# UNIVERSIDAD DE SONORA
# DIVISIÓN DE INGENIERÍA

POSGRADO EN INGENIERÍA INDUSTRIAL
**MAESTRÍA EN INGENIERÍA EN SISTEMAS Y TECNOLOGÍA**

DESARROLLO DE UN SISTEMA PARA LA GESTIÓN DE DISPOSITIVOS CIBER-FÍSICOS. CASO: MONITOREO DE UNA EDIFICACIÓN INTELIGENTE

# T E S I S


PRESENTADA POR

**GUSTAVO CÉSAR SOTO PÉREZ**


Desarrollada para cumplir con uno de los
requerimientos parciales para obtener
el grado de Maestro en Ingeniería

DIRECTOR DE TESIS
DR. VICTOR HUGO BENITEZ BALTAZAR

HERMOSILLO, SONORA, MÉXICO. OCTUBRE 2021

# Universidad de Sonora

Repositorio Institucional UNISON


# UNIVERSIDAD DE SONORA

División de Ingeniería
Posgrado en Ingeniería Industrial
Maestría en Ingeniería en Sistemas y Tecnología

Hermosillo, Sonora a 28 de septiembre de 2021.

**GUSTAVO CESAR SOTO PEREZ**

Con fundamento en el artículo 66, fracción III, del Reglamento de Estudios de Posgrado vigente, otorgamos a usted nuestra aprobación de la fase escrita del examen de grado, como requisito parcial para la obtención del Grado de Maestro(a) en Ingeniería: Ingeniería en Sistemas y Tecnología.

Por tal motivo este jurado extiende su autorización para que se proceda a la impresión final del documento de tesis: **DESARROLLO DE UN SISTEMA PARA LA GESTIÓN DE DISPOSITIVOS CIBER-FÍSICOS. CASO: MONITOREO DE UNA EDIFICACIÓN INTELIGENTE** y posteriormente efectuar la fase oral del examen de grado.

ATENTAMENTE

DR. VICTOR HUGO BENITEZ BALTAZAR
Director(a) de tesis y Presidente del jurado

DR. JESUS HORACIO PACHECO RAMIREZ
Secretario(a) del Jurado

DRA. MARIA ELENA ANAYA PEREZ
Vocal del Jurado

DR. PEDRO GONZALEZ ZAMORA
Vocal del Jurado

Hermosillo, Sonora, México, a 29 de septiembre de 2021

**GUSTAVO CÉSAR SOTO PÉREZ**

Con fundamento en el artículo 66, fracción III, del Reglamento de Estudios de Posgrado de la Universidad de Sonora, otorgo a usted mi aprobación de la fase escrita del examen profesional, como requisito parcial para la obtención del Grado de Maestro en Ingeniería: Ingeniería en Sistemas y Tecnología.

Por tal motivo, como sinodal externo y vocal del jurado, extiendo mi autorización para que se proceda a la impresión final del documento de tesis: **DESARROLLO DE UN SISTEMA PARA LA GESTIÓN DE DISPOSITIVOS CIBER-FÍSICOS. CASO: MONITOREO DE UNA EDIFICACIÓN INTELIGENTE** y posteriormente efectuar la fase oral del examen de grado.

ATENTAMENTE

DR. LUIS CARLOS FÉLIX HERRÁN
INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
Sinodal Externo y Vocal del Jurado

# RESUMEN

El presente proyecto presenta una metodología para el desarrollo de un sistema para la gestión de dispositivos cíber-físicos, atendiendo al caso del monitoreo de una edificación inteligente. Este sistema fue utilizado para presentar una propuesta de solución en temas de seguridad ciudadana del estado de Sonora. El propósito de esta implementación es el desarrollar un sistema capaz de administrar los dispositivos ciber-físicos instalados en una edificación inteligente, asegurar su comunicación, conectividad, registro y almacenamiento, al presentarse eventos en los dispositivos ciber-físicos haciendo uso de las técnicas y/o tecnologías del Internet de las Cosas.
Dicha implementación se realizó en siete etapas, en la cual se llevó a cabo el análisis del espacio que se pretende automatizar, con el fin de definir las técnicas y/o tecnologías a emplear para llevar a cabo el diseño y el desarrollo del sistema que nos permita tener una comunicación segura entre los dispositivos, para posteriormente implementarlo y realizar la evaluación correspondiente, y en caso de ser necesario efectuar los ajustes para mantener la integridad de los datos.

Es a través de esta implementación que se logró desarrollar un sistema que permite establecer una relación social entre los dispositivos ciber-físicos instalados en las edificaciones inteligentes y los usuarios de dichas edificaciones, el cual favorece el tiempo de respuesta de los usuarios en caso de presentarse algún evento atípico en alguno de los dispositivos haciendo uso de alertas visuales a través de la red social Facebook y utilizando la plataforma IFTTT en paralelo para enviar alertas a los dispositivos móviles; mientras que a través de una plataforma IoT se efectúa el control, análisis y almacenamiento de datos generados por cada dispositivo.

# ABSTRACT

This project presents a methodology for the development of a system for the management of the cyber-physical devices, focusing on the case of the monitoring of an intelligent building. This system was used to present a proposal to solve the citizen security of Sonora state. The purpose of this implementation is to develop a system, which is able to manage the cyber-physical devices installed in an intelligent building, to assure its communication, connectivity, registration and storage when some events emerge in the cyber-physical devices using the techniques and/or the Internet of Things' technologies.

Such implementation was done in seven stages, in which has been implemented the analysis of the space that is intended to automatize, in order to define the techniques and/or technologies to be used to make the design and the system's development that allows us to have secure communication among the devices, to subsequently implement it and do the appropriate evaluation, and if necessary, make the adjustments to keep the data security.

It is through this implementation that it was possible to develop a system that stablish a social relationship between the cyber-physical devices installed in smart buildings and their users, which favors the response time of users in case of presenting an atypical event on any of the devices, making use of visual alerts through the social network Facebook and using the IFTTT platform in parallel to send alerts to mobile devices; while through an IoT platform the control, analysis and storage of data generated by each device is carried out.

# AGRADECIMIENTOS

Primeramente quiero agradecer a Dios por haberme dado la oportunidad de ingresar a este posgrado, quien me dio la fortaleza, la sabiduría y los recursos necesarios para llevar a cabo cada una de las actividades que se me solicitaron desde el primer día que inicié el proceso de inscripción, por poner a personas extraordinarias en mi camino que sacaron la mejor versión de mi a través de sus enseñanzas, jamás imaginé que con mis incapacidades pudiese culminar un trabajo de esta índole pero fue EL quien se mantuvo a mi lado poniendo todo a mi favor para lograrlo.

Agradezco inmensamente a mis padres Guadalupe Pérez García y Gustavo César Soto Alapizco por todo el apoyo que me han brindado, gracias por enseñarme que lo mejor de la vida se obtiene a través del esfuerzo y la dedicación, por predicarme con su ejemplo, de unos padres inagotables que lo han dado todo por sus hijos, gracias porque a pesar de sus limitantes siempre me han apoyado en cada uno de mis proyectos, me han escuchado, han estado ahí para ayudarme alcanzar mis metas y siempre han buscado lo mejor para mí.

A mis hermanas Grecia y Gisel Soto porque con amor y cariño me ayudaban a distraerme en esos momentos donde las ideas ya no fluían más, gracias porque cada día me motivan a querer ser un gran ejemplo para ustedes. LAS AMO.

Infinitas gracias al Dr. Víctor H. Benítez B. por haberme aceptado como su tesista, por brindarme su amistad, por compartir tanto conocimiento conmigo y dedicarme su tiempo para hablar de diversos temas de tecnología, gracias por su paciencia y esfuerzo conmigo y por impulsarme a publicar y presentar un artículo en una conferencia internacional, estoy bastante satisfecho con ese logro.

Muchas gracias al Dr. Luis C. Félix H. por aceptar la invitación del Dr. Benítez para codirigir mi tesis y contribuir a enriquecer el contenido y apoyarme a sacar la mejor versión del tema.

Al coordinador del posgrado, Dr. Alonso Pérez Soltero, por ser tan dedicado en atender con detalle a cada uno de los alumnos del posgrado, gracias por brindarnos toda la información necesaria para concluir con éxito.

Gracias a cada uno de mis amigos que estuvieron conmigo durante este proceso levantando mis brazos para continuar, a mis compañeros del posgrado con los que compartí algunas experiencias y a todos los que estuvieron directa o indirectamente relacionados.

Por último, gracias al Consejo Nacional de Ciencia y Tecnología (CONACYT) y al Programa de Fortalecimiento de la Calidad Educativa (PFCE) por su apoyo económico brindado en mi estudio de posgrado.

Gracias, que el Señor les bendiga a cada uno de ustedes.

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# 1. INTRODUCCIÓN

La sinergia de los componentes de red físicos y computacionales que conducen al Internet de las Cosas (IoT, por sus siglas en inglés), datos y servicios ha sido posible gracias al uso de sistemas ciber-físicos (CPS, por sus siglas en inglés). La ingeniería de CPS promete impactar de manera importante el monitoreo de los sistemas para una amplia gama de campos, desde atención médica, fabricación y transporte hasta aeroespacial y de guerra. Los CPS en las aplicaciones de monitoreo del entorno transforma completamente las interacciones de persona a persona, de persona a máquina y de máquina a máquina con el uso del cómputo en la nube. CPS consiste en proporcionar un entorno virtual que incorpore una red interactiva de elementos del sistema con entradas y salidas físicas en ambos extremos (Ali *et al.*, 2015). Hoy en día se ha vuelto común la interacción de los objetos de la vida cotidiana con el Internet, a lo cual se le conoce como Internet de las Cosas.

El presente capítulo aborda la descripción de la empresa y en particular de la problemática para cual se diseñó una metodología para dar solución a su situación, además, se plantean los objetivos y la hipótesis relacionada a esta investigación.

## 1.1. Presentación

El proyecto se llevará a cabo para una empresa desarrolladora de productos tecnológicos. La empresa cuenta con 5 áreas de desarrollo, las cuales hacen referencia al tipo de producto que ofrecen al cliente y cada una se encarga de presentar soluciones mediante el uso de distintos tipos de tecnología. Estas áreas son las siguientes: Diseño Electrónico y Desarrollo de Software, Diseño y Fabricación de PCB’s Calidad Producción, Desarrollo de tecnología RFID (proximidad) y Huella Digital, Diseño de Prototipos y Productos listos para producción industrial y Seguridad Electrónica.

Desde hace un par de años la empresa ha incurrido a través de sus áreas de diseño electrónico, desarrollo de software y seguridad electrónica en temas del IoT, proponiendo soluciones integrales para el control y monitoreo de acceso, control de asistencia de personal, control y monitoreo de cisternas, entre otros. Recientemente,

debido a las demandas de un mayor desempeño requeridas en los sistemas de monitoreo y control en los espacios públicos y privados tales como:

- Hacer más eficaz la comunicación entre los dispositivos ciber-físicos,
- asegurar la conectividad a la red,
- registrar y almacenar de eventos ante la activación de sensores;

la empresa, inicia una serie de proyectos con el objetivo de desarrollar productos y/o servicios que satisfagan las demandas anteriores.
Para acelerar el desarrollo de dichos proyectos, la empresa, requiere la integración de diferentes áreas de ingeniería, por lo cual solicita apoyo en el diseño de un sistema de gestión de dispositivos ciber-físicos, que posean la capacidad de ser enlazados a la nube con el fin de tener acceso a la información de dichos dispositivos de manera más eficiente y generar alerta-respuesta en caso del cambio de estado lógico del dispositivo, así como el desarrollo de la ingeniería necesaria para dotar de capacidades del IoT a los bienes que se encuentran en un espacio ya sea público o privado, (casa habitación, oficina, edificio público, etc.).

## 1.2. Planteamiento del problema

Debido a la demanda de un alto desempeño en los sistemas de monitoreo convencionales; la falta de alerta-respuesta en tiempos convenientes y la ineficiencia de su infraestructura, la empresa solicita apoyo en el desarrollo de un sistema para la gestión de dispositivos ciber-físicos instalados en una edificación inteligente con el fin de superar las deficiencias que los sistemas comunes presentan. Por lo tanto, surge la necesidad de integrar sus áreas de diseño electrónico, desarrollo de software y seguridad electrónica, para lograr el desarrollo de la ingeniería necesaria a través de técnicas y/o tecnologías del IoT que permita la gestión de dispositivos ciber-físicos y mejore el desempeño en términos de monitoreo en la edificación.

## 1.3. Objetivo general

Llevar a cabo una metodología que permita el desarrollo de un sistema para la gestión de dispositivos ciber-físicos instalados en una edificación mediante el uso de técnicas y/o tecnologías de IoT, que asegure comunicación, conectividad, registro y almacenamiento, al presentarse eventos en los dispositivos.

## 1.4 Objetivos específicos

- Analizar y diagnosticar el espacio que será dotado de capacidades del IoT con el fin de definir las técnicas y/o tecnologías a desarrollar.
- Desarrollar un sistema con las capacidades para gestionar dispositivos ciber-físicos, monitorear, dar alertas y registrar los eventos con técnicas y/o tecnologías del IoT.
- Asegurar la comunicación entre los dispositivos ciber-físicos con el sistema a desarrollar.
- Evaluar la implementación del sistema.

## 1.5. Hipótesis

Mediante el diseño de un sistema de gestión de dispositivos ciber-físicos para edificaciones, se logrará hacer más eficaz la comunicación entre los dispositivos implementando protocolos de comunicación del IoT y evaluando la transferencia de datos; asegurar la conectividad a la red, el registro y almacenamiento de eventos sin comprometer la información disponible en red.

## 1.6. Alcances y delimitaciones

El proyecto se llevará a cabo en un espacio a definir por parte de la empresa, puesto que el objetivo principal es desarrollar un sistema capaz de gestionar los dispositivos ciber-físicos, con el fin de elevar la seguridad en los espacios requeridos y mantener la protección de sus bienes.

Para propósitos demostrativos, la investigación se limitará al desarrollo de una solución para la protección de un edificio con dos espacios inteligentes tipo oficina y a la gestión de sus recursos mediante un sistema conectado a la nube con técnicas del IoT, la cual asegure: comunicación, conectividad, registro y almacenamiento de datos, al presentarse el cambio de estado lógico de los dispositivos ciber-físicos.

## 1.7. Justificación

Los casos de fallas en los sistemas de monitoreo se presentan con frecuencia, en los cuales se comprometen tanto el monitoreo, como los eventos detectados, falsos positivos, falsos negativos, etc., esto último sucede bajo la infraestructura convencional que poseen. Sin embargo, mediante la tecnología del IoT es posible almacenar registros en base a los eventos y generar un protocolo de seguridad que facilite la respuesta rápida a los usuarios, por tal motivo, surge la necesidad de hacer uso de técnicas del IoT con el fin de elevar la seguridad en los espacios requeridos y mantener la protección de sus bienes.

El hacer uso de técnicas del IoT para elevar la seguridad en los espacios públicos y/o privados permite tener acceso a la información de los dispositivos ciber-físicos con el fin de hacer la vida más eficiente y segura para las personas**,** para ello se requiere la integración de las diversas áreas de ingeniería con las que la empresa cuenta abarcando temas en telecomunicaciones y sistemas. Por otra parte, el desarrollo de la ingeniería expande el panorama de la empresa y será factible la integración del conocimiento en sus áreas de trabajo para aumentar la escalabilidad del proyecto.

# 2. MARCO DE REFERENCIA

En este capítulo se realizará el análisis de literatura con el fin de dar sustento a esta investigación. A lo largo del capítulo se describirán algunas definiciones básicas que permitan la mejor comprensión del estudio contemplando temas como: Sistemas ciber-físicos, Internet de las Cosas, edificaciones inteligentes, ciber-seguridad, protocolos de comunicación entre dispositivos, Internet of Everything, entre otros.

## 2.1 Sistemas ciber-físicos

Según Moufaddal, Benghabrit and Bouhaddou (2021) un Sistema Ciber-Físico o CPS, por sus siglas en inglés, es todo aquel dispositivo que integra capacidades de computación, almacenamiento y comunicación, esto, con el fin de controlar e interactuar con un proceso físico. Estos sistemas se encuentran generalmente interconectados entre sí y además cuentan con un enlace a servicios remotos de almacenamiento y gestión de datos. Fragal, Ribeiro and Baldo (2021) mencionan que otra de las características de estos sistemas se encuentra la recopilación de datos de campo, la cual retroalimenta las diferentes etapas del ciclo de vida y el uso de un producto; esto permite realizar inversiones asertivas para mejorar productos, procesos y servicios, así como abrir nuevas posibilidades para los modelos de negocio.

Mois, Sanislav and Folea (2016) señalan que este tipo de sistemas ha traído el surgimiento de una nueva generación de tecnologías digitales, la cual, ha surgido a raíz de los constantes intentos de los organismos sociales y económicos por el desarrollo de procesos para mejorar la eficiencia energética, reducir la contaminación, disminuir el costo de la computación y la creación y detección de redes. Fragal, Ribeiro and Baldo (2021) sustentan que para el año 2025 alrededor del 80% de las industrias manufactureras harán uso de la tecnología que ofrecen los CPS, debido a que a través de los distintos dispositivos como microcontroladores, sensores y actuadores conectados a una computadora es posible monitorear los procesos físicos y enlazarlos al mundo digital.

Según Maru, Nannapaneni and Krishnan (2020) los dispositivos ciber-físicos operan en el ámbito global del IoT, ofreciendo distintas ventajas significativas en diversas áreas como la automatización industrial, la logística inteligente, la gestión de la cadena de suministro

y el transporte inteligente. Es aquí donde el IoT toma un papel importante, pues es a través de este, que los distintos dispositivos ciber-físicos se comunican entre sí para compartir el estado actual de sus sensores (Virmani and Pillai, 2021).

## 2.2 Internet de las Cosas

El IoT es un sistema de dispositivos informáticos conformado por máquinas mecánicas y digitales, objetos, animales o personas que cuentan con identificadores únicos y poseen la capacidad de transferir datos a través de una red sin la intervención de un humano, esto significa que a través de este concepto los dispositivos ciber-físicos enlazados a este sistema pueden comunicarse entre sí de manera autónoma como se apunta en Kishore and Sharma, 2016)

Según Chin, Callaghan and Ben Allouch (2019) los orígenes de esta tecnología se remontan a los sistemas de identificación por radiofrecuencia (RFID), donde el término IoT fue utilizado por primera vez por Kevin Ashton en 1999 en el laboratorio “Auto-ID” del MIT; inicialmente, el término se refería a capacidades de comunicación inalámbrica integradas con sensores y dispositivos informáticos, que permitió que elementos identificables de forma única compartieran información a través de internet con muy poca o ninguna interacción humana.

El IoT precisa de una participación importante de las tecnologías web, debido a que en ellas es posible establecer una conexión remota que permite el acceso a servicios y aplicaciones para monitorizar y controlar los dispositivos conectados al IoT. Es así, que, a través de la capa de aplicación, existen protocolos y tecnologías dentro de la arquitectura tecnológica del IoT que son indispensables para permitir la comunicación entre objetos. Por lo que es necesario un análisis de estos protocolos, que son criterios establecidos acorde a un cierto tipo de aplicación IoT, que den la posibilidad de escoger la mejor tecnología para su desarrollo (Tkachenko, Alla and Maryna, 2018)

### 2.2.1 Arquitectura del Internet de las Cosas

Sharma et al. (2020) menciona que la arquitectura del IoT se compone de 3 capas tal como se muestra en la figura 2.2.

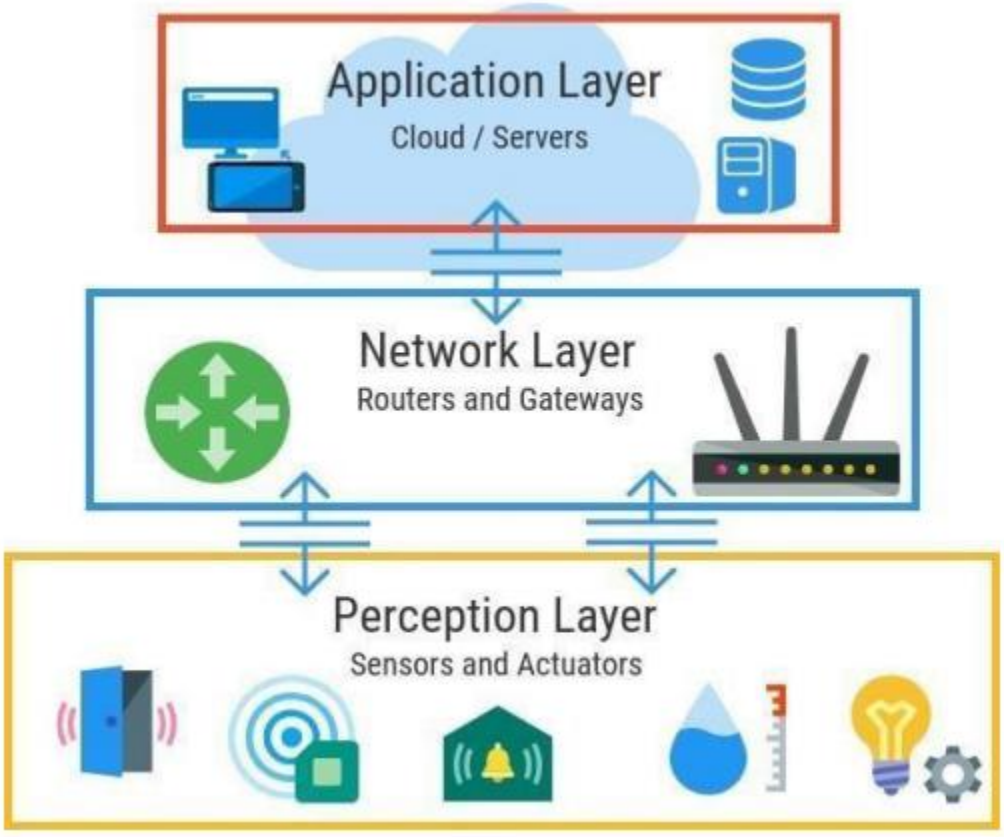


***Figura 2.1*** *Arquitectura del internet de las cosas* (Machado and Calderón, 2016).

La capa de percepción, también llamada la capa de sensores en el IoT, es aquella que captura la información del entorno mediante el uso de sensores. El trabajo de esta capa es observar, recolectar y procesar la información de los sensores antes de enviarlos a la capa de red. Además, en esta capa se lleva a cabo la agrupación de nodos del IoT en redes locales y de pequeño alcance.

Por otro lado, la tarea de las capas de red del IoT es distribuir la información y comunicarse con los distintos tipos de dispositivos y concentradores del IoT en la red. En esta capa se utilizan distintos tipos de tecnologías de comunicación, por ejemplo, WiFi, LTE, Bluetooth, 3G, Zigbee, etc., que brindan a las redes la posibilidad de ejecutar una puerta de enlace de internet, conmutación y dispositivos utilizados para la distribución de información. La puerta de enlace de red opera como negociador entre varios nodos de IoT que combinan, filtran y comunican datos de varios sensores.

Por último, la autenticación, la integración y la confidencialidad de los datos está dada por la capa de aplicación en el entorno del IoT, es a través de está capa que se lleva a cabo la ejecución de la creación de entornos inteligentes que permiten el control, monitoreo y almacenamiento de los distintos datos y dispositivos conectados.

### 2.2.2 Middleware para el Internet de las Cosas

Un middleware es un software distribuido, que en el modelo de capas mostrado en la figura 2.2 se sitúa entre las capas inferiores que corresponde a la capa física de los objetos y las capas de aplicaciones con el objetivo de establecer comunicación e interactuar con todos los objetos del IoT. Este puede ofrecer servicios comunes para aplicaciones y facilitar su desarrollo mediante la integración de dispositivos de comunicaciones, apoyando la interoperabilidad dentro de las diversas aplicaciones y servicios que se ejecutan en estos dispositivos. En general, estos residen en los dispositivos físicos y proporcionan las funcionalidades necesarias para permitir la implementación del servicio (Razzaque et al., 2016)

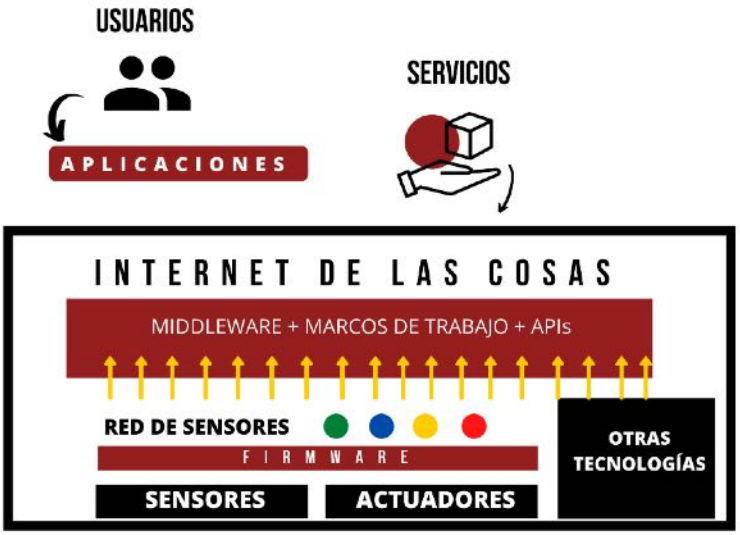


***Figura 2.2*** *Middleware para Internet de las Cosas* (Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, 2014).

### 2.2.3 Objetos Inteligentes

Según Madakam (2015), los objetos inteligentes son un grupo de dispositivos que pueden ser monitoreados y controlados haciendo uso de un equipo central capaz de procesar sus

datos a través de servicios web. Estos objetos pueden poseer capacidad de almacenamiento y procesamiento, ya sea mediante el uso de un software o haciendo uso de sistemas embebidos.

Entre los objetos inteligentes encontramos dos clasificaciones:

**Objetos asistidos**

Son aquellos que requieren de procesamiento adicional para operar, estos son controlados a través de la programación de algún microcontrolador que ejecute las tareas previamente programadas por el usuario. Ej.: Lector de huella digital.

**Objetos simples**

Este tipo de objeto se puede catalogar como cualquier "objeto" que no posee capacidades de cómputo ni procesamiento, pero si contiene un almacenamiento menor. Ej. Etiquetas RFID, NFC, códigos de barra o QR.

### 2.2.4 Identificación de objetos en el IoT

Algunas de las tecnologías más empleadas en la identificación y/o comunicación de objetos en el IoT según Fernandez-Carames and Fraga-Lamas (2018) son la identificación por radio frecuencia (RFID), comunicación de campo cercano (NFC), el control de acceso al medio (MAC), códigos de barra y códigos QR.

**RFID (Identificación por Radio Frecuencia)**

La identificación por radiofrecuencia es una forma de tecnología de comunicación de datos sin contacto en la que los usuarios pueden enviar señales de radiofrecuencia a la etiqueta a través de un lector y recibir información de respuesta de la etiqueta (Duan and Cao, 2020)

**NFC (Comunicación de Campo Cercano)**

Es una tecnología de comunicación nueva y en desarrollo, que se utiliza a menudo en la red IoT móvil. Funciona principalmente en la banda de 13,56 MHz con una velocidad de transmisión de datos de 106 a 424 kbps. La diferencia entre NFC y RFID tradicional es que NFC enfatiza la comunicación sin contacto de corta distancia y utiliza una tecnología de atenuación de señal única y el alcance de radio efectivo es inferior a 20 cm (Fan et al., 2018)

**Control de Acceso al Medio (MAC)**

El Control de Acceso al Medio (MAC) es un identificador exclusivo que se encuentra accesible en el controlador de interfaz de red y otros equipamientos de red. Un equipo que se encuentra conectado a la red se puede reconocer mediante sus direcciones MAC e IP (Symantec, 2013)

### 2.2.5 Hardware para IoT

Ojo et al. (2018) divide al hardware IoT en 3 clasificaciones:

**Dispositivos IoT de Gama Baja**

Estos dispositivos se denominan así por estar limitados en términos de recursos, debido a que no pueden ejecutar sistemas operativos tradicionales como Linux o Windows 10 IoT Core. Estos dispositivos se fabrican principalmente para aplicaciones básicas de detección y actuación, y se programan utilizando firmware de bajo nivel o un sistema operativo de redes de sensores inalámbricos (WSN por sus siglas en inglés) de muy baja funcionalidad.

**Dispositivos IoT de Gama Media**

Se denominan así por ser dispositivos que proporcionan mejores funciones con mayores capacidades de procesamiento en comparación con los dispositivos IoT de gamma baja, entre sus características está el reconocimiento de imágenes mediante la ejecución de algoritmos de visión por computadora a bajo nivel y pueden llegar albergar más de una tecnología de comunicación. Ejemplo: Arduino Yun, Netduino, etc.

**Dispositivos IoT de Gama Alta**

Se caracterizan por ser en su mayoría, Computadoras de placa única, con suficientes recursos como una unidad de procesamiento potente, mucha RAM y un posible volumen de almacenamiento alto, con la capacidad de ejecutar un sistema operativo tradicional como Linux, Windows 10 IoT Core, etc. Estos dispositivos pueden ejecutar algoritmos de aprendizaje automático y se utilizan a menudo como puertas de enlace de IoT para dar cabida a nuevos servicios como análisis inteligente. Por ejemplo; Raspberry Pi, etc.

### 2.2.6 Aplicaciones de Software para IoT

Isikdag (2015) menciona que el Hardware IoT requiere del software que permite que los sistemas operativos funcionen y sea posible implementar protocolos de comunicación para comunicarse con otros dispositivos y humanos, puesto que estas aplicaciones se caracterizan por definir la lógica en la que operará el dispositivo estableciendo su comportamiento y la respuesta del objeto o “cosa” del sistema, dotando de cierta inteligencia a los objetos.

### 2.2.7 Servicios en la nube para IoT

Los servicios en la nube son empleados para gestionar los componentes en el IoT, dado que son maduros y brindan excelentes capacidades elásticas de computación y administración de datos, estos servicios actúan como plataformas computacionales y de procesamiento permitiendo una mejor gestión de los dispositivos. Estas se dividen en 3 grupos, la nube pública, en la cual, es posible obtener el acceso desde cualquier parte del mundo con ciertos condicionamientos, la nube privada que se implementa de manera local en una empresa para su uso exclusivo y por último la nube hibrida, la cual es una combinación de las anteriores (Truong and Dustdar, 2015)

Según Salami and Yari (2018) algunas de las plataformas públicas más importantes en la nube son:

**ThinkSpeak**

Esta Plataforma permite almacenar, examinar y ver los datos obtenidos por los sensores o aplicaciones y es capaz de enlazar objetos, servicios y publicar la información de los objetos conectados en canales.

**Microsoft Azure IoT Hub**

A través de esta plataforma en la nube es posible administrar datos, dispositivos ciber-físicos y además tener servicios adicionales. Soporta los protocolos de comunicación más comunes cómo: MQTT, MQTT sobre Websockets, AMQP, AMQP sobre WebSockets y HTTP.

**Google Cloud IoT**

Esta Plataforma brinda servicios en la nube que permiten enlazar, gestionar y transferir información de los objetos conectados en distintas ubicaciones, además, permite escalar los sistemas con respecto a la cantidad de tráfico de datos, ver y monitorizar en tiempo real los dispositivos para la toma de decisiones según corresponda. Es compatible con los protocolos estándar de comunicación HTTP y MQTT, sin embargo, es de pago pero ofrece un período gratuito.

**IBM Watson IoT**

Esta aplicación desarrollada por IBM proporciona distintos servicios de IoT, clasificados por áreas específicas como: energía, electrónica, automóviles e industria. Ofrece la posibilidad de gestionar los dispositivos, tener acceso a aplicaciones más eficientes y analizar datos en tiempo real a través del protocolo de comunicación MQTT.

**AWS IoT**

Esta plataforma se encuentra alojada en la nube de Amazon y proporciona servicios de captura, análisis y administración de datos y comunicación entre servicios en tiempo real. Es una plataforma de pago que depende de los servicios que se utilicen; ofrece servicios para controlar y administrar los dispositivos además del procesamiento de datos y también soporta los protocolos MQTT, HTTP y WebSockets.

**Ubidots**

Esta plataforma permite capturar datos del entorno y convertir esos datos a parámetros que indiquen ejecutar acciones en tiempo real. Es una herramienta que permite observar los datos de forma interactiva en tiempo real, personalizar la plataforma con su código y tener acceso a los dispositivos a través de protocolos como HTTP y MQTT. Esta plataforma ofrece distintos tipos de cuenta según las necesidades del proyecto, estas van desde una versión gratuita que permite enlazar tres dispositivos hasta una versión de paga denominada “scale” que permite enlazar hasta 4,000 dispositivos.

### 2.2.8 Aplicaciones Web para IoT

Tal como muestran los casos de aplicaciones Web para IoT presentados en Panda et al. (2018), Ferencz and Domokos (2020), las cuales son aplicaciones de software que se ejecutan a través de un navegador web y son ideales para satisfacer las peticiones concurrentes, puesto que permiten servir a varias aplicaciones usando un bucle libre de entrada-salida sin bloquear los procesos. Algunos de los entornos de trabajo en tiempo real más usados se muestran en la tabla 2.1 a continuación.

| Entorno de trabajo | Modelo de Ejecución | Características | Lenguaje de programación soportado | URL |
|---|---|---|---|---|
| Node.js | No bloqueante | • Capacidad nativa de trabajo con websockets.<br>• Incluye librerías IoT para hardware abierto (Arduino, Raspberry, Beaglebone, entre otros.) | JavaScript | https://nodejs.org/es/ |
| Tomado | Bloqueante | • Maneja miles de conexiones concurrentes.<br>• Posee herramientas de seguridad y autenticación.<br>• Usa bucle de eventos de un subproceso. | Python | http://www.tornadoweb.org/en/stable/ |
| Play | No bloqueante | • Soporta conexiones concurrentes.<br>• Soporte para bases de datos y websockets.<br>• Es full stack (viene con herramientas incorporadas) | Java o Scala | https://www.playframework.com/ |

***Tabla 2.1*** *Entornos de trabajo en tiempo real.*

### 2.2.9 Protocolos para IoT

Los protocolos de comunicación son las descripciones adecuadas de transmisión, diseño y reglas de cualquier mensaje digital. Estos protocolos forman la columna vertebral de las redes de IoT, debido a que les permiten acoplarse y conectarse a servicios y aplicaciones inteligentes. Además, permiten que cosas y dispositivos inteligentes intercambien sus datos detectados a través de estas redes (Kassab and Darabkh, 2020)

Ray, (2018) menciona que los protocolos de comunicación definen las siguientes características; esquemas de direccionamiento de dispositivos inteligentes, formatos de datos transmitidos, codificación de datos, control de flujo, formas de retransmisión de

paquetes perdidos y proceso de enrutamiento de paquetes de IoT desde los nodos de origen hacia los nodos de destino. Un ejemplo del uso cotidiano que se le da a los protocolos de comunicación dentro del IoT es mostrado en la figura 2.3.

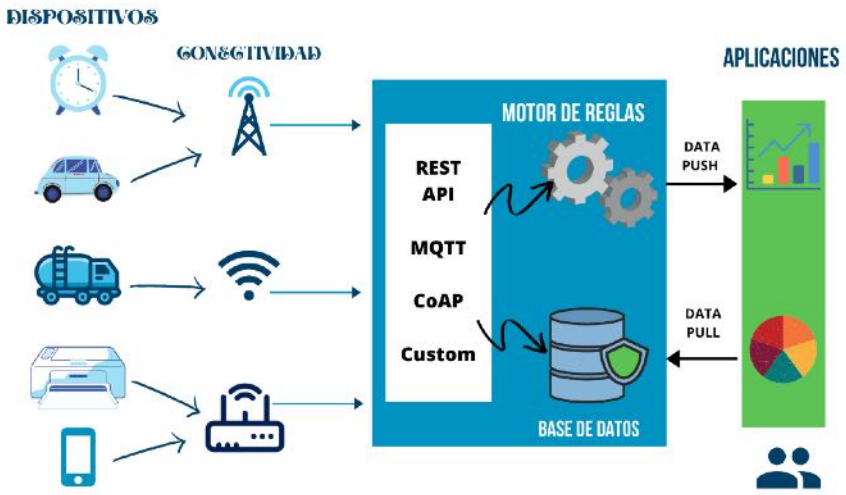


***Figura 2.3*** *Protocolos para IoT* (Hedi, Špeh and Šarabok, 2017).

Antes de introducirnos a los protocolos de IoT, es importante describir conceptos que se mencionan a lo largo de este documento.

**Modelo Publicador/Subscriptor**

Este modelo permite la comunicación débilmente acoplada entre productores de datos llamados “editores” y consumidores de datos llamados “suscriptores”. Los eventos llamados “publicaciones” fluyen desde los editores a través de una red superpuesta de agentes, que enrutan el tráfico de mensajes hacia los destinatarios previstos (Zhang and Jacobsen, 2013)

El PUB/SUB no se conocen entre sí, pero existe un tercer componente llamado “bróker” que es el encargado de filtrar los mensajes entrantes y los distribuye.

Una vez definido lo anterior, procedemos a definir los protocolos comúnmente empleados en el IoT.

**Protocolo MQTT (Message Queue Telemetry Transport)**

Según Soni and Makwana (2017), MQTT es un protocolo Push de Publicación/Suscripción estandarizado que fue lanzado por IBM en 1999, con el fin de enviar datos con precisión bajo la condición de red de largo retraso y bajo ancho de banda.

Tiene la capacidad de intercambiar una gama de paquetes de control de manera específica.

**Protocolo de Aplicación Restringida (Constrained Application Protocol, CoAP)**

CoAP es un protocolo M2M ligero del grupo de trabajo IETF CoRE (entornos RESTful restringidos), está desarrollado principalmente para interoperar con HTTP y la web RESTful a través de simples proxy. A diferencia de MQTT, CoAP utiliza un Identificador de recursos universal (URI) en lugar de temas, el editor publica datos en el URI y el suscriptor se suscribe a un recurso particular indicado por el URI. Cuando un editor publica nuevos datos en el URI, se notifica a todos los suscriptores sobre el nuevo valor según lo indicado por el URI (Naik, 2017)

**Protocolo de Cola de Mensajes Avanzado (Advanced Message Queuing Protocol, AMQP)**

AMQP es un protocolo M2M ligero, que fue desarrollado por John O'Hara en JPMorgan Chase en Londres, Reino Unido en 2003. Es un protocolo de mensajería corporativa diseñado para brindar confiabilidad, seguridad, aprovisionamiento e interoperabilidad. AMQP admite tanto la arquitectura de solicitud/respuesta como de publicación/ suscripción y ofrece una amplia gama de funciones relacionadas con la mensajería, como una cola fiable, mensajería de suscripción y publicación basada en temas, enrutamiento flexible y transacciones. El sistema de comunicación AMQP requiere que el editor o el consumidor creen un "intercambio" con un nombre dado y luego difunden ese nombre. Los editores y los consumidores utilizan el nombre de este intercambio para conocerse mutuamente, posteriormente, un consumidor crea una "cola" y la adjunta al intercambio al mismo tiempo, los mensajes recibidos por el intercambio deben coincidir con la cola mediante un proceso llamado "vinculación" (Naik, 2017)

**Transferencia de Estado Representacional (Representational State Transfer, REST)**

La arquitectura REST fue introducida en el año 2000, por Thomas Fielding, y se basa en los principios que sustentan la World Wide Web. En resumen, de acuerdo con los principios REST, las interfaces REST se basan exclusivamente en identificadores uniformes de recursos (URI) para la detección e interacción de recursos, y generalmente en el Protocolo de transferencia de hipertexto (HTTP) para la transferencia de mensajes. Un URI de servicio REST solo proporciona la ubicación y el nombre del recurso, que sirve como un identificador de recurso único, aquí, los verbos HTTP predefinidos se utilizan para definir el tipo de operación que se debe realizar en el recurso seleccionado (por ejemplo, GET para recuperar, DELETE para eliminar un recurso) (Neumann, Laranjeiro and Bernardino, 2018)

**Protocolo de Mensajería de Aplicaciones Web (Web Application Messaging Protocol, WAMP)**

WAMP es un sub-protocolo estándar abierto de Web Socket que es útil para aplicaciones de IoT, mientras que REST define un conjunto de principios arquitectónicos mediante los cuales se pueden diseñar los servicios web que se centran en los recursos de un sistema, incluida la forma en que los estados de los recursos se tratan y transfieren a través de HTTP. La comunicación se logra mediante los protocolos de llamadas a procedimiento remoto (RPC) y publicación/suscripción (PubSub). Ej.: Crossbar.io es un enrutador WAMP avanzado fabricado y respaldado por Crossbar.io Gmbh (creadores de WAMP) (Doxopoulos et al., 2018)

## 2.3 Edificaciones inteligentes

Un edificio inteligente es aquel que posee las capacidades para permitir que una persona tome decisiones más informadas sobre ese edificio en función de los datos que proporciona. Estos datos se agregan a través de controles y sensores del IoT en una aplicación alojada en la web, desde la cual, es posible monitorear, controlar y actuar sobre los equipos en tiempo real. Estos edificios sirven para ayudar a los administradores de las propiedades a obtener información sobre el funcionamiento detallado de sus ubicaciones y recopilar datos útiles para mejorar el rendimiento y la eficiencia del edificio. En general,

los edificios inteligentes están optimizados para la eficiencia energética, la comodidad y la seguridad (Aguilar, Peralta and Mauricio, 2020)

Según Al Dakheel et al. (2020) las edificaciones inteligentes poseen 5 características fundamentales:

1. Automatización: es la capacidad de administrar dispositivos autómatas o realizar funciones automáticas.
2. Multifuncionalidad: es la capacidad de llevar a cabo más de una función o proceso en un edificio.
3. Adaptabilidad: es la capacidad de aprender, predecir y satisfacer las necesidades de los usuarios y el entorno externo.
4. Interactividad: es la capacidad de permitir la interacción entre usuarios.
5. Eficiencia: es la capacidad de proporcionar eficiencia energética y ahorrar tiempo y costos.

Por otro lado Verbeke et al. (2017) menciona que existen tres aspectos clave a considerar para que un edificio sea considerado como inteligente:

1. Disponibilidad para adaptarse en respuesta a las necesidades de los ocupantes y capacitar a los ocupantes del edificio para que tomen el control directo de su consumo de energía.
2. Disponibilidad para adaptarse en respuesta a las necesidades o situación de la red.
3. Disponibilidad para facilitar el mantenimiento y funcionamiento eficiente del edificio de una forma más automatizada y controlada.

## 2.4 Domótica

Según lo que describe Paz Corrales (2020) la Domótica se define como el sistema que interconecta los distintos dispositivos de una vivienda a la red para que logren una comunicación entre sí y permitan una interacción con el usuario.

Es a través de las nuevas tecnologías y dispositivos incorporadas al equipamiento de una vivienda que es posible recopilar información, procesarla y enviar ordenes que automatizan distintas acciones que el usuario puede programar, con el fin de controlar de forma centralizada cada una de las tareas y aparatos que conforman dicho sistema.

En este sistema, los dispositivos disponen de sensores para capturar la información del entorno y establecer comunicación entre sí, es decir, se establece una red de comunicación. Este sistema le permite al usuario controlar los dispositivos de forma centralizada y mantener en supervisión todas las actividades que se llevan a cabo en el hogar, además de permitir el control remoto acorde a sus necesidades.

## 2.5 Inmótica

De acuerdo con el estudio elaborado por Montalbán Pozas et al. (2018) los sistemas de automatización y control electrónico son incorporados en edificios de uso terciario o industrial como oficinas, edificios corporativos, hoteles, empresas y similares a través de la Inmótica, con el objetivo de ahorrar energía, lograr un mayor confort y tener una mejor seguridad en el entorno.

A pesar de que el concepto de Inmótica no es muy distinto al concepto de domótica existe la diferencia en que la Inmótica concentra su enfoque a los edificios de uso terciario o industrial en función de que la actividad que se desarrolle en el edificio, los sistemas y las redes de automatización sean distintas y adaptadas a las necesidades específicas del mismo; es por ello que para nada sería igual la implementación tecnológica de la Inmótica en un hotel que en una fábrica de zapatos o en un taller de motores, sin embargo la domótica de un departamento, casa o piso es similar, debido a que las funciones que se pueden automatizar en una casa por lo general ya se encuentran definidas.

## 2.6 Internet de Todo

Acorde a Langley et al. (2021) la internet de Todo (Internet of everything, IoE, por sus siglas en inglés) es un concepto que extiende el énfasis del IoT en las comunicaciones de máquina a máquina (M2M) para describir un sistema más complejo que también abarca personas y procesos.

El concepto fue originado por la empresa CISCO, el cual se encuentra definido como la conexión inteligente de personas, procesos, datos y cosas. Es dentro del IoT que todas las comunicaciones dadas entre máquinas, IoT y M2M a veces son considerados iguales; sin embargo, el concepto IoE es más extenso porque que aborda las comunicaciones

maquina a máquina (M2M) y las interacciones de máquina a persona (M2P) y a si mismo las de persona a persona (P2P) asistida por tecnología.

## 2.7 Internet Social de las Cosas

Los estudios de investigación efectuados por Atzori, Iera and Morabito (2014) y Ejaz et al. (2016) han evaluado la interacción entre dispositivos, las relaciones resultantes y los servicios compuestos junto con los aspectos relacionados de la confiabilidad, esto debido al interés que el Internet Social de las Cosas ha atraído a la comunidad investigadora en los últimos años.

Afzal et al. (2019) define el Internet Social de las Cosas (“SIoT” por sus siglas en inglés) como el establecimiento de relaciones sociales entre objetos inteligentes que interactúan entre sí; en este se pueden tener numerosas aplicaciones en atmósferas hiperconectadas, como ciudades inteligentes habilitadas para IoT, comunidades inteligentes, redes inteligentes, telemedicina, etc.

El SIoT aborda el establecimiento de relaciones debido a la interacción de los dispositivos IoT entre sí y con sus usuarios dentro de un periodo de tiempo, estos dispositivos en las aplicaciones de IoT brindan un tipo diferente de servicios integrados para lograr un objetivo común y ser mutuamente beneficiosos.

Baccarelli et al. (2018) menciona que la introducción de los vínculos sociales antes mencionados en el ámbito del IoT modifica la forma en que los seres humanos y las cosas utilizan los modelos de interacción de persona a persona (H2H), computadora a computadora (C2C) y persona a computadora (H2C), con el fin de establecer lazos de vínculos sociales, en donde la interacción de persona a persona se lleva a cabo a través de construir vínculos sociales utilizando las redes sociales humanas como Facebook, Instagram, Whatsapp, etc., estas plataformas tecnológicas comunican y brindan información como los intereses de los usuarios, la ubicación y las características de las relaciones de individuos o comunidades de personas. Por otro lado, el modelo C2C se refiere al intercambio de información a través de dispositivos inteligentes inalámbricos o cableados que ocurre con una mínima participación humana, estos establecen reglas generales, con el fin de definir la comunidad de dispositivos inteligentes en colaboración y los servicios que proporcionará la comunidad de dispositivos; es aquí en donde los

dispositivos son tanto productores como consumidores de datos e información, por último el modelo tradicional, cliente-servidor, es donde se lleva a cabo la interacción de persona a computadora, en este los humanos actúan como clientes en donde consumen los datos y controlan la actividad de la computadora paso a paso, y las computadoras actúan como servidores e informan los datos requeridos por los humanos y es así como se lleva a cabo la minería de datos.

Finalmente, los modelos de interacción mencionados anteriormente nos permiten observar formalmente las características de los paradigmas del IoT y el SIoT obteniendo como resultado el panorama mostrado en la figura 2.4.

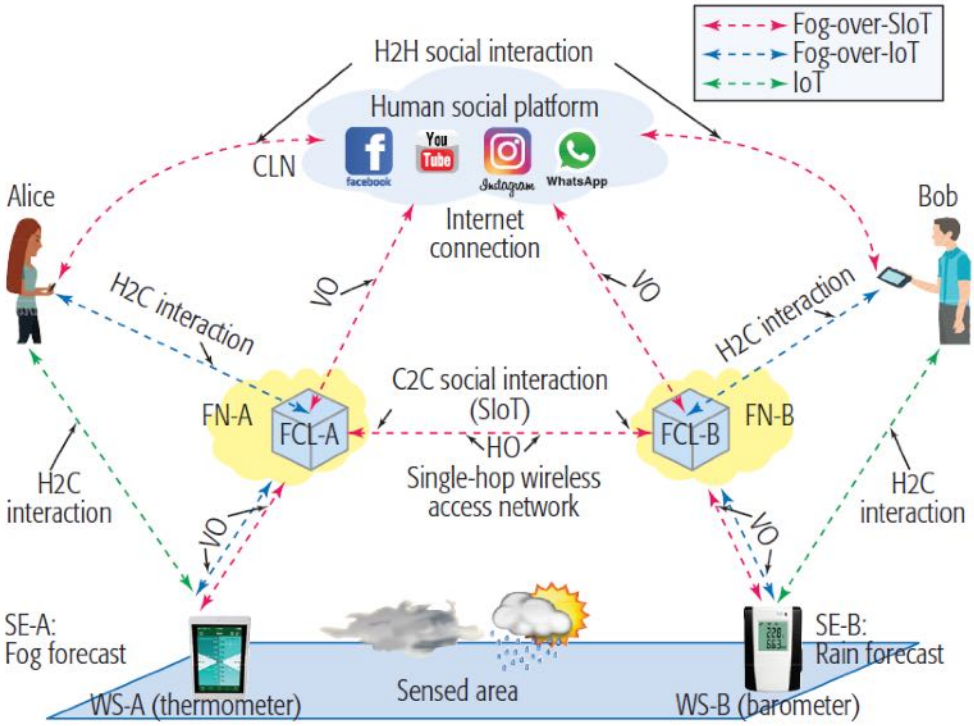


***Figura 2.4*** *Concepto global del Social Internet of Things* (Baccarelli *et al.*, 2018).

Se puede observar que bajo el concepto anterior se cumplen los modelos previamente descritos, dado que se muestra una plataforma social humana alojada en una nube remota y los usuarios intervinientes explotan las capacidades para respaldar las interacciones H2H mediante el establecimiento de conexiones sociales de amistad entre humanos, en ella también se muestran distintos centros de datos virtualizados, interconectados y equipados con recursos de pequeño tamaño (FN-A, FCL-B), estos albergan clones de los dispositivos físicos involucrados para aumentar las capacidades de comunicación

informática de los dispositivos asociados, esto permite la interacción C2C a través de una red social superpuesta entre clones, es decir, la red SIoT.

## 2.8 Desafíos, riesgos y seguridad en el Internet Social de las Cosas

Según (Imran *et al.*, 2019) además de los desafíos heredados por el IoT y las redes sociales, el SIoT tiene su propia lista de desafíos desde las perspectivas de privacidad, confiabilidad, seguridad, tolerancia a fallas, interacción e interfaces, solo por nombrar algunos. Aunque SIoT se encuentra aún en una edad temprana, sus componentes están ahora en una etapa de madurez significativa y es posible apreciar en la literatura varios esfuerzos para presentar soluciones tanto convencionales y no convencionales, lo que ha permitido identificar distintas brechas tecnológicas en función de diversos desafíos.

Algunos de estos desafíos se muestran en el estudio realizado por (Faqihi, Ramakrishnan and Mavaluru, 2020) y son abordados de la siguiente manera:

1. **Falta de seguridad:**
   Como cada sistema posee sus vulnerabilidades, el SIoT no se encuentra exento, la mayoría de los dispositivos que están conectados en una red son fácilmente penetrables y esto se informó en 2015 cuando un automóvil que se conducía solo fue atacado, por lo tanto, la seguridad juega un papel fundamental debido a que la información que se sobre carga a internet cada segundo a través de esta red es crucial.
2. **Falta de privacidad:**
   De manera variable, los dispositivos IoT están sujetos a tener una gran cantidad de datos confidenciales de un usuario y pueden estar sujetos a vulnerabilidad y pueden ser atacados de cualquier forma a través de la red y aun-que existen un gran número de técnicas de preservación de la privacidad para el SIoT, todavía parece haber más vulnerabilidad y aún persisten desafíos de investigación abiertos en esta área.
3. **Problemas de almacenamiento:**
   Si se imprimieran los datos que están disponibles en internet, la impresión tomaría la distancia desde el planeta tierra hasta marte, y es de esperarse que los datos

generados por los dispositivos inteligentes aumentaran en un futuro, por lo que es necesario poseer mecanismos adecuados para manejar los datos crecientes generados por los dispositivos IoT.

4. **Residuos electrónicos:**

   Hoy en día los países siguen desarrollándose activamente, además de tener un crecimiento en el desarrollo comercial, por lo tanto, la producción de desechos electrónicos irá en aumento gradualmente. Solo una pequeña parte de los desechos se recicla y el resto se deja desatendido.

5. **Consumo energético**

   En el año 2018, se estimó que el funcionamiento del internet necesitaba 90 mil millones de vatios de potencia durante un año. Por lo tanto, las nuevas tecnologías deben diseñarse para el uso eficiente de la energía o dispositivos de menor potencia.

6. **Nuevos casos de uso:**

   En la implementación de nuevas tecnologías, como cada dispositivo que se integra al mercado, los dispositivos IoT también deben recibir un manual de cómo usarlo. Aunque a la fecha se encuentran innumerables manuales disponibles, el propósito real surge solo después de la implementación.

Por otro lado, (Khan *et al.*, 2017) menciona que con el fin de disminuir los riesgos y aumentar la seguridad en el entorno SIoT, los investigadores están motivados en proporcionar protocolos de gestión de confianza, puesto que, como se mencionaba anteriormente pueden existir propietarios y objetos que tengan un comportamiento atípico dentro de la red y hacer mal uso de las relaciones sociales que los dispositivos integran para iniciar ataques discriminatorios al sistema de gestión de la confianza. El objetivo de estos objetos o propietarios es adquirir beneficios en forma de servicios o recursos mediante la cooperación de otros objetos y/o dispositivos que son capaces de consumir estos servicios en red, es por tal motivo que la gestión de servicios basada en la confianza en SIoT es de suma importancia, por lo que se abre en la siguiente sección algunos aspectos en ciber-seguridad a considerar para la implementación del SIoT.

## 2.9 Ciber-seguridad

Actualmente, el IoT está centralizado en mejorar la calidad de vida conectando las cosas a internet, sin embargo, un menor control de seguridad podría convertir esta tecnología en una amenaza. Según Cisco Inc., se prevé que existan alrededor de 50 mil millones de dispositivos conectados hasta 2020. Esta conectividad permitirá acceder a todo tipo de datos personales e información sofisticada. Sin el uso de medidas de seguridad precisas, se permitirá a los intrusos obtener el control de datos enormes (Oyshi et al., 2021)

Según Yedle et al. (2021) existen tres aspectos de seguridad a considerarse en el entorno del IoT:

1. Confidencialidad: Esto significa evitar que usuarios no autorizados accedan a información sensible. Existen varias formas de proporcionar confidencialidad, como el cifrado de datos, la gestión del acceso a los datos y la autenticación del usuario.
2. Integridad: Esto significa que los datos deben mantener la precisión, la coherencia y la confiabilidad de la información. Los datos no deben alterarse durante la comunicación, como la modificación de datos por parte de un tercero o verse afectados debido a otros factores que no están controlados por humanos, incluido el bloqueo del servidor.
3. Disponibilidad: la disponibilidad de datos significa que la información debe estar disponible para los usuarios cuando sea necesario. Garantiza el acceso inmediato de la información a los usuarios autorizados.

Tal como se mencionó en la sección 2.1, el IoT se compone de tres capas; en este sentido, Patnaik, Padhy and Srujan Raju (2021) sustentan que tal arquitectura contiene una gran cantidad de dispositivos y equipos con un servidor de gama alta con problemas de seguridad en cada uno de sus niveles descritos a continuación:

1. **Capa de percepción:** En esta capa se presentan los “ataques de interferencia” donde este tipo de ataque se realiza disminuyendo la señal de frecuencia de envío de la red sin seguir los protocolos específicos. La interferencia de radio afecta principalmente al funcionamiento de la red, como el envío y la recepción de datos

en IoT. Por otro lado, se presenta la “inicialización insegura” es por eso que para garantizar un servicio de red adecuado y seguro en IoT, debemos inicializar y configurar los dispositivos de IoT en la capa de percepción haciendo uso de identificadores únicos por dispositivo de tal forma que se validen en el servidor para asegurar que estos pertenezcan al sistema.

2. **Capa de red:** en esta capa se ven comprometidos los protocolos de comunicación, la gestión de sesiones y el enrutamiento.
3. **Capa de aplicación:** Para esta capa es necesaria la aplicación de seguridad restringida en los protocolos que utilizan las aplicaciones, esta capa hace uso de diversas aplicaciones para distintos propósitos, que son vulnerables a atacantes no autorizados.

Osisiogu (2019) menciona que los desafíos de la seguridad ciber-física para edificios inteligentes se están volviendo rápidamente a complejos y únicos. Esto a su vez, forma un panorama de amenazas formidable que consolida sensores, actuadores, computacionales, redes, dispositivos electrónicos, mecánicos y humanos.

Debido a que éstos se ven involucrados en el panorama de ataques en la ciberseguridad convencional, se proponen algunas soluciones para mitigar y defender el panorama ciber-físico de los edificios inteligentes:

1. Defensas contra ataques DoS.
2. Prevención y detección de intrusos.
3. Criptografía basada en defensas.
4. Defensas de red y datos en tránsito.
5. Protocolos de comunicación específicos para defensas.
6. Manual de mejores prácticas.

## 2.10 Estudios previos

Con el fin de realizar un análisis detallado del estado del arte con relación a la aplicación final del proyecto, se debe buscar estudios de preferencia, las variables a medir sean las mismas y los objetivos de investigación sean similares. Realizar una recopilación de tecnologías actuales similares que contengan la realización de prototipos de monitoreo de

edificaciones inteligentes, enfocándose en aquellas que por sus resultados obtenidos, posean más importancia para el proyecto.

Para llevar a cabo este análisis es necesario consultar una base de datos confiable y basta en información, por lo que se realizó la consulta de la base de datos bibliográfica “Scopus”, en vista de que la evaluación experta realizada por Codina et al., (2020) acerca del uso de Scopus para investigar, menciona que esta cubre áreas de: ciencia, tecnología, medicina y ciencias sociales. Por otro lado Elsevier (2019), menciona que Scopus es la mayor base de datos de citas y resúmenes de bibliografía revisada por pares: revistas científicas, libros y actas de conferencias, incluyendo herramientas inteligentes para hacer un seguimiento, analizar y visualizar la investigación; por lo tanto, su veracidad, enfoque y amplitud en contenido serán suficientes para dar sustento a esta investigación.

Por otro lado, los estudios de mayor relevancia son aquellos donde las investigaciones se desarrollen a nivel prototipo, llevando a cabo la automatización de edificaciones y en los que se realice una plataforma software para el análisis e interpretación de los datos. Los estudios que sobrepasen los objetivos de esta investigación también serán considerados, principalmente aquellos que, entre sus variables de medición, contengan las variables mencionadas.

Finalmente llevar a cabo una comparación del compendio de metodologías enfocándose en los aspectos individuales que más proporcionen valor a esta investigación. Cabe mencionar que los estudios que se deben de incluir tendrán que poseer el enfoque principal de monitorear y controlar los dispositivos ciber-físicos instalados en edificaciones inteligentes en tiempos convenientes haciendo uso de redes de sensores.

También serán considerados estudios que su área de aplicación sea el desarrollo de software o tecnologías de información, enfocados a la administración de ciudades inteligentes, procesos inteligentes, ciber-seguridad, entre otros.

Con el fin de definir la metodología apropiada para llevar a cabo el desarrollo de un sistema para la gestión de dispositivos ciber-físicos se evalúan los estudios que posean

la misma naturaleza de esta investigación, por lo que según el estudio realizado por (Che Soh *et al.*, 2018) en donde se lleva a cabo el desarrollo de un sistema IoT para realizar la medición del consumo de agua en casa habitación y generar alertas, es de suma importancia partir con el análisis de la problemática y/o el espacio en el cual se pretende realizar la implementación del sistema, dado que a través de esta etapa se determinan las necesidades a cubrir para posteriormente definir con certeza las técnicas y/o tecnologías que satisfagan dichas necesidades. Por otro lado, con el fin de llevar a cabo la interconexión de los dispositivos ciber-físicos con el internet (Ali *et al.*, 2020) propone diseñar un sistema que posea la compatibilidad con las técnicas y/o tecnologías del IoT previamente definidas, puesto que esto permitirá asegurar correctamente la disponibilidad de recursos en hardware en la plataforma. Posteriormente, ambos estudios plantean la implementación cómo la configuración apropiada de los dispositivos ciber-físicos para dotarlos con la capacidad de transmitir la información capturada en el entorno hacía el sistema.

Por último, algunos estudios cómo los de (Gayathri, 2019), (Aheleroff *et al.*, 2020) y (Che Soh *et al.*, 2019), entre otros, en donde se lleva a cabo la implementación de un sistema para la gestión de dispositivos ciber-físicos, evalúan sus datos a través de las gráficas generadas por el sistema al recibir la información del entorno capturada por los dispositivos ciber-físicos y en caso de detectar datos atípicos se lleva a cabo el ajuste calibrando correctamente cada uno de los sensores y/o actuadores.

# 3. METODOLOGÍA

En este capítulo se describe la metodología para el sistema de monitoreo de edificaciones inteligentes. Debido a los objetivos planteados en esta investigación, la metodología es de naturaleza experimental puesto que se realizarán pruebas en las que se analicen los datos capturados por los sensores con el fin de estudiar y mitigar los posibles falsos positivos y/o falsos negativos, a esto se le conoce como calibración de sensores según (Mustapaa et al., 2020).

Sampieri (2010) define el experimento como el estudio donde se manipulan intencionalmente una o más variables independientes, para analizar las consecuencias que la manipulación tiene sobre una o más variables dependientes, dentro de una situación de control para el investigador.

A continuación, se propone la metodología mostrada en la figura 3.1 en base a los criterios definidos en la sección 2.10 de la presente investigación.


***Figura 3.1*** *Metodología propuesta (Elaboración propia).*

Este proyecto se divide en siete etapas; la primera tiene como resultado el comprender el entorno y/o la problemática que se pretende resolver, posteriormente, la segunda etapa nos permitirá seleccionar aquellas técnicas y/o tecnologías que satisfagan las necesidades del entorno y/o problema previamente analizado, posteriormente, la tercera etapa nos direcciona a añadir valor a la información que se desea capturar para digitalizarla y obtener un sistema capaz de alertar, monitorear y controlar los dispositivos disponibles en la red, una vez teniendo el diseño, es necesario asegurar que los dispositivos se encuentren disponibles en red, por lo que la cuarta etapa nos encamina a realizar un análisis en las comunicación de los dispositivos con el sistema; la quinta etapa consiste en implementar el sistema previamente diseñado con el fin de ponerlo a prueba y asegurar el correcto funcionamiento, posteriormente, en la sexta etapa se lleva a cabo la evaluación de los datos capturados por el sistema con el fin de verificar si existen falsos negativos y/o falsos positivos que comprometan la veracidad de los datos y así finalizar con la séptima etapa, el ajuste de los dispositivos en caso de ser necesario.

## 3.1 Análisis y diagnóstico del espacio a automatizar.

En esta etapa es necesario tomar en cuenta a los actores que intervienen en los procesos, los datos que corresponden a las actividades realizadas en el entorno y trabajos que relacionen a la Domótica y la Inmótica; a tales efectos se llevan a cabo entrevistas con los encargados de planificación en infraestructura, con responsables de área, y personas consideradas clave o expertas con el fin de cubrir la mayor cantidad de información existente y de planificaciones acordadas previamente.

Se toman en cuenta como ejes temáticos los siguientes: conectividad, seguridad, movilidad, calidad ambiental, energía, habitabilidad y conectividad.

Por otro lado, el análisis se lleva a cabo teniendo en cuenta en la evaluación de los espacios que tienen el fin de implementar tecnologías en el diseño de sistemas IoT los siguientes aspectos:

- Escalabilidad: Se inicia evaluando el alcance del proyecto, que dicho sistema pueda satisfacer a largo plazo las necesidades de la edificación, además de permitir la integración de nuevos dispositivos en caso de que se presenten nuevas necesidades.

- Avances tecnológicos: los sistemas que poseen tecnologías que no evolucionan se vuelven obsoletos con el paso del tiempo, lo que disminuye la duración de la inversión y genera costos de operación adicionales.
- Misión del sistema: En este tipo de sistemas no se debe de depender de un solo fabricante, por lo tanto se evitará estar sujeto a las decisiones del fabricante.

Una vez teniendo en cuenta los parámetros, es necesario dimensionar el espacio que se pretende automatizar, con el fin de conocer las distancias entre el emisor y el receptor, la naturaleza de los obstáculos, distorsión de ruido y por último considerar las regulaciones gubernamentales.

El análisis puede llevarse a cabo mediante inspección visual del espacio y realizar mediciones de las áreas en las que se pretenden instalar los dispositivos ciber-físicos; por otro lado es necesario definir qué acción, proceso o entorno pretende captarse o controlarse para definir el tipo de dato que se estará manipulando, el tipo de actuador que será necesario, el nivel de energía que será necesario para provocar el movimiento o el traslado de los datos.
Las distancias en esta etapa se consideran importantes para definir el protocolo de comunicación que se estará implementando, dado que los protocolos tienen un rango amplio de cobertura, se puede partir de una medición empírica y realizar pruebas.

## 3.2 Definición de técnicas y/o tecnologías.

Basados en la etapa de análisis y medición es como se procede a definir las técnicas y/o tecnologías adecuadas para cada escenario; según sea el entorno y/o el dispositivo a automatizar se selecciona la técnica y/o tecnología que cumpla con las funciones de monitoreo y control de dicho entorno, por otro lado, es capaz de hacer viajar la información a través del protocolo de comunicación a seleccionar e interconectar el entorno físico con el virtual.

Para la selección de estas se toma en cuenta lo siguiente:

1. **Etapa de procesamiento.**

   Uno de los requisitos deseables en el IoT que los dispositivos deben ser de bajo consumo de potencia eléctrica, esto quiere decir que a comparación de los procesadores utilizados convencionalmente es necesario proponer algo mucho más pequeño y de menor consumo, es por eso que las soluciones de ARM cumplen con las expectativas.

2. **Etapa de sensores.**

   Los sensores son el elemento hardware que permite la interacción entre la tecnología y el entorno, puesto que captura los datos requeridos (según sea el caso), por ende, el procesador y la plataforma se encargaran de administrar la información que será recabada por el sensor.

   Es a través de este elemento que la información será capturada para los objetos, y son capaces de captar todo tipo de información, como sonidos, intensidad de luz, distancia, presencia de humo, entre otros.

3. **Comunicación de bajo consumo.**

   A razón de que no todos los dispositivos tienen la capacidad de tener grandes bancos de baterías, se siguen desarrollando dispositivos de bajo consumo y de menor tamaño y que a su vez puedan mantener la calidad de la transmisión, debido a que es necesario para enlazar todo tipo de dispositivos en el IoT y mantener una comunicación ágil.

La duración de la batería, memoria, ancho de banda, entre otros, son algunos de los aspectos que se deben tomar en cuenta para elegir un protocolo de comunicación, debido a que estos influyen en el rendimiento de cada dispositivo que se encuentra conectado a IoT. Entre los protocolos que fueron creados para este tipo de aplicaciones en específico se encuentran: MQTT, AMQP, XMPP, CoAP y WAMP. Sin embargo, en ambientes en donde se requiere transmitir grandes cantidades de información prevalecen los protocolos de WebSockets y HTTP.

A continuación la tabla 3.1 muestra un análisis comparativo de las tecnologías y protocolos para IoT con el fin de tomar la decisión más conveniente para el proyecto.

| | Características | Arquitectura | Protocolo Transporte | Codificación | Web nativa | Estandarización /recomendación | Seguridad | QoS | Compatibilidad |
|---|---|---|---|---|---|---|---|---|---|
| MQTT | Ligero, simple y reducido consumo de energía | PUB/SUB | TCP | Binaria, Json, Personalizado. | No | OASIS (estándar abierto) | SSL/TLS | Si | Sofia2, Microsoft Azure IoT, Fiware, IBM Watson, Artik, Ubidots, Google Cloud IoT, AWS IoT |
| AMQP | Fiabilidad, Interoperabilidad, Transaccionalidad | PUB/SUB | TCP | Binaria | No | OASIS (estándar abierto) | SSL/TLS, SASL | --- | Microsoft Azure IoT, Sofía2. |
| XMPP | Envía mensajes en tiempo real | PUB/SUB | TCP | XML | Si | IETF (estándar abierto) | Cifrado, autenticación, Autorización. | --- | XMPP-IoT |
| CoAP | Arq. REST, acerca el modelo HTTP a dispositivos restringidos. | Cli/Serv. | UDP | Binaria, Json | Si | IETF (estándar abierto) | DTLS Datagram Transport Layer Security | Si (Ack) | Sofia2, Fiware, Microsoft Azure, Ubidots, Google Cloud IoT, AWS IoT. |
| Websockets | Comunicación bidireccional independientemente de la plataforma. | Cli/Serv. | TCP | Binaria, texto, Json. | Si | IETF (estándar abierto) | TSL/SSL | --- | Sofia2, Azure IoT, AWS IoT, Artik. |
| REST | Estilo de arquitectura de software, ampliamente utilizado para aplicaciones web. | REQ/RES | TCP | XML,Json | Si | Recomendación no oficial. Está basado en estándares HTTP, URL, tipos MIME. | TSL/SSL | --- | Azure IoT, Artik. |

***Tabla 3.1*** *Comparación de Protocolos y Tecnologías IoT.*

Tomando en cuenta los aspectos que se evalúan en la tabla 3.1, es necesario identificar aquellos protocolos que proporcionen una alta compatibilidad tanto con los dispositivos ciber-físicos como con las plataformas IoT, esto con el fin de permitir la escalabilidad del proyecto en caso de que se presenten necesidades a futuro dentro del entorno. Otro aspecto importante que considerar es la seguridad que ofrece el protocolo al transportar los datos para evitar comprometer la información y mantener la privacidad. Además de la tabla 3.1, es importante conocer cada uno de los protocolos y/o tecnologías comúnmente usadas en el diseño de sistemas IoT, por lo que se describe en la sección 2.2.9 de esta investigación cada uno de los protocolos para mejorar la toma de decisión en el proceso de selección.

## 3.3 Diseño y desarrollo del sistema.

Se parte por comprender con exactitud cómo es que las tecnologías del IoT permiten a su vez la integración de nuevos productos y servicios para entender la naturaleza plena de los desafíos del diseño. Una buena manera para ilustrar la arquitectura es la modelación del flujo a través de un sistema que refleje el valor contenido en los productos conectados,

es aquí donde el lazo del valor de la información de Deloitte, según Odusote, Ayo Naik, Sujit Ashish, Tiwari Arora (2016), ilustra cómo la tecnología del IoT se conecta dando acceso a nuevas tecnologías para crear un nuevo valor para las compañías y para los clientes. (Figura 3.3)

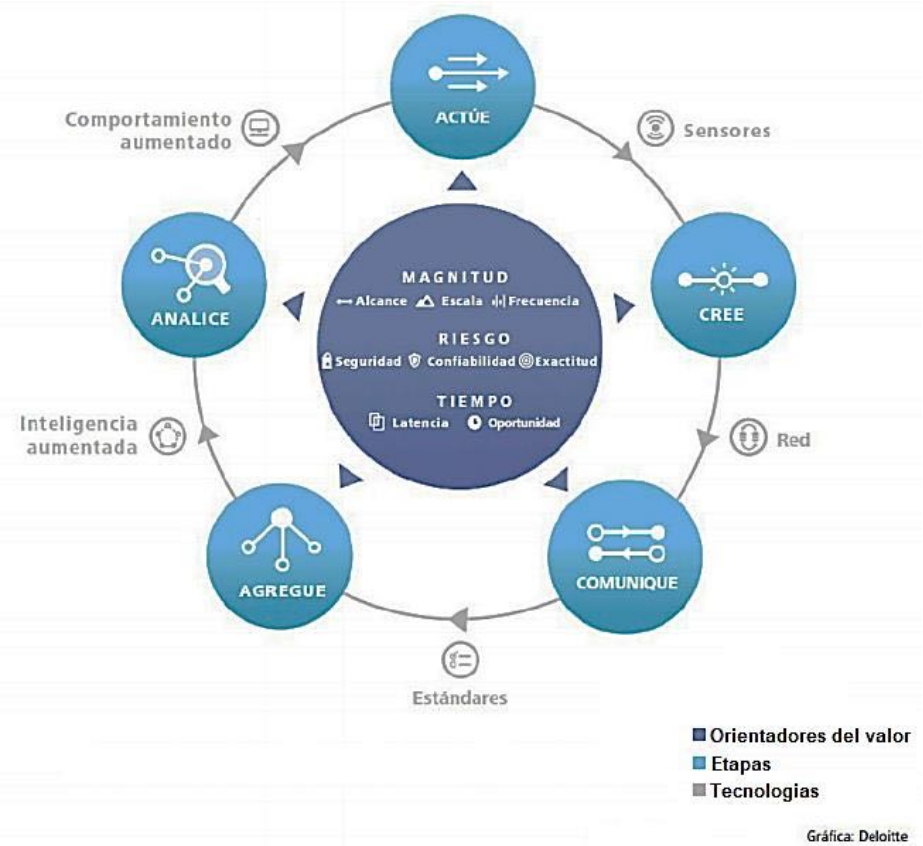


***Figura 3.3*** *Lazo de valor de la información* (Odusote, Ayo Naik, Sujit Ashish, Tiwari Arora, 2016).

La conectividad del IoT además de ser un desafío adicional, añade al proceso un nivel de complejidad mucho más elevado, puesto que la conectividad remodela los desafíos junto con la complejidad del diseño del producto y la interconectividad que define la tecnología impone nuevos requerimientos. Podemos comenzar a categorizar el impacto de la tecnología o de los productos del IoT y del diseño del producto en cuatro transformaciones principales:

1. Unir a los mundos físico y digital.
2. Mantenerse “siempre” y constantemente conectado.
3. Moverse desde un objeto aislado hacia parte de un sistema más grande.
4. Usos y ciclos de vida en constante evolución.

Tomando en cuenta lo anterior, el proceso de diseño hoy en día se ha vuelto menos complejo, considerando que existe gran diversidad de plataformas capaces de manipular hardware haciendo uso del protocolo de comunicación MQTT entre dispositivos, es necesario seleccionar una plataforma que sea compatible con el hardware, ya sea que se haga uso de microcontroladores, PLC, tarjetas de adquisición de datos, dispositivos móviles, entre otros.

(Hejazi *et al.*, 2019) proponen 3 aspectos importantes a considerar durante el proceso de selección de la plataforma IoT:

**1.- Estabilidad en la plataforma:** existe la posibilidad dentro de las plataformas actualmente disponibles en el mercado de que algunas de estas desaparezcan, por lo que es indispensable indagar en proyectos actuales y pasados para conocer la estabilidad y la fiabilidad de esta, considerando que si el proveedor se retira podría ser un desperdicio en la inversión.

**2.- Escalabilidad y flexibilidad:** es necesario asegurar que la plataforma funcione desde un proyecto pequeño hasta en uno a gran escala, tomando en cuenta que se presente el caso de la necesidad de implementar nuevas técnicas y/o tecnologías este debe poseer la capacidad de soportarlas. Además de ser escalable, la plataforma debe ser lo suficientemente flexible para mantenerse al día con los protocolos, tecnologías o características que cambian rápidamente.

**3.- El modelo de precios y negocio:** diversas plataformas ofrecen pruebas de concepto gratuitas por un periodo de tiempo establecido o cuentas limitadas para llevar a cabo proyectos pequeños, sin embargo, los proveedores de una plataforma son explícitos en sus precios, algunos mostraran una tarifa previa y luego aumentara significativamente cuando se establezca un contrato.

El proceso de compatibilidad consiste en poner a prueba el hardware, desarrollando un código de prueba tal y como se muestra en la figura 3.4 con el fin de darle la capacidad de alimentar al dispositivo a través de los sensores previamente instalados, para que la comunicación se vuelva efectiva; la plataforma a seleccionar provee los servicios necesarios para realizar el diseño acorde a los espacios que se pretenden monitorear y/o

controlar, gestionar los datos haciendo uso de bases de datos, visualizarlos a través de graficas en el tiempo y generar alertas.

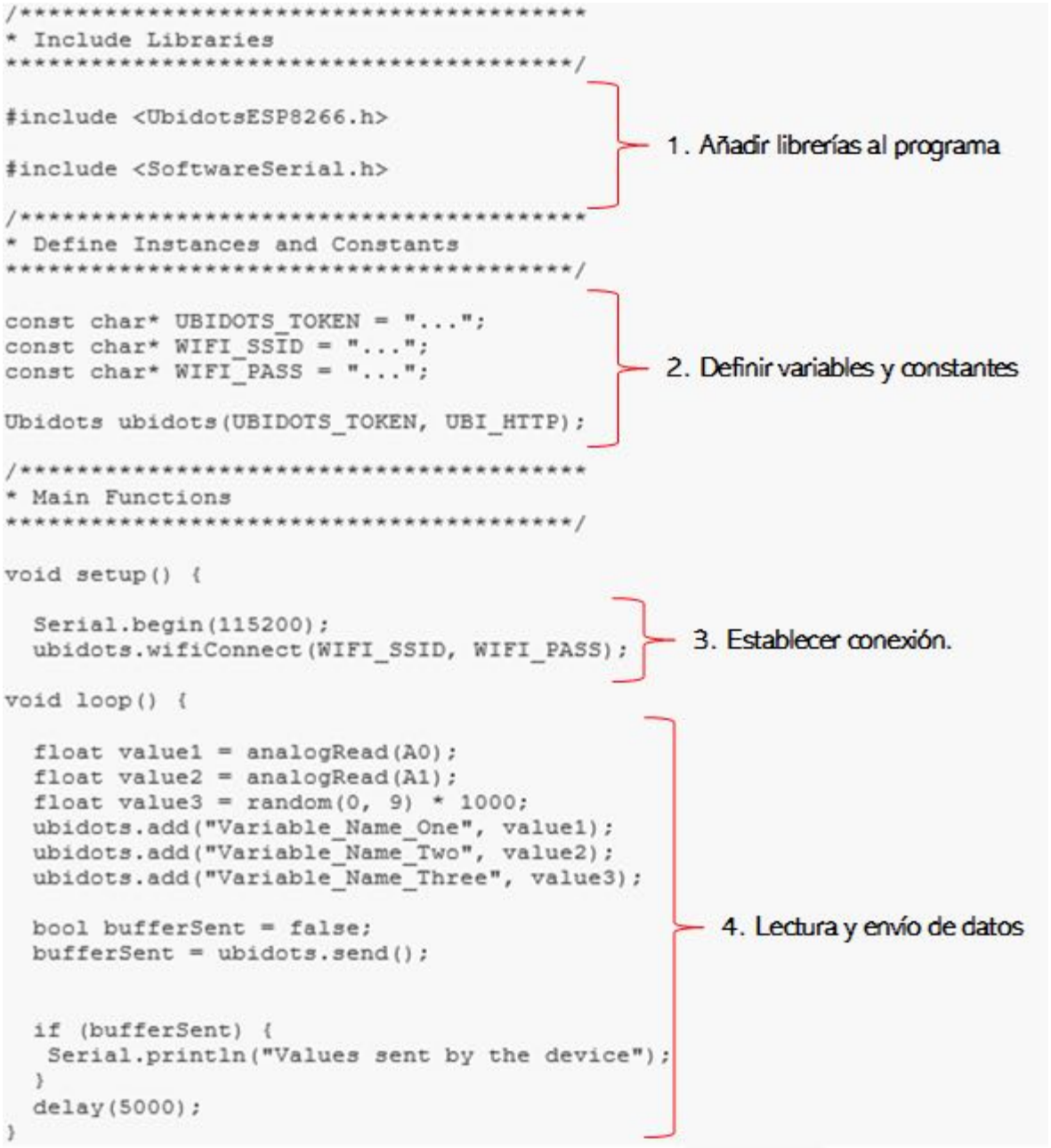


***Figura 3.4*** *Código de prueba de dispositivo ciber-físico (Elaboración propia).*

Para ser más explícitos, el código mostrado en la figura 3.4 puede descomponerse en 4 etapas, inicialmente es necesario añadir las librerías que permitan al dispositivo comprender el lenguaje en el que trabaja la plataforma IoT, posteriormente se definen las variables y constantes que permiten establecer una conexión segura entre el dispositivo y la plataforma, la tercera etapa lleva a cabo la conexión a la red y por último, la cuarta

etapa almacena dentro de las variables la información que los sensores están capturando para posteriormente enviarla hacía la plataforma IoT.

**UBIDOTS**

El propósito de esta plataforma consiste en hacer del producto físico, un producto virtual, tal como se muestra en la figura 3.5 el dispositivo ciber-físico se encuentra disponible en la plataforma, y es así que los sensores son capaces de capturar y transmitir datos acerca de ese producto sobre una red. El sistema entonces analiza los datos y, con base en ese análisis, actúa.

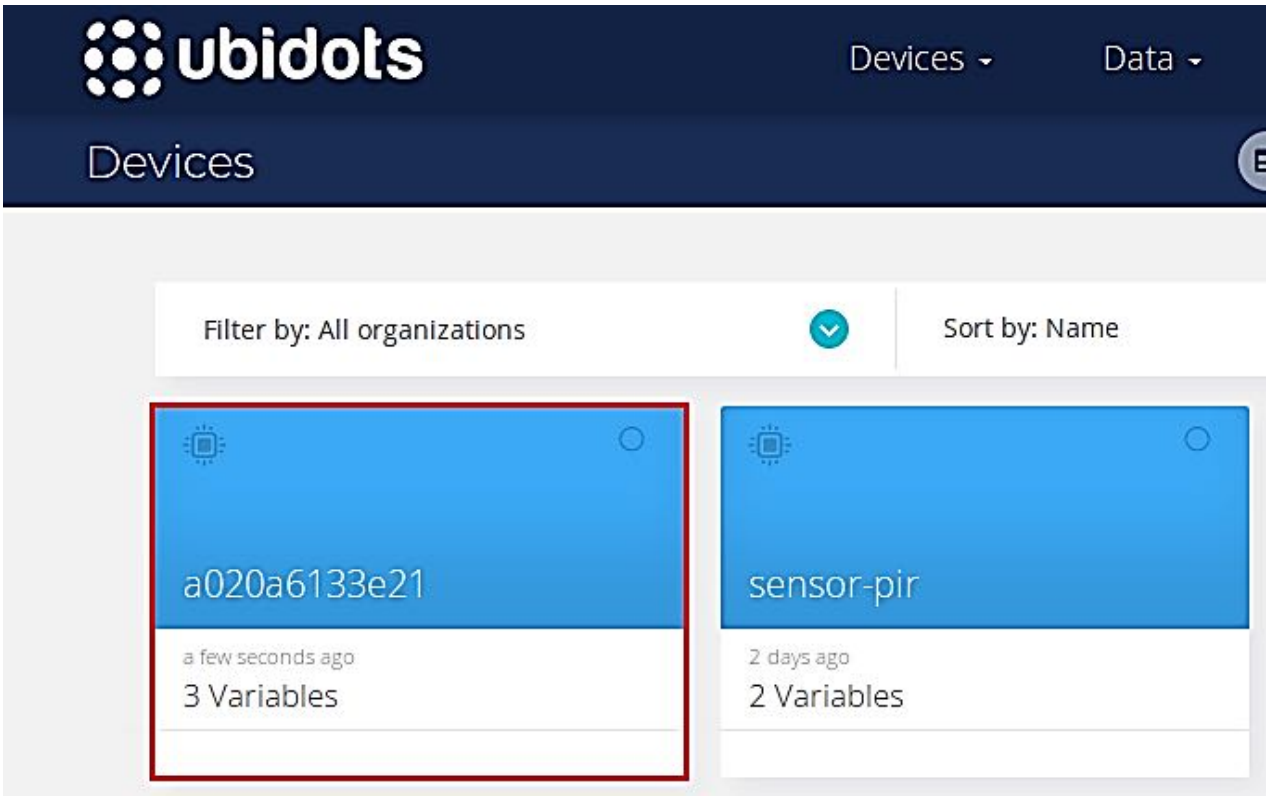


***Figura 3.5*** *Dispositivos ciber-físicos alojados en la plataforma IoT (Elaboración propia).*

Por otra parte, durante esta etapa en ocasiones es necesario realizar ajustes en el sistema, mismos que surgen una vez que se llevó a cabo la implementación, porque el ajuste a considerar parte de la evaluación de la información que entregan los dispositivos ciber-físicos para alimentar la base de datos del sistema, si al evaluar la información se manifiesta un falso negativo o un falso positivo es necesario realizar ajustes en la

codificación del sistema con el fin de ajustar los datos que son captados por el sensor y desplegar de forma más precisa la información en el panel de control.

## 3.4 Asegurar la comunicación entre dispositivos

Es importante considerar que el producto debe actuar de manera autónoma además de crear y consumir información, esto permitirá una mayor eficiencia en el sistema a la hora de toma de decisiones en conjunto, además, es necesario crear una interfaz amigable para el usuario con la simplicidad de uso, incluso mientras se encuentra en el proceso de elaboración de un objeto inteligente, el diseñador debe mantener contacto con el cliente, su conjunto mental y el uso que se le dará al producto.

Para llevar a cabo lo planteado se debe hacer uso de las prestaciones que previamente ofrece la plataforma seleccionada, es por eso por lo que es necesario seleccionar una plataforma que permita el diseño y el desarrollo en un entorno seguro, ofreciendo protección a los datos y un protocolo de respuesta en caso de desconexión.

Cada dispositivo ciber-físico debe ser programado haciendo uso de los certificados de seguridad que la plataforma ofrece tal como se muestra en la figura 3.6 y además crear en el código la funcionalidad de operación autónoma si se presenta una pérdida de comunicación, además de crear alertas en caso de que ocurra para notificar al usuario.

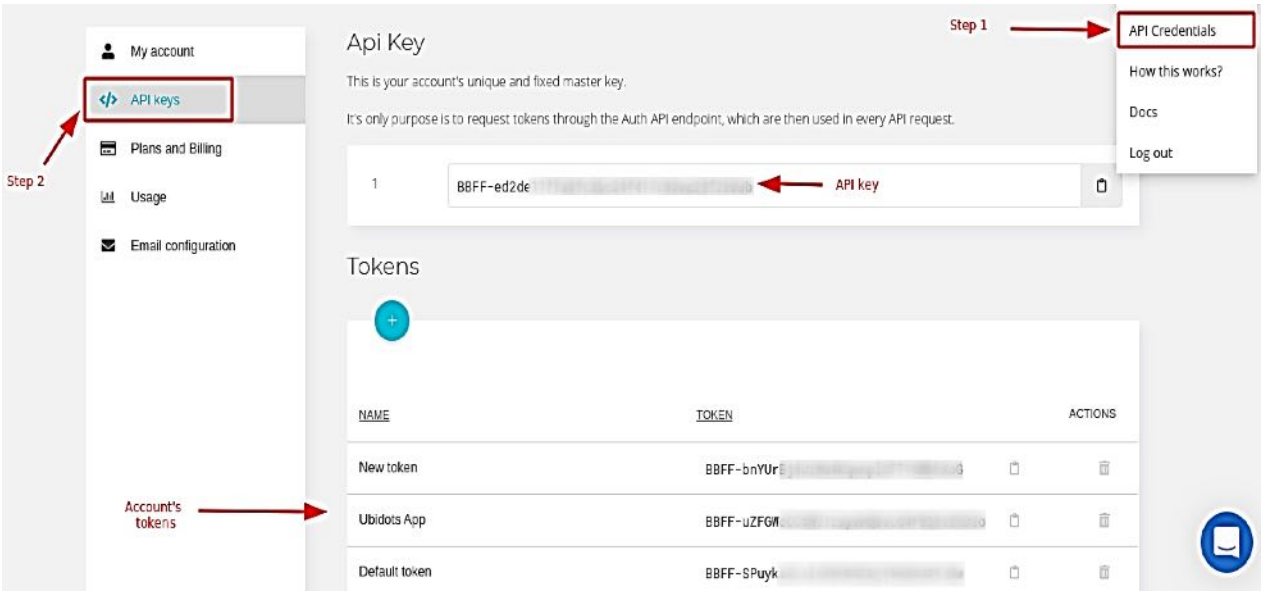


***Figura 3.6*** *Generar tokens de seguridad para dispositivos ciber-físicos. (Elaboración propia).*

En el caso de utilización del protocolo MQTT que ofrecen las múltiples plataformas IoT se hace uso de la seguridad SSL/TLS para la transportación de los datos, por otro lado, se hace uso de un certificado de autenticación en cada dispositivo que debe ser instalado tal como se muestra en la figura 3.7 para asegurar la conexión y evitar cualquier acceso no autorizado.

```
/****************************************
* Include Libraries
****************************************/

#include <UbidotsESP8266.h>

#include <SoftwareSerial.h>

/****************************************
* Define Instances and Constants
****************************************/

const char* UBIDOTS_TOKEN = "...";  // Put here your Ubidots TOKEN
const char* WIFI_SSID = "...";      // Put here your Wi-Fi SSID
const char* WIFI_PASS = "...";      // Put here your Wi-Fi password

Ubidots ubidots(UBIDOTS_TOKEN, UBI_MQTT);
```

***Figura 3.7*** *Instalar tokens de seguridad en dispositivos ciber-físicos (Elaboración propia).*

Es necesario prepararse para las consecuencias del malfuncionamiento y la pérdida de conectividad cuando un producto está conectado y se espera que siempre esté así, también, hay que tomar en cuenta no solo el objeto en sí, si no las entidades con las cuales interactúa, sus múltiples dimensiones y sus componentes. No se debe tratar por separado cada componente ni descomponer el proceso de diseño, más bien, debe tomarse en cuenta las implicaciones de seguridad, las interacciones e incluso las implicaciones legales como parte del todo más grande.

## 3.5 Implementación

Para implementar un servicio de esta índole es necesario tener establecidos los siguientes aspectos antes de realizar el ajuste:

1. El análisis reveló cada uno de los espacios, entornos, dispositivos, objetos, procesos a automatizar.

2. El proceso de selección de técnicas y/o tecnologías permitió seleccionar aquel hardware capaz de satisfacer las necesidades planteadas por el análisis, además de seleccionar el protocolo de comunicación conveniente para el tráfico de datos.
3. Se desarrolló el sistema acorde a cada uno de los dispositivos ciber-físicos instalados en la edificación.
4. Se aseguró la comunicación haciendo uso de los certificados del desarrollador de la plataforma.

La implementación del servicio consiste en la configuración de cada dispositivo instalado para conectarse de manera segura a la plataforma, esto se logra programando cada uno de los dispositivos para permitir el tráfico de datos que proporcionan los sensores instalados o enviar aquellos pulsos necesarios para manipular un actuador, estos datos son recibidos y procesados por el microcontrolador, PLC, PC, tarjeta de adquisición de datos, entre otros; para posteriormente tomar una decisión: Actuar de manera local o enviar la información a la plataforma en la nube.

La plataforma por su parte debe ser configurada de tal forma que solo se permita el acceso a aquellos dispositivos que posean el certificado del fabricante, por otro lado, es necesario realizar un segundo paso de seguridad, autorizando el acceso del dispositivo mediante el uso de la dirección física de este.

Una vez configurados los dispositivos, se ejecuta la prueba de conexión en cada uno de ellos, enviando los datos correspondientes directamente hacía la base de datos que almacena el estado actual de cada uno de ellos, una vez almacenada la información, el diseño del sistema tiene que ser interactivo y permitir que el usuario pueda manipularlo y visualizar la información que se encuentra almacenada en la base de datos; por último, el sistema se configura de tal manera que al recibir cierto tipo de información pueda generar alertas al usuario para que este pueda interactuar a la distancia y conocer el estado actual de los sensores en caso de que se genere alguna emergencia.

## 3.6 Evaluación

La evaluación se lleva a cabo monitoreando a través de la plataforma cada uno de los espacios de la edificación o proceso, cotejando que los datos que se presentan en la plataforma sean los datos esperados o reales, que la información llegue en tiempo real o tiempos convenientes para que el usuario pueda crear algún plan de acción en caso de ser necesario, esta etapa tiene la finalidad de detectar los falsos positivos o falsos negativos que pudiesen estar causando inestabilidad en el sistema, o saturando de información inservible la base de datos, puesto que esto puede alterar el proceso y poner en riesgo la integridad de la edificación.

## 3.7 Ajuste

El ajuste del sistema se lleva a cabo una vez identificados aquellos dispositivos que envían falsos positivos o falsos negativos al sistema, posteriormente se realiza la medición adecuada en cada uno de los sensores que captan el espacio de la edificación y se realiza el ajuste hasta corroborar que el sensor se encuentra calibrado y enviando la información acorde a la calibración efectuada en el dispositivo ciber-físico, una vez que el dispositivo ciber-físico recibe la información y la procesa de manera esperada para enviarla a la plataforma, se analiza el dato que recibe la base de datos y se procesa dentro de la plataforma para que pueda ser mostrado de manera correcta en el panel de control.

Es importante mencionar que dentro del esquema mostrado anteriormente en la figura 3.1 de la metodología propuesta, el ajuste retroalimenta hacía la etapa 3 de la metodología o diseño del sistema, debido a que el sistema recibe la información que los dispositivos ciber-físicos se encuentran capturando, y este la procesa con el fin de mostrar información precisa dentro del panel de control, por lo tanto, en caso de ser necesario un ajuste en los dispositivos por alguna causa, tales como un falso positivo o falso negativo, el sistema requiere de un rediseño en la etapa que procesa la información recibida para afinar la información que será desplegada en el panel de control.

Para cerrar este capítulo podemos destacar que al implementar esta metodología propuesta nos permite obtener en resultado un sistema capaz de manipular y controlar de

forma remota los dispositivos ciber-físicos instalados en una edificación, la cual, al poseer este tipo de infraestructura tal como se mencionó en el capítulo 2 de este trabajo, puede ser denominada como “edificación inteligente”, debido a que cumple con la disponibilidad para adaptarse en respuesta a las necesidades de los ocupantes, la disponibilidad para adaptarse en respuesta a las necesidades o situación de la red y disponibilidad para facilitar el mantenimiento y funcionamiento eficiente del edificio en forma automatizada y controlada.

# 4. IMPLEMENTACIÓN

En este capítulo se describe la implementación del caso de seguridad ciudadana haciendo uso de una plataforma IoT que cumple con las características según el caso planteado en esta sección. En resumen, se realizó un análisis de la problemática planteada por la empresa para poder desarrollar un sistema de protección ciudadana. Después se realizó la selección de los elementos de hardware para comenzar con la elaboración del sistema nodo.

## 4.1 Análisis y diagnostico

Para dar inició a la implementación del proyecto se decidió en común acuerdo con la empresa y el director de tesis aplicar la metodología en edificaciones inteligentes con un enfoque en seguridad ciudadana como caso de estudio, para tales efectos se consultaron las bases de datos correspondientes y así dar sustento a la investigación.

Actualmente en el Estado de Sonora, según (*Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública Principales Resultados Sonora*, 2019) (ENVIPE) 2019, se cometieron 50,861 delitos durante el 2018 y 39,759 delitos durante el 2017, representando una variación del 27.9%, asociados a 31,853 víctimas para el 2018 y 31,184 víctimas para el 2017, por cada 100,000 habitantes, de los cuales, según el propósito de este artículo, el 13% de la cifra para el 2018 representa el robo a casa habitación, el cual, toma el cuarto lugar en la lista de delitos del estado.

En base a los reportes estadísticos que proporciona la ENVIPE se puede inferir que los programas de seguridad actualmente no son los suficientemente efectivos, debido a que se encontró un aumento gradual en los delitos del estado con un margen del 27.9% y una monitorización prácticamente nula debido a que el 88.1% de los delitos no se denuncian por pérdida de tiempo o desconfianza en la autoridad, esto ha provocado que algunas ciudades opten por implementar un programa social llamado “vecinos vigilando”, el cual consiste en la organización de los habitantes de la zona con el fin de mantener la vigilancia activa durante las 24 horas del día los 365 días del año. Sin embargo, estos programas

sociales no suelen ser muy eficientes debido a que se genera un esfuerzo bastante grande al añadirle la carga laboral del día y las actividades de la vida cotidiana.

Por lo anterior, en este caso de estudio se adopta el concepto de hogar inteligente Kesavan, Sanjeevi and Viswanathan (2016), con el fin de dotar de capacidades del Internet de las Cosas a un vecindario completo y mantener activa la vigilancia las 24 horas del día los 365 días del año, además de ser una propuesta efectiva para alimentar en forma automática la base de datos del “Mapa Interactivo Hermosillo Seguro”. Al-Ali et al. (2017), Escobar and Salinas (2016) muestran que el concepto de hogar inteligente no solo brinda la capacidad de elevar la seguridad para prevenir robos, además, brindaría la capacidad de generar informes respecto al consumo de agua y energía eléctrica, monitorear los signos vitales de habitantes con algún tipo de enfermedad, generar alertas en caso de incendios, etc. Toda esta información sería enviada a una serie de microcontroladores instalados en el hogar, que recibirían los datos de los sensores para organizar, clasificar y presentar información relevante en una interfaz humano-maquina con capacidades del IoT; capaz de monitorear y controlar actuadores del hogar para incrementar la seguridad o responder adecuadamente a un potencial de intento de robo.

## 4.2 Definición de técnicas y/o tecnologías.

Una vez definida la arquitectura y las características del hogar inteligente podemos definir el concepto de red social de hogares. La idea principal de este concepto radica en dotar de las aplicaciones previamente definidas cada uno de los hogares de una vecindad, con el fin de establecer comunicación entre ellos tal y como se muestra en la Figura 4.1.

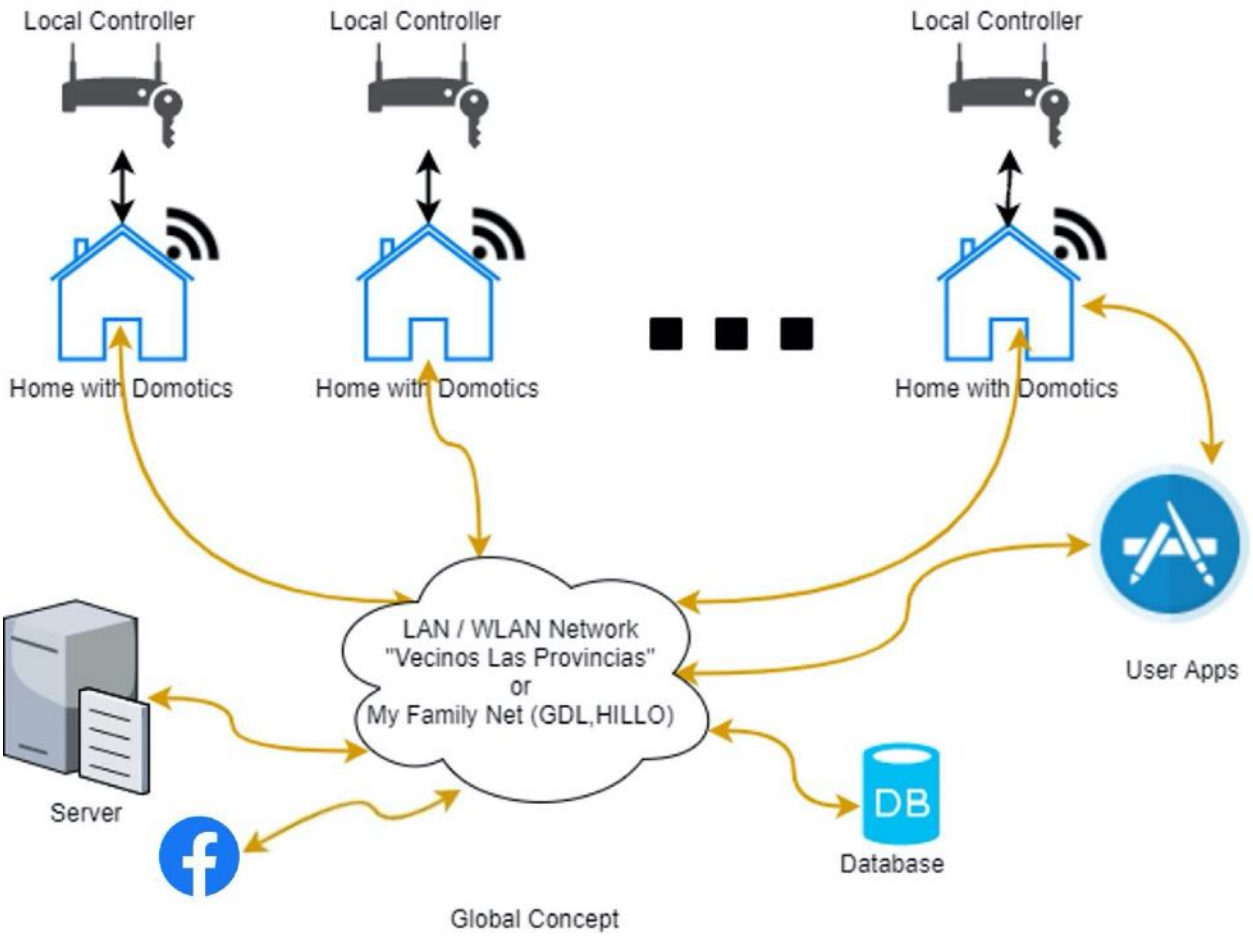


***Figura 4.1*** *Concepto global de la red social de hogares. (Elaboración Propia).*

Al establecer comunicación entre los hogares a través de una plataforma IoT, es posible generar distintos tipos de alerta según sea la situación que se presente, y con ello, establecer protocolos de seguridad entre los vecinos que permitan un nivel de respuesta inmediata ante la inminencia de una situación de riesgo para el hogar. Por otro lado, cada uno de los hogares tendrá un identificador y una cuenta de enlace a una de las redes sociales más utilizadas en el mundo, “Facebook”, en la cual, a través de una página exclusiva para los hogares del vecindario alojada en esta red social, publicarán la información actual de cada uno los sensores del hogar. Este concepto brinda al usuario la posibilidad de permitir o no, el monitoreo de los espacios de su vivienda a la comunidad que cuente con acceso a la plataforma, lo cual facilita la respuesta entre los usuarios con el fin de prevenir incidencias en el hogar y resguardar la integridad de este.

## 4.2.1 Descripción de la arquitectura de las técnicas y/o tecnologías a utilizar

A continuación, se presenta la arquitectura del hardware instalado en cada hogar inteligente como se muestra en la figura 4.2

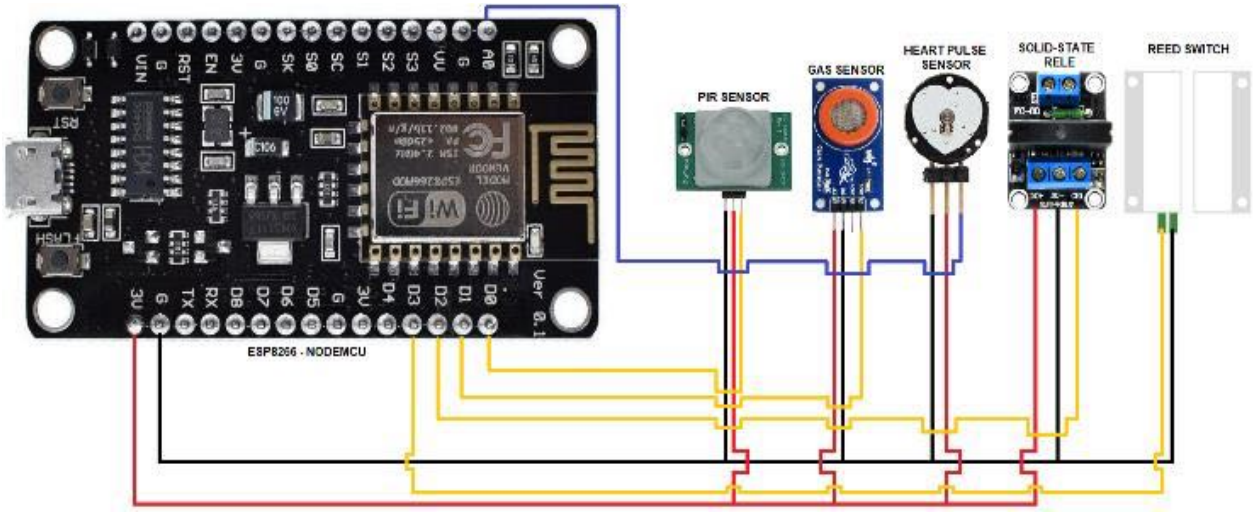


***Figura 4.2*** *Arquitectura del hardware del hogar inteligente. (Elaboración propia).*

### *A. ESP8266-12*

El ESP8266-12 consta de un microcontrolador Tensilica (32 bits) e interfaces de periféricos digitales y ADC de 10 bits. Es compatible con WiFi de 2,4 GHz (802.11 b / g / n). Tiene 16 interfaces GPIO, Inter-Integrated Circuit (I2C), SPI, I2S y UART. La placa de desarrollo ESP8266, un sistema en chip (SoC) obtiene acceso a la red WiFi con pila de protocolo TCP / IP integrada.

### *B. SENSOR PIR HC-SR501*

El sensor PIR (movimiento infrarrojo pasivo) es un sensor electrónico que funciona con radiación IR. El sensor emite y crea una región de campo de rayos infrarrojos. Dado que los rayos son infrarrojos, los humanos no pueden verlos a simple vista. Cuando un humano pasa por este campo, emite su propia firma de calor que produce un cambio en el campo del sensor PIR, por lo que el sensor detecta un organismo vivo.

### *C. SENSOR DE RITMO CARDIACO (PLSNSR1)*

Este tipo de sensor se utiliza comúnmente para encontrar la frecuencia cardiaca a través de un microcontrolador que permita interpretar la señal y traducirla a pulsos por minuto. Este sensor opera correctamente en conjunto a ESP8266-12 y permite enviar la información recabada a un servidor en la nube y puede ser aplicable para que los médicos puedan adquirir esta información en tiempo real y evaluarla fácilmente.

### *D. RELEVADOR DE ESTADO SOLIDO*

Este relevador a diferencia de los relevadores electromecánicos utiliza un acoplamiento óptico y es empleado en este tipo de proyectos para encender o apagar los aparatos cuando se aplica un pequeño voltaje en sus terminales de control. Se utiliza una señal de corriente o tensión como señal de control para activar el led que ilumina y activa un diodo fotosensible, y así, posteriormente activar un tiristor, SCR o MOSFET para conmutar la carga.

### *E. SENSOR MAGNETICO*

Un sensor magnético es un elemento que consta de un par de contactos metálicos y un par de terminales que permiten acceder a los contactos contenidos en una capsula de vidrio. Los contactos se encuentran por lo general eléctricamente aislados uno del otro y cuando un campo magnético que posee la magnitud adecuada se aproxima, estos contactos tienden a cerrarse. Este tipo de sensores comúnmente se utilizan para detectar la apertura o cierre de las puertas de un hogar.

### *F. PLATFORMA UBIDOTS IOT*

Ubidots es un servidor en la nube que se utiliza para enviar datos de sensores y almacenar datos en la nube, además, es posible crear tableros que desplieguen la información recabada por los sensores, haciendo más sencilla la interpretación de los datos; este también permite el control de dispositivos a través de los widgets que ofrece, en él es posible crear una cuenta titular, la cual contiene una clave de autenticación única y una clave de token para brindar seguridad a la conexión entre los dispositivos que envían datos a la plataforma y además posee la ventaja de generar alertas hacia los dispositivos móviles registrados en caso de que el estado de una variable presente una anomalía.

***G. IFTTT***

IFTTT (If This Then That) es un servicio en una plataforma web que permite al usuario crear applets que automatizan la tarea especificada. En este proyecto, IFTTT actúa como una plataforma intermediaria que conecta al microcontrolador y facebook, haciendo uso del servicio “webhooks”, esto con el fin de publicar el estado actual de los sensores del hogar y que los usuarios de los distintos hogares puedan consultarlos en cualquier momento desde sus cuentas privadas.

## 4.3 Diseño y desarrollo del sistema

A continuación, se presenta a través de la figura 4.3 el marco propuesto para construir una red social doméstica constituida por grupos que son incorporados por hogares con la capacidad de compartir el estado de sus sensores y el clúster brinda la capacidad a las familias y vecinos de protegerse.

Cada uno de los microcontroladores instalados se programará de acuerdo con la estructura que se muestra en la Figura 4.3, este se encargará de enviar la información a la plataforma IoT e IFTTT según sea el caso.

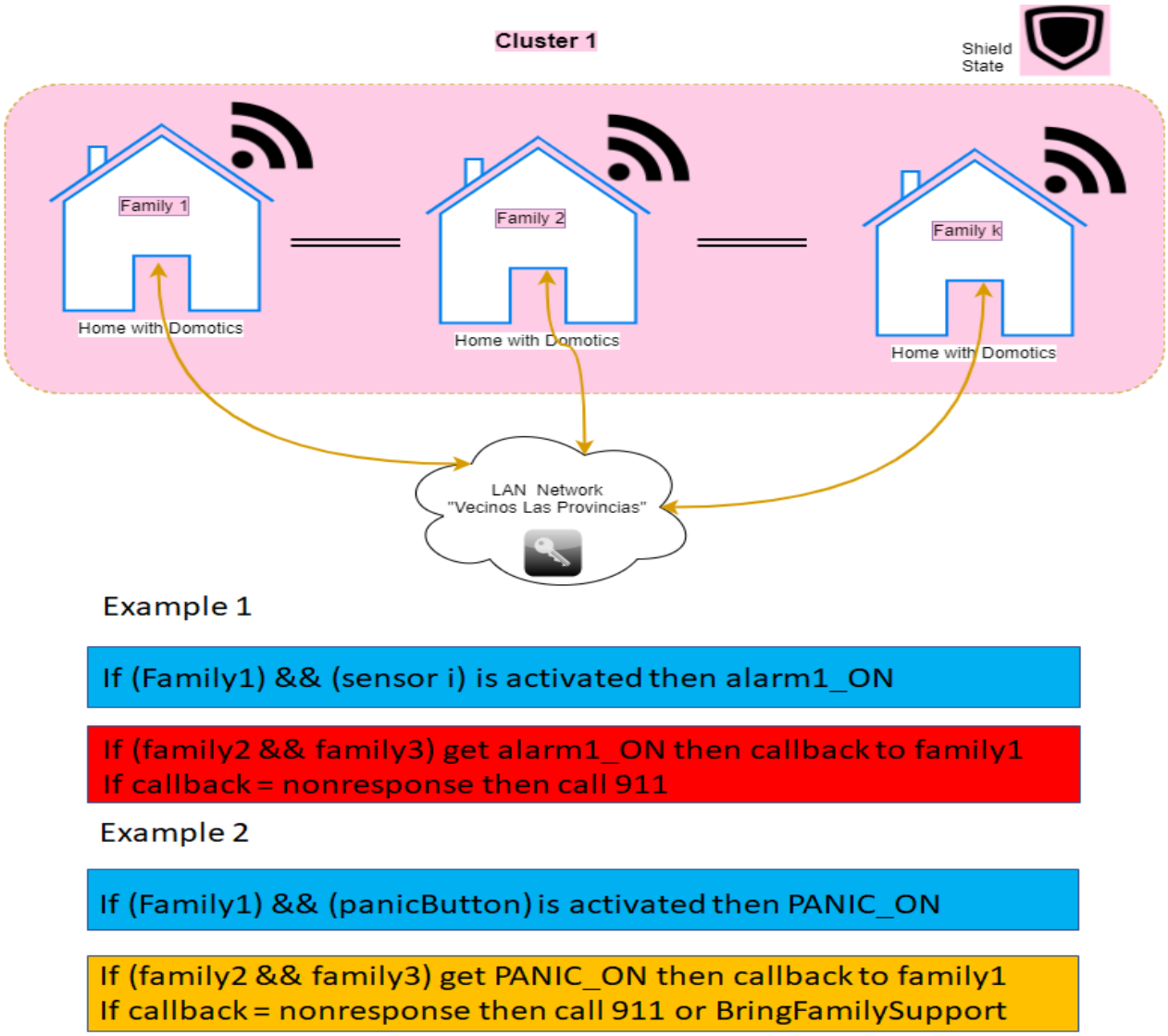


***Figura 4.3*** *Marco propuesto – Red social domestica (Elaboración propia).*

Con el fin de explicar cada una de las etapas de operación de manera clara y concisa, se lleva a cabo el modelado del sistema haciendo uso de un diagrama de actividades tal como se muestra en la figura 4.4, en el cual se pueden apreciar las cuatro etapas del funcionamiento del sistema; la primera consiste en la autenticación del usuario para acceder a la plataforma IoT, la segunda etapa consiste en representar el envío de información de los sensores al microcontrolador instalado en cada hogar, el cual procesa la información para enviarla mediante un certificado de autenticación que permite ingresar los datos a la plataforma, como tercera etapa, el acceso a las plataformas se muestra una vez que se validó la información proveniente del usuario y el microcontrolador, posteriormente, en la etapa final, el usuario puede visualizar los datos y recibir alertas.

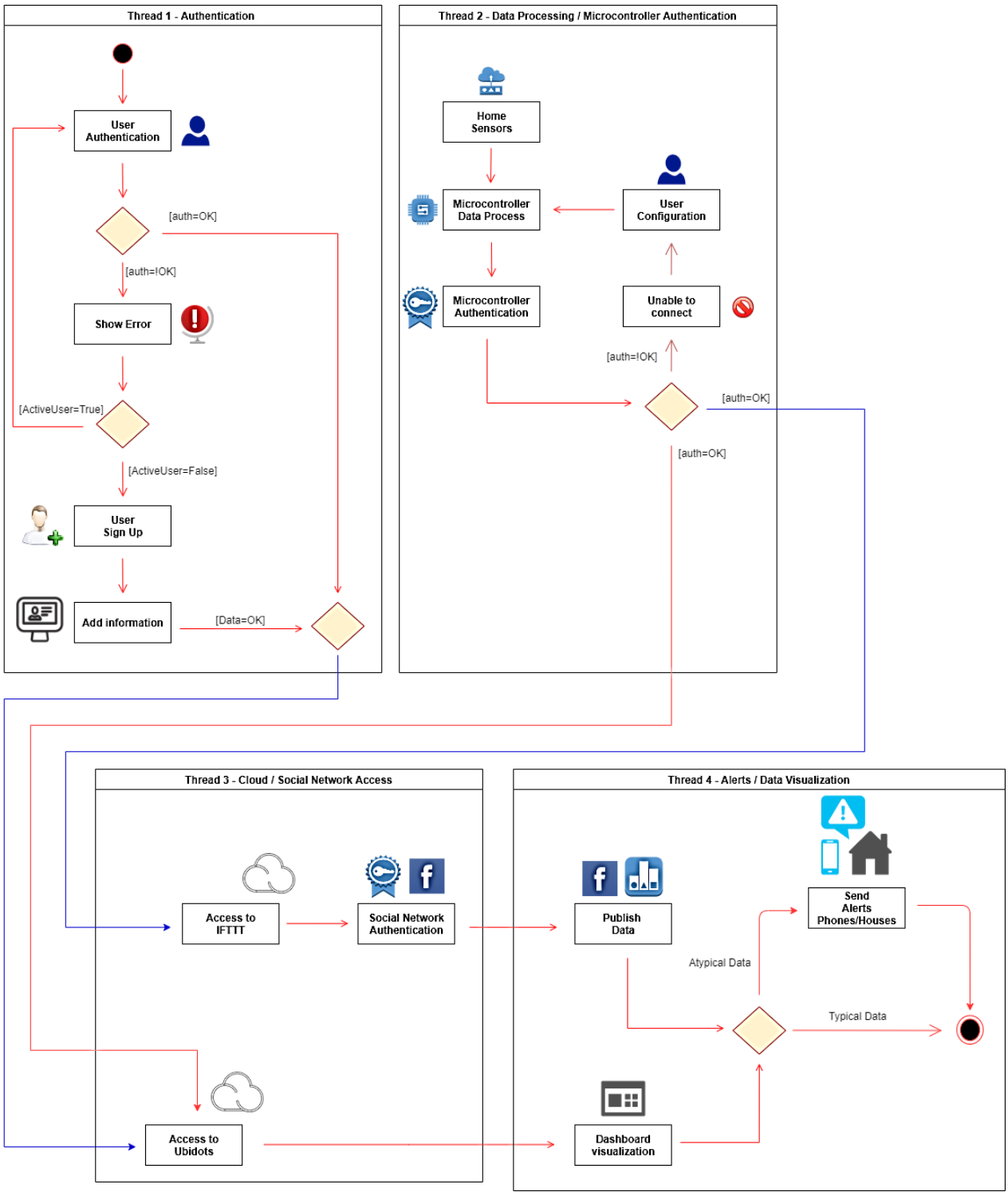


***Figura 4.4*** *Diagrama de actividades UML para sistema de red social domestica (Elaboración propia).*

## 4.4 Asegurar la comunicación

Según lo planteado en el capítulo 2 respecto a la seguridad, se menciona que existen tres aspectos a considerar en el entorno del IoT: confidencialidad, integridad y disponibilidad. García, (2021) menciona que Ubidots cuenta con 2 protocolos de encriptación de datos:

**Http con SSL:**

El uso de HTTPS implica el uso de un certificado SSL, este crea una conexión segura encriptada entre los servidores de Ubidots y los dispositivos, donde HTTPS, nos ayuda a garantizar la confidencialidad, autenticidad e integridad.

**MQTT con TLS:**

Ubidots soporta el uso del protocolo MQTT, el cual admite el cifrado TLS, este protocolo utiliza un mecanismo de enlace denominado “handshake” (o establecimiento de comunicación, en español) para crear una conexión segura entre el cliente y el servidor, una vez que este se completa, se establece una comunicación cifrada entre el cliente y el servidor.

**Autenticación basada en token:**

Otra de las prestaciones que la plataforma ofrece, la cual es implementada en cada uno de los dispositivos instalados en el hogar, es la autenticación basada en “tokens”, esta, a diferencia de la autenticación tradicional basada en servidor, asigna un token firmado después de la primera solicitud, que luego se puede usar para las siguientes peticiones puesto que este se envía en cada solicitud.

**Funcionamiento de la autenticación basada en token:**

1. El cliente solicita un token de seguridad mediante una clave de API.
2. La aplicación valida la clave API.
3. La aplicación proporciona un token firmado al cliente.
4. El cliente almacena ese token y lo envía junto con cada solicitud.
5. El servidor verifica el token y acepta solicitudes.

6. Si el Cliente no usa el token durante más de 6 horas, deberá solicitar un nuevo token con la clave API, esto debido al protocolo de seguridad que posee la plataforma IoT.

## 4.5 Caso de estudio

A continuación, las figuras 4.5 y 4.6 muestran como a través de la plataforma Ubidots es posible realizar el monitoreo y control de un hogar inteligente, en donde cada una de las familias poseen el control independiente de cada panel de control y el administrador puede asignar privilegios a los usuarios; por ejemplo, acceder al área de monitoreo de los espacios de otra familia si es necesario.

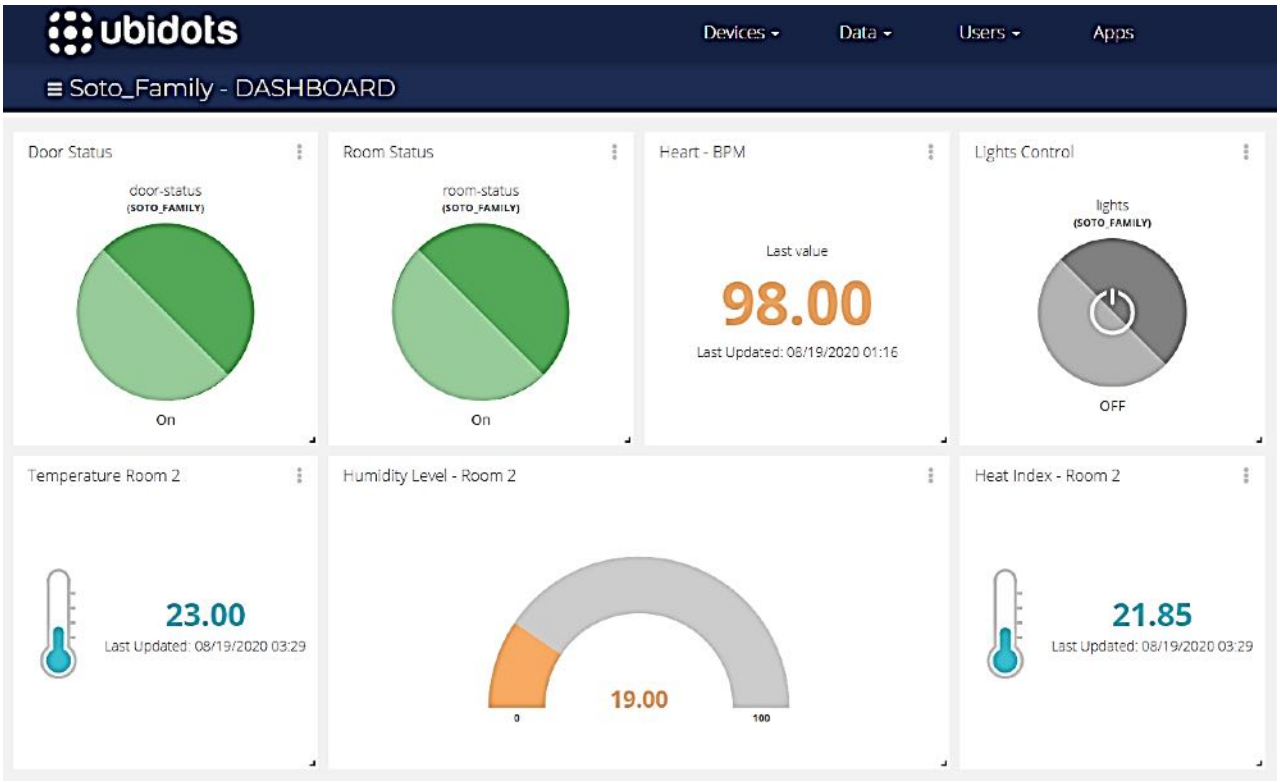


***Figura 4.5*** *Panel de control Familia 1 (Elaboración propia).*

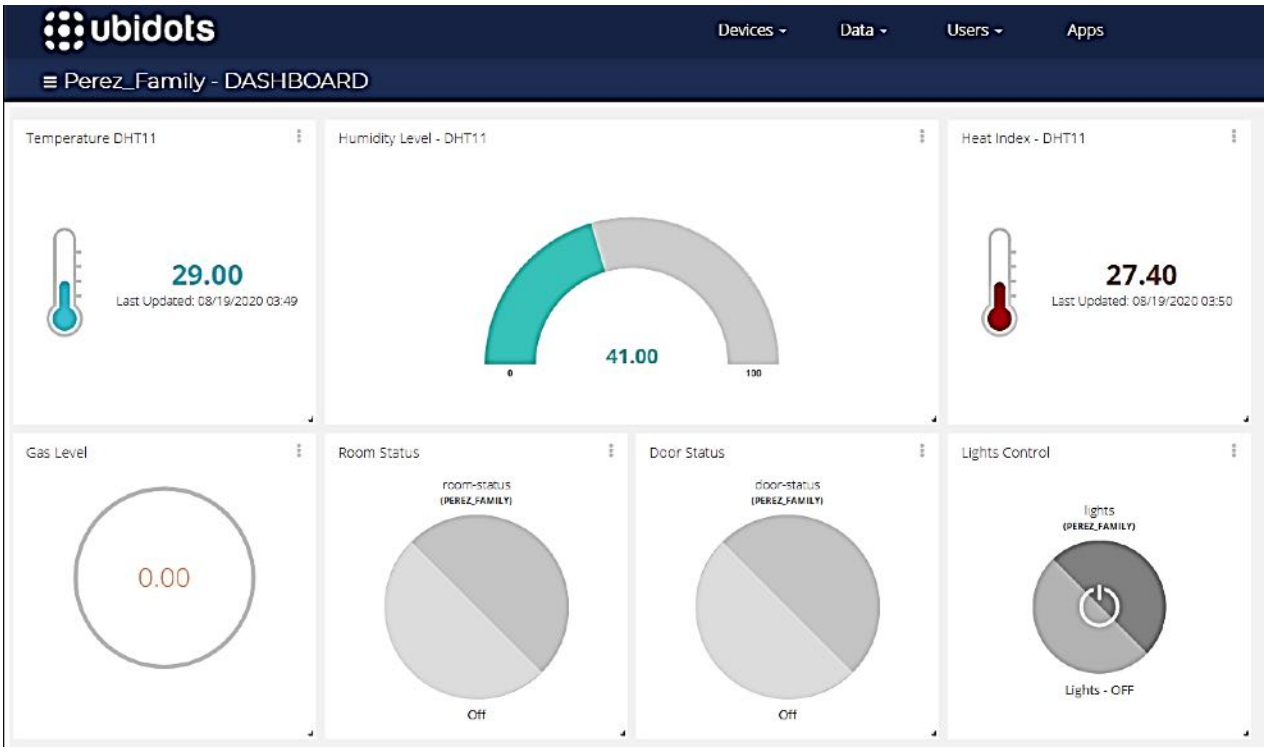


***Figura 4.6*** *Panel de control Familia 2 (Elaboración propia).*

Cada uno de los eventos permite que una solicitud Http transporte los valores del sensor a la red social, realizando una publicación en una página, como se muestra en la Figura 4.7.

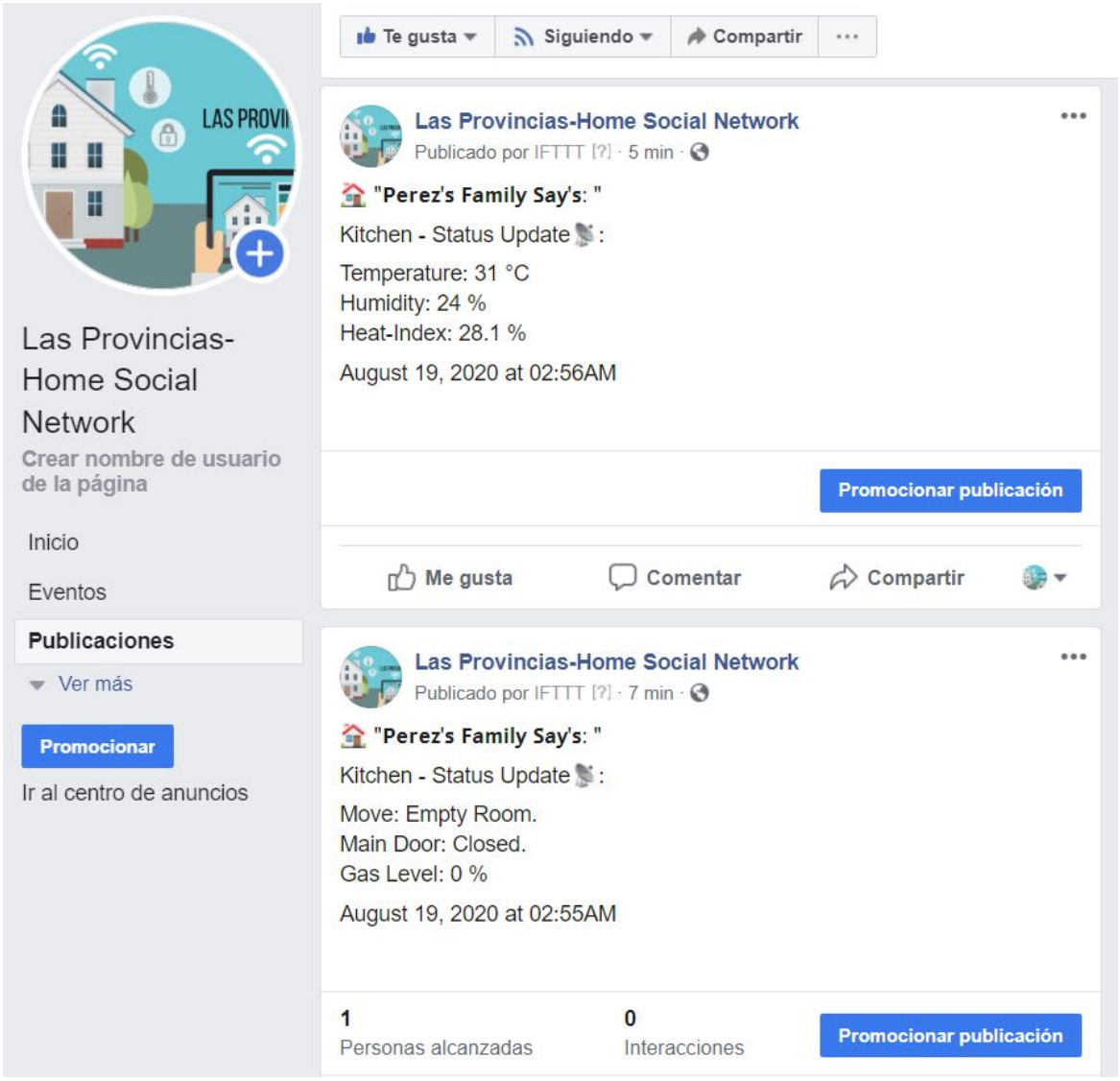


***Figura 4.7*** *Pagina en Facebook: "Las provincias – Red de Hogares inteligentes" (Elaboración propia).*

Cada uno de los hogares publica información actualizada en una página no pública en Facebook, la cual es administrada por un "Super usuario" que otorga privilegios a cada uno de los representantes del hogar para consultar la información que se publica.

Por otro lado, Cuando se presenta un dato atípico durante la captura de información del sensor, se genera una alerta mayormente visible en la página de Facebook, para que los usuarios de la página puedan verla fácilmente. La Figura 4.8 muestra una publicación creada por el servicio IFTTT, que contiene la información actual de los sensores y una instrucción de acción, para que los usuarios puedan tomar una respuesta para verificar el problema.


***Figura 4.8*** *Publicación por alerta de sensor (Elaboración propia).*

## 4.6 Evaluación

Con el fin de realizar una evaluación para comprobar que los datos que se muestran en la página de Facebook son correctos, la plataforma cuenta con una base de datos donde almacena un historial de cada una de las variables asignadas a los microcontroladores que se instalan en el hogar, la figura 4.9 muestra el menú que ofrece la plataforma para acceder a cada una de estas variables. En este menú es posible visualizar los datos que transmiten en tiempo real cada uno de los sensores instalados en los dispositivos ciber-físicos, posteriormente, a cada uno de estos datos se le asigna una variable que será la encargada de almacenar y crear el historial de la información recabada durante el

funcionamiento activo del dispositivo. Por lo tanto, este menú brinda la posibilidad de evaluar que los datos que el microcontrolador está recibiendo son iguales a los datos que está capturando la variable.

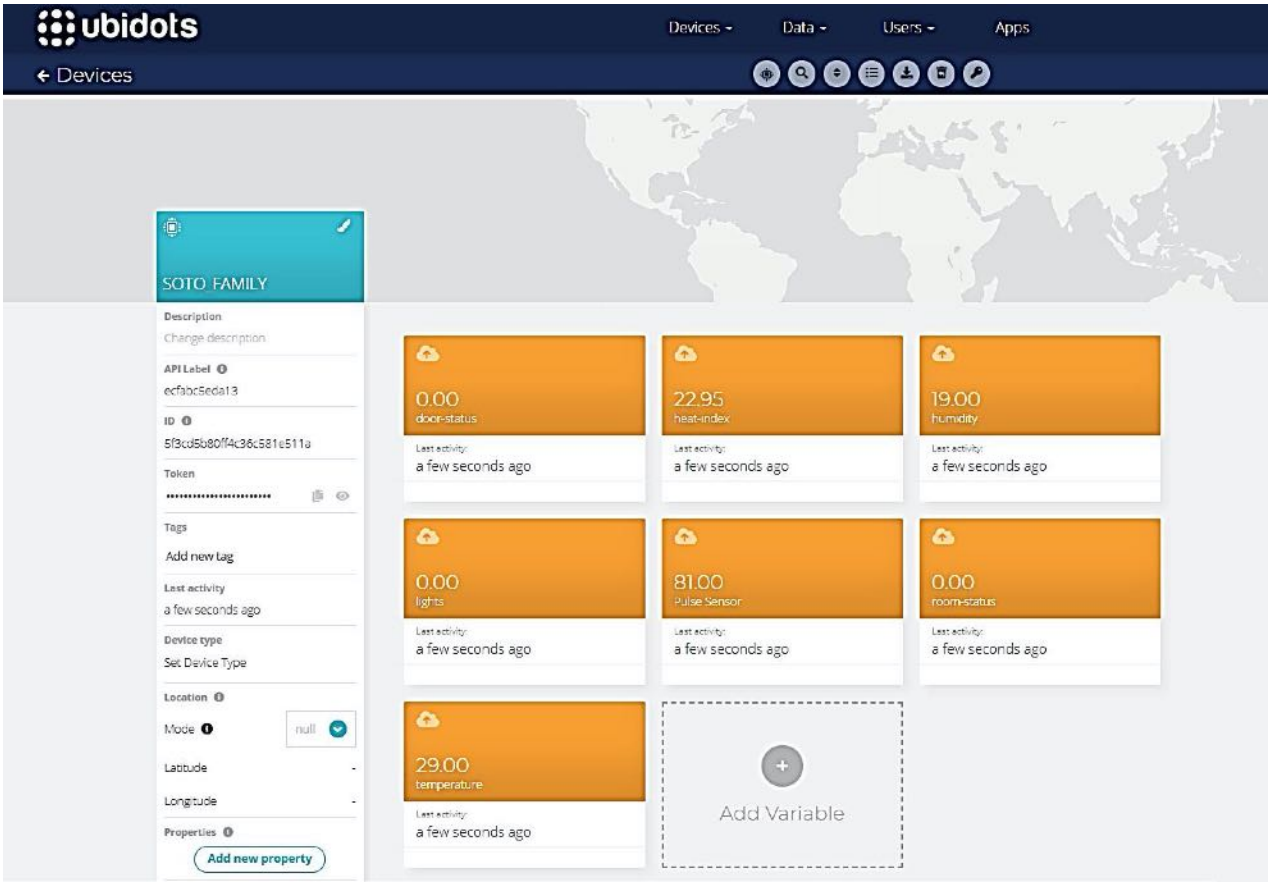


***Figura 4.9*** *Menú de variables de la familia 1 (Elaboración propia).*

## 4.7 Ajuste

En caso de ser necesario, según los resultados obtenidos en la etapa de evaluación, es posible llevar a cabo una introspección en aquella variable que estuviese mostrando algún dato atípico, para realizar esta acción nos introducimos a la variable, en donde la Figura 4.10 muestra el gráfico del comportamiento del sensor ubicado en una de las habitaciones de la vivienda, que puede ser monitoreado por el administrador del sistema.

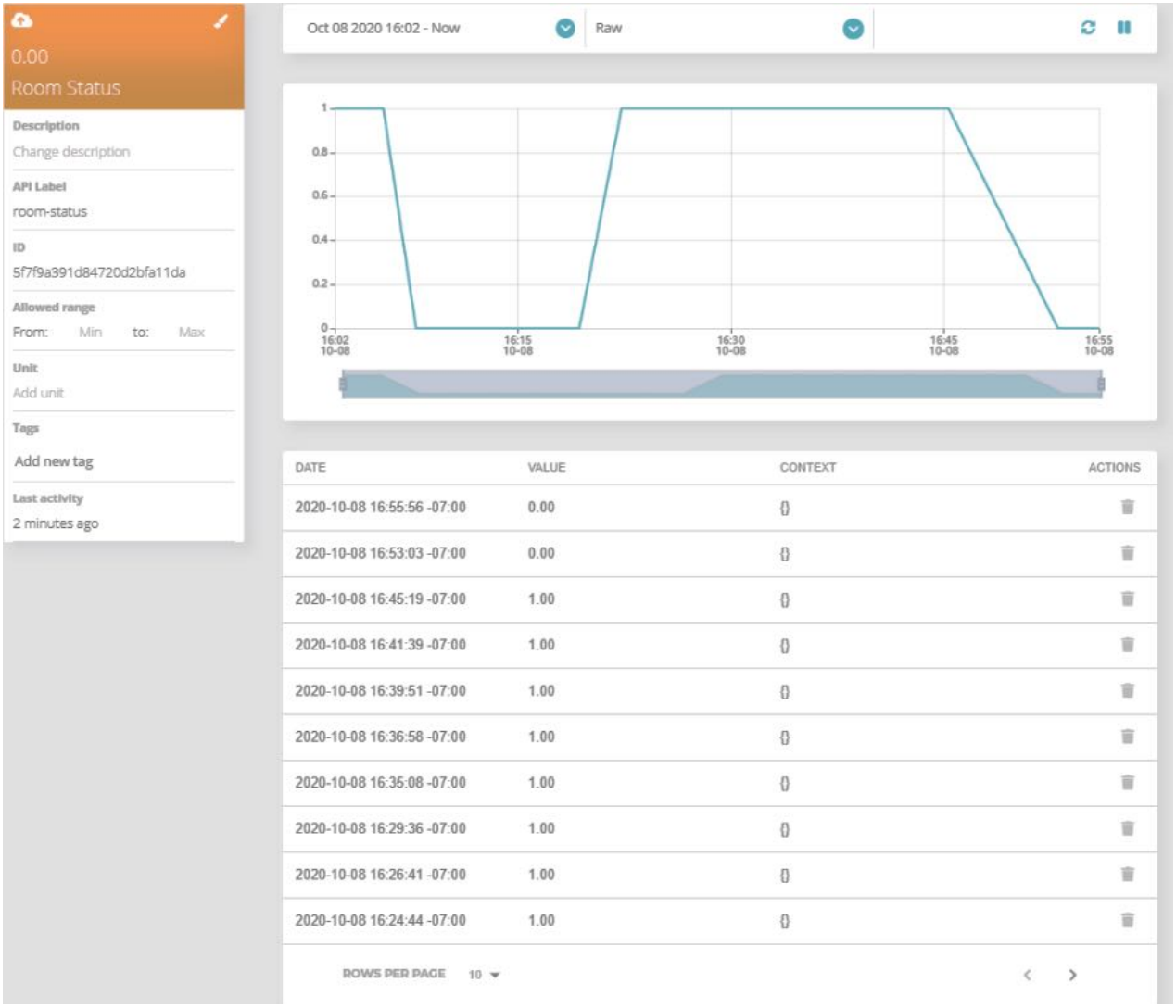


***Figura 4.10*** *Estado del sensor de la habitación (Elaboración propia).*

Para el sensor inspeccionado, en la figura 4.10 se muestra el análisis del estado lógico del sensor, es decir, este envía una señal de “unos” y “ceros”, los cuales el sistema interpretará en el panel de control mostrado anteriormente en la figura 4.5 como el estado actual de la habitación a través de un indicador luminoso que se enciende al recibir el valor “uno” (que se interpreta como una habitación ocupada) y se apaga al recibir el valor “cero” (que se interpreta como una habitación vacía).

A continuación, la figura 4.11 muestra la configuración actual del microcontrolador que captura la información del sensor, el cual se encuentra programado para acondicionar la señal recibida e interpretarla como “unos” y “ceros”


***Figura 4.11*** *Programación del dispositivo ciber-físico para el envío de datos (Elaboración propia).*

En caso de ser necesario, el ajuste se iniciaría en el dispositivo ciber-físico en la etapa de acondicionamiento del sensor hasta ajustar la señal y tener el dato listo para enviarlo a la plataforma. Es por dicha razón que la retroalimentación planteada en el esquema de la metodología se dirige hacia la etapa tres. Una vez que el ajuste en el dispositivo se llevó a cabo, se procede a realizar los ajustes necesarios en el sistema, para ello, el sistema cuenta con un menú de edición en cada uno de los componentes del panel de control como se muestra en la figura 4.12.

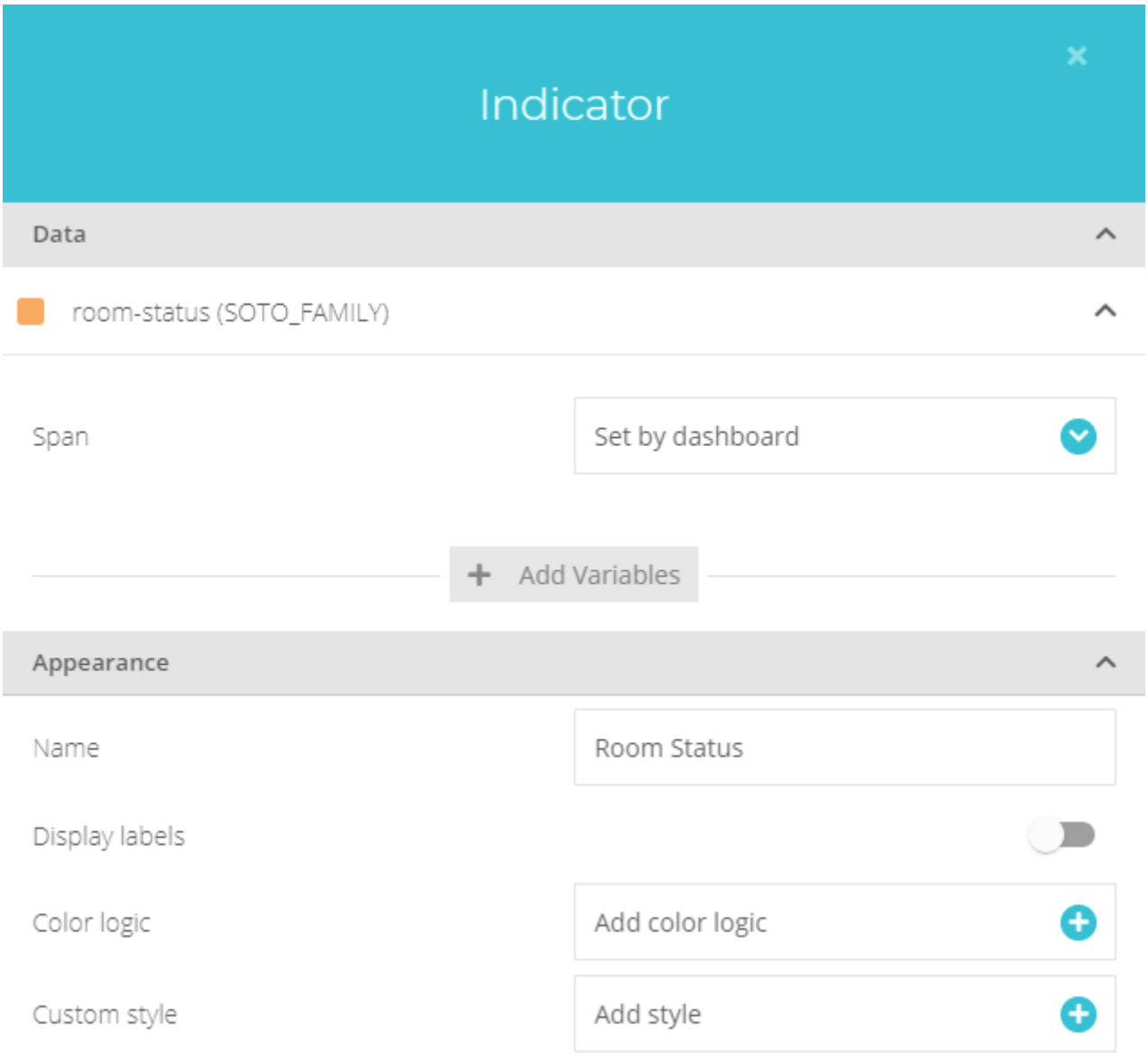


***Figura 4.12*** *Menú de edición de componente del panel de control (Elaboración propia).*

El menú mostrado en la figura 4.12 brinda al administrador la oportunidad de modificar la apariencia del componente, pero además, permite asignarle el rango de valores que va a recibir desde la variable que se le asignó al sensor y llevar a cabo una acción en base a los valores que recibe. Cómo parte final del ajuste dicho ejemplo se muestra en la figura 4.13 a continuación.

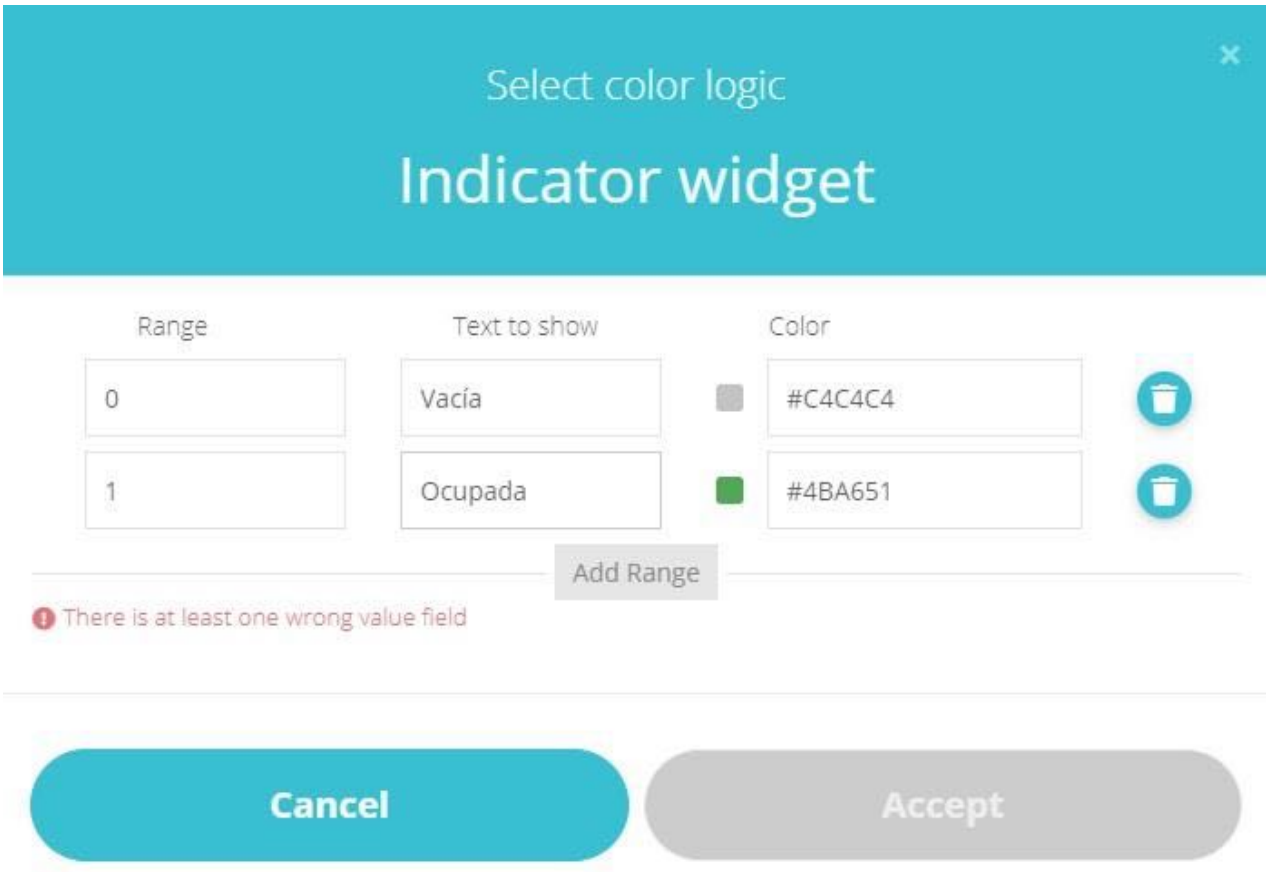


***Figura 4.13*** *Menú de ajuste de rango en componente del panel de control (Elaboración propia).*

Por último, solo basta con realizar modificaciones al rango de los valores en los que estará trabajando el sensor para llevar a cabo una acción. En el caso mostrado en la figura 4.13 al recibir el valor “cero” mostrará el texto “Vacía” y mantendrá al indicador luminoso en color gris y al recibir el valor “uno” mostrará el texto “Ocupada” y mantendrá el indicador luminoso en color verde hasta recibir de nueva cuenta el valor “cero”.

# 5. DISCUSIÓN, CONCLUSIONES Y TRABAJO FUTURO

A continuación, se presenta una breve discusión de las implicaciones del trabajo desarrollado, en el cual se describen aquellas limitaciones y/o vulnerabilidades que el sistema pudiese tener y que serán consideradas como punto de partida para trabajo futuro.

## 5.1 DISCUSIÓN.

Retomando el análisis que se llevó a cabo en la sección 2.8 de esta investigación con el fin de concluir en temas de desafíos, riesgos y seguridad en el SIoT, podemos realizar una observación en la implementación de la metodología, dado que durante esta etapa como bien se menciona en el apartado 6 de la sección 2.8, los retos reales y específicos del proyecto surgen solo después de la implementación, por lo que al hacer disponible los objetos inteligentes de una edificación aún dentro de plataformas que poseen altos niveles de seguridad en el transporte de datos surgen las vulnerabilidades como en cualquier sistema informático y aun que dichas vulnerabilidades son tratadas durante la implementación haciendo uso de los procedimientos de seguridad que denotan los desarrolladores de las plataformas que se utilizaron y las sugerencias de los estudios que se tomaron en cuenta para esta investigación es necesario llevar a cabo las distintas pruebas de ciber-seguridad que existen ante ataques cibernéticos, sin embargo, no es el objetivo de esta investigación crear protocolos de ataque al sistema para comprometer los datos y encontrar las vulnerabilidades dentro del entorno IoT.

Por otro lado, en base al análisis de los estudios y la etapa de evaluación de la investigación es posible concluir que el sistema posee un nivel de seguridad apropiado para su uso, debido a que cuenta con los certificados de seguridad estándar de los desarrolladores del hardware y plataformas, no obstante, se realizará una propuesta como trabajo futuro para crear las condiciones adecuadas y llevar a cabo un análisis en temas de ciber-seguridad.

## 5.2 CONCLUSIONES.

Se propone un nuevo enfoque para integrar hogares inteligentes a las redes sociales utilizando la tecnología que ofrece el Internet de las Cosas, debido a que este brinda a los usuarios una mayor capacidad de respuesta ante la inminencia de un delito en el hogar. Este concepto está dedicado a la monitorización y control de espacios con la ayuda de sensores (PIR, magnéticos, Gas, etc.) que se integran en el microcontrolador ESP8266-12, que envía la información a las plataformas IoT mediante comunicación WiFi.

Para ello fue necesario llevar a cabo el análisis y diagnóstico de los espacios en los que se realizó la implementación como parte importante del proyecto, dado que a través de esta etapa fue posible definir las técnicas y tecnologías que se emplearon para el desarrollo del sistema, donde se comprobó que haciendo uso del microcontrolador ESP8266-12 en conjunto con las plataformas Ubidots e IFTTT, nos permiten realizar un monitoreo y control efectivo, pues la información presentada en las plataformas es monitoreada en tiempo real y el usuario puede consultarlas desde cualquier parte del mundo. Por otro lado, hacer pública la información a través de una red social para los miembros de la red doméstica inteligente hace más efectiva la comunicación entre hogares y usuarios, puesto que es posible interactuar en cada una de las publicaciones efectuadas por el sistema dentro de la página de Facebook y consultar al propietario de la vivienda inteligente que envía dicha información. Por último el sistema es evaluado haciendo uso de las gráficas que proporciona la plataforma IoT con el fin de eliminar falsos positivos y/o falsos negativos y así entregar información confiable a los usuarios.

Se están realizando investigaciones en nuestro laboratorio para validar la confiabilidad del enfoque y descubrir algunos otros aspectos relevantes, como los problemas de seguridad, puesto que el caso de estudio es una validación de la metodología propuesta. En los términos planteados la metodología permitió ir del diseño a un esquema de mejora continua; paso a paso con un orden lógico, en el cual se logró implementar cada una de las etapas mencionadas y obtener provecho de la capacidad de la plataforma IoT al integrar diversas tecnologías.

Proponemos este sistema con el fin de brindar seguridad a las ciudades que tienen una alta tasa de criminalidad en el hogar, problemas de salud en el hogar, incendios, etc. implementando la tecnología que ofrece el IoT para generar una respuesta de atención a los diferentes problemas que se presenten. Este sistema aumenta el desarrollo de la tecnología en las ciudades, convirtiéndolas en comunidades inteligentes que se protegen entre sí.

## 5.3 TRABAJO FUTURO

Partiendo de la sección 2.9 de esta investigación, con el fin de enriquecer y satisfacer una de las necesidades más importantes dentro de los sistemas IoT, la ciber-seguridad, se propone crear un entorno en donde puedan ser descubiertas las vulnerabilidades que una SIoT pueda poseer, implementando las soluciones que se proponen en la sección 2.9 para mitigar y defender el panorama ciber-físico. Es a través de estas soluciones que se hará una exploración en cada una de las capas del IoT en donde se pretende crear una metodología que nos guíe en el proceso de “detección de vulnerabilidades en sistemas ciber-físicos” que pueda ser capaz de ser implementada en las redes del SIoT.

Por otro lado, la metodología propuesta en esta investigación es aplicable dentro de áreas cómo la agricultura, la industria, la medicina, entre otras, dado que la plataforma permite la integración de diversas tecnologías que actualmente se utilizan para el monitoreo y control de espacios en este tipo de áreas; según la diversidad de sujetos que abarca el IoT como se menciona en la sección 2.2, un sistema IoT brinda la posibilidad de monitorear desde un cultivo y hasta monitorear y controlar una fábrica, por lo que se pretende poner a prueba el sistema en un entorno distinto al planteado en esta investigación.

# 6. REFERENCIAS

Afzal, B. *et al.* (2019) “Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges,” *Future Generation Computer Systems*, 92, pp. 718–731. doi: 10.1016/j.future.2017.12.002.

Aguilar, L., Peralta, S. and Mauricio, D. (2020) “Technological architecture for IoT smart buildings,” (June), pp. 1–6. doi: 10.1109/icecce49384.2020.9179358.

Aheleroff, S. *et al.* (2020) “IoT-enabled smart appliances under industry 4.0: A case study,” *Advanced Engineering Informatics*, 43(May 2019), p. 101043. doi: 10.1016/j.aei.2020.101043.

Al-Ali, A. R. *et al.* (2017) “A smart home energy management system using IoT and big data analytics approach,” *IEEE Transactions on Consumer Electronics*, 63(4), pp. 426–434. doi: 10.1109/TCE.2017.015014.

Ali, M. *et al.* (2020) “An IoT based approach for efficient home automation with ThingSpeak,” *International Journal of Advanced Computer Science and Applications*, 11(6), pp. 118–124. doi: 10.14569/IJACSA.2020.0110615.

Ali, S. *et al.* (2015) “Network challenges for cyber physical systems with tiny wireless devices: A case study on reliable pipeline condition monitoring,” *Sensors (Switzerland)*, 15(4), pp. 7172–7205. doi: 10.3390/s150407172.

Atzori, L., Iera, A. and Morabito, G. (2014) “From ‘smart objects’ to ‘social objects’: The next evolutionary step of the internet of things,” *IEEE Communications Magazine*, 52(1), pp. 97–105. doi: 10.1109/MCOM.2014.6710070.

Baccarelli, E. *et al.* (2018a) “Fog of Social IoT: When the Fog Becomes Social,” *IEEE Network*, 32(4), pp. 68–80. doi: 10.1109/MNET.2018.1700031.

Baccarelli, E. *et al.* (2018b) “Fog of Social IoT: When the Fog Becomes Social,” *IEEE Network*, 32(4), pp. 68–80. doi: 10.1109/MNET.2018.1700031.

Che Soh, Z. H. *et al.* (2018) “IoT Water Consumption Monitoring Alert System,” *Proceedings - 2nd 2018 International Conference on Electrical Engineering and Informatics, ICELTICs 2018*, pp. 168–172. doi: 10.1109/ICELTICS.2018.8548930.

Che Soh, Z. H. *et al.* (2019) “Energy consumption monitoring and alert system via IoT,” *Proceedings - 2019 International Conference on Future Internet of Things and Cloud, FiCloud 2019*, pp. 265–269. doi: 10.1109/FiCloud.2019.00044.

Chin, J., Callaghan, V. and ben Allouch, S. (2019) “The Internet-of-Things: Reflections on the past, present and future from a user-centered and smart environment perspective,” *Journal of Ambient Intelligence and Smart Environments*, 11(1), pp. 45–69. doi: 10.3233/AIS-180506.

Codina, L. *et al.* (2020) “Uso de Scopus y Web of Science para investigar y evaluar en comunicación social: análisis comparativo y caracterización,” *Index Comunicacion*, 10(3), pp. 235–261. doi: 10.33732/ixc/10/03usodes.

al Dakheel, J. *et al.* (2020) “Smart buildings features and key performance indicators: A review,” *Sustainable Cities and Society*, 61, p. 102328. doi: 10.1016/j.scs.2020.102328.

Doxopoulos, P. *et al.* (2018) “Creating an extrovert robotic assistant via IoT networking devices,” *arXiv*.

Duan, K. K. and Cao, S. Y. (2020) “Emerging RFID technology in structural engineering – A review,” *Structures*, 28(October), pp. 2404–2414. doi: 10.1016/j.istruc.2020.10.036.

Ejaz, A. *et al.* (2016) “Social-Aware Resource Allocation and Optimization for D2D Communication,” *Technology*, 3(June), pp. 353–364.

Elsevier (2019) *Scopus | La mayor base de datos de bibliografía revisada por pares | Elsevier*, *Institucional*. Available at: https://www.elsevier.com/es-mx/solutions/scopus (Accessed: March 3, 2021).

*Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública Principales Resultados Sonora* (2019).

Escobar, L. J. V. and Salinas, S. A. (2016) “E-Health prototype system for cardiac telemonitoring,” *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 2016-Octob, pp. 4399–4402. doi: 10.1109/EMBC.2016.7591702.

Fan, K. *et al.* (2018) “Lightweight NFC protocol for privacy protection in mobile IoT,” *Applied Sciences (Switzerland)*, 8(12), pp. 1–14. doi: 10.3390/app8122506.

Faqihi, R., Ramakrishnan, J. and Mavaluru, D. (2020) “An evolutionary study on the threats, trust, security, and challenges in SIoT (social internet of things),” *Materials Today: Proceedings*. doi: 10.1016/j.matpr.2020.09.618.

Ferencz, K. and Domokos, J. (2020) “Rapid Prototyping of IoT Applications for the Industry,” *2020 22nd IEEE International Conference on Automation, Quality and Testing, Robotics - THETA, AQTR 2020 - Proceedings*. doi: 10.1109/AQTR49680.2020.9129934.

Fernandez-Carames, T. M. and Fraga-Lamas, P. (2018) “A Review on Human-Centered IoT-Connected Smart Labels for the Industry 4.0,” *IEEE Access*, 6(c), pp. 25939–25957. doi: 10.1109/ACCESS.2018.2833501.

Fragal, A. C., Ribeiro, A. O. and Baldo, C. R. (2021) *A cyber physical system approach to customer services of home appliances*, *Smart Innovation, Systems and Technologies*. Springer International Publishing. doi: 10.1007/978-3-030-55374-6_4.

García, J. (2021) *Security: Is Ubidots Secure? | Ubidots Help Center*, *https://help.ubidots.com/en/articles/*. Available at: https://help.ubidots.com/en/articles/889691-security-is-ubidots-secure (Accessed: March 5, 2021).

Gayathri, K. (2019) “Implementation of Environment Parameters Monitoring in a Manufacturing Industry using IOT,” *2019 5th International Conference on Advanced*

*Computing and Communication Systems, ICACCS 2019*, pp. 858–862. doi: 10.1109/ICACCS.2019.8728365.

Hedi, I., Špeh, I. and Šarabok, A. (2017) "IoT network protocols comparison for the purpose of IoT constrained networks," *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, pp. 501–505. doi: 10.23919/MIPRO.2017.7973477.

Hejazi, H. *et al.* (2019) *Survey of Platforms for Massive IoT*.

Imran, M. *et al.* (2019) "Enabling technologies for Social Internet of Things," *Future Generation Computer Systems*. Elsevier B.V., pp. 715–717. doi: 10.1016/j.future.2018.11.018.

Isikdag, U. (2015) "Internet of Things: Software Platforms," *Enhanced Building Information Models: Using IoT Services and Integration Patterns*, pp. 1–121. doi: 10.1007/978-3-319-21825-0.

Kassab, W. and Darabkh, K. A. (2020) "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, 163(September 2019), p. 102663. doi: 10.1016/j.jnca.2020.102663.

Kesavan, G., Sanjeevi, P. and Viswanathan, P. (2016) "A 24 hour IoT framework for monitoring and managing home automation," *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016*, 1. doi: 10.1109/INVENTIVE.2016.7823205.

Khan, W. Z. *et al.* (2017) "When social objects collaborate: Concepts, processing elements, attacks and challenges," *Computers and Electrical Engineering*, 58, pp. 397–411. doi: 10.1016/j.compeleceng.2016.11.014.

Kishore, K. and Sharma, S. (2016) "Evolution of Wireless Sensor Networks as the framework of Internet of Things-A Review," (December).

Langley, D. J. *et al.* (2021) "The Internet of Everything: Smart things and their impact on business models," *Journal of Business Research*, 122(June 2018), pp. 853–863. doi: 10.1016/j.jbusres.2019.12.035.

Machado, D. B. and Calderón, C. A. (2016) "Propuesta de arquitectura para Internet de las Cosas Network Management View project," (November 2016). Available at: https://www.researchgate.net/publication/320353907.

Madakam, S. (2015) "Internet of Things: Smart Things," *International Journal of Future Computer and Communication*, 4(4), pp. 250–253. doi: 10.7763/ijfcc.2015.v4.395.

Maru, V., Nannapaneni, S. and Krishnan, K. (2020) "Internet of things based cyber-physical system framework for real-time operations," *Proceedings - 2020 IEEE 23rd International Symposium on Real-Time Distributed Computing, ISORC 2020*, pp. 146–147. doi: 10.1109/ISORC49007.2020.00031.

Mois, G., Sanislav, T. and Folea, S. C. (2016) “A Cyber-Physical System for Environmental Monitoring,” *IEEE Transactions on Instrumentation and Measurement*, 65(6), pp. 1463–1471. doi: 10.1109/TIM.2016.2526669.

Montalbán Pozas, B. *et al.* (2018) “Mejora de la eficiencia energética en edificios públicos a través de inmótica social,” *Rehabend*, (221479), pp. 1638–1646.

Moufaddal, M., Benghabrit, A. and Bouhaddou, I. (2021) “A Cyber-Physical Warehouse Management System Architecture in an Industry 4.0 Context,” in, pp. 125–148. doi: 10.1007/978-3-030-51186-9_9.

Mustapaa, T. *et al.* (2020) “Digital Metrology for the Internet of Things,” in *GIoTS 2020 - Global Internet of Things Summit, Proceedings*. Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/GIOTS49054.2020.9119603.

Naik, N. (2017) “Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTPNaik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE International Symposium on Systems Engineering, ISSE 2017 -,” *2017 IEEE International Symposium on Systems Engineering, ISSE 2017 - Proceedings*, pp. 1–7. Available at: http://ieeexplore.ieee.org/document/8088251/.

Neumann, A., Laranjeiro, N. and Bernardino, J. (2018) “An Analysis of Public REST Web Service APIs,” *IEEE Transactions on Services Computing*, (November). doi: 10.1109/TSC.2018.2847344.

Odusote, Ayo Naik, Sujit Ashish, Tiwari Arora, G. (2016) “Convirtiendo valor en ingresos ordinarios.”

Ojo, M. O. *et al.* (2018) “A Review of Low-End, Middle-End, and High-End Iot Devices,” *IEEE Access*, 6, pp. 70528–70554. doi: 10.1109/ACCESS.2018.2879615.

Osisiogu, U. (2019) “A review on cyber -physical security of smart buildings and infrastructure,” *2019 15th International Conference on Electronics, Computer and Computation, ICECCO 2019*, (Icecco), pp. 47–50. doi: 10.1109/ICECCO48375.2019.9043207.

Oyshi, M. T. *et al.* (2021) “IoT Security Issues and Possible Solution Using Blockchain Technology,” in *Lecture Notes in Networks and Systems*. Springer, pp. 113–121. doi: 10.1007/978-981-15-4218-3_12.

Panda, N. K. *et al.* (2018) “IOT based advanced medicine dispenser integrated with an interactive web application,” *International Journal of Engineering and Technology(UAE)*, 7(4), pp. 46–48. doi: 10.14419/ijet.v7i4.10.20704.

Patnaik, R., Padhy, N. and Srujan Raju, K. (2021) “A systematic survey on iot security issues, vulnerability and open challenges,” in *Advances in Intelligent Systems and Computing*. Springer, pp. 723–730. doi: 10.1007/978-981-15-5400-1_68.

Paz Corrales, M. A. (2020) “Analizar el uso de la domótica y su influencia en la comodidad de los hogares arequipeños.”

Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D. (2014) “Context aware computing for the internet of things: A survey. Communications Surveys Tutorials,” *Ieee*, 16(1), pp. 414 – 454.

Ray, P. P. (2018) “A survey on Internet of Things architectures,” *Journal of King Saud University - Computer and Information Sciences*, 30(3), pp. 291–319. doi: 10.1016/j.jksuci.2016.10.003.

Razzaque, M. A. *et al.* (2016) “Middleware for internet of things: A survey,” *IEEE Internet of Things Journal*, 3(1), pp. 70–95. doi: 10.1109/JIOT.2015.2498900.

Salami, A. and Yari, A. (2018) “A framework for comparing quantitative and qualitative criteria of IoT platforms,” *2018 4th International Conference on Web Research, ICWR 2018*, pp. 34–39. doi: 10.1109/ICWR.2018.8387234.

Sharma, P. *et al.* (2020) “A study of routing protocols, security issues and attacks in network layer of internet of things framework,” *2nd International Conference on Data, Engineering and Applications, IDEA 2020*, pp. 11–16. doi: 10.1109/IDEA49133.2020.9170741.

Soni, D. and Makwana, A. (2017) “A survey on mqtt: a protocol of internet of things(IoT),” *International Conference on Telecommunication, Power Analysis and Computing Techniques (Ictpact - 2017)*, (April), pp. 0–5. Available at: https://www.researchgate.net/publication/316018571_A_SURVEY_ON_MQTT_A_PROTOCOL_OF_INTERNET_OF_THINGSIOT.

Symantec, Corporation. (2013) *MAC address (dirección MAC)*. Available at: https://web.archive.org/web/20131202225520/http://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=m&word=mac-address (Accessed: February 1, 2021).

Tkachenko, V., Alla, G. and Maryna, K. (2018) “Communication Messaging Models in IoT/WoT: Survey and Application,” pp. 417–422.

Truong, H. L. and Dustdar, S. (2015) “Principles for engineering IoT cloud systems,” *IEEE Cloud Computing*, 2(2), pp. 68–76. doi: 10.1109/MCC.2015.23.

Verbeke, S. *et al.* (2017) “EU DG Energy: Support for setting up a Smart Readiness Indicator for buildings and related impact assessment: Interim report,” (December).

Virmani, C. and Pillai, A. (2021) “Internet of Things and Cyber Physical Systems: An Insight,” in *Studies in Systems, Decision and Control*. Springer, pp. 379–401. doi: 10.1007/978-3-030-47411-9_21.

Yedle, B. *et al.* (2021) “A Survey: Security Issues and Challenges in Internet of Things,” in *Lecture Notes in Networks and Systems*. Springer, pp. 75–86. doi: 10.1007/978-981-15-4218-3_8.

Zhang, K. and Jacobsen, H.-A. (2013) “SDN-like: The Next Generation of Pub/Sub.” Available at: http://arxiv.org/abs/1308.0056.