mensaje con la información a enviar. La figura 7 representa el envío de un payload a un topic suscripto en el broker.

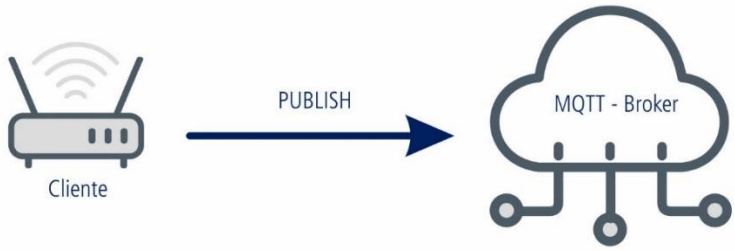

Figura 7. Envío de información en MQTT.

Hemos mencionado las conexiones desde los clientes hacia el servidor o broker. Por parte del servidor este debe suscribirse a las temáticas para poder recibir

la información que se le envía y transmite. Para mayor claridad y control las temáticas se dividen en sub temáticas, estos son denominados subtopics. Esto permite organizar las comunicaciones jerárquicamente. Un ejemplo de esto puede ser el de la instalación de sensores de movimiento en una universidad. Los topic y subtopic podrían ser, por ejemplo, en el caso de uno en el laboratorio de electrónica se puede describir de la siguiente manera, /Universidad/Ingeniería/Laboratorio-Electrónica/Pañol-elementos/Sensor. En este caso el servidor central recibe solo la información que envía dicho sensor. Gracias a la flexibilidad del protocolo podemos leer todos los subtopics de un topic utilizando el comando #. Por ejemplo, podemos subscribirnos a todos los clientes y leer la información de toda la facultad de ingeniería accediendo al topic de la siguiente manera /Universidad/Ingeniería/#. Esta versatilidad permite que el protocolo de comunicación sea muy potente y ágil.

Para garantizar una conexión activa, los clientes envían periódicamente un mensaje al servidor, el mismo es pingreq que obtiene como respuesta pingresp.

Por último, pero no menos importante, existen los dispositivos que se denominan suscriptores o suscribers estos únicamente toman información del broker, se suscriben a una temática y leen la información recibida. Un ejemplo de esto puede ser una pantalla que lea la información que envía un sensor de temperatura al broker.

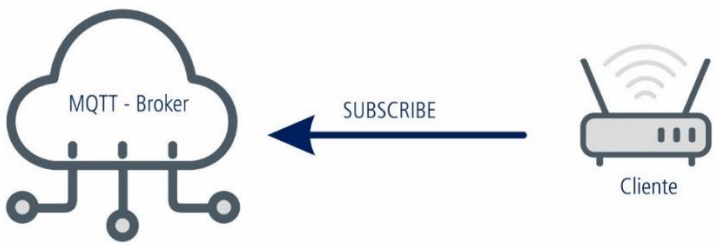

Figura 8. Suscripción al broker central.

Tal como se presentó previamente, el formato y estructura del protocolo es muy útil para el tipo de sistema a crear. Cuenta con una comunicación bidireccional simple en la cual se organiza por tópicos. Donde cada elemento envía su información a un colector (broker) central que la almacena y deja disponible para que sea procesada.

La base de la agilidad del protocolo está en la definición y tipología de los mensajes. Cada mensaje consta de 3 partes. Si se desarrolla cada uno de los elementos podemos comprender mejor el uso de cada sección.

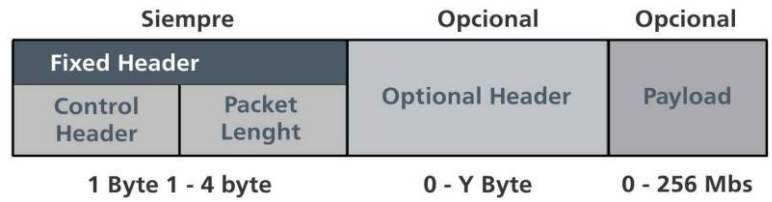

Figura 9. Composición del mensaje del protocolo.

- **Cabecera fija (Fixed Header):** Es un código de control que identifica el tipo de mensaje enviado y la longitud del mismo. Ocupa de 2 a 5 bytes obligatoriamente.

- **Cabecera variable (Optional Header):** Contiene información adicional que es necesaria en ciertos mensajes o situaciones. El uso de este es opcional.

- **Contenido (Payload)**: Contiene el mensaje que se desea enviar. Puede tener un máximo de 256 Mb. En implementaciones reales el máximo es de 2 a 4 kB.

Seguridad del protocolo MQTT

La seguridad es un aspecto fundamental en cualquier protocolo de comunicación M2M. Como es de común conocimiento la seguridad en conceptos informáticos es muy compleja de cuantificar y garantizar. Lo que se debe intentar es utilizar la mayor cantidad de herramientas para evitar cualquier tipo de intrusión o violación de la misma. En estos aspectos MQTT incluye transporte SSL/TLS y autenticación por usuario y contraseña o mediante certificado. Debido a la importancia de este aspecto para nuestro sistema se profundiza sobre cada uno de estos conceptos.

En primer lugar, SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), esta tecnología sirve para que todos los datos que se transfieren entre usuarios, entre sistemas o sistemas y sitios web sean imposibles de descifrar, leer o manipular. SSL utiliza algoritmos de cifrado para codificar la información que se transmite e impedir que cualquier externo pueda acceder a ellos.

Por otra parte, TLS es Transport Layer Security, este como su nombre lo indica hace referencia a la capa de transporte de información y es solo una versión actualizada y más segura que SSL. Normalmente al adquirir SSL estamos comprando un servicio de TLS.

QoS (Quality of Service)

En cuanto a la estabilidad y fiabilidad del protocolo se debe analizar la transmisión y recepción de la información. La calidad que presenta el protocolo se puede subdividir en 3 niveles. Cada uno de ellos con la siguiente lógica. A mayor nivel, mayor es el requerimiento computacional.

- **QoS 0 – "unacknowledged (at most one)":** El mensaje se envía una única vez. En caso de fallo el mensaje no llegará al destinatario.
- **QoS 1 – "acknowledged (at least one)":** El mensaje se envía hasta que se garantiza la entrega. En caso de algún fallo el receptor puede recibir algún mensaje duplicado.
- **QoS 2 - "assured (exactly one)":** Se garantiza que cada mensaje se entrega al suscriptor y únicamente una vez.

Un protocolo capaz de transmitir con el menor consumo de recursos computacionales, pero preservando la calidad y seguridad de la información es una gran herramienta para el sistema.

La información con su topología y métodos se transmite mediante dispositivos físicos aptos, capaces de cumplir con los requerimientos técnicos.

Microcontrolador

La conexión a Internet es indispensable para un sistema basado en el concepto de Internet de las cosas para lograr la vinculación y transmisión de información. Esto es posible gracias a los dispositivos conocidos como microcontroladores.

Hoy en día se pueden encontrar numerosas marcas y modelos, la gran demanda ha ampliado el abanico de productos creando muchos con características particulares y especializados en aplicaciones puntuales.

Partiendo de la necesidad de un bajo costo del proyecto y de un protocolo de conexión inalámbrico muy extendido y con gran alcance como es el WiFi, se puede encontrar el chip esp8266 como solución. Dicho chip es un SoC (System on Chip) que reúne un procesador de propósito general con toda la pila TCP/IP necesaria para una conectividad WiFi completa.

Gracias al enorme trabajo de la comunidad y su uso de manera masiva se desarrolló un firmware denominado NodeMCU. Este permite programar el chip con LUA y otros softwares libres de programación a bajo nivel. Este permite programar los chips en entornos como Arduino, reduciendo la complejidad de la tarea en una gran proporción. El previamente mencionado, se basa en el lenguaje de programación C++ con un agregado de métodos y funciones específicas para su uso. Junto a la herramienta de Arduino, el firmware NodeMCU de la ESP8266 le permite al usuario abstraerse de la lógica interna del sistema y darle mayor foco y énfasis al desarrollo de la lógica del proyecto.

.

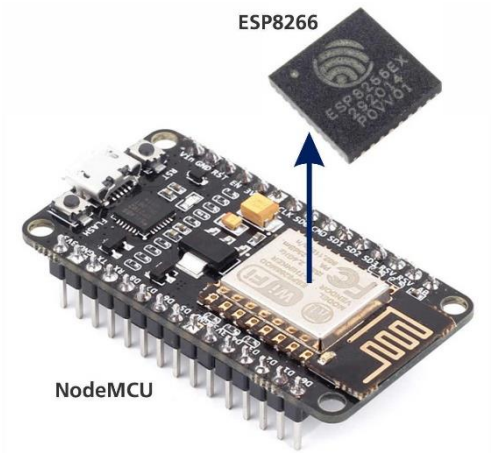

Figura 10. Microcontrolador NodeMCU ESP8266. Getting Started with ESP8266 NodeMCU Programming Using Arduino IDE. (s/f). Mytectutor.com. https://mytectutor.com/getting-started-with-esp8266-nodemcu-programming-using-arduino-ide/

Este microcontrolador de 32 bits posee una frecuencia de 80 MHz y memoria flash de 4MB. Cuenta con 11 entradas y salidas digitales y una única entrada analógica con una resolución de 10 bits. También posee varios protocolos de comunicación, como UART, i2c, SPI, entre otros.

La mayor ventaja que posee este controlador es la conectividad Wifi-integrada, sin necesidad de periféricos externos. En el mundo actual la conexión a una red Wifi pasó a ser uno de los requisitos esenciales de cualquier sistema. La ESP8266 NodeMCU tiene la funcionalidad de conectarse, e incluso, generar una red wifi propia en modo de Acces Point. El mencionado previamente sirve para crear una red inalámbrica tipo LAN que nos permite interconectar dispositivos.

El esquemático de la figura 11 presenta los GPIO de la placa de desarrollo.

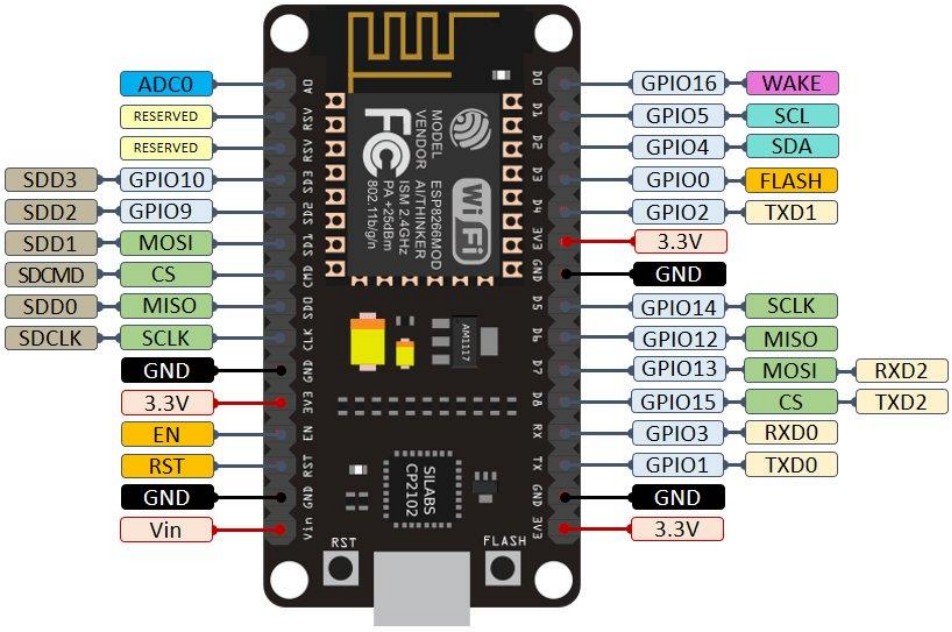

Figura 11. Descripción GPIO placa de desarrollo. ESP8266 Pinout Reference: Which GPIO pins should you use? (2019, mayo). Random Nerd Tutorials. https://randomnerdtutorials.com/esp8266-pinout-reference-gpios/

Una versión más compacta, limitada, económica y robusta de esta placa de desarrollo es la ESP 01. Esta versión cuenta con conexión wifi y 4 GPIO de lectura y escritura digital. Su distribución en la siguiente.

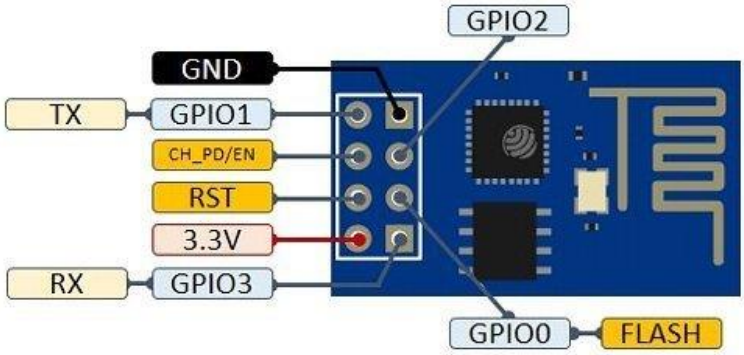

Figura 12. Descripción de la ESP 01 y sus GPIO. ESP8266 Pinout Reference: Which GPIO pins should you use? (2019, mayo). Random Nerd Tutorials. https://randomnerdtutorials.com/esp8266-pinout-reference-gpios/

Sensores y componentes electrónicos

El uso único de microcontroladores no es de mucha utilidad, esta se aprovecha cuando se le acoplan sensores y elementos externos que tengan la capacidad de sensar, medir, analizar y diagnosticar una situación o caso en particular.

Poder captar las señales de forma efectiva a un costo y complejidad baja es importante, es por esto que se investigó en profundidad sensores y componentes aptos para esto. Entre algunas de las utilidades del IoT en la domótica, la lectura de la tensión de red es de mucho interés si se está trabajando con señales enviadas por WiFi y queremos verificar si hay alimentación eléctrica en un lugar lejano o aislado.

Para la medición de la misma utilizaremos el módulo ZMPT101B. Este componente nos permite verificar el voltaje de la tensión de línea de la red con una placa de desarrollo como la ESP8266. El módulo reduce el voltaje AC de entrada a un voltaje CC menor que puede ser leído por un dispositivo con conectividad WiFi.

El componente está integrado por un transformador, que además de reducir el voltaje proporciona aislamiento galvánico para mayor seguridad. Del lado del primario se conecta el voltaje alterno a medir y del lado secundario se encuentra un divisor de tensión y un circuito con amplificador operacional (OPAMP LM358) para añadirle un desplazamiento a la salida analógica.

El módulo soporta hasta 250 VAC y su estabilidad y precisión es de valores aceptables para el mercado IoT.

Figura 13. Módulo ZMPTB101B. Akbari, M. (2020, octubre). Interfacing ZMPT101B AC Voltage Sensor Module w/ Arduino. Electropeak. https://electropeak.com/learn/interfacing-zmpt101b-voltage-sensor-with-arduino/

Similar al dispositivo anterior, contamos con un componente para leer el voltaje de una batería con una placa de desarrollo. Este módulo se conforma de un divisor de voltaje que permite una correcta medición de una tensión continua no superior a los 25 voltios, esta información puede ser recolectada con una placa de desarrollo como el ESP8266 NodeMCU.

En la figura 14 se visualiza el sensor mencionado previamente, por la izquierda se conecta la señal a medir, a la derecha se encuentra la alimentación del módulo y la señal de salida obtenida.

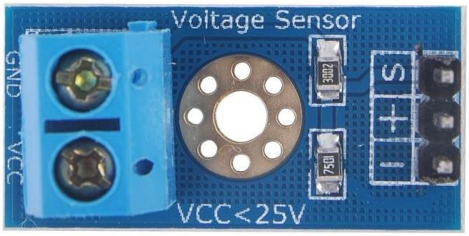

Figura 14. Módulo lectura de batería. 0-25V voltage sensor. (2021, junio). Arduino Forum. https://forum.arduino.cc/t/0-25v-voltage-sensor-issue/869458

Tanto como sensores, en el desarrollo de las aplicaciones del IoT se utilizan componentes para adaptar señales y niveles de voltaje. Ambos, sensores y kits de desarrollo se deben alimentar con su debido voltaje, elementos como reductores y conmutadores son de mucha utilidad para adecuar a las señales a las necesidades de cada uno.

El módulo LM2596 es un ejemplo de esto. Este componente es de gran ayuda para reducir los voltajes y poder operar correctamente componentes.

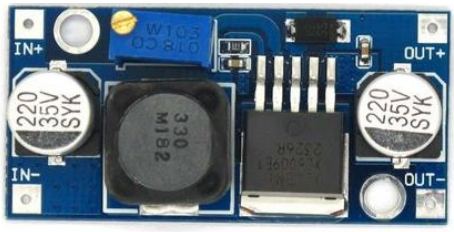

Figura 15. Módulo regulador de voltaje. Wilson, J. (2020, septiembre). LM2596 buck converter datasheet, pinout, features, applications. The Engineering Projects. https://www.theengineeringprojects.com/2020/09/lm2596-buck-converter-datasheet-pinout-features-applications.html

El módulo es un regulador de voltaje conmutado. Estos reguladores conmutados tienen una gran eficiencia, excelente regulación de línea y bajo voltaje de rizado. El componente admite un voltaje de entrada de 3 a 40 voltios con la posibilidad de ajustar su salida entre 1.25 y 35 voltios, la corriente máxima de salida que puede proporcionar son 3 amperes.

Sensores PIR

El módulo más importante del sistema es un detector de cuerpos, el sensor PIR. Este sensor es capaz de recibir las variaciones de radiación infrarroja del medio ambiente que cubre. Tienen el diseño solo para reaccionar ante determinadas fuentes de energía tales como el calor del cuerpo humano o animales. Son capaces de detectar la presencia de un cuerpo a través de la diferencia de calor emitido por el cuerpo humano y el espacio alrededor. En la figura 16 se puede observar un modelo comercial de estos sensores.

Figura 16. Modelo comercial del sensor PIR. Sensor Infrarrojo Movimiento Interior MD 65-MPXH X28 Alarmas. (s/f). Ottech.ar. Recuperado el 27 de noviembre de 2022, de https://ottech.ar/producto/sensor-infrarrojo-movimiento-interior-md-65-mpxh-x28-alarmas/

Es un sensor pasivo, esto quiere decir que no emite radiaciones, sino que las recibe. Su componente principal son los sensores piroeléctricos. Este es un elemento electrónico diseñado para detectar cambios en la radiación infrarroja recibida. Generalmente dentro de su encapsulado incorporan un transistor de efecto de campo que amplifica la señal eléctrica que se genera cuando se produce dicha variación de radiación recibida.

La información infrarroja llega al sensor piroeléctrico a través de una lente de Fresnel que divide el área protegida en sectores. Se distribuyen lentes con diferentes características: gran angular, cortina, corredor, anti-mascotas, entre otros. La elección del lente depende del lugar donde se instale el sensor y el uso que se le vaya a dar.

La señal eléctrica que generan los sensores piroeléctricos cuando detectan un cambio es procesada por un circuito electrónico de control que activará un relé en el caso que la señal tenga ciertas características y condiciones como amplitud, frecuencia, duración, entre otras.

Al iniciarse estos dispositivos por primera vez, realizan un paneo de todo el ambiente, captando la radiación infrarroja del espacio. Todos los cuerpos con una temperatura mayor a 0° Kelvin emiten radiación infrarroja negativa, esta radiación infrarroja aumenta si aumenta la temperatura del cuerpo en cuestión.

Es decir, su funcionamiento se basa en recibir información en el instante cero y luego al estabilizarse cuando detecta un cambio de energía en el ambiente alerta al usuario dando una condición de alarma.

Con objeto de lograr total confiabilidad, esta tecnología integra, además, un filtro especial de luz que elimina toda posibilidad de falsas detecciones causadas por la luz visible (rayos solares), así como circuitos especiales que dan mayor inmunidad a ondas de radio frecuencia. Una vez realizada la calibración y ajuste del detector, el led de prueba deberá quedar apagado por norma de instalación y se encenderá cada vez que el sensor se active.

Como fue mencionado previamente la zona de detección del sensor depende del lente que se le coloque, uno de los más famosos y utilizados el de Fresnell ya que da una gran apertura y campo de visión a través del uso de una técnica de diseño.

En la figura 17 se puede observar la diferencia de un lente convencional convexo y uno de Fresnel.

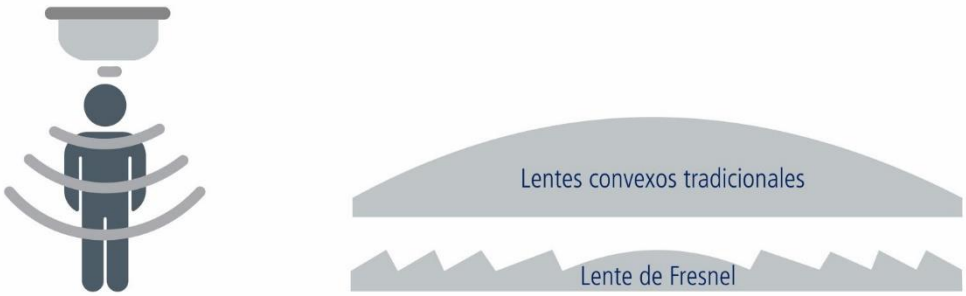

Figura 17. Radiación infrarroja y comparación de lentes.

Servidor web

Como punto de conexión entre los sensores y el usuario se puede utilizar un servidor web encargado del procesamiento de los datos. Analizando alternativas para implementar uno de estos nos encontramos con dos posibilidades, físico o en la nube. Optamos por un ordenador Raspberry Pi ya que su costo es relativamente bajo y, aun así, de gran capacidad computacional.

A lo largo de los años, la familia Raspberry Pi ha sido presentada en 4 modelos con distintas versiones en cada uno. En este caso utilizaremos una del modelo 3, versión B+, la cual posee un procesador ARM de 4 núcleos a velocidad de 1,4 GHz, 1 GB de memoria RAM, conectividad Wifi integrada y la posibilidad de alimentación del circuito a través de la red LAN. El sistema de almacenamiento puede ser a través de una tarjeta microSD donde se instala el sistema operativo o por medio de un disco externo conectado vía USB.

Los puertos del ordenador son los presentados en la figura 18.

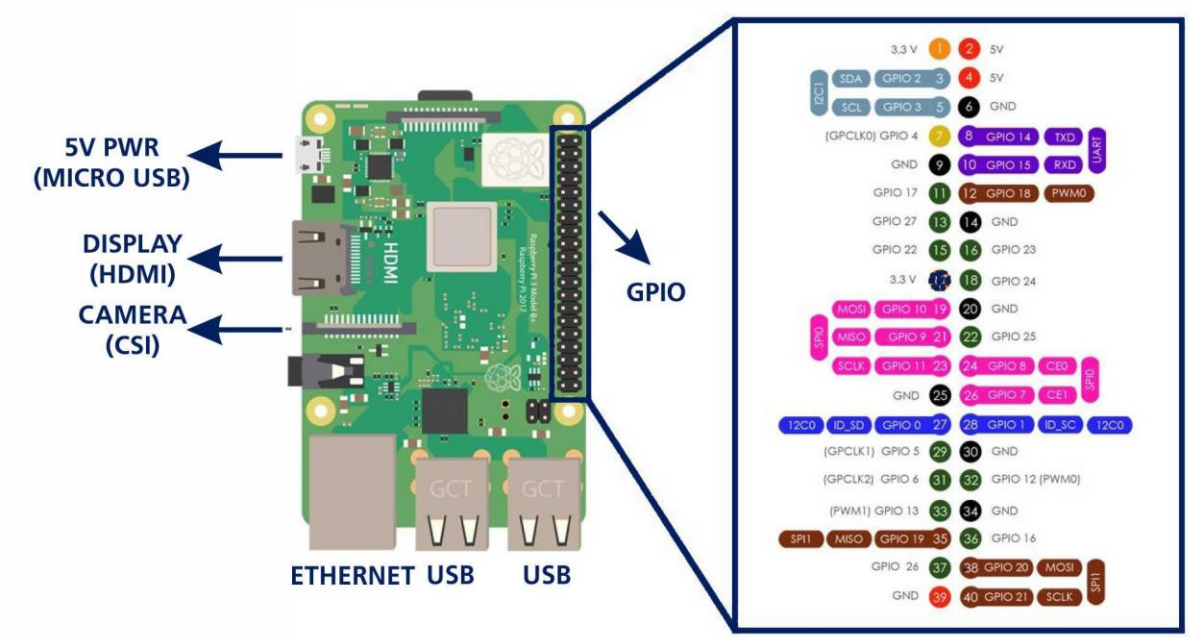

Figura 18. Representación Raspberry Pi con sus GPIO. Shaw, A. (2021, marzo 11). What is Raspberry Pi 3B +? Pinout, Specs, Projects & Datasheet. The Engineering Projects. https://www.theengineeringprojects.com/2021/03/what-is-raspberry-pi-4-pinout-specs-projects-datasheet.html

La principal función de los servidores web consiste almacenar, en web hosting[2], todos los archivos que componen una página web (imágenes, textos, videos, etc.) y transmitirlos a los usuarios a través de los navegadores. Para el desarrollo de la página web se seleccionó uno de los lenguajes de programación del lado del servidor más conocidos y usados hasta el día de hoy, PHP (acrónimo de Hypertext Preprocessor). Este permite administrar contenido dinámico, base de datos y seguimiento de sesiones.

Figura 19. Logo PHP.

[2] Web hosting. Servicio para alojar sitios web en línea, es decir, todos los contenidos de una página web para que los usuarios puedan acceder a él en todo momento a través de diferentes dispositivos.

Si bien hoy en día se presentan múltiples opciones al momento de elegir un lenguaje web, empresas de gran magnitud como Facebook, Wikipedia, Yahoo!, Wordpress, entre otras lo siguen eligiendo para sus plataformas. Pero, ¿por qué sigue siendo tan importante? Analicemos algunas características de la tecnología:

- **Sencillez**: una de las principales razones por las que PHP se volvió popular es por la sencillez de su sintaxis y de sus comandos.
- **Versátil**: es independiente de la plataforma, es decir que se puede usar en MacOS, Windows, Linux.
- **Código abierto y gratuito**: su instalación es rápida y libre de costos.
- **Soporte de la comunidad**: gracias a su antigüedad y su uso frecuente, este tiene una comunidad activa que brinda soporte online para los nuevos usuarios con tutoriales y consejos.

Al momento de desarrollar sistemas web en PHP se podría adoptar un framework para que, a través de sus bibliotecas de funciones comunes, reduzcamos el esfuerzo que conlleva la escritura de dicho código sin perder de vista las buenas prácticas de codificación. A continuación, en la figura 20, se presenta un gráfico con los más utilizados en el 2022 según la empresa dedicada a desarrollo de software Excellent WebWorld.

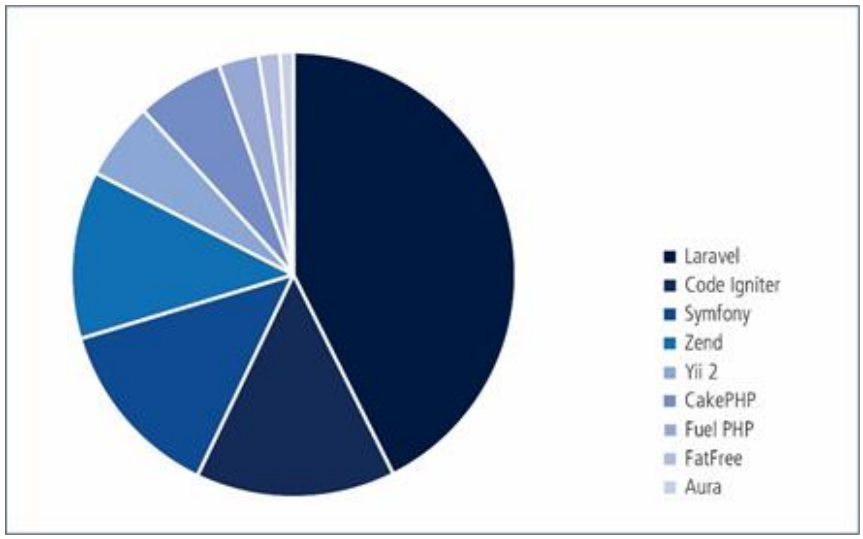

Figura 20. Gráfico comparativo de frameworks. Excellent web world. (2022) Pie-Chart of PHP Frameworks usage in Web Projects. Excellent Webworld. https://www.excellentwebworld.com/best-php-frameworks/

Profundizando en el concepto de frameworks, Laravel, es uno de los frameworks más populares en lo que respecta a PHP. Fue desarrollado por Taylor Otwell en 2011 proporcionando herramientas y recursos para el desarrollo de aplicaciones web y móviles con requerimientos complejos de backend.

Figura 21. Logo de Laravel.

Se destaca por incluir una gran biblioteca de funcionalidades preprogramadas, como el registro y autenticación de usuarios, conexión y gestión de base de datos (Eloquent ORM) para simplificar la manipulación de datos. Algunas otras razones para incluir Laravel en nuestros proyectos:

- Mapeo relacional de objetos: incluye Eloquent, un ORM que presenta las tablas de la base de datos como clases para facilitar el acceso y la manipulación de los datos.

- Plantillas: utiliza el motor de plantillas Blade, agilizando la escritura del código de una forma más simple. Se destaca sobre otros motores por su flexibilidad y la rapidez de procesamiento en el momento que Laravel captura las vistas. Además, permite a los desarrolladores crear macros, definir secciones, extender plantillas a distintas vistas y administrar bucles.

- Autenticación y autorización simplificada.

Esta herramienta utiliza el patrón arquitectónico **MVC (Modelo-Vista-Controlador)** en la cual la aplicación es dividida en tres partes:

- El “Modelo” administra los datos, es decir representa la forma de los datos con los que opera la aplicación.

- Las “Vistas” son las interfaces de usuario con las que el modelo se conecta.

- El “Controlador” contiene la lógica de la aplicación e interactúa con el modelo y lo actualiza en base a las entradas de los usuarios. El controlador manipula la información del modelo para construir una vista.

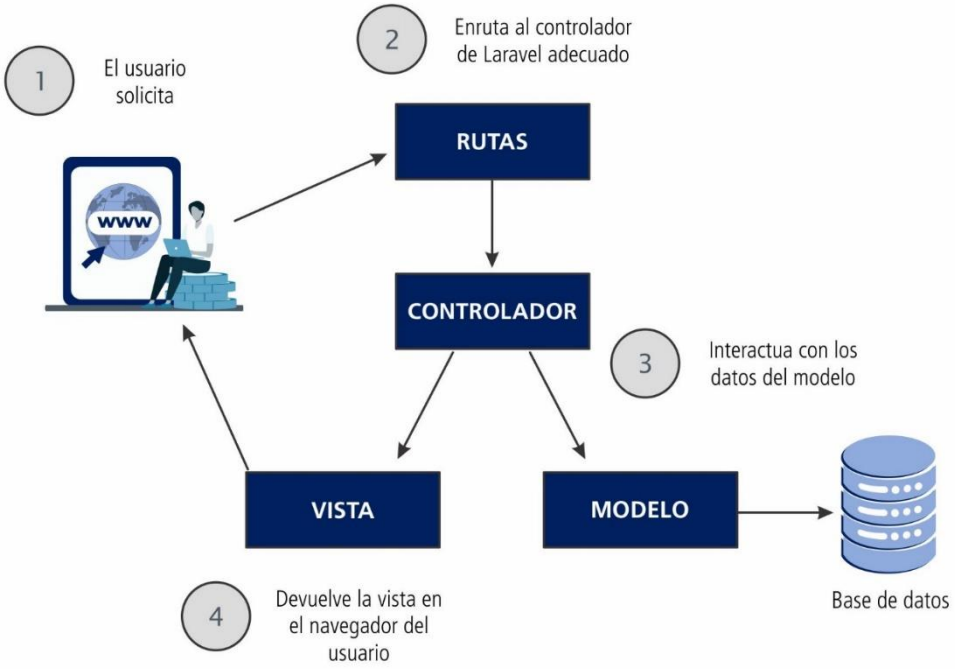

Figura 22. Arquitectura MVC.

Se ha optado por este tipo de arquitectura ya que esta organización en áreas lógicas permite estructurar la aplicación de manera que el código sea más organizado y fácil de depurar, facilitando así el mantenimiento y futuro escalamiento de la aplicación.

Por otro lado, al momento de desarrollar páginas web dinámicas, donde se requiere actualizaciones regulares cada vez que se realiza una solicitud, debemos considerar una infraestructura especial a la que se denomina **LAMP** (figura 23). Esta arquitectura agrupa cuatro tecnologías: un sistema operativo derivado que utiliza el núcleo Linux, Apache como servidor web, la base de datos que deriva de MySQL y PHP para el procesamiento de contenido dinámico.

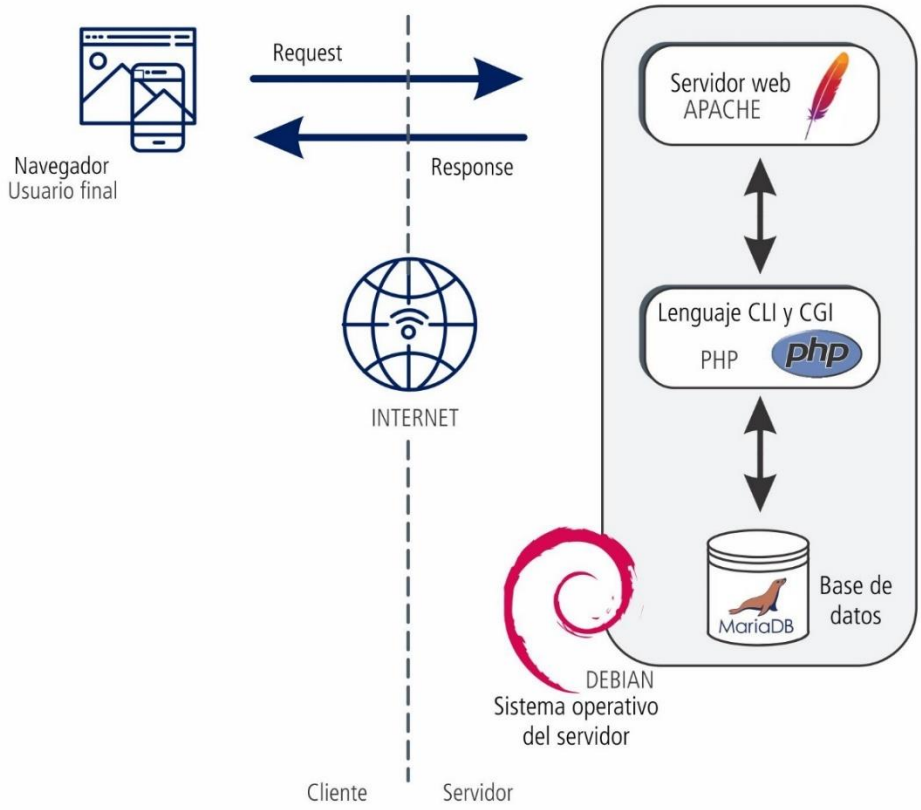

Figura 23. Infraestructura del software.

Cron Jobs

El término “cron” significa *“command run on notice”, es decir, “comando que se ejecuta previo aviso”. De esta manera, c*uando hacemos referencia al término “cron job" hablamos de un administrador o programador de tareas el cual, mediante la ejecución de comandos cada determinadas horas, fechas o intervalos de tiempo específicos, automatizará procesos secuenciales y repetitivos.

Laravel ofrece una manera simple de gestionarlos definiendo un comando con la lógica de la tarea, por ejemplo, limpiar la base de datos mediante la eliminación de entradas, y la periodicidad en que se debe ejecutar.

```
$schedule -> command(´database:cron´) -> monthly();
```

Comando a ejecutar — Periodicidad

Figura 24. Estructura de un cron job.

Base de datos

Sabiendo que el servidor web recibirá cientos de datos por parte de los sensores, debemos definir una base de datos en la cual almacenarlos para así permitir su posterior procesamiento. Entre las opciones de bases de datos relacionales (SQL[3]), se optó por MariaDB: una versión mejorada del tradicional sistema de gestión de bases de datos MySQL.

Figura 25. Logo MariaDB.

Respecto a este, MariaDB posee numerosas funciones incorporadas y mejoras de usabilidad, seguridad y rendimiento. Sin embargo, cuenta con algunas limitaciones. A continuación, en la tabla 1, analizaremos algunas diferencias y similitudes entre estas:

Parámetro	MariaDB	MySQL
Velocidad	Presenta mejoras respecto a MySQL	Exhibe una velocidad reducida respecto a MariaDB
Sistemas operativos de servidor	FreeBSD Linux macOS Solaris Windows	FreeBSD Linux OS X Solaris Windows
Cache / indexación	Un INSERT puede ser completado 24% más rápido que en MySQL estándar	El motor de almacenamiento de memoria es más lento respecto a MariaDB
Replicación	La replicación puede hacerse rápida y segura. Las actualizaciones se realizan 2 veces más rápidas que en MySQL	Según la edición (community o enterprise) se permite un número determinado de subprocesos de conexión.

Tabla 1. Comparación de MariaDB y MySQL.

[3] SQL (Structured Query Lenguage). Lenguaje de consulta estructurado que permite trabajar con un conjunto de datos relacionados ayudando a responder preguntas sobre estos.

ANÁLISIS Y DISEÑO DE LA SOLUCIÓN

IDENTIFICACIÓN DE LOS INTERESADOS

El proyecto está limitado a su MVP, esto quiere decir que una vez concluida esta versión del producto el mismo continuará evolucionando para adaptarse a las necesidades del cliente.

Para poder establecer el alcance del mismo, se comenzará por diferenciar a los distintos interesados que intervienen en la definición y desarrollo del producto:

- Autoridades del área IT, informática e infraestructura: encargados de comunicar los requerimientos del sistema.
- Departamento de seguridad: grupo de personas que manipularán el sistema.
- Secretarías: responsables del control de activación de las alarmas.
- Equipo de desarrollo: grupo de personas que construirán el sistema.

Relevamiento y análisis de requerimientos

En base al contexto de la problemática expuesta con anterioridad, se ha representado en un diagrama de casos de uso cada una de las funcionalidades del sistema que comprenden el alcance del primer MVP propuesto, sus asociaciones y relaciones entre sí para ofrecerle a los distintos usuarios la administración, gestión y conocimiento de los datos recibidos por los sensores de alarma.

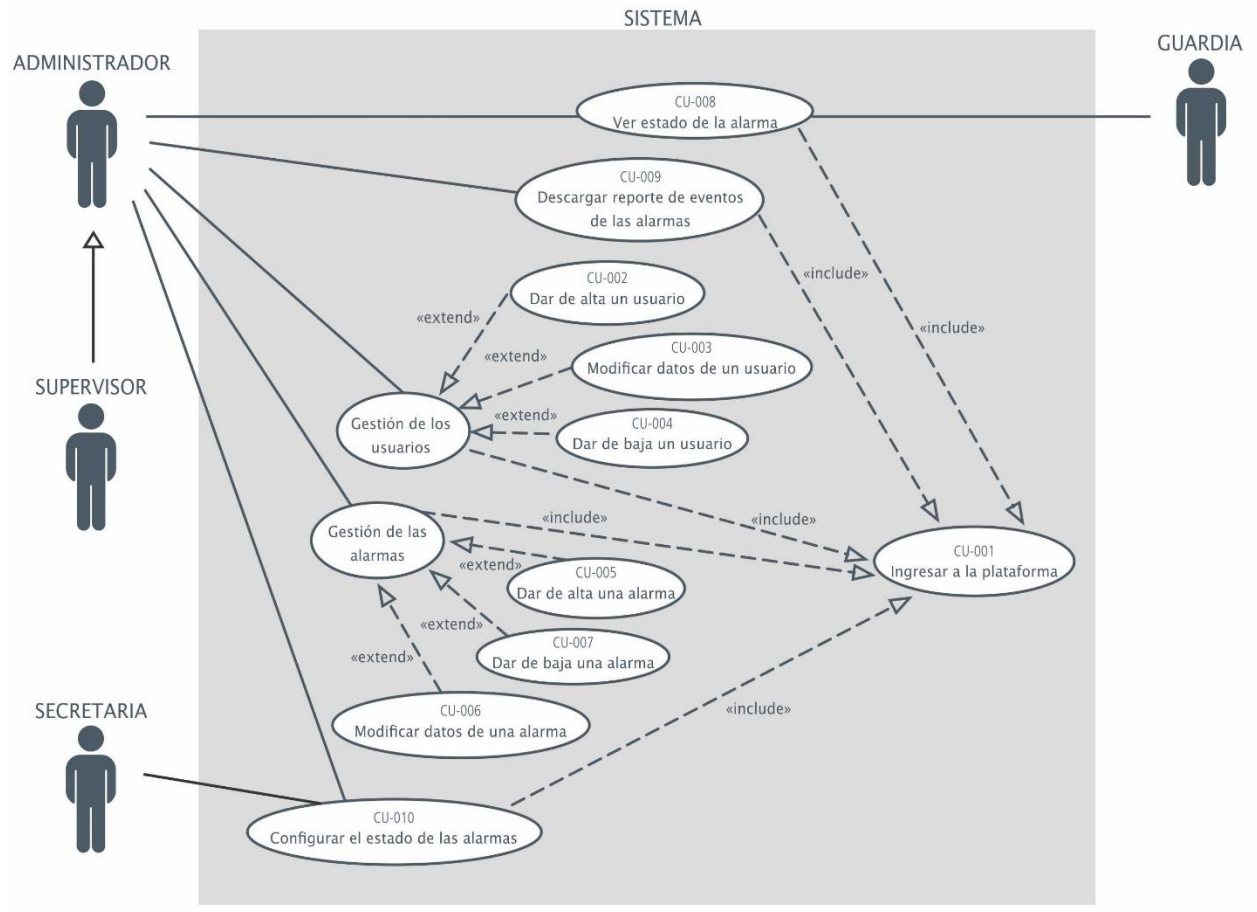

Figura 26. Diagrama de caso de uso de la propuesta.

En este se observan cuatro tipos de roles de usuarios, quienes tendrán interacción con el sistema en base a un conjunto de operaciones permitidas dentro de la plataforma, los cuales se detallan en la matriz a continuación:

OPERACIÓN	Usuario Administrador	Usuario Supervisor	Usuario Guardia	Usuario Secretaria
Identificación en la plataforma	x	x	x	x
Visualización de notificaciones de estado de las alarmas	x	x	x	
Registrar comentarios acerca de la notificación de estado de las alarmas	x	x	x	
Consultar los datos de los usuarios	x	x		
Registrar usuarios de tipo "Supervisor"	x			
Registrar usuarios de tipo "Guardia"	x	x		
Registrar usuarios de tipo "Secretaria"	x	x		
Editar datos de los usuarios	x	x		

Eliminar usuarios	x	x		
Consultar los datos de las alarmas	x	x		
Registrar alarmas	x	x		
Editar datos de las alarmas	x	x		
Eliminar alarmas	x	x		
Descarga de reportes históricos de las alarmas	x	x		
Configurar estado de la alarma	x			x

Tabla 2. Matriz de permisos de los usuarios.

Especificaciones de caso de uso

En base al diagrama de casos de uso, a continuación, se detalla cada una de las funcionalidades disponibles para la gestión de los eventos de las alarmas.

CU-001 Ingresar a la plataforma

Caso de Uso	Ingresar a la plataforma	Id: CU-001
Resumen	Ingreso a la plataforma.	
Actores	Administrador, Supervisor, Guardia, Secretaria.	
Precondición	El usuario debe estar registrado en el sistema.	
Postcondición	El usuario ingresa en la plataforma como Usuario Administrador / Usuario Supervisor / Usuario Guardia / Usuario Secretaria y accede al contenido al cual le es permitido.	

Tabla 3. Descripción del caso de uso "Ingresar a la plataforma".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la dirección de la plataforma.
2	Sistema	Redirige al usuario a la página de ingreso de la plataforma.
3	Usuario	Ingresa su nombre de usuario y contraseña.
4	Sistema	Verifica la condición de registro del usuario controlando el estado de completitud de su registro.
5	Sistema	Muestra las funcionalidades disponibles según sus permisos.

Tabla 4. Descripción del flujo normal del caso de uso "Ingreso a la plataforma".

Flujos Alternos

Nro.	Descripción de acciones alternas
Alt-1	4.1. Si el usuario o la contraseña son incorrectos, el sistema notifica el error.

Tabla 5. Descripción del flujo alterno del caso de uso "Ingresar a la plataforma".

CU-002 Dar de alta de un usuario.

Caso de Uso	Dar de alta de un usuario	Id: CU-002
Resumen	Registro de los datos de un usuario para darle acceso al sistema.	
Actores	Administrador, Supervisor.	
Precondición	El usuario debe estar identificado en el sistema.	
Postcondición	El usuario registra un usuario concediendo acceso a las funcionalidades permitidas para dicho rol.	

Tabla 6. Descripción del caso de uso "Dar de alta un usuario".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Usuarios" y selecciona "Nuevo usuario".
2	Sistema	Redirige al usuario al formulario de registro de nuevos usuarios.
3	Usuario	Ingresa los datos para la dada de alta del usuario: • Nombre. • Apellido. • DNI. • Permisos. • Edificios a cargo. • Usuario. • Contraseña. y envía el formulario.
4	Sistema	Verifica el estado de completitud de los campos solicitados.
5	Sistema	Verifica que el nombre de usuario ingresado no se encuentre registrado.
6	Sistema	Almacena los datos en la base de datos.
7	Sistema	Redirige a la pantalla con la lista de los guardias creados.

Tabla 7. Descripción del flujo normal del caso de uso "Dar de alta un usuario".

Flujos Alternos

Nro.	Descripción de acciones alternas
Alt-1	4.1. Si el usuario envía el formulario con algún dato requerido por el sistema faltante, este notifica que faltan datos para dar de alta el usuario.
Alt-2	5.1. Si el nombre de usuario ya existe le notifica al usuario.

Tabla 8. Descripción del flujo alterno del caso de uso "Dar de alta un usuario".

CU-003 Modificar los datos de un usuario.

Caso de Uso	Modificar los datos de un usuario	Id: CU-003
Resumen	Modificación de los datos de un usuario	
Actores	Administrador, Supervisor.	
Precondición	El usuario debe estar identificado en el sistema. El usuario a modificar, debe estar registrado en el sistema.	
Postcondición	El usuario modifica los datos de un usuario.	

Tabla 9. Descripción del caso de uso "Modificar los datos de un usuario".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Usuario".
2	Sistema	Redirige a la pantalla con la lista de los usuarios creados.
3	Usuario	Selecciona la opción Editar en el usuario deseado.
4	Sistema	Redirige al usuario al formulario de registro de usuarios.
5	Sistema	Modifica cualquiera de los datos del usuarios: • Nombre. • Apellido. • DNI. • Permisos. • Edificios a cargo. • Usuario. • Contraseña. y envía el formulario.
6	Sistema	Verifica el estado de completitud de los campos solicitados.
7	Sistema	Verifica que el nombre de usuario ingresado no se encuentre registrado.
8	Sistema	Almacena los datos en la base de datos.
9	Sistema	Redirige a la pantalla con la lista de los usuarios creados.

Tabla 10. Descripción del flujo normal del caso de uso "Modificar los datos de un usuario".

Flujos Alternos

Nro.	Descripción de acciones alternas
Alt-1	6.1. Si el usuario envía el formulario con algún dato requerido por el sistema faltante, este notifica que faltan datos para dar de alta el usuarios.
Alt-2	7.1. Si el usuario edita el nombre de usuario y este ya existe le notifica al usuario.

Tabla 11. : Descripción del flujo alterno del caso de uso "Modificar los datos de un usuario".

CU-004 Dar de baja un usuario

Caso de Uso	Dar de baja un usuario	Id: CU-004
Resumen	Dada de baja un usuario en el sistema.	
Actores	Administrador, Supervisor.	
Precondición	El usuario debe estar identificado en el sistema. El usuario a dar de baja debe estar registrado en el sistema.	
Postcondición	El usuario eliminado no podrá ingresar nuevamente al sistema.	

Tabla 12. Descripción del caso de uso "Dar de baja un usuario".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Usuarios".
2	Sistema	Redirige a la pantalla con la lista de los usuarios creados.
3	Usuario	Selecciona la opción Eliminar en el usuario deseado.
4	Sistema	Solicita confirmación de la acción a través de un modal.
5	Sistema	Confirma la acción de eliminar el usuario.
6	Sistema	Elimina el usuario de la base de datos.
7	Sistema	Redirige al usuario a la pantalla con la lista de los usuarios registrados.

Tabla 13. Descripción del flujo normal del caso de uso "Dar de baja un usuario".

Flujos Alternos

Nro.	Descripción de acciones alternas
Alt-1	4.1. Si el usuario cancel a la operación, el sistema ignora la solicitud.

Tabla 14. Descripción del flujo alterno del caso de uso "Dar de baja un usuario".

CU-005 Dar de alta una alarma

Caso de Uso	Dar de alta una alarma	Id: CU-005
Resumen	Registro de los datos de una alarma para darla de alta en el sistema.	
Actores	Administrador, Supervisor.	
Precondición	El usuario debe estar identificado en el sistema.	
Postcondición	El usuario registra una alarma en el sistema.	

Tabla 15. Descripción del caso de uso "Dar de alta una alarma".

Flujo Normal.

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Alarmas" y selecciona "Nueva alarma".
2	Sistema	Redirige al usuario al formulario de registro de nuevas alarmas.
3	Usuario	Ingresa los datos para la dada de alta de la alarma: • Nombre. • Sitio. • Facultad / Edificio. • Aula o Dependencia donde se ubican el/los componentes. • Número identificador del componente. • Tipo de componente. • Nombre y Apellido del responsable. • Email. • Teléfono celular. y envía el formulario. Podrá registrar más de un componente y un responsable en el mismo formulario. Opcionalmente ingresará el procedimiento correspondiente a la alarma.
4	Sistema	Verifica el estado de completitud de los campos solicitados.
5	Sistema	Almacena los datos en la base de datos.
6	Sistema	Redirige a la pantalla con la lista de las alarmas dadas de alta.

Tabla 16. Descripción del flujo normal del caso de uso "Dar de alta una alarma".

Flujos Alternos

Nro.	Descripción de acciones alternas
Alt-1	4.1. Si el usuario envía el formulario con algún dato requerido por el sistema faltante, este notifica que faltan datos para dar de alta el guardia.

Tabla 17. Descripción del flujo alterno del caso de uso "Dar de alta una alarma".

CU-006 Modificar los datos de una alarma

Caso de Uso	Modificar los datos de una alarma	Id: CU-006
Resumen	Modificación de los datos de una alarma.	
Actores	Administrador, Supervisor.	
Precondición	El usuario debe estar identificado en el sistema. La alarma debe estar registrada en el sistema.	
Postcondición	El usuario modifica los datos de un alarma.	

Tabla 18. Descripción del caso de uso "Modificar los datos de una alarma".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Alarmas".
2	Sistema	Redirige a la pantalla con la lista de las alarmas creadas.
3	Usuario	Selecciona la opción Editar en la alarma deseada.
4	Sistema	Redirige al usuario al formulario de registro de las alarmas.
5	Usuario	Modifica los datos para la dada de alta de la alarma: • Nombre. • Sitio. • Facultad / Edificio. • Aula o Dependencia donde se ubican el/los componentes. • Número identificador del componente. • Tipo de componente. • Nombre y Apellido del responsable. • Email. • Teléfono celular. • Procedimiento. y envía el formulario. En caso que la alarma tenga mas de un componente y mas de un responsable registrado, todos ellos podrán ser editados.
6	Sistema	Verifica el estado de completitud de los campos solicitados.
7	Sistema	Almacena los datos en la base de datos.
8	Sistema	Redirige a la pantalla con la lista de las alarmas creadas.

Tabla 19. Descripción del flujo normal del caso de uso "Modificar los datos de una alarma".

Flujos Alternos

Nro.	Descripción de acciones alternas
Alt–1	6.1. Si el usuario envía el formulario con algún dato requerido por el sistema faltante, este notifica que faltan datos para dar de alta la alarma.

Tabla 20. Descripción del flujo alterno del caso de uso "Modificar los datos de una alarma".

CU-007 Dar de baja una alarma

Caso de Uso	Dar de baja una alarma	Id: CU-007
Resumen	Dada de baja de una alarma en el sistema.	
Actores	Administrador, Supervisor.	
Precondición	El usuario debe estar identificado en el sistema. La alarma debe estar registrada en el sistema	
Postcondición	Los eventos de la alarma eliminada no serán registrados en el sistema.	

Tabla 21. Descripción del caso de uso "Dar de baja una alarma".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Alarmas".
2	Sistema	Redirige a la pantalla con la lista de las alarmas creadas.
3	Usuario	Selecciona la opción Eliminar en la alarma deseada.
4	Sistema	Solicita confirmación de la acción a través de un modal.
5	Usuario	Confirma la acción de eliminar la alarma.
6	Sistema	Elimina la alarma de la base de datos.
7	Sistema	Redirige al usuario a la pantalla con la lista de las alarmas dadas de alta.

Tabla 22. Descripción del flujo normal del caso de uso "Dar de baja una alarma".

Flujos Alternos

Nro.	Descripción de acciones alternas
Alt-1	4.1. Si el usuario cancela la operación, el sistema ignora la solicitud.

Tabla 23. Descripción del flujo alterno del caso de uso "Dar de baja una alarma".

CU-008 Ver el estado de la alarma

Caso de Uso	Ver el estado de la alarma	Id: CU-008
Resumen	Visualización del estado de una alarma	
Actores	Administrador, Supervisor, Guardia	
Precondición	El usuario debe estar identificado en el sistema. La alarma debe estar registrada en el sistema.	
Postcondición	El usuario es notificado acerca de un evento de la alarma.	

Tabla 24. Descripción del caso de uso "Ver el estado de la alarma".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la página principal de la aplicación.
2	Sistema	El sistema genera las notificaciones de los eventos (tensión, batería o activación de un sensor.
3	Usuario	Confirma que fue notificado acerca del evento.
4	Sistema	Registra la confirmación y la hora y fecha de la misma en la base de datos.

Tabla 25. Descripción del flujo normal del caso de uso "Ver el estado de la alarma".

Flujos Alternos.

Nro.	Descripción de acciones alternas
Alt-1	3.1. Si la notificación es por activación del sensor, el usuario puede registrar un comentario sobre el mismo.

Tabla 26. Descripción del flujo alterno del caso de uso "Ver el estado de la alarma".

CU-009 Descargar reporte de eventos de las alarmas

Caso de Uso	Descargar reporte de eventos de la alarma	Id: CU-009
Resumen	Descarga de reporte de historial de eventos de las alarmas en un periodo determinado.	
Actores	Administrador, Supervisor.	
Precondición	El usuario debe estar identificado en el sistema.	
Postcondición	El usuario obtiene un reporte histórico de las alarmas.	

Tabla 27. Descripción del caso de uso "Descargar reporte de eventos de la alarma".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Alarmas".
2	Sistema	Redirige a la pantalla con la lista de las alarmas creadas.
3	Usuario	Selecciona la opción Descargar reporte.
4	Sistema	Disponibiliza el modal donde se solicita la selección del rango de fechas.
5	Usuario	Selecciona el rango de fecha del reporte y aplica la selección.
6	Sistema	Solicita la confirmación de descarga del reporte.
7	Sistema	Descarga el archivo en formato .xlsx con los históricos dentro del rango de fecha.

Tabla 28. Descripción del flujo normal del caso de uso "Descargar reporte de eventos de la alarma".

Flujos Alternos.

Nro.	Descripción de acciones alternas
Alt-1	6.1. Si el usuario cancela la operación, el sistema ignora la solicitud.

Tabla 29. Descripción del flujo alterno del caso de uso "Descargar reporte de eventos de la alarma".

CU-010 Configurar el estado de las alarmas

Caso de Uso	Configurar el estado de las alarmas	Id: CU-010
Resumen	Configuración de las alarmas (activadas o desactivadas).	
Actores	Administrador, Supervisor, Secretaria.	
Precondición	El usuario debe estar identificado en el sistema. La alarma debe estar registrada en el sistema.	
Postcondición	El usuario activa o desactiva una alarma específica.	

Tabla 30. Descripción del caso de uso "Configurar el estado de las alarmas".

Flujo Normal

Nro.	Ejecutor	Paso o Actividad
1	Usuario	Ingresa a la sección "Panel de control".
2	Sistema	Redirige a la pantalla con la lista de las alarmas correspondientes a los edificios asignados.
3	Usuario	Actualiza el estado de la alarma mediante el interruptor.
4	Sistema	Almacena el nuevo estado de la alarma en la base de datos.

Tabla 31. Descripción del flujo normal del caso de uso "Configurar el estado de las alarmas".

Flujos Alternos

Nro.	Descripción de acciones alternas
	N/A

Tabla 32. Descripción del flujo alterno del caso de uso "Configurar el estado de las alarmas".

Por otro lado, en la tabla 33 se presentan los casos de uso correspondientes a los módulos de hardware que conforman el sistema.

Acción	Respuesta
El desarrollador conecta las placas de desarrollo a una computadora para cargar su firmware.	Se inicializan las placas de desarrollo y se cargan sus configuraciones por primera vez.
El desarrollador ensambla los módulos siguiendo los diagramas de conexión	Se generan los 3 módulos completos con todas sus conexiones pertinentes.
El desarrollador conecta los módulos a las fuentes de alimentación.	Los módulos se inicializan, se conectan a la red WiFi y comienzan la comunicación con el Broker MQTT
El desarrollador ingresa al Broker MQTT para visualizar la recepción de las señales enviadas.	Se visualiza en el Broker la recepción de las señales de cada uno de los módulos instalados e inicializados.
Se quiere agregar un módulo nuevo	Se carga un nuevo sensor en el sistema web. Se inicializa el módulo por primera vez cargando el código, configuración correspondiente y se ensambla.
Se agrega un módulo nuevo	Se lo alimenta por primera vez,se lo inicializa, se conecta a la red WiFi y comienza la comunicación con el Broker MQTT
Se pierde la conexión WiFi	Se reconecta automáticamente y vuelve a enviar información al servidor MQTT
Ocurre un corte de suministro eléctrico y luego de un tiempo regresa a su estado normal.	El módulo de lectura de tensión y de batería se conectan nuevamente al regresar la tensión eléctrica y vuelven a enviar la información.

Tabla 33. Casos de uso del hardware.

Diseño de la base de datos

Como parte del diseño de la solución se modeló la estructura de almacenamiento y acceso a los datos empleando los diagramas Relacional y de Entidad-Relación. A continuación, se presentan los modelos que se utilizarán para la construcción de la base de datos del sistema de monitoreo.

Modelo entidad relación.

El modelo de datos entidad-relación permite presentar el mundo real con un conjunto de objetos básicos, denominados entidades, y de las relaciones entre esos objetos. Además, estas entidades se describen mediante sus atributos.

De esta manera, se tomaron los requerimientos funcionales y los datos necesarios para conseguir desarrollar la solución propuesta para plantear las

colecciones de objetos que se deberían implementar como se muestra a continuación en la figura 27.

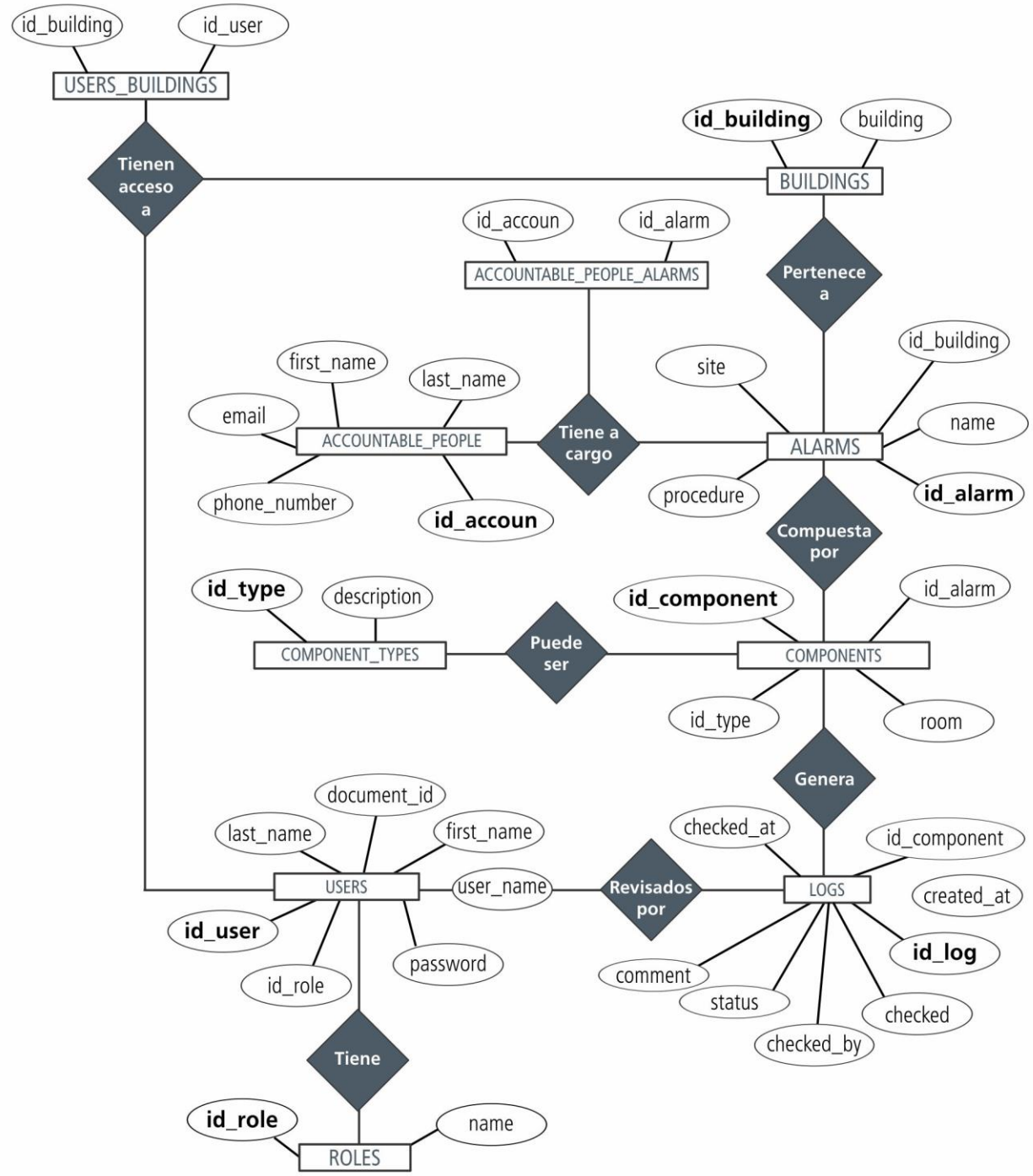

Figura 27. Modelo entidad - relación.

Descripción de las entidades del sistema

A continuación, se describen las entidades representadas en el Modelo E/R. La notación utilizada en la columna Tipo para cada identificador de entidad es la siguiente:

Abreviatura	Significado
SP/SC	Simple/Compuesto
OB/OP	Obligatorio/Opcional
PK	Clave primaria
FK	Clave ajena

Tabla 34. Descripción de los tipos.

- **USERS:** Almacena los datos de todos los usuarios del sistema.

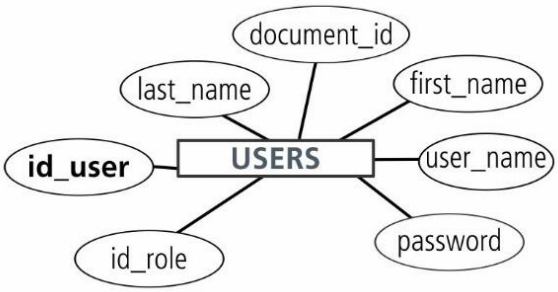

Figura 28. Entidad USERS.

Está compuesta por los siguientes identificadores:

Entidad USERS			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_user	PK, SP, OB	bigint(20)	Identificador de usuario
id_role	FK, SP, OB	bigint(20)	Identificador del rol
first_name	SP, OB	varchar(256)	Nombre del usuario
last_name	SP, OB	varchar(256)	Apellido del usuario
document_id	SP, OB	varchar(16)	DNI del usuario
user_name	SP, OB	varchar(256)	Nombre del usuario para el ingreso a la plataforma
password	SP, OB	varchar(256)	Contraseña del usuario para el ingreso a la plataforma
RESTRICCIONES			
El atributo id_user es un identificador generado de forma secuencial.			

Tabla 35. Descripción entidad USERS.

- **ROLES:** Almacena los datos de los roles de los usuarios del sistema.

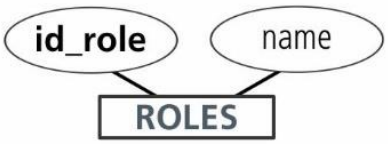

Figura 29. Entidad ROLES.

Está compuesta por los siguientes identificadores:

Entidad ROLES			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_role	PK, SP, OB	bigint(20)	Identificador del rol
name	SP, OB	varchar(256)	Nombre del rol
RESTRICCIONES			
El atributo id_role es un identificador generado de forma secuencial.			

Tabla 36. Descripción entidad ROLES.

- **BUILDINGS:** Almacena los datos de los edificios/facultades del sistema.

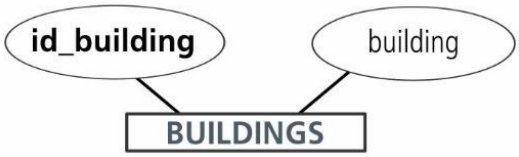

Figura 30. Entidad BUILDINGS.

Está compuesta por los siguientes identificadores:

Entidad BUILDINGS			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_building	PK, SP, OB	bigint(20)	Identificador del edificio / facultad.
building	SP, OB	varchar(256)	Nombre del edificio / facultad.
RESTRICCIONES			
El atributo id_building es un identificador generado de forma secuencial.			

Tabla 37. Descripción entidad BUILDINGS.

- **USERS_BUILDINGS:** Almacena los datos de asociación de los edificios/facultades y las alarmas registradas en el sistema.

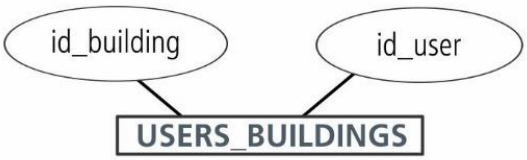

Figura 31. Entidad USERS_BUILDINGS.

Está compuesta por los siguientes identificadores:

Entidad USERS_BUILDINGS			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_building	PK, FK, SP, OB	bigint(20)	Identificador del edificio / facultad.
id_user	PK, FK, SP, OB	bigint(20)	Identificador del responsable
RESTRICCIONES			
El atributo id_building es un identificador generado de forma secuencial.			

Tabla 38. Descripción entidad USERS_BUILDINGS.

- **ALARMS:** Almacena los datos de las alarmas del sistema.

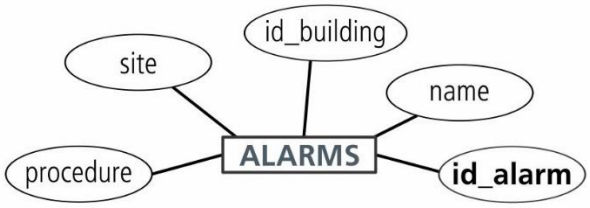

Figura 32. Entidad ALARMS.

Está compuesta por los siguientes identificadores:

Entidad ALARMS			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_alarm	PK, SP, OB	bigint(20)	Identificador de la alarma
id_building	FK,SP,OB	bigint(20)	Identificador del edificio / facultad
name	SP, OB	varchar(256)	Nombre de la alarma
site	SP, OB	varchar(64)	Nombre de la sede o predio donde se ubica la alarma
procedure	SP, OP	text	Procedimiento a seguir
RESTRICCIONES			
El atributo id_alarm es un identificador generado de forma secuencial.			

Tabla 39. Descripción entidad ALARMS.

- **ACCOUNTABLE_PEOPLE:** Almacena los datos de los responsables de las alarmas registradas en el sistema.

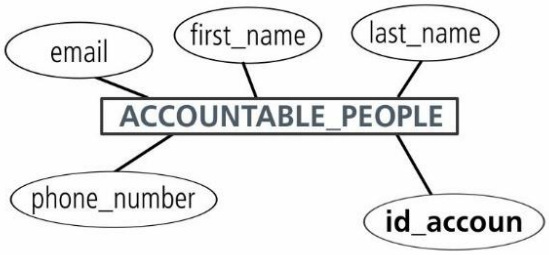

Figura 33. Entidad ACCOUNTABLE_PEOPLE.

Está compuesta por los siguientes identificadores:

Entidad ACCOUNTABLE_PEOPLE			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_accoun	PK, SP, OB	bigint(20)	Identificador del responsable
first_name	SP, OB	varchar(256)	Nombre del responsable
last_name	SP, OB	varchar(256)	Apellido del responsable
phone_number	SP, OB	varchar(64)	Número de teléfono para contacto del responsable
email	SP, OB	varchar(256)	Email del responsable
RESTRICCIONES			
El atributo id_accoun es un identificador generado de forma secuencial.			

Tabla 40. Descripción entidad ACCOUNTABLE_PEOPLE.

- **ACCOUNTABLE_PEOPLE_ALARMS:** Almacena los datos de asociación de los responsables y las alarmas registradas en el sistema.

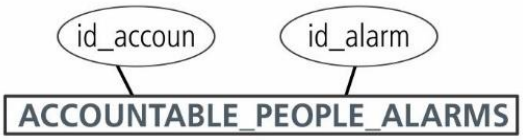

Figura 34. Entidad ACCOUNTABLE_PEOPLE_ALARMS

Está compuesta por los siguientes identificadores:

Entidad ACCOUNTABLE_PEOPLE			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_accoun	PK, SP, OB	bigint(20)	Identificador del responsable
first_name	SP, OB	varchar(256)	Nombre del responsable
last_name	SP, OB	varchar(256)	Apellido del responsable
phone_number	SP, OB	varchar(64)	Número de teléfono para contacto del responsable
email	SP, OB	varchar(256)	Email del responsable
RESTRICCIONES			
El atributo id_accoun es un identificador generado de forma secuencial.			

Tabla 41. Descripción entidad ACCOUNTABLE_PEOPLE_ALARMS.

- **COMPONENTS:** Almacena los datos de los componentes pertenecientes a las alarmas.

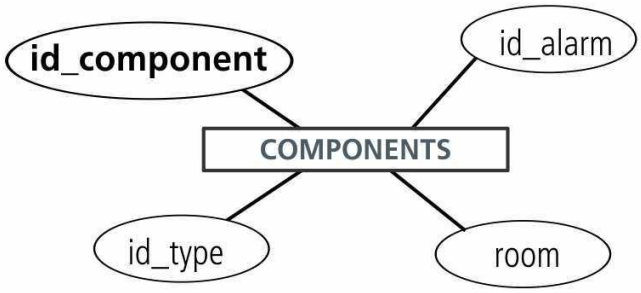

Figura 35. Entidad COMPONENTS.

Está compuesta por los siguientes identificadores:

Entidad COMPONENTS			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_component	PK, SP, OB	bigint(20)	Identificador del componente
id_type	FK, SP, OB	bigint(20)	Identificador del tipo del componente
id_alarm	FK, SP, OB	bigint(20)	Identificador de la alarma
room	SP, OB	varchar(256)	Nombre de la dependencia o aula donde se ubica el componente

Tabla 42. Descripción entidad COMPONENTS.

- **COMPONENT_TYPES:** Almacena los datos de asociación de los componentes y su tipo.

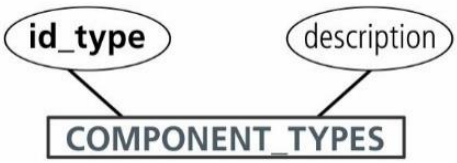

Figura 36. Entidad COMPONENT_TYPES.

Está compuesta por los siguientes identificadores:

Entidad COMPONENT_TYPES			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_type	PK, SP, OB	bigint(20)	Identificador del tipo de componente
name	SP, OB	varchar(256)	Nombre del componente
RESTRICCIONES			
El atributo id_type es un identificador generado de forma secuencial.			

Tabla 43. Descripción entidad COMPONENTS_TYPES.

- **LOGS:** Almacena los datos históricos de los eventos de las alarmas.

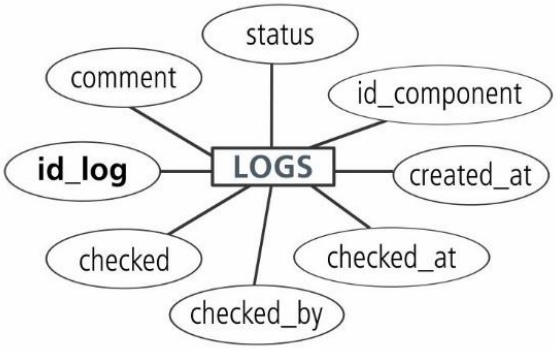

Figura 37. Entidad LOGS.

Está compuesta por los siguientes identificadores:

Entidad LOGS			
ATRIBUTO	**TIPO**	**FORMATO**	**DESCRIPCIÓN**
id_log	PK, SP, OB	bigint(20)	Identificador del historial
id_component	FK, SP, OB	bigint(20)	Identificador del componente
status	SP, OB	varchar(256)	Estado del componente
comment	SP, OP	varchar(1024)	Comentario acerca del evento del componente

created_at	SP, OB	datetime	Fecha y hora de generación del historial
checked	SP, OB	tinyint(1)	Confirmación de lectura
checked_at	SP, OB	datetime	Fecha y hora de la confirmación de lectura
checked_by	SP, OB	bigint(20)	Identificador del usuario quien confirmó la lectura

RESTRICCIONES

El atributo id_log es un identificador generado de forma secuencial.
El atributo status tomará valor:

- 0 si la alarma no se ha disparado.
- 1 si la alarma se dispara.

El atributo checked tomará valor:

- 0 si la notificación no fue leída.
- 1 si la notificación fue leída.

Tabla 44. Descripción entidad LOGS.

Modelo relacional de datos

Una vez completado el diseño conceptual, se plantea el diseño lógico donde se describe la estructura de la base de datos. El modelo relacional (figura 38) se conforma de tablas y relaciones entre ellas siguiendo el diagrama anterior. Las tablas son la unidad de almacenamiento principal donde, mediante las filas y columnas que la componen, se almacenarán cada uno de los registros de la entidad.

En el modelo relacional de datos se observan las principales colecciones de datos que harán posible el administrar, gestionar y consultar los datos obtenidos de los sensores del sistema de monitoreo. Dentro de las tablas, o colecciones, se destacan: Alarmas (Alarms), la cual almacena los datos del registro de estas en el sistema; e Historial (Logs), que contiene los datos recibidos por los sensores y cómo se actúa frente a la alerta.

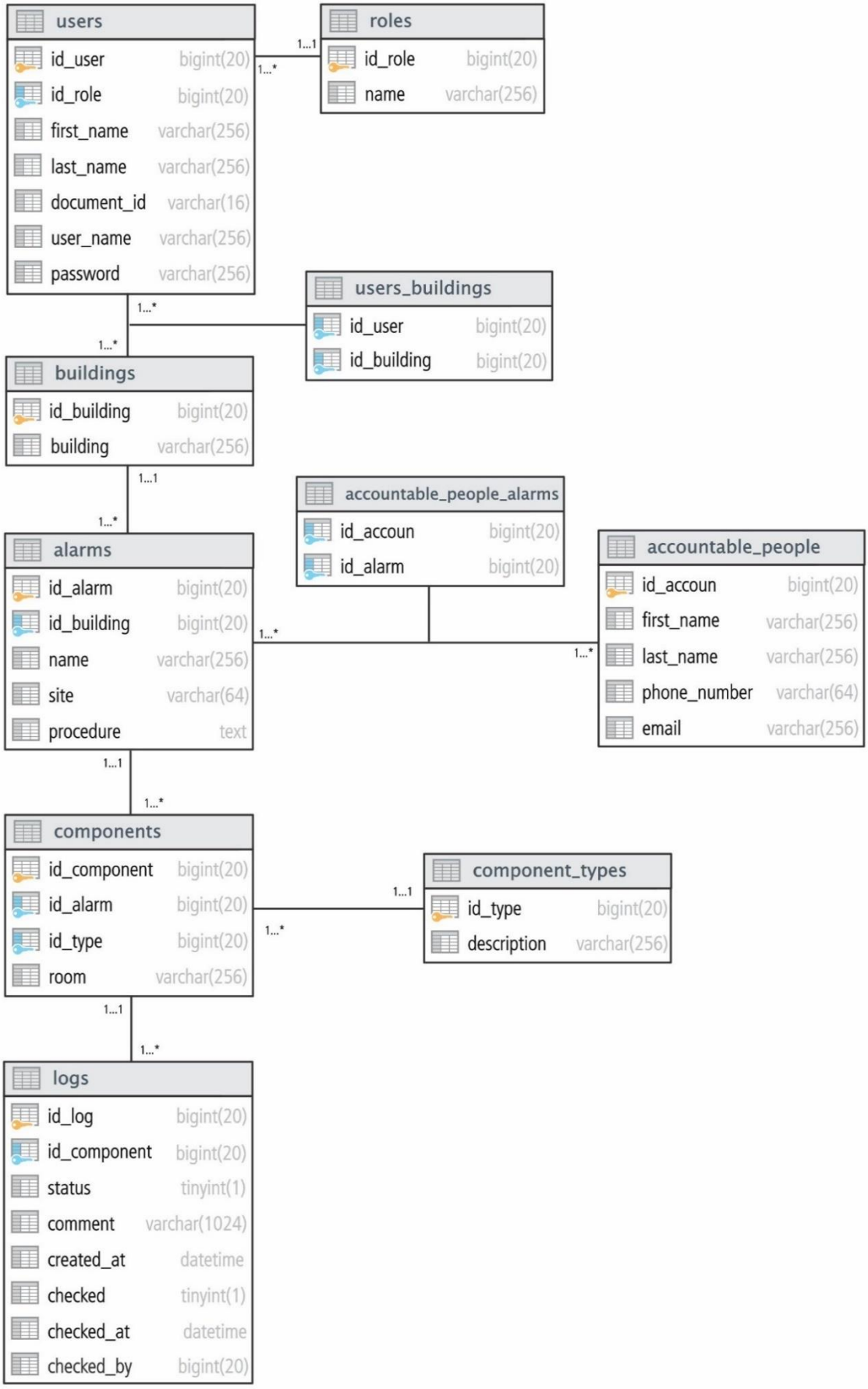

Figura 38. Modelo relacional de datos.

Diseño de interfaces de usuario

Partiendo del hecho que la aplicación será implementada en la Universidad Católica, se aplicará en las interfaces de usuario el logotipo, la paleta de colores y tipografía señalados en el manual de identidad visual. En las figuras 39 y 40 se pueden observar los elementos principales a utilizar.

Figura 39. Logotipo de la Universidad. UNIVERSIDAD CATÓLICA DE CÓRDOBA. (n.d.). https://www.ucc.edu.ar/archivos/documentos/MANUAL_DE_IDENTIDAD_2018/MANUAL-DE-USO-DE-LA-IDENTIDAD-VISUAL-UCC-18-1.pdf

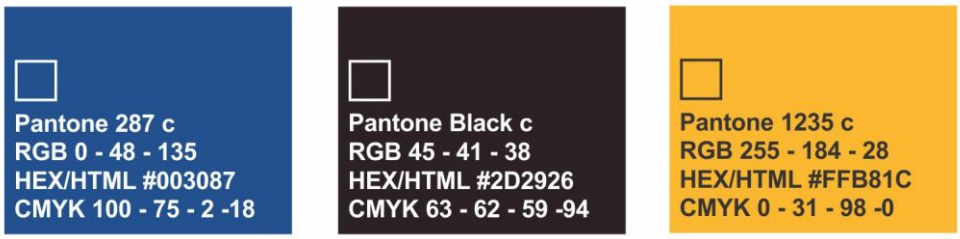

Figura 40. Colores institucionales de la universidad. UNIVERSIDAD CATÓLICA DE CÓRDOBA. (n.d.). https://www.ucc.edu.ar/archivos/documentos/MANUAL_DE_IDENTIDAD_2018/MANUAL-DE-USO-DE-LA-IDENTIDAD-VISUAL-UCC-18-1.

DESARROLLO DE LA PROPUESTA

En este capítulo se detalla el desarrollo llevado a cabo para la consecución de los objetivos del MVP propuesto en tres etapas: en la primera se describe la solución en general, en las siguientes la misma desde una perspectiva de hardware y de software. Se detallará además la arquitectura general elegida y la justificación de la elección de la misma.

Descripción general de la solución

Este proyecto fue planteado frente a la necesidad de la Universidad Católica de Córdoba de centralizar las alertas del sistema de alarmas extendido en las tres sedes y optimizar el tiempo de respuesta de los guardias frente a estas. A diferencia de las propuestas existentes en el mercado, se busca una solución económica, escalable y que se adapte a la necesidad de la organización actual de la misma.

Arquitectura

El sistema en su totalidad se divide en dos partes: el desarrollo del software y del hardware. La primera estará conformada por la aplicación web, el Broker MQTT, el firmware de los módulos y el desarrollo de un módulo virtual, por otro lado, el hardware contará con el desarrollo de 3 módulos capaces de captar señales y comunicarlas a través de WiFi utilizando un protocolo MQTT. Los módulos ensamblados contarán con un microprocesador y una serie de sensores y elementos de alimentación para la correcta lectura de la información.

Se plantea una red de topología en estrella, teniendo así un único controlador que recibe los datos y, mediante una interfaz de usuario, permite manipularlos. La figura 41 muestra la arquitectura general del sistema, teniendo en cuenta los componentes, la interacción entre estos y los dispositivos de los usuarios finales.

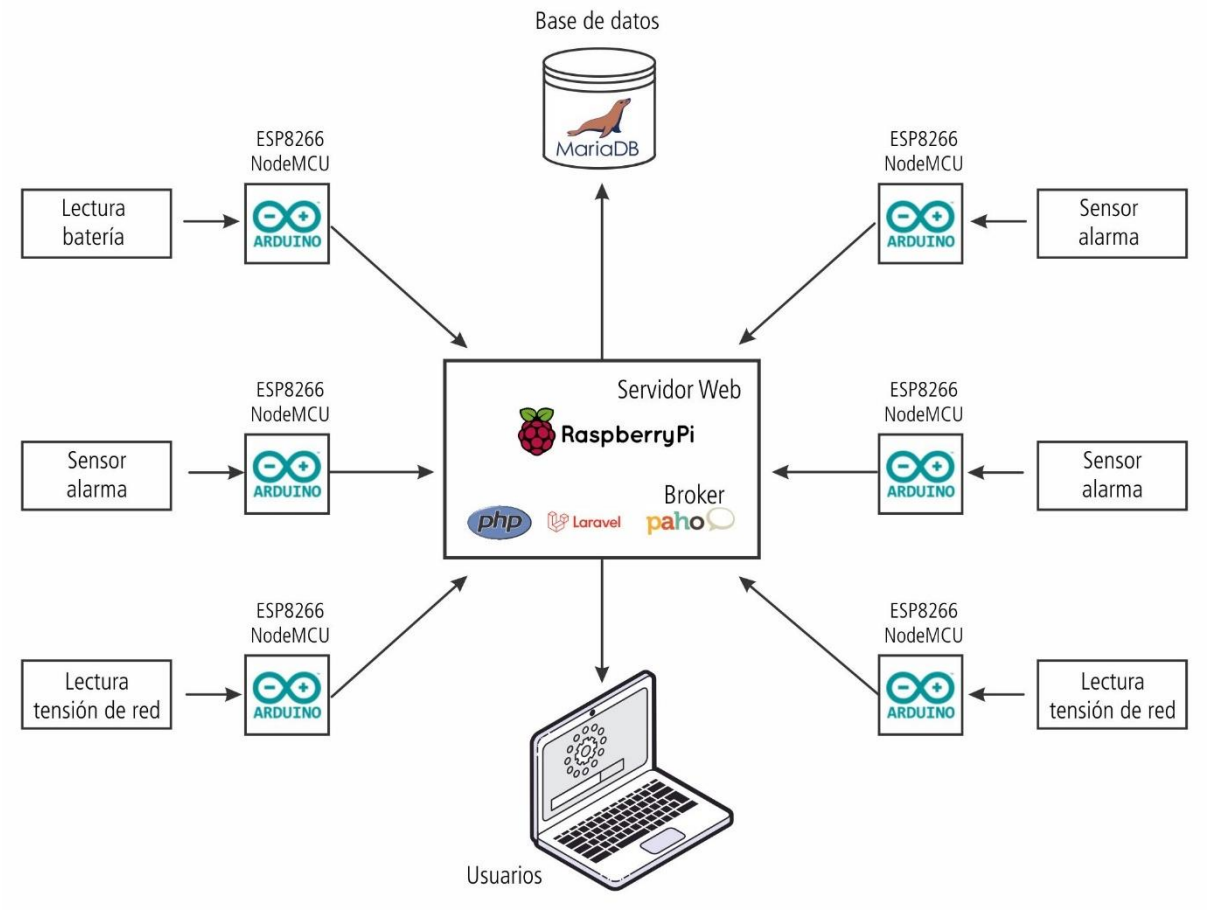

Figura 41. Arquitectura general del sistema.

El flujo de información comienza con el constante análisis del entorno por parte de los sensores PIR, la lectura de la tensión de red, la batería del sistema de alarma y el estado de los botones de activación.

Los módulos ESP8266 en conjunto con diversos sensores captan información y la transmiten mediante WiFi aplicando el protocolo de transmisión MQTT, al broker alojado en la Raspberry Pi. En el servidor web, se aloja el modelo de la base de datos utilizando MariaDB, la aplicación web desarrollada en Laravel y un módulo de botones de activación digital.

Seguridad

Debido a que es un sistema de alarma de seguridad, la confiabilidad, estabilidad y seguridad del proyecto es uno de los temas más delicados del desarrollo.

Por parte del hardware cada uno de los módulos se comunicará con el servidor web utilizando el protocolo MQTT, como fue mencionado anteriormente, el protocolo tiene el transporte de la información con tecnología SSL/TLS. En nuestro sistema, las comunicaciones son unidireccionales, es decir que los componentes envían información al servidor. Esto proporciona una capa más de seguridad, ya que si acceden a la red o descifran el protocolo de comunicación solo podrán ver la información que envían los sensores a la central sin tener la capacidad de visualizar el estado de la central ni de manipular información saliente de la central.

Por parte del software, la aplicación web tiene un ingreso con nombre de usuario y contraseña. Cada usuario será dado de alta por el supervisor o administrador en el caso que corresponda y en la creación del mismo se le otorgarán los permisos pertinentes. La aplicación será ejecutada de manera local, esto quiere decir que no se publicará en la red pública donde cualquier usuario puede acceder a ella mediante una dirección URL, sino que su acceso estará dado mediante una dirección IP de uso interno. Se debe estar conectado a la red WiFi de la universidad para poder acceder al sitio.

Análisis Funcional

Para ilustrar y analizar la problemática nos basaremos en el siguiente caso práctico que se representa en la figura 42: la Facultad de Ingeniería se compone de numerosas aulas y oficinas en las cuales podemos encontrar distintos componentes referentes al sistema de seguridad de la misma: sensores de movimiento y botones de activación de las alarmas. A su vez, cada alarma transmitirá datos acerca del estado de su batería o tensión.

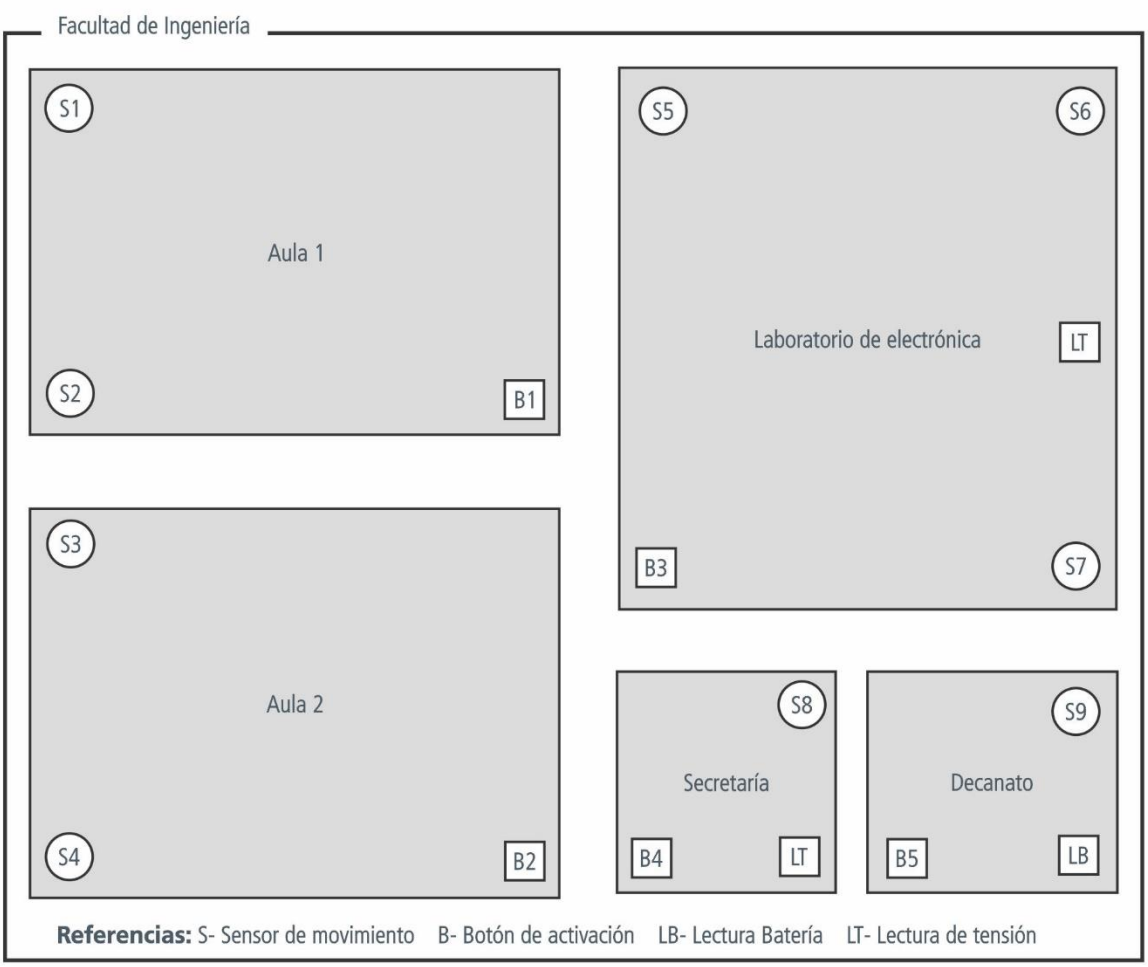

Figura 42. Caso práctico: sistema de alarmas de la Facultad de Ingeniería.

Cabe destacar que los módulos relacionados a la lectura de batería, tensión y movimiento serán implementados de forma física mientras que el botón, por cuestiones de seguridad, será accionado desde el panel dentro de la aplicación web por quienes tengan el acceso permitido. Todos estos deberán comunicarse unidireccional e independientemente con un servidor web. En la figura 43 se presenta un diagrama del envió de información de los módulos al Broker MQTT.

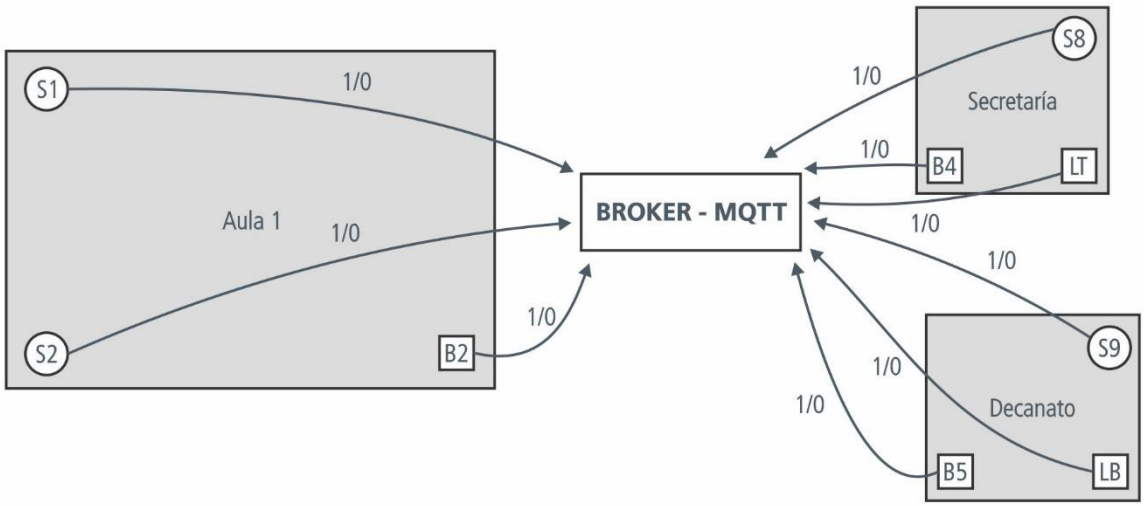

Figura 43. Representación del envío de información.

De esta manera, la aplicación debería detectar tres casos principales que derivan de la transmisión de estos componentes:

- **Detección de falla de tensión eléctrica:** cuando el módulo de lectura de tensión (LT) detecta una disminución en el voltaje de red envía la señal al servidor central interpretandolo como un 1. Este procesa este valor activando la alerta de falla de tensión de red. En el caso que la tensión sea la habitual el módulo envía el valor 0 periódicamente.

```
{"data": [{ "component_id": 21,"status": "1.00","type": "alarm_status"}]}
```

Figura 44. Payload lectura de tensión eléctrica.

- **Detección de una falla en la batería de la alarma:** La batería será constantemente analizada por su respectivo sensor (LB), en el caso que este detecte una disminución del voltaje por debajo de un margen de seguridad, el sensor se activa y envía un 1 al servidor, este al recibirlo emite una alerta para que la batería sea modificada o verificada por un especialista. En el caso contrario el módulo envía un valor 0 periódicamente.

```
{"data": [{ "component_id": 3,"status": "1.00","type": "alarm_status"}]}
```

Figura 45. Payload lectura de batería.

- Por último, la **detección de movimiento por los sensores PIR y la activación de los botones**: estos son dependientes uno del otro ya que los sensores registran constantemente el ambiente y al detectar movimiento envían un 1 al servidor web. Al mismo tiempo, para que una notificación emerja en el sistema, el botón relacionado a la misma alarma a la que pertenece el sensor deberá encontrarse en estado “Activada”.


```
{"data": [{ "component_id": 5,"status": "1.00","type": "alarm_status"}]}
```


Figura 46. Payload de detección de movimiento por los sensores PIR.

Retomando el ejemplo anterior, analicemos el caso de detección de movimiento en detalle: para alertar un caso de intrusión en el aula 1 debe darse la condición que el S1 o S2 estén activados y que la secretaría haya activado el B1 desde la aplicación. De ser así el sistema notificará al guardia para accionar de inmediato. Como caso contrario, si B4 está activado y el S1 y S2 también, al no haber relación entre los sensores y el botón, no se emitirá una notificación en el sistema.

Hardware

El desarrollo del hardware del proyecto se basa en el ensamblaje de distintos módulos a los cuales solo los desarrolladores y equipo de instalación pueden acceder y configurar. Al ser un sistema de seguridad cualquier alteración que sufran los equipos puede ser un riesgo en la fiabilidad del sistema en su totalidad. Si bien la instalación de los módulos es sencilla y práctica, el único componente que puede ser instalado por el usuario es el módulo de lectura de tensión ya que su implementación consiste en conectarlo a la red. Los demás módulos deben ser instalados por el personal de seguridad ya que se deben intervenir componentes que ya forman parte del sistema de alarmas.

A continuación, se describen cada uno de ellos, sus diagramas de conexión y funcionamiento.

Módulo 1

Se encarga de leer la tensión de la red eléctrica. Con el uso del sensor ZMPTB101 se recolecta la información del voltaje y con una placa de desarrollo ESP8266 NodeMCU se transmite vía WiFi al Broker MQTT.

En cuanto a su funcionamiento, el regulador de voltaje es alimentado por una fuente de alimentación de 12 voltios. A la salida del mismo se reduce a solo 5 voltios para alimentar el sensor. A través de un divisor resistivo se logra obtener la correcta alimentación para la placa de desarrollo. La salida del sensor es captada por el pin A0 del kit de desarrollo. Este es representado en la figura 47.

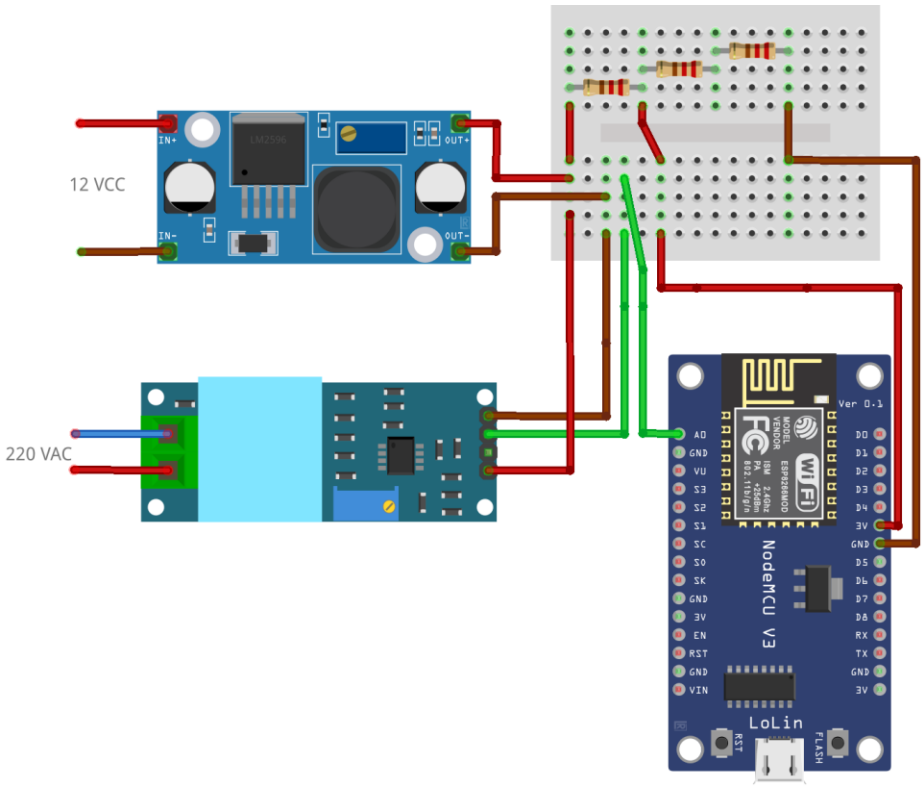

Figura 47. Módulo de lectura de voltaje de red.

Módulo 2

Tiene la tarea de leer la carga de la batería. A través del sensor VCC se mide el voltaje de la batería y se capta esa señal con la ESP8266. Utilizando la capacidad de conexión WiFi de la placa de desarrollo se transmite este valor al Broker MQTT.

La actividad del módulo se puede presentar de la siguiente manera: el regulador de voltaje es alimentado por una fuente de 12 voltios. A la salida del regulador se obtienen 3.3 voltios para suministrar tensión al sensor y la placa de desarrollo. Mediante el pin A0 de la ESP8266 digitalizamos el valor y lo transmitimos al servidor. Este se puede visualizar en la figura 48.

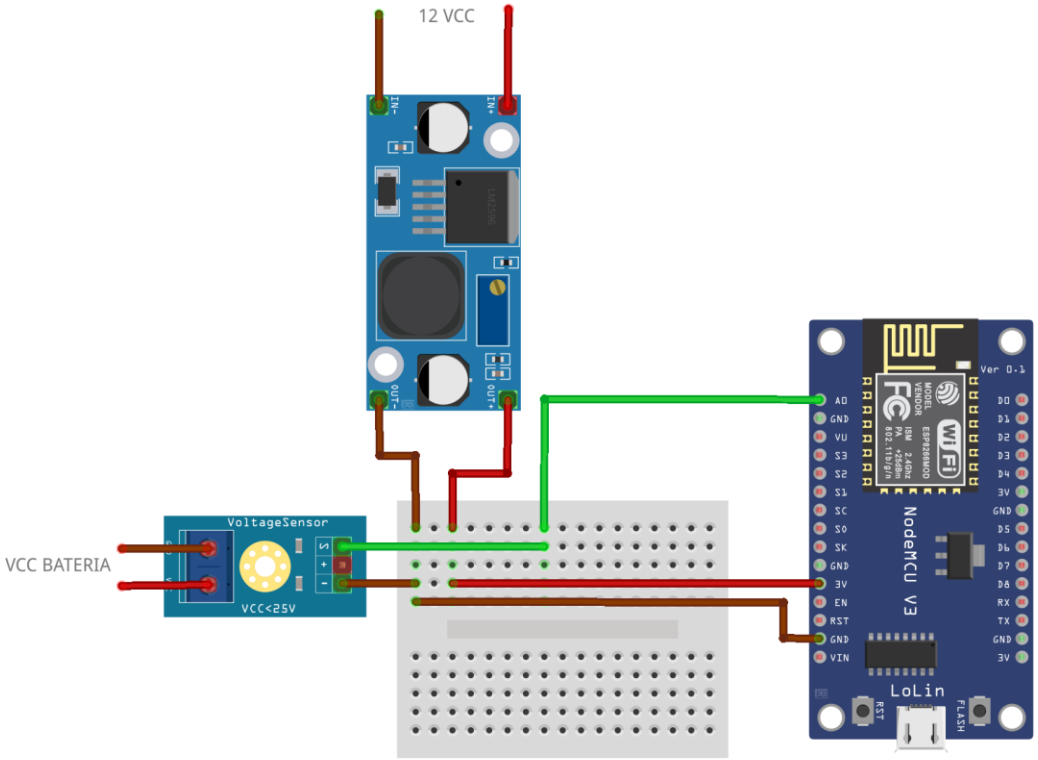

Figura 48. Módulo de lectura de batería.

Módulo 3

En este módulo intervienen los sensores PIR instalados en la Universidad. La finalidad de este dispositivo es detectar cuando se activa el sensor. Cuando el PIR sensa la presencia de un cuerpo abre un interruptor y con el uso de una ESP8266 se capta esta señal emitida. Una vez registrado y procesado este dato se lo transmite al Broker MQTT vía WiFi.

Su funcionamiento se puede resumir de la siguiente manera: la fuente de 12 voltios alimenta el regulador de voltaje y el sensor PIR, y a la salida de este se obtienen 3.3 voltios para suministrar de energía la placa de desarrollo. Finalmente,

con el uso del pin A0 se toma la señal del detector de movimiento. Podemos observar este módulo en la figura 49.

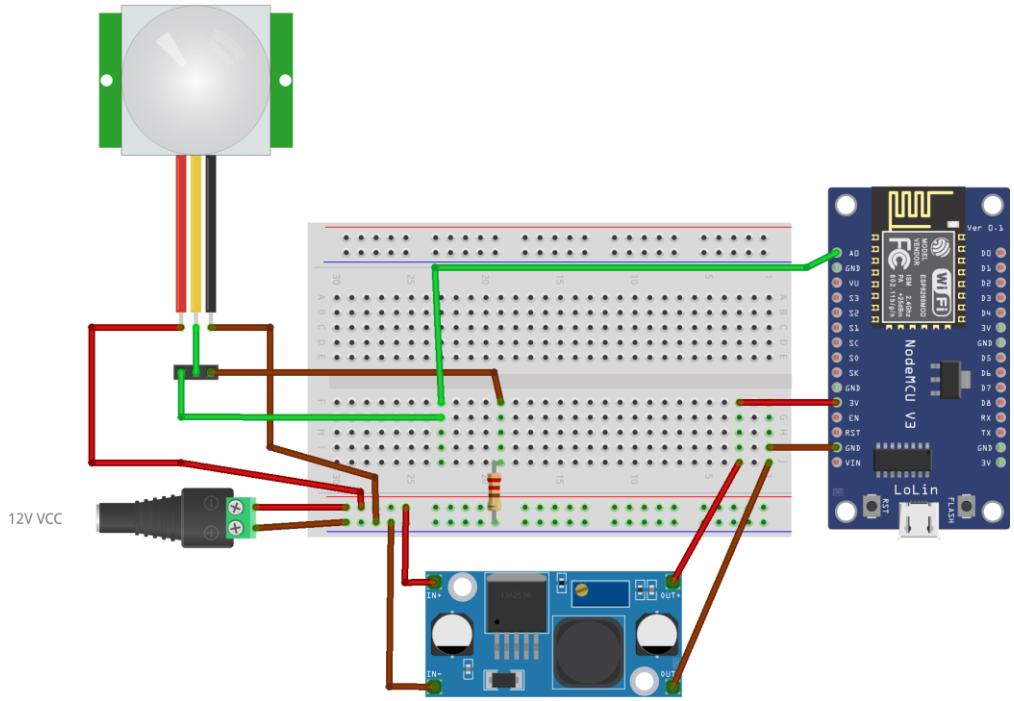

Figura 49. Módulo de detección del estado del sensor PIR.

Controlador

Como se presentó en el apartado de la arquitectura general propuesta, todos los dispositivos desarrollados interactúan entre sí mediante el servidor web alojado en la Raspberry Pi. Al tratarse de una topología en forma de estrella debe existir un nodo central ocupado por el controlador que se comunique con los distintos dispositivos creados y que permita al usuario controlarlos. Los dispositivos se comunican mediante el protocolo de comunicación MQTT que utiliza la red WiFi como canal de transmisión.

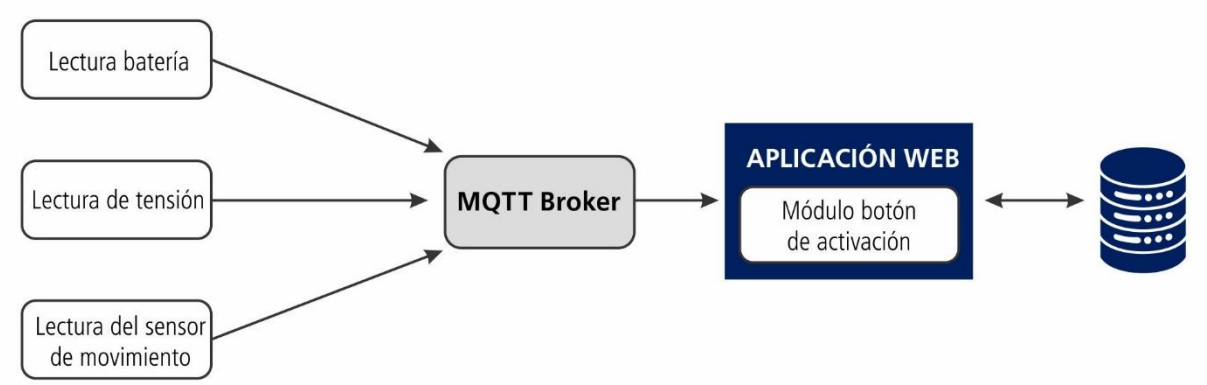

Figura 50. Flujo de información de los módulos.

Por parte del hardware, el desarrollo se realizó sobre la tecnología de los kits de desarrollo ESP y el entorno de programación Arduino. Se opera con 3 módulos cada uno con su funcionalidad (lectura de batería, tensión o movimiento) y configuración pertinente. La elección de la tecnología ha sido enfocada en la idea de la escalabilidad del producto ya que el hecho de agregar un módulo nuevo solo requiere duplicar uno de los modelos iniciales. Todos estos tendrán como objetivo la transmisión de la información recolectada al Broker MQTT y así facilitarla a la aplicación Web.

Respecto al software que consume el controlador, la Raspberry PI corre sobre el sistema operativo llamado Raspberry Pi OS (antes conocido como Raspbian), siendo este una versión actualizada de Debian y el más empleado para propósito general. Sobre este adoptamos la arquitectura LAMP.

Aplicación Web

En las siguientes páginas se describe la interfaz del sistema mediante la cual el usuario podrá monitorizar los datos recibidos de los múltiples dispositivos. La aplicación web ha sido desarrollada en base al framework de código abierto llamado Laravel, basado en el patrón arquitectónico MVC (Modelo-Vista-Controlador) y diseñado para facilitar el desarrollo de aplicaciones web ofreciendo una serie de funcionalidades integradas.

En base a los requerimientos descritos, la aplicación se conforma de cuatro módulos: uno para la gestión de información personal de los usuarios, el segundo para la gestión de las alarmas y los restantes para la configuración de activación y notificaciones como resultado de los datos de estado transmitidos desde estas.

Para ingresar a la plataforma, el usuario debe completar el formulario de identificación donde se solicita el nombre de usuario y contraseña provistos por el administrador o el supervisor con anterioridad.

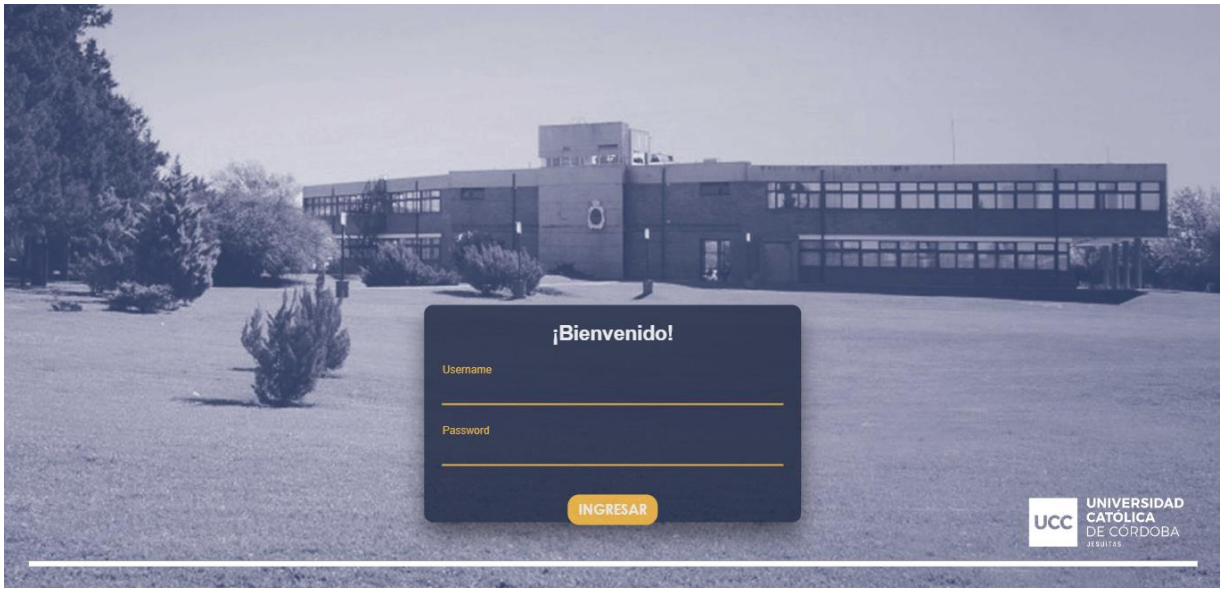

Figura 51. Ingreso a la plataforma.

Como página principal del sistema, se presenta un centro de notificaciones en donde se listan las alertas de determinado evento sobre una alarma. Tal como se aprecia en la Figura 52, se distinguen tres tipos de alertas: si se trata de una alarma disparada por intrusión, por ejemplo, se mostrará una notificación de urgencia, y, por otro lado, si se trata de un problema de tensión o batería se mostrará un mensaje de precaución.

Figura 52. Pantalla principal, notificaciones.

Figura 53. Modal de ingreso de observaciones.

En todos ellos se solicitará al guardia o responsable de seguridad la confirmación de lectura de las mismas siendo estas registradas y disponibilizadas en el reporte histórico de las alarmas. En el caso de tratarse de una notificación proveniente de un sensor se muestra también el plan de acción establecido para dicha alarma y la posibilidad de ingresar un comentario sobre lo sucedido.

La sección “Usuarios” engloba todas aquellas acciones de gestión sobre los datos personales de los usuarios. La figura 54 representa la primera vista compuesta

por la lista de los usuarios registrados con las opciones de edición y dada de baja de estos. Además, tal como se observa en la figura 55, se presenta la posibilidad de dar de alta un nuevo usuario permitiendo asignar permisos según el rol de la persona en cuestión.

Figura 54. Lista de usuarios.

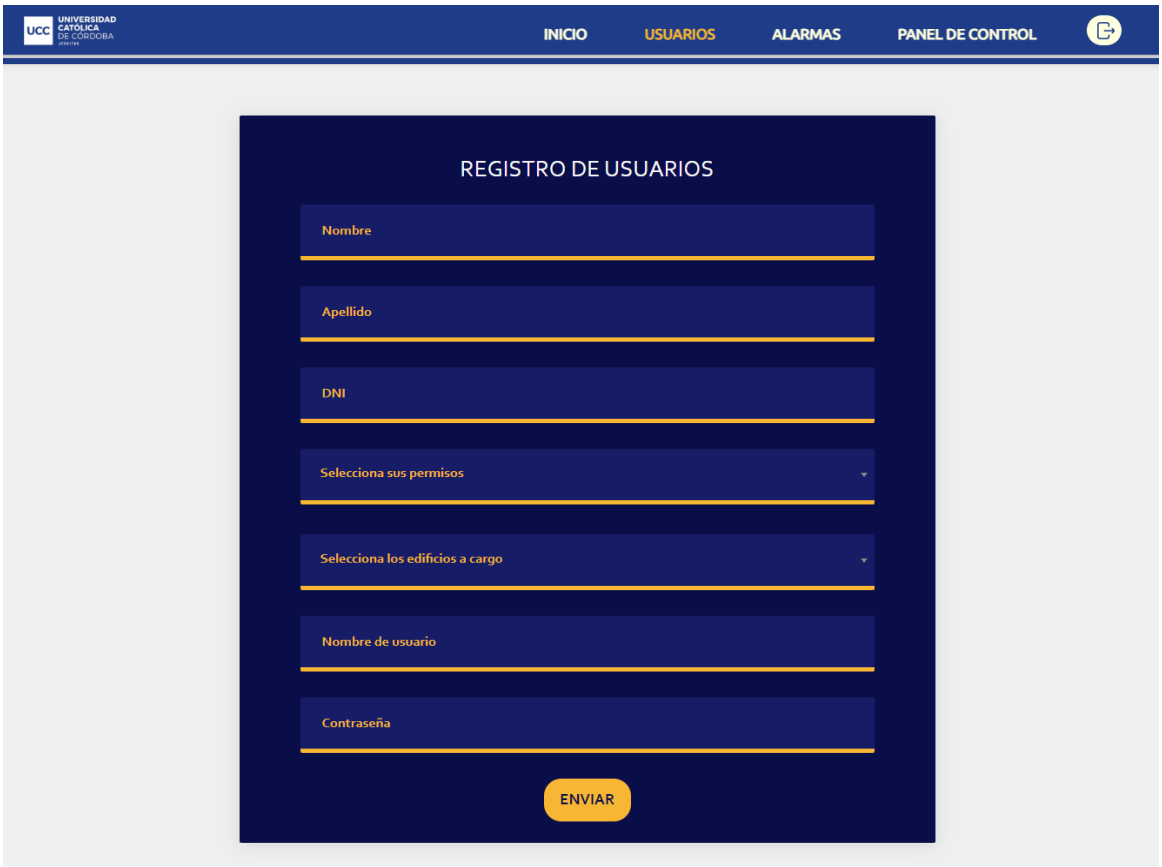

Figura 55. Formulario de dada de alta de usuarios.

En la sección “Alarmas” se dispone una lista que expone los datos principales de las alarmas registradas, de las cuales se recibirán los datos de estado para su notificación. El usuario dispone de un filtro según la sede a la que corresponde determinada alarma y la posibilidad de descargar un reporte del historial de eventos en un rango de fechas.

Figura 56. Lista de alarmas.

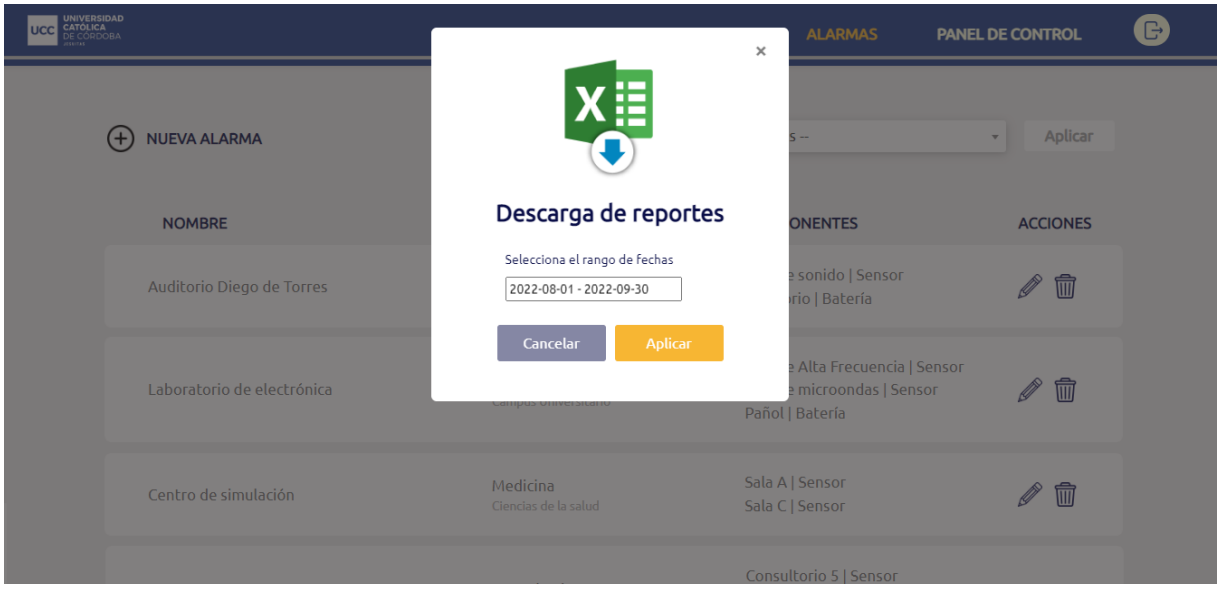

Figura 57. Modal de descarga de reportes.

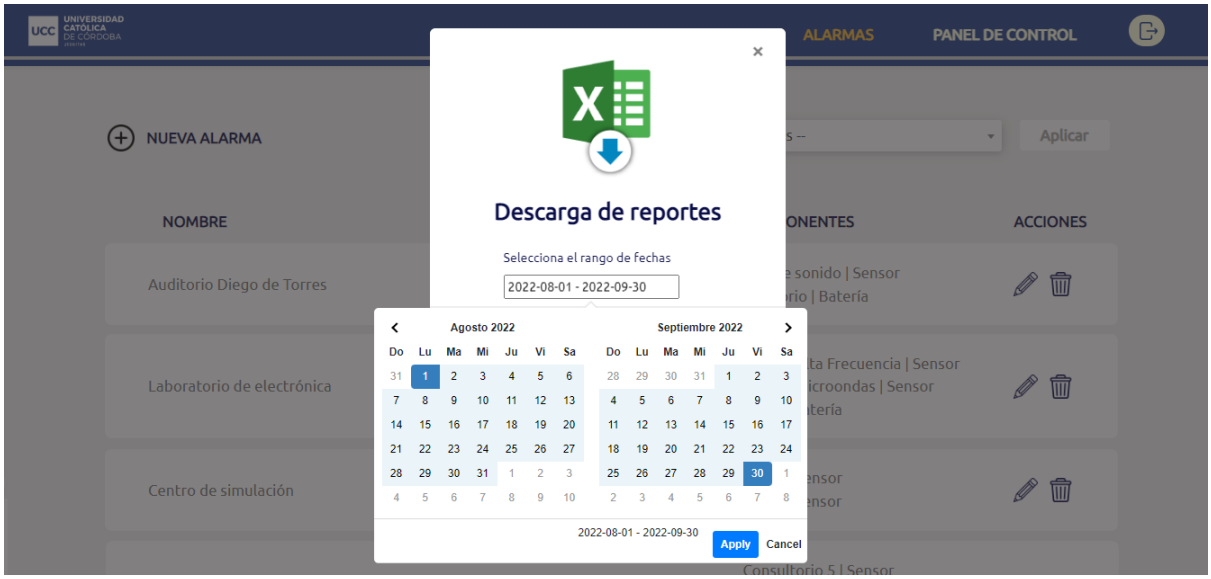

Figura 58. Modal de descarga de reportes con el selector de rango de fechas.

En la figura 59 se muestra un ejemplo del reporte histórico de eventos en un rango de fechas designado por el solicitante. Una vez que confirmada la descarga de este, se exporta un archivo con formato .xlsx donde se informa fecha y hora del incidente, nombre de la alarma, ubicación, componente en cuestión, momento en que se realizó la confirmación de lectura y los comentarios ingresados por el personal de seguridad.

	A	B	C	D	E	F	G	H	I	J	K
1	Fecha y hora	Nombre	Sitio	Facultad/Edificio	Dependencia/Aula	ID componente	Tipo de componente	Estado	Confirmación de lectura	Usuario	Comentarios
2	2022-08-14 20:41:11	Laboratorio de electrónica	Campus Universitario	Ingeniería	Secretaria	1	Botón	1			
3	2022-08-14 20:41:13	Auditorio Diego de Torres	Centro	Auditorio	Auditorio	13	Batería	1	2022-08-14 20:41:13	Miguel Alonso	
4	2022-08-14 20:41:14	Auditorio Diego de Torres	Centro	Auditorio	Sala de sonido	2	Botón	1			
5	2022-08-14 20:41:15	Centro de simulación	Ciencias de la salud	Medicina	Sala A	19	Sensor	1	2022-08-14 20:41:15	Juan Ramirez	
6	2022-08-14 20:41:17	Centro de simulación	Ciencias de la salud	Medicina	Secretaria	20	Botón	1			
7	2022-08-14 20:41:18	Hospital Veterinario	Campus Universitario	Consultorio externo	Recepcion	5	Sensor	1	2022-08-14 20:41:18	Miguel Alonso	
8	2022-08-14 20:41:19	Laboratorio de electrónica	Campus Universitario	Ingeniería	Secretaria	1	Botón	1			
9	2022-08-14 20:41:21	Auditorio Diego de Torres	Centro	Auditorio	Secretaria	2	Botón	1			
10	2022-08-14 20:41:22	Auditorio Diego de Torres	Centro	Auditorio	Secretaria	2	Botón	1			
11	2022-08-14 20:41:23	Laboratorio de electrónica	Campus Universitario	Ingeniería	Secretaria	1	Botón	1			
12	2022-08-14 20:41:24	Centro de simulación	Ciencias de la salud	Medicina	Sala A	19	Sensor	1	2022-08-14 20:41:24	Juan Ramirez	
13	2022-08-14 20:41:25	Hospital Veterinario	Campus Universitario	Consultorio externo	Sala A	5	Sensor	1	2022-08-14 20:41:25	Miguel Alonso	

Figura 59. Reporte histórico, archivo .xlsx.

Al momento de dar de alta una alarma en el sistema se solicitan datos específicos como la ubicación de la misma, los componentes asociados (botón, sensor movimiento, lectura batería y tensión) y otros sobre el responsable y el procedimiento a seguir en caso de sucederle alguna anomalía (disparo por intrusión, problemas de tensión, etc.).

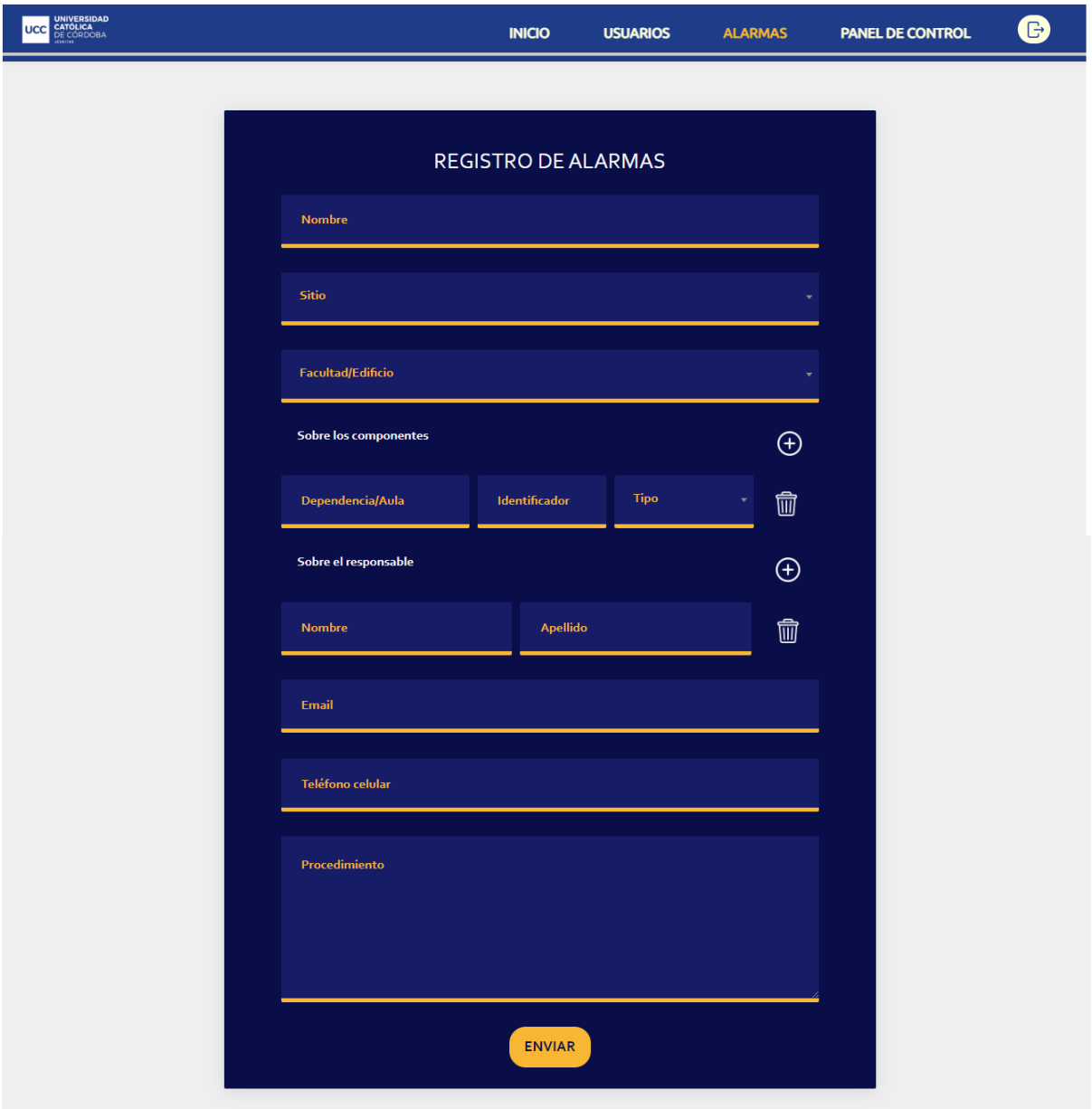

Figura 60. Formulario de dada de alta de una alarma.

El panel de control del estado de las alarmas donde los usuarios autorizados las activarán y desactivarán impactando en la generación de las notificaciones. Teniendo en cuenta los numerosos espacios que cuenta la universidad (unidades académicas, espacios de recreación, etc.), la aplicación ofrece un filtro de alarmas por la ubicación de las mismas.

Figura 61. Panel de control.

Por último, para facilitar ciertas tareas de mantenimiento del sistema se implementaron tres cron jobs descriptos a continuación.

Partiendo del hecho de que el sistema debe estar siempre ejecutándose cumpliendo su objetivo y evitando así inconvenientes de seguridad en la Universidad, se configuró uno encargado de analizar cada minuto si el sistema está recibiendo datos correctamente y otro para validar cada media hora que todas las alarmas estén transmitiendo.

Además, teniendo en cuenta la extensión de la organización y la cantidad de datos históricos que pueden ingresar en un día, se desarrolló un cron job capaz de borrar la base de datos una vez al mes y así liberar espacio de la misma.

IMPACTO ECONÓMICO

La solución planteada ha sido desarrollada a medida de los requerimientos de la Universidad Católica de Córdoba. Si bien existen opciones similares en el mercado, este software tiene en cuenta todos las particularidades y necesidades en cuanto adaptación al sistema actual, seguridad de acceso y gestión de recursos. Además, el mismo permitirá su evolución flexible y adaptable al futuro.

Estructura de costos

Analizando los costos que intervienen en el proyecto, se destaca principalmente las horas de análisis, modelado y desarrollo invertidas en la aplicación web y módulos de conexión inalámbrica para dar con la solución especificada.

Recurso	Horas estimadas	Valor/hora (USD)
Analista funcional Sr.	100 hs	$ 45,00
Desarrollador Sr.	300 hs	$ 50,00
Especialista IoT Sr.	250 hs	$ 50,00
Arquitecto Sr.	80 hs	$ 50,00
QA Sr.	100 hs	$ 35,00

Tabla 45. Análisis de costos de recursos humanos.

En total, para un proyecto de 830 hs de desarrollo, el costo es de USD $39.500.

En cuanto al hardware, al adaptar los componentes ya vigentes en el sistema de seguridad de la organización no solo se reduce el valor económico del producto, sino que también disminuye el impacto ambiental.

Al referirnos a los módulos, se hace referencia al ordenador Raspberry Pi 3B+, al microcontrolador ESP8266 NodeMCU, a los sensores, circuitos de alimentación y a los componentes de conexión.

Recurso	Precio (USD)
Raspberry Pi	$ 35
ESP8266 NodeMCU	$ 3,25
Elementos de conexión	$ 2
Sensores	$ 5

Tabla 46. Costo de elementos físicos.

Para poder estimar el costo de estos componentes se plantea una instalación para un sector de la Universidad, en este caso la Facultad de Ingeniería. En este caso se proyectan: 40 sensores (movimiento, lectura batería y tensión). 40 ESP8266 NodeMCU, 10 unidades de elementos de conexión y 1 Raspberry Pi 3B +.

El costo de los elementos físicos será de USD $455.

En cuanto al valor de la mano de obra especializada para implementar el producto, este tiene un costo variable con respecto a la cantidad de unidades instaladas. Su costo es el 25% del valor de los elementos a instalar. En el caso previo, este tendrá un costo de USD $113,75

Por último, se presenta el costo de mantenimiento del producto. Este depende de la cantidad de unidades sensoriales a las que se brinda soporte. El costo será de USD $2,5 por unidad.

De esta manera, el costo final se resume en la tabla 47.

Recurso	Precio (USD)
Desarrollo	$ 39.500,00
Hardware	$ 455,00
Implementación	$ 113,75
Mantenimiento	$ 100,00

Tabla 47. Resumen del costo del desarrollo.

El costo total de esta propuesta es de USD $40.368,75.

Cabe destacar que el costo de desarrollo se abona en una sola ocasión, luego se pueden añadir la cantidad de sensores y usuarios que sean necesarios.

POSIBILIDADES DE CRECIMIENTO DEL PRODUCTO

En base al concepto adoptado de MVP para este proyecto, el producto evolucionará en el tiempo permitiendo sumar nuevas funcionalidades o mejoras a éste.

La digitalización del pedido de llaves para aulas y espacios especiales.

Hoy en día para solicitar el acceso a un Laboratorio o aula, el profesor debe acercarse a secretaría y solicitar la llave del mismo asentando en una planilla sus datos y firma en acto de conformidad del retiro de las llaves.

Este procedimiento puede ser optimizado registrando digitalmente sus datos con el fin de centralizar la información referida a la seguridad de la Universidad en el mismo sistema, visualizar los espacios disponibles para su asignación y evitar posibles extravíos o daños del material.

Control de la actividad diaria por edificio.

Para evitar la tarea de activación manual de las alarmas por espacio, el sistema de seguridad podría nutrirse de los horarios de clases y actividades diarias para detectar situaciones anómalas en horarios no estipulados de uso.

Por ejemplo, en el aula 2 de la facultad de Ingeniería se dicta Álgebra de 8 am a 9 am y, en la misma aula, Análisis matemático de 10:30 am a 11:30 am. Teniendo un lapso de tolerancia de 10 minutos, si el sistema detecta movimiento luego de este debe dar aviso al personal de seguridad para su inmediata actuación.

Datos biométricos para la autenticación de usuarios.

A nivel de seguridad de la aplicación web se pueden implementar mejoras en la autenticación de usuarios. Para el ingreso al sistema se puede implementar el reconocimiento facial o lector de huellas dactilares, como una autenticación de dos pasos.

Integración con el sistema de domótica de la Universidad.

Si bien no todos los edificios cuentan con la implementación de este, esta es una opción para centralizar y unificar el sistema de seguridad teniendo como uno de sus fines la trazabilidad de la actividad desarrollada en cada uno de sus espacios. Cada docente cuenta con su credencial universitaria la cual está autorizada para abrir y cerrar las puertas de las aulas. Una vez que este se identifica pasándola sobre el lector de tarjetas el sistema podría desactivar la alarma haciendo que cualquier movimiento en horas de clases no sea tomado como intrusión.

Sistema de videovigilancia.

La vinculación de las cámaras con espacios que están bajo vigilancia de una alarma permitirá que al activarse una de estas, en la misma pantalla el agente de seguridad visualice la cámara que enfoca el espacio comprometido en vivo, brindándole así la capacidad de actuar con mayor certeza ante un incidente.

Exportación de datos.

En la primera versión del producto, se concede al usuario la posibilidad de descargar los datos históricos en un archivo sin procesar. El equipo de seguridad y autoridades de la Universidad podrían necesitar indicadores puntuales acerca del rendimiento del sistema de alarmas y el equipo encargado de su supervisión.

CONCLUSIÓN

La posibilidad de haber desarrollado un proyecto interdisciplinario nos permitió conocer más acerca del trabajo en equipo y la complementariedad de las carreras de Ingeniería. Para ambos este significó un reto, donde aplicando los conocimientos adquiridos durante estos años, logramos desarrollar e implementar un sistema que centralizará el esquema de seguridad de la Universidad Católica de Córdoba. El haber diseñado su arquitectura de forma flexible nos permitió adaptarnos a los desafíos que surgieron durante la marcha entendiendo que el dominio puede cambiar en cualquier momento en cuanto a necesidades y requerimientos.

El producto logrado centraliza las alertas de estado de las alarmas facilitando la actividad diaria del equipo de seguridad y al mismo tiempo proporciona indicadores a la Universidad para la toma de decisiones futuras en cuanto a contratación de más personal, nuevos puestos de vigilancia, inversiones en equipamiento de seguridad, etc.

Destacamos que esta fue nuestra primera aproximación al mundo del desarrollo desde cero, lo que nos permitió empaparnos de nuevas tecnologías y tendencias del mercado para tomar la decisión de qué componentes o lenguajes de programación usar, siempre teniendo como primer objetivo el concepto de arquitectura escalable. Fue un periodo de estudio, investigación y sin dudas de crecimiento personal y profesional que será recordado como el punto de partida para nuestras carreras.

ANEXO I

Propuesta alternativa

En este anexo se presenta una alternativa a la propuesta desarrollada donde el módulo de botones de activación no es implementado de forma virtual, embebido en la aplicación web, sino que se lo realiza físicamente. Esta opción es óptima para aplicaciones donde se requiera el uso de interruptores físicos para mayor practicidad, por ejemplo, en el sector agropecuario o en sistemas de seguridad a menor escala y con un número reducido de operarios que intervengan el uso diario.

En cuanto a complejidad, los cambios a realizar sobre el modelo actual no son demasiados. Como fue mencionado previamente el desarrollo actual soporta esta transformación de virtual a físico requiriendo solo la integración del siguiente componente.

Módulo botón de activación manual.

El módulo cumple la función de determinar si la alarma está activada o desactivada. Para ello se utiliza un botón *switch* con dos opciones, estado *ON* y *OFF*. El estado es captado por la placa de desarrollo ESP01 y enviado al Broker MQTT via WiFi.

En cuanto a la articulación de los componentes los podemos resumir de la siguiente manera, la placa de desarrollo y el botón switch están alimentados por el conjunto de baterías. La salida del botón switch es captada por el pin GPIO 2 de la ESP 01 para poder leer su valor. En la figura 62 se pueden ver las conexiones y disposición de este módulo.

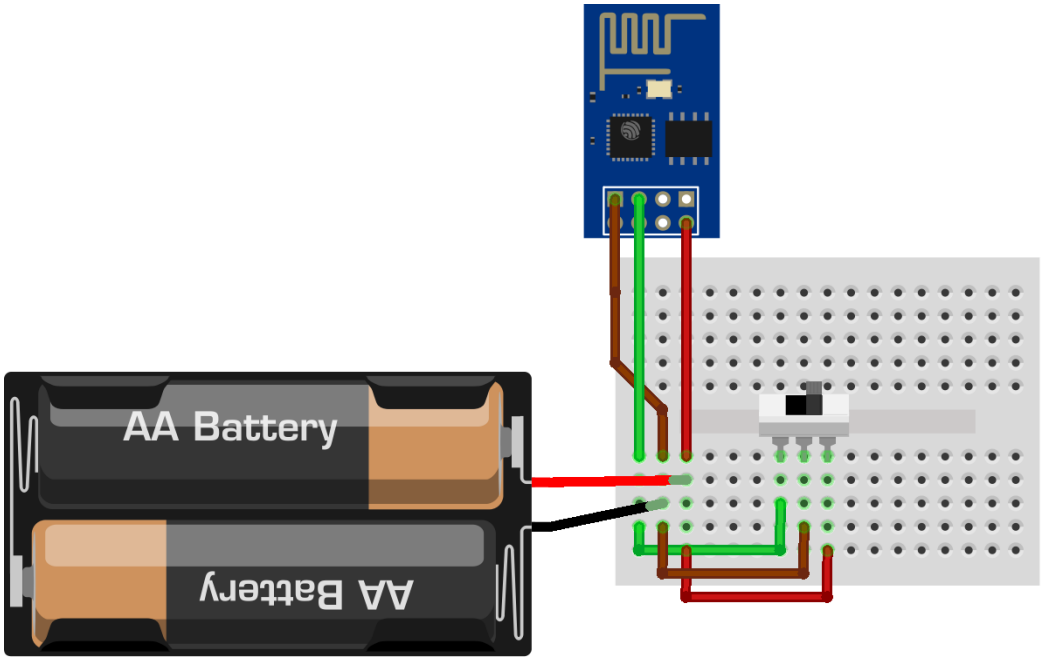

Figura 62. Módulo de botón activación.

El nuevo diagrama de comunicaciones resultaría de la siguiente manera:

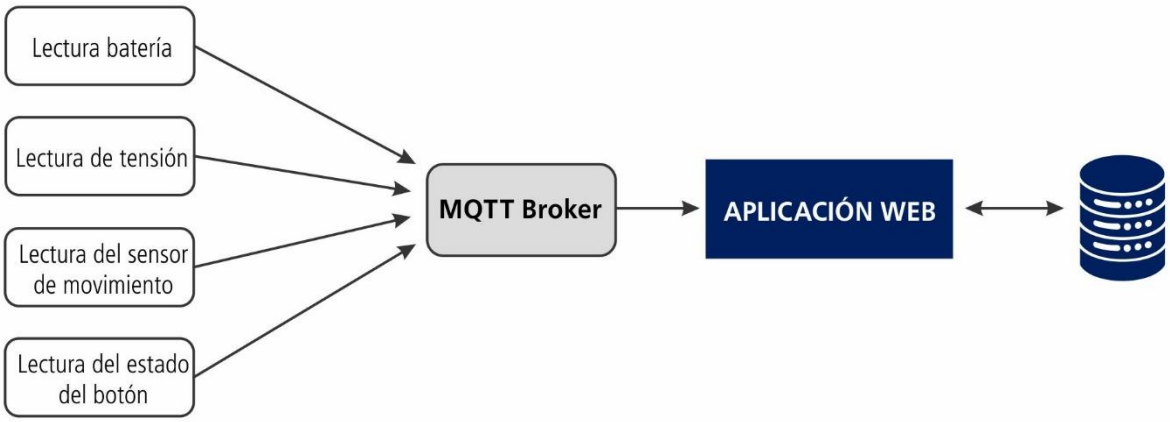

Figura 63. Flujo de información y arquitectura de los módulos.

En este se observa que, a diferencia del caso original, el procesamiento de la información del botón de activación es realizado por el Broker MQTT y eso es facilitado a la aplicación.

Por último, la topología en estrella quedará conformada de la siguiente forma.

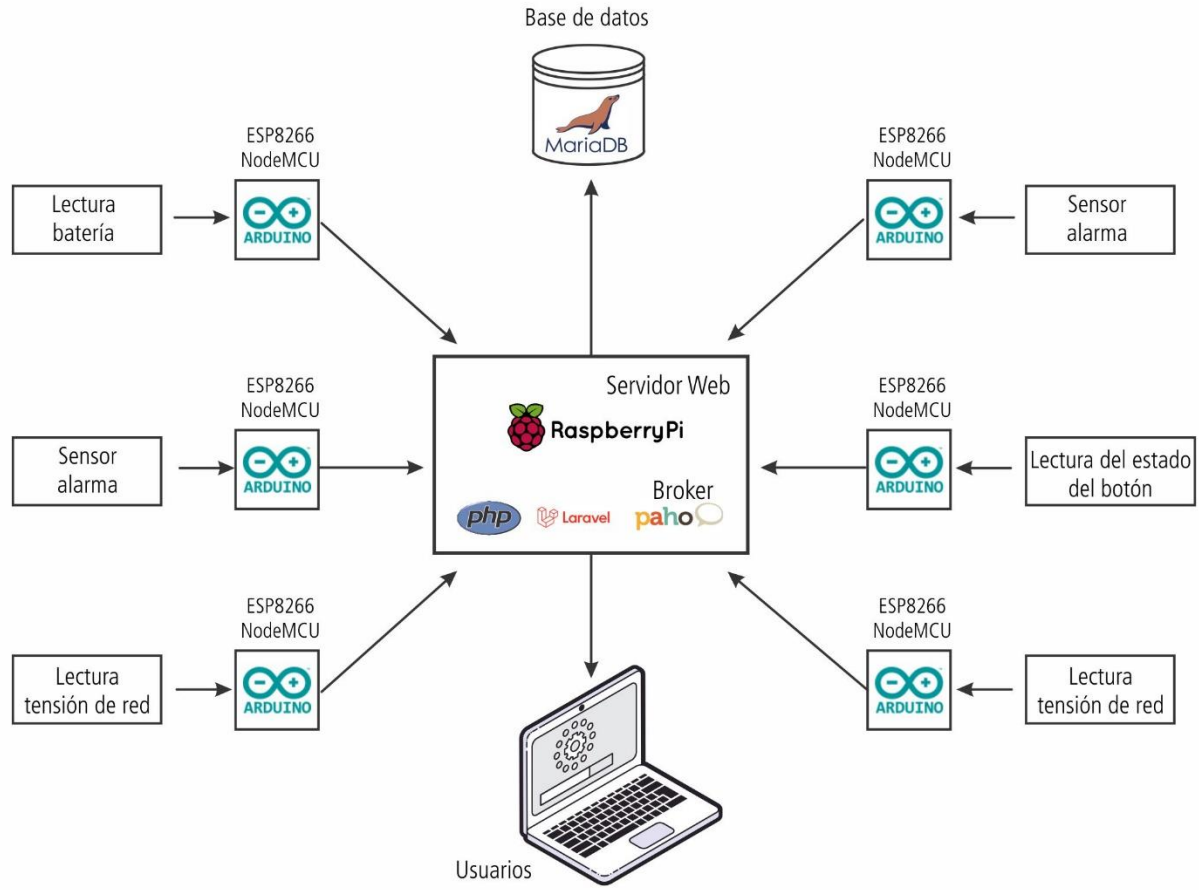

Figura 64. Arquitectura del sistema.

BIBLIOGRAFÍA

Fontán, Salazar y Arias. (2022). El impacto de las TIC desde el punto de vista de la ingeniería. - https://sites.google.com/site/fotansalazaryarias/nuestras-busquedas/el-impacto-de-las-tics-desde-el-punto-de-vista-de-la-ingeniería

Universidad de Ingeniería y tecnología. UTEC. (2020, December 10). ¿Cuál es la importancia de la ciencia y la tecnología en la humanidad? https://utec.edu.pe/blog-de-carreras/utec/cual-es-la-importancia-de-la-ciencia-y-la-tecnologia-en-la-humanidad

Revista Politécnica. Vista de Enfoque integral del ingeniero del siglo XXI: una revisión de la literatura (2022).. https://revistas.elpoli.edu.co/index.php/pol/article/view/972/1487

Delgado A.. ¿Qué es Raspberry Pi y para qué sirve? (2020, November 21) GEEKNETIC https://www.geeknetic.es/Raspberry-Pi/que-es-y-para-que-sirve

Aprendiendo Arduino. (2022, April 16). Modelos Raspberry Pi – Aprendiendo Arduino. Aprendiendo Arduino; https://aprendiendoarduino.wordpress.com/tag/modelos-raspberry-pi/

8 reasons why PHP is still so important for web development. Jobsity. (n.d.). https://www.jobsity.com/blog/8-reasons-why-php-is-still-so-important-for-web-development.

What is php? PHP Tutorial. (2021, November 3). https://www.phptutorial.net/php-tutorial/what-is-php/.

SILBERSCHATZ, A, KORTH, H. y SUDARSHAN, S. (2006). Introducción. En C. Sánchez González (Ed.), Fundamentos de bases de datos (pp. 13-14). McGRAW-HILL/INTERAMERICANA DE ESPAÑA, S.A.U.

OASIS Standard. (2019, March 7). MQTT Version 5.0. MQTT. https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf

Pastor, J. P. (2018, April 16). Raspberry Pi 3 Model B+. https://www.xataka.com/ordenadores/raspberry-pi-3-model-b-analisis-mas-potencia-y-mejor-wifi-para-un-minipc-que-sigue-asombrando

Hernandez, L. V. H. (2019, October 2). ESP8266. https://programarfacil.com/podcast/esp8266-wifi-coste-arduino/

Karunatilake, E. K. (2020, May 2). ESP8266 NodeMCU.ESP8266 Forum. https://www.esp8266.com/

Tecno Seguro. (n.d.). Sensores de Movimiento PIR. https://www.tecnoseguro.com/faqs/alarma/que-es-un-detector-de-movimiento-pasivo-o-pir

Solé, Roberto. “Raspberry Pi: Crea Proyectos DIY Por Muy Poco Dinero.” Profesional Review, Profesional Review, www.profesionalreview.com/2021/07/18/que-es-raspberry-pi/ .

Wikipedia.org, Wikimedia Foundation, Inc., es.wikipedia.org/wiki/GNU/Linux.

“Reclu IT.” Recluit.com, 2020, recluit.com/que-es-lamp-stack/#.Y3ggvXaZOUl. http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/rivera_l_a/capitulo2.pdf

Introduction to IoT. (2018, January 22). Networking Academy. https://www.netacad.com/es/courses/iot/introduction-iot

¿Qué es IoT (Internet Of Things)? (2019, January 8). Deloitte Spain. https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

¿Qué es el Internet de las cosas (IoT)? (2014). Oracle.com. https://www.oracle.com/ar/internet-of-things/what-is-iot/

Gillis, A. S. (2022). What is the internet of things (IoT)? IoT Agenda; TechTarget. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

Qué es la cuarta revolución industrial (y por qué debería preocuparnos) (2016, October 12)- BBC News Mundo. BBC News Mundo; BBC News Mundo. https://www.bbc.com/mundo/noticias-37631834

¿Qué es la Cuarta Revolución Industrial? (2018). Blog de Salesforce. https://www.salesforce.com/mx/blog/2018/4/Que-es-la-Cuarta-Revolucion-Industrial.html

CRISTINA SÁINZ DE LA FLOR. (2020, October 22). Manual para entender la Cuarta Revolución Industrial. Wearemarketing.com; WeAreMarketing.com. https://www.wearemarketing.com/es/blog/que-es-la-cuarta-revolucion-industrial.html

Protek Seguridad. (2020, January 27). ¿Cómo funciona una alarma monitoreada? - Protek Que lo importante nunca cambie. Protek. https://www.protek.com.py/novedades/alarma-monitoreada/

¿Qué es la Cuarta Revolución Industrial o Industria 4.0? | Repsol. https://www.repsol.com/es/energia-innovacion/energia-futuro/tecnologia-innovacion/cuarta-revolucion-industrial/index.cshtml

Espressif Systems. (2020, octubre). ESP8266EX Datasheet. Espressif. https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf

Espressif Systems. (2020, octubre). ESP8266EX Technical Reference. Espressif. https://www.espressif.com/sites/default/files/documentation/esp8266-technical_reference_en.pdf

Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. (s. f.). Wi-Fi MQTT. Dev Ti.

https://dev.ti.com/tirex/explore/node?node=AHJ8YEDDQKAGTuUKvUm0ig__fc2e6sr__LATEST

Craggs, I. (s. f.). Eclipse Paho | The Eclipse Foundation. Eclipse Foundation. https://www.eclipse.org/paho/index.php?page=clients/python/docs/index.php

Craggs, I. (s. f.-b). Eclipse Paho | The Eclipse Foundation. Eclipse Foundation - Paho. https://www.eclipse.org/paho/

R. A. Light, "Mosquitto: server and client implementation of the MQTT protocol," The Journal of Open Source Software, vol. 2, no. 13, May 2017, http://dx.doi.org/10.21105/joss.00265

Paho MQTT. (2021, 21 octubre). paho-mqtt. PyPI. https://pypi.org/project/paho-mqtt/

Toolan, B. (2021). ESP8266 Programming Tutorial: Programming With Arduino: Esp-01 Programming With Arduino Ide. Independently Published.

Campbell, R. (2020). Arduino: The Master Guide to Learn Arduino Programming with Easy-To-Follow Methods, Tools And Strategies: 1. Robert Campbell.

International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). (2019). IOT Home Automation with PIR Sensor Security using ESP8266 WI-FI Chip and GSM.