UNIVERSO IOT

SENSORES DISPOSITIVOS REDES Y PROTOCOLOS DE COMUNICACIÓN EN EL INTERNET DE LAS COSAS

Isaac David Torres Paredes Narcisa de Jesús Salazar Álvarez Alex Ricardo Guamán Andrade

SOLUZIONINNOVATIVE S.A.S.

SOLUZIONINNOVATIVE
S.A.S.
EDITORIAL

UNIVERSO IoT: Sensores, dispositivos, redes y protocolos de comunicación en el internet de las cosas

ISBN: 978-1988-7294-5-3

Autores:

Isaac David Torres Paredes

Narcisa de Jesús Salazar Álvarez

Alex Ricardo Guamán Andrade

SOLUZIONINNOVATIVE S.A.S.

EDITORIAL

Primera Edición, diciembre 2024

ISBN: 978-9942-7294-5-3

Editado por:

Sello editorial: ©Soluzioninnovative S.A.S. Editorial

No Radicación: 169086

Editorial: ©Soluzioninnovative S.A.S. Editorial

Los Andes y El Sufragio

Dirección de Publicaciones Científicas Soluzioninnovative S.A.S.

Editorial Riobamba, Chimborazo, Ecuador

Teléfono: +593967468602

Código Postal: 060108

https://orcid.org/0009-0001-7057-9316

https://orcid.org/0000-0002-6467-0906

https://orcid.org/0000-0001-8862-8350

https://doi.org/10.61396/editorialsoluzioninnovative.lib14

ÍNDICE

ÍNDICE DE ACRÓNIMOS

ADC (Analog to Digital Converter)**:** Convertidor de Analógico a Digital
AMCA: Adaptación Multicanal Asincrónica
AMQP (Advanced Message Queuing Protocol)**:** Protocolo Avanzado de Encolado de Mensajes
API (Application Programming Interface)**:** Interfaz de Programación de Aplicaciones
ARM (Advanced RISC Machine)**:** Máquina RISC Avanzada
ARPANET (Advanced Research Projects Agency Network)**:** Red de la Agencia de Proyectos de Investigación Avanzada
AWS (Amazon Web Services)**:** Servicios Web de Amazon
CAN (Controller Area Network)**:** Red de Área del Controlador
CARP (Common Address Redundancy Protocol)**:** Protocolo Común de Redundancia de Direcciones
CC (Cloud Computing)**:** Computación en la Nube
CDMA (Code Division Multiple Access)**:** Acceso Múltiple por División de Código
CoAP (Constrained Application Protocol)**:** Protocolo de Aplicación Constriñida
CRC (Cyclic Redundancy Check)**:** Verificación de Redundancia Cíclica
CWMP (CPE WAN Management Protocol)**:** Protocolo de Gestión WAN de CPE
D-C (Device to Cloud)**:** Dispositivo a la Nube
D-D (Device to Device)**:** Comunicación Directa entre Dispositivos
D-E-C (Device to Edge to Cloud)**:** Dispositivo al Borde a la Nube
DAC (Digital to Analog Converter)**:** Convertidor de Digital a Analógico
DASH7 (Data Exchange for DASH7 Alliance Protocol)**:** Intercambio de Datos para el Protocolo de la Alianza DASH7
DSME (Deterministic and Synchronous Multi-Channel Extension)**:** Extensión Multicanal Determinista y Sincrónica
EC (Edge Computing)**:** Computación en el Borde
EC-GSM (Extended Coverage GSM)**:** Cobertura Extendida GSM

EAP (Extensible Authentication Protocol)**:** Protocolo de Autenticación Extensible

FC (Fog Computing)**:** Computación en la Niebla

FIWARE (Future Internet Ware)**:** Software de Internet del Futuro

FLL (Frequency-Locked Loop)**:** Bucle de Enganche de Frecuencia

GPRS (General Packet Radio Service)**:** Servicio General de Paquetes por Radio

GPS (Global Positioning System)**:** Sistema de Posicionamiento Global

GPIO (General Purpose Input/Output)**:** Entrada/Salida de Propósito General

HDFS (Hadoop Distributed File System)**:** Sistema de Archivos Distribuido de Hadoop

HPC (High Performance Computing Clusters)**:** Clústeres de Computación de Alto Rendimiento

H**TTP** (Hypertext Transfer Protocol)**:** Protocolo de Transferencia de Hipertexto

I2C (Inter-Integrated Circuit)**:** Circuito Inter-Integrado

I2S (Integrated Interchip Sound)**:** Sonido Interchip Integrado

IEC (International Electrotechnical Commission)**:** Comisión Electrotécnica Internacional

IEEE (Institute of Electrical and Electronics Engineers)**:** Instituto de Ingenieros Eléctricos y Electrónicos

IETF (Internet Engineering Task Force)**:** Fuerza de Tareas de Ingeniería de Internet

IKEv2 (Internet Key Exchange version 2)**:** Intercambio de Claves de Internet versión 2

IoT (Internet of Things)**:** Internet de las Cosas

IP (Internet Protocol)**:** Protocolo de Internet

I**SO** (International Organization for Standardization)**:** Organización Internacional de Normalización

ISM (Industrial, Scientific and Medical)**:** Industrial, Científico y Médico

LLDN (Low Latency Deterministic Network)**:** Red Determinista de Baja Latencia

LoRa (Long Range)**:** Largo Alcance

LoRaWAN (Long Range Wide Area Network)**:** Red de Área Amplia de Largo Alcance

LPWA (Low Power Wide Area)**:** Área Amplia de Baja Potencia

LPWAN (Low Power Wide Area Network)**:** Red de Área Amplia de Baja Potencia

LTE (Long Term Evolution)**:** Evolución a Largo Plazo

LTE-1 (LTE Release 1)**:** Primera Versión de LTE

LTE-M (LTE for Machines)**:** LTE para Máquinas

M2M (Machine to Machine)**:** Máquina a Máquina

MILNET (Military Network)**:** Red Militar

MQTT (Message Queuing Telemetry Transport)**:** Transporte de Telemetría de Encolado de Mensajes

NB-IoT (Narrowband IoT): IoT de Banda Angosta

NFC (Near Field Communication)**:** Comunicación de Campo Cercano

NIST (National Institute of Standards and Technology)**:** Instituto Nacional de Estándares y Tecnología

NTC (Negative Temperature Coefficient)**:** Coeficiente de Temperatura Negativo

OAuth (Open Authorization)**:** Autorización Abierta

OMA (Open Mobile Alliance)**:** Alianza de Móviles Abiertos

OSI (Open Systems Interconnection)**:** Interconexión de Sistemas Abiertos

PAN (Personal Area Network)**:** Red de Área Personal

PANA (Protocol for Carrying Authentication for Network Access)**:** Protocolo para Llevar Autenticación para Acceso a la Red

PLL (Phase-Locked Loop)**:** Bucle de Enganche de Fase

PLC (Power Line Communication)**:** Comunicación por Línea de Energía

PTC (Positive Temperature Coefficient)**:** Coeficiente de Temperatura Positivo

RTD (Resistance Temperature Detector)**:** Detector de Temperatura de Resistencia

RDDs (Resilient Distributed Datasets)**:** Conjuntos de Datos Distribuidos y Resilientes

RFID (Radio Frequency Identification)**:** Identificación por Radiofrecuencia

ROI (Return on Investment)**:** Retorno de la Inversión

SDHC (Secure Digital High Capacity)**:** Alta Capacidad Digital Segura

SBC (Single Board Computer)**:** Computadora de Placa Única

SNMP (Simple Network Management Protocol)**:** Protocolo Simple de Administración de Red

SoC (System on Chip)**:** Sistema en un Chip

SPI (Serial Peripheral Interface)**:** Interfaz Periférica Serial

UART (Universal Asynchronous Receiver-Transmitter)**:** Receptor-Transmisor Asíncrono Universal

USB (Universal Serial Bus)**:** Bus Serial Universal

UUID (Universally Unique Identifier)**:** Identificador Único Universal

WBAN (Wireless Body Area Network)**:** Red de Área Corporal Inalámbrica

Wi-Fi (Wireless Fidelity)**:** Fidelidad Inalámbrica

WiMax (Worldwide Interoperability for Microwave Access)**:** Interoperabilidad Mundial para el Acceso por Microondas

WLAN (Wireless Local Area Network)**:** Red de Área Local Inalámbrica

WSN (Wireless Sensor Network)**:** Red de Sensores Inalámbrica

YARN (Yet Another Resource Negotiator)**:** Otro Negociador de Recursos Más

ZigBee (Wireless Mesh Network Standard)**:** Estándar de Red en Malla Inalámbrica

INTRODUCCIÓN

A nivel mundial, el internet de las Cosas (IoT) ha surgido como una tecnología que impulsa a la innovación y transformación digital, integrando objetos cotidianos en una red interconectada que facilita una interacción más eficiente y efectiva con el entorno. Desde hogares inteligentes hasta ciudades enteras optimizadas para el bienestar de los habitantes, el IoT está transformando la manera en que vivimos, trabajamos y nos relacionamos con el mundo que nos rodea. La proyección de crecimiento de esta tecnología es exponencial, el IoT promete revolucionar industrias, mejorar servicios y generar nuevas oportunidades económicas y sociales a nivel global. En este universo interconectado, cada objeto, desde los más pequeños sensores hasta los complejos sistemas industriales, convergen en una red universal que transforma la manera en que interactuamos con el mundo que nos rodea.

En Ecuador, el desarrollo y la adopción del IoT se encuentran en etapas iniciales. Aunque existen iniciativas puntuales y proyectos innovadores en áreas como la agricultura, industria y la gestión de recursos, la inserción del IoT aún no ha alcanzado su máximo potencial. Las barreras tecnológicas y la falta de infraestructura e incluso la preparación académica en las personas son desafíos que el país enfrenta para aprovechar plenamente los beneficios del IoT. Sin embargo, el interés en esta tecnología está creciendo, y cada vez más instituciones académicas y empresas comienzan a explorar las posibilidades que ofrece el IoT para impulsar el desarrollo económico y mejorar la calidad de vida de los ecuatorianos.

En la provincia de Chimborazo, el conocimiento y la aplicación del IoT son todavía más limitados. A pesar de su potencial para transformar sectores clave como la agricultura, ganadería, turismo y la gestión de recursos naturales con los que cuenta esta provincia, la implementación de soluciones IoT en esta región ha sido escasa. La falta de información y formación en esta área tecnológica es un obstáculo que de cierta manera impide a la provincia aprovechar plenamente las ventajas del IoT.

La creación del libro "Universo IoT" responde a la necesidad de aportar al conocimiento en el ámbito del Internet de las Cosas en la provincia de Chimborazo y el Ecuador. Este libro tiene como objetivo proporcionar un enfoque general en cuanto a esta tecnología emergente, desde sus fundamentos hasta sus aplicaciones prácticas. Al hacerlo, se espera capacitar a estudiantes profesionales y empresarios locales para que puedan considerar de mejor manera el implementar y aprovechar las tecnologías del IoT en sus respectivos campos. De esta manera, "Universo IoT" no solo busca educar, sino también inspirar y fomentar el desarrollo tecnológico en una región que tiene gran potencial para beneficiarse de la revolución del Internet de las Cosas.

En el **Capítulo I**, denominado: Fundamentos Capas y Componentes del IoT, se presentan los principios básicos, además, se explora que, el Internet de las Cosas (IoT), es una amalgama de objetos cotidianos conectados a la red, que ha irrumpido en nuestras vidas de forma casi imperceptible. Esta evolución tecnológica, lejos de ser un mero añadido, transforma la esencia misma de los objetos que nos rodean dotándolos de una nueva vida digital.

En un mundo cada vez más interconectado, Internet se erige como el canal de comunicación por excelencia, con cerca de 4 mil millones de usuarios. El IoT se suma a este panorama expandiendo las posibilidades de interacción y comunicación más allá del ámbito humano. Esta simbiosis entre objetos y red abre un sinfín de posibilidades, desde hogares inteligentes que se adaptan a nuestras necesidades hasta ciudades que optimizan recursos y servicios, el IoT tiene el potencial de transformar radicalmente nuestro modo de vida. Finalmente se presentan los cimientos sobre los cuales se erige este vasto ecosistema tecnológico. Desde la arquitectura básica hasta los principios subyacentes, este capítulo sienta las bases para comprender la complejidad y la amplitud del IoT.

El **Capítulo II**, denominado: Hardware en el IoT, se da a conocer que, los dispositivos, en conjunto con los sensores, la conectividad y las plataformas, constituyen uno de los fundamentos del IoT. Estos dispositivos

suelen estar integrados o vinculados a diversos objetos convirtiéndolos en "cosas" dentro del ecosistema IoT. Su función principal radica en emplear sensores y actuadores para recopilar información sobre el entorno y tomar acciones en función de dichos datos. Es fundamental que estos dispositivos puedan transmitir esta información a un servidor o realizar algún tipo de procesamiento interno para intervenir en el entorno de manera efectiva. Durante el desarrollo de un dispositivo o la implementación de una aplicación IoT, es importante interactuar con el entorno cercano para recopilar datos o ajustar el entorno según nuestras necesidades. Un sensor se encarga de convertir un fenómeno físico, como la temperatura o la presión, en una señal eléctrica. Tres cualidades básicas definen un sensor de calidad: debe ser sensible al fenómeno que está midiendo, no debe verse afectado por otros fenómenos físicos y no debe alterar el fenómeno que está midiendo durante el proceso de medición. De esta forma nos ofrece un panorama claro de esta red global de interconexión. Desde los sensores que capturan datos del mundo físico hasta los actuadores que ejecutan acciones en respuesta, pasando por los controladores, microprocesadores, software de control y sus características.

En el **Capítulo III**, Protocolos y Redes de Comunicación, se muestra que, los sensores y otros dispositivos se integran en redes que emplean una variedad de dispositivos de red, como *hubs, gateways, routers,* puentes de red y conmutadores, según lo requiera la aplicación específica. En el contexto del Internet de las Cosas, la conectividad presenta una amplia gama de alternativas: desde conexiones móviles, satelitales, *Wi-Fi, Bluetooth,* RFID y NFC hasta redes de baja energía y *Ethernet*, entre otras.

El Internet de las cosas se basa principalmente en tecnologías de redes inalámbricas, siendo el 5G la opción destacada en la actualidad. Esta nueva generación de tecnología móvil promete incrementar la velocidad de conexión y minimizar la latencia, lo que resultará en una proliferación exponencial de dispositivos conectados.. Dicho de otro modo, el 5G habilitará una conectividad constante y veloz entre dispositivos, permitiendo una interacción fluida. Además del 5G, también se emplean otras tecnologías ina-

lámbricas como las LPWAN, diseñadas para transmitir pequeñas cantidades de datos a grandes distancias con un consumo energético mínimo. Además, se describen también otras redes de comunicación utilizadas en el IoT como, LoRa, RFID, DASH7, NFC y varias más. Todo esto teniendo en cuenta las redes por las cuales fluye la información en este universo digital. Desde los protocolos de comunicación más comunes hasta las redes especializadas que sustentan esta infraestructura de la conectividad en el IoT.

Finalmente, **Capítulo IV**, que tiene por título: Tratamiento y estudio de datos en las verticales del IoT se presenta un enfoque hacia las aplicaciones concretas y los sectores verticales que se benefician de esta revolución tecnológica. Evidenciando que la evolución de nuevos casos de aplicación en el ámbito del IoT continúa impulsando el progreso tecnológico y la adopción de nuevos enfoques para superar los desafíos existentes. Los sistemas IoT generan una gran cantidad de datos, que provienen de diversas fuentes, tales como: datos públicos proporcionados por entidades gubernamentales organizaciones estatales y comunidades. Estos datos se pueden emplear para ofrecer servicios tanto a organismos públicos como privados. Ejemplos de estos datos incluyen información meteorológica y datos demográficos. Además, se obtienen datos de dispositivos físicos como dispositivos móviles (como *smartphones, tablets y* ***smartwatches***), vehículos equipados con sistemas de posicionamiento GPS y sensores que recopilan información sobre diversos parámetros como el nivel de llenado de contenedores, la concentración de partículas contaminantes en el aire y el nivel de luminosidad en las calles. También se accede a datos comunitarios, los cuales son extraídos de fuentes no estructuradas en entornos sociales en línea, como redes sociales y sitios web donde se comparten opiniones sobre productos o se realizan encuestas.

Este capítulo además ofrece una visión de las diversas aplicaciones dentro del ámbito del Internet de las Cosas. Sin embargo, es importante tener en cuenta que estas muestras siempre serán parciales dado que constantemente surgen nuevas áreas de aplicación y casos de uso en este campo. Algunas de estas aplicaciones, actualmente en implementación en diversos

entornos, incluyen la automatización y control remoto de edificios, sistemas de seguridad, gestión de energía inteligente, atención médica, domótica, así como servicios en sectores como ventas y turismo. Es evidente que los entornos industriales representan el próximo gran avance para el Internet de las Cosas, impulsando lo que se conoce como la próxima revolución industrial, enfocada en la captura de datos, el mantenimiento predictivo, y la optimización de procesos, entre otros aspectos clave.

CAPÍTULO I:
FUNDAMENTOS CAPAS Y COMPONENTES DEL IoT

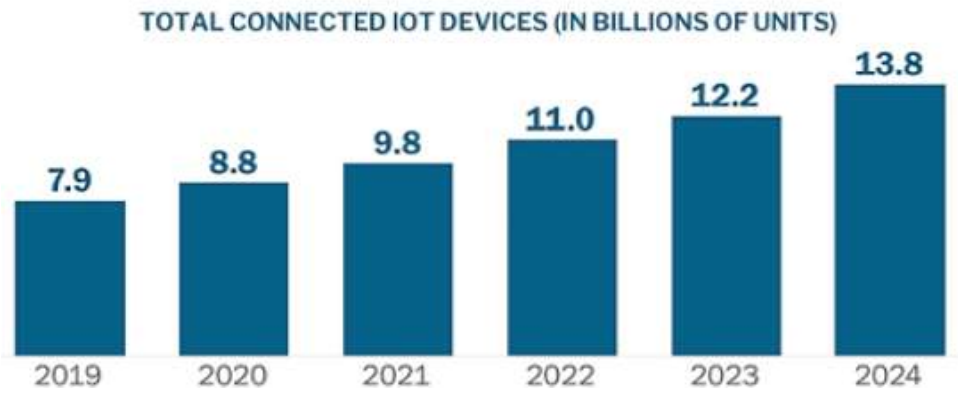
1.1 Introducción y Objetivos del capítulo

El Internet de las Cosas (IoT), esa amalgama de objetos cotidianos conectados a la red, ha irrumpido en nuestras vidas de forma casi imperceptible. Esta evolución tecnológica, lejos de ser un mero añadido, transforma la esencia misma de los objetos que nos rodean dotándolos de una nueva vida digital.

En un mundo cada vez más interconectado, Internet se erige como el canal de comunicación por excelencia, con cerca de 4 mil millones de usuarios. El IoT se suma a este panorama expandiendo las posibilidades de interacción y comunicación más allá del ámbito humano. Esta simbiosis entre objetos y red abre un sinfín de posibilidades, desde hogares inteligentes que se adaptan a nuestras necesidades hasta ciudades que optimizan recursos y servicios, el IoT tiene el potencial de transformar radicalmente nuestro modo de vida. En la Figura 1.1 se muestra según (Tech&Business, 2019), el crecimiento que tiene los dispositivos IoT a nivel mundial.

Figura 1.1

Crecimiento de los dispositivos IoT



Fuente: (Tech&Business, 2019)

Lejos de ser una simple mejora incremental, el IoT irrumpe como una revolución que transforma radicalmente diversos sectores, desde la edu-

cación y la salud hasta el entretenimiento, la industria automotriz y la manufactura. Su robusta base tecnológica cimentada en años de desarrollo en áreas como la ciencia de datos, la electrónica, la inteligencia ambiental y la computación de alto rendimiento, impulsa su potencial hacia un futuro donde los objetos cobran vida y habilitan tareas hasta ahora inimaginables.

En los últimos años, se ha observado un florecimiento de sistemas IoT desarrollados por empresas e instituciones de investigación. Estos sistemas se han diseñado para atender a una amplia gama de casos de uso, desde la automatización del hogar hasta la gestión de ciudades inteligentes. Aunque es viable realizar el procesamiento local de los datos generados por estos sistemas, una estrategia mucho más sensata, escalable y adaptable para cualquier escenario que demande baja latencia implica el empleo de plataformas en la nube dedicadas al procesamiento y análisis de conjuntos de datos extensos, en los últimos años han surgido diversas plataformas de este tipo, como AWS IoT, FIWARE, OpenMTC SmartThings, entre muchas otras.

La multiplicidad de soluciones IoT genera un desafío al momento de seleccionar la plataforma adecuada para un caso específico. La disparidad de tecnologías y terminologías entre las opciones existentes complica la decisión.

La arquitectura de capas emerge como una respuesta enfocándose en organizar los componentes y tecnologías en diferentes niveles, permitiendo una mayor flexibilidad y modularidad. Cada capa puede implementarse con tecnologías específicas, adaptándose a las necesidades del proyecto. Algunas ventajas notorias de una arquitectura de n capas son:

Conectividad simplificada esto quiere decir que facilita la interacción con los dispositivos IoT, incluso a través de cortafuegos y traductores de direcciones de red. La **escalabilidad** y disponibilidad permite la gestión eficiente de millones de dispositivos, con mecanismos de alta disponibilidad y recuperación ante desastres. La **actualización y gestión** remota esto simplifica la actualización y gestión de dispositivos con recursos limitados,po-

sibilitando su uso cotidiano sin interrupciones. La **seguridad y privacidad**, brinda un marco para la gestión de la identidad, control de acceso y protección de datos personales La **integración** por su parte permite la interconexión de diversos sistemas y dispositivos, creando un ecosistema IoT cohesivo.

Es importante resaltar que no existe un modelo único y universal para la arquitectura de IoT. Cada organización, empresa y asociación define su propia estructura. Sin embargo, al analizar las numerosas propuestas existentes, se observa una convergencia en ciertos aspectos clave. En base a esta introducción se establecen los siguientes objetivos a ser alcanzados luego de leer y comprender este primer capítulo.

- Reconocer la significativa relevancia de los datos dentro del ámbito del Internet de las Cosas comprendiendo cómo su análisis posibilita la deducción de conocimientos novedosos.

- Ubicar el Internet de las Cosas en el contexto de su evolución histórica, destacando su desarrollo a lo largo del tiempo.

- Adquirir un profundo conocimiento acerca de los elementos que componen un ecosistema completo de IoT.

- Familiarizarse con las características inherentes a una pila arquitectónica diseñada específicamente para el paradigma del Internet de las Cosas.

- Reconocer los puntos de intersección entre los diversos componentes que constituyen un entorno tecnológico adaptado a IoT, así como comprender las responsabilidades asignadas a cada módulo.

- Desarrollar una comprensión integral de la estructura en capas de una implementación, con el fin de identificar los elementos principales presentes en cualquier arquitectura comercial, facilitando así la selección de la más apropiada.

1.2 Principios básicos del Internet de las Cosas

Internet ha revolucionado la forma en que se interactúa con el

mundo, desde la comunicación hasta el comercio, la educación y el entretenimiento, la red ha transformado nuestras vidas de maneras inimaginables y mientras el internet continúa evolucionando, una cosa es segura, la información seguirá siendo su activo más valioso.

1.2.1 La red mundial, el porvenir y la importancia de los datos

La web, ese universo digital omnipresente en nuestras vidas, ha recorrido un largo camino desde sus inicios. Un viaje que ha transformado la forma en que interactuamos, consumimos información y hacemos negocios. A lo largo de su historia, la web ha experimentado diferentes etapas evolutivas, cada una con sus características y aportes específicos.

En sus albores, la web era un terreno virgen, un espacio forjado para la investigación y el desarrollo militar, conocida como ARPANET, la red conectaba instituciones académicas y centros de investigación, sentando las bases para el futuro ecosistema digital.

La segunda etapa trajo consigo una explosión de sitios web publicitarios. Las empresas se apresuraron a establecer su presencia en Internet, creando escaparates virtuales donde promocionar sus productos y servicios. La fiebre por los nombres de dominio alcanzó niveles históricos, reflejando la importancia que cobraba este nuevo espacio digital.

La tercera fase marcó un antes y un después, la web se volvió transaccional, el comercio electrónico despegó, permitiendo a los usuarios comprar y vender productos y servicios de forma online. Surgieron las famosas "punto com", empresas que revolucionaron el panorama comercial y, en algunos casos, sucumbieron ante la vorágine de un mercado en constante cambio.

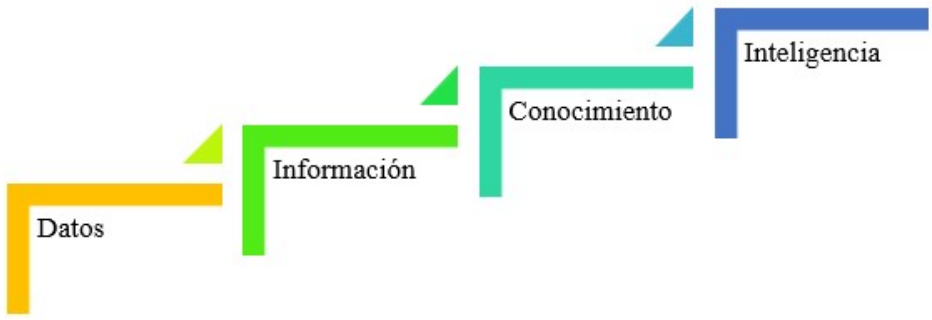
En la actualidad, se encuentra en la era de la web social. Las redes sociales han transformado la forma de comunicación, compartir información e interactuar con el mundo. La web se ha convertido en un espacio de interacción constante, donde las personas comparten sus experiencias, ideas y opiniones, creando una comunidad global sin precedentes.

Aunque el propósito fundamental de Internet es facilitar el proceso

de comunicación, su esencia radica en la transmisión de datos. En la actualidad, se otorga una gran relevancia a estos datos, los cuales, en su forma individual, carecen de utilidad real; constituyen simplemente la materia prima que, al ser procesada, se convierte en información. No obstante, esta materia prima adquiere utilidad cuando se dispone de ella en cantidades suficientes, posibilitando la identificación de tendencias y patrones, es decir, la obtención de conocimiento. A partir de este conocimiento, puede surgir la inteligencia, que se gesta al combinar el conocimiento con la experiencia. Mientras que el conocimiento evoluciona con el tiempo, la inteligencia se revela atemporal, pero su gestación inicia con la adquisición de datos. En la Figura 1.2 se muestra las partes de la evolución del dato hasta convertirse en inteligencia.

Figura 1.2

Metamorfosis de datos a inteligencia



La red global se ha convertido en un componente fundamental en el proceso de adquisición de conocimiento humano al posibilitar la libre circulación de información. Se establece una conexión directa entre la entrada de datos y la generación de inteligencia.

El concepto de **Internet del Futuro** se presenta como un esfuerzo dirigido hacia la mejora de un entorno tecnológico, así como hacia la adopción de nuevos principios arquitectónicos. En este contexto, se han identificado cuatro pilares fundamentales: Internet de las Personas,Internet de los Contenidos y el Conocimiento, Internet de los Servicios e Internet de las Cosas. Este enfoque normativo europeo establece las pautas tecnológicas para el desarrollo futuro de Internet, como se muestra en la Figura 1.3.

Figura 1.3

Bases para el internet del futuro

El internet para y por las personas se enfoca en que la próxima generación de Internet debe tener la capacidad de facilitar el intercambio de información a lo largo del tiempo, considerando el constante aumento en la cantidad de usuarios conectados. Debe cumplir con las expectativas tanto de los usuarios existentes como de los recién llegados, permitiendo al mismo tiempo la autorregulación y la sostenibilidad. En este contexto, se espera que el Internet del Futuro cumpla con diversos objetivos, como mejorar la vida diaria de individuos, comunidades y organizaciones, posibilitar la creación de negocios de cualquier tamaño y ámbito, y eliminar las barreras entre productores y consumidores de información, dando lugar a la figura de los "prosumidores". Se busca que la creación de contenidos no requiera experiencia profesional, incluso para contenidos de alta calidad,

con limitaciones de tiempo y presupuesto. Estos principios facilitarían el intercambio rápido y sencillo de conocimientos distribuidos, promoviendo la formación de comunidades virtuales y el acceso a su inteligecncia. En base a esto, surge el concepto de Web 3.0, que abarca tecnologías semánticas, intercambio de conocimientos y procesamiento automático de información. Estas tecnologías son fundamentales para gestionar la enorme cantidad de datos disponible actualmente y en el futuro, lo que conduce al segundo pilar, el Internet de los Contenidos y el Conocimiento.

El enfoque del **internet del contenido y el conocimiento** está más allá de la convencional función de Internet como un propio repositorio de contenidos, la red está experimentando una transformación hacia comportamientos racionales conscientes, abarcando áreas como el pensamiento, aprendizaje, razonamiento y memoria. Para lograr este avance, se requiere la implementación de mecanismos de difusión del conocimiento que puedan cumplir con las expectativas de los usuarios. La Web 3.0 introduce la inteligencia cognitiva, capacitando a las aplicaciones web para suministrar información personalizada según las necesidades de los usuarios. *Tim Berners-Lee*, considerado el padre de la Web, promueve activamente el concepto de datos abiertos enlazados, buscando la integración a gran escala de datos en la Web. Esta iniciativa facilita el establecimiento de relaciones entre datos, la extracción de conocimiento y la generación de inteligencia, transformando efectivamente a Internet en una vasta base de datos y conocimiento. Para ello, cada elemento se etiqueta, permitiendo la entrega de información derivada a través de inferencias.

En la realidad laboral, se enfrenta a desafíos asociados con la digitalización de datos, el crecimiento cuantitativo y cualitativo de la información, así como la introducción de nuevos formatos, como la realidad virtual y la televisión digital, entre otros.

Por su parte el IoT se enfoca en la creación de escenarios que, a primera vista, podrían considerarse como ficticios, ya que implica que los objetos adquieran vida y posean capacidades inteligentes, como la identificación de comportamientos y la capacidad de reaccionar a estímulos

ambientales mediante el razonamiento. Esta afirmación abarca no solo a los ordenadores, sino también a electrodomésticos, dispositivos móviles y prácticamente cualquier objeto imaginable. En el pasado, Internet solía ser una colección bastante uniforme de objetos, como sitios web y aplicaciones, aunque no homogénea. Sin embargo, con la introducción del IoT, se ha producido una gran heterogeneidad debido a la inclusión de objetos con funcionalidades, tecnologías y campos de aplicación totalmente diversos. Estos objetos tienen la capacidad de comunicarse entre sí, tomar decisiones conjuntas y seguir comportamientos predeterminados. Se podría argumentar que la combinación de modelos de comunicación y sensores en objetos asequibles pero robustos ha permitido la evolución de Internet desde un paradigma basado en petición-respuesta a otro basado en la obtención y procesamiento de datos.

La utilización de objetos inteligentes posibilita la captura y el control autónomo de una variedad de procesos, lo cual, junto con una comunicación continua, facilita la ejecución de actividades coordinadas. En la actualidad, es factible llevar a cabo tareas complejas en entornos empresariales, como el control industrial, la gestión de redes eléctricas descentralizadas y el control de procesos de fabricación, entre otros.

Efectivamente, la aparición constante de aplicaciones innovadoras marca un progreso significativo en diversos campos. Algunas de estas innovaciones, como edificaciones inteligentes, robots y vehículos avanzados, son fácilmente discernibles y tienen como objetivo mejorar la calidad de vida de las personas. No obstante, hay numerosos ejemplos adicionales, como la evolución de las redes sociales hacia la formación de comunidades físicas a nivel global. Por otro lado, la medicina experimenta avances significativos que prometen una atención más precisa, personalizada y proactiva. Es innegable que se suceden innumerables avances en diversas esferas, como tejidos inteligentes, comercio electrónico y otros. La expansión de IoT se atribuye al hecho de que los individuos pueden participar activamente en este nuevo paradigma de mundo conectado, integrándose de manera activa en este contexto de comunicación instantánea. La conectividad

de los objetos permitirá la creación de un entorno de razonamiento propio en el cual el usuario participará activamente, como se muestra en la Figura 1.4.

Figura 1.4

Sectores de aplicación IoT

Fuente: (Vergara & Ocampo, 2017)

El **Internet de los Servicios** se presenta como un marco integral que engloba diversas categorías de servicios promocionados y gestionados a través de la red. Este ámbito abarca una variedad de servicios, como industriales, de fabricación, logísticos, financieros, energéticos y médicos, entre otros. La concepción de estos servicios se basa en tres conceptos fundamentales: servicios orientados a Internet, contextualización y orquestación.

La distribución de servicios computacionales a través de Internet ha llevado a una evolución en el diseño, el modelo de ejecución y el mantenimiento de aplicaciones. Los servicios orientados a Internet facilitan el acceso a diversas capacidades informáticas, ya sean de infraestructura, plataforma o aplicaciones, dando lugar al concepto de Cloud Computing (CC).

En los últimos años, tanto la industria tecnológica como la comuni-

dad científica han invertido significativos esfuerzos en la investigación e implementación del paradigma tecnológico CC. Este fenómeno ha resultado en un rápido crecimiento del número de plataformas, tanto privadas como públicas. La aceptación social de este paradigma, impulsada en gran medida por el interés económico de las grandes empresas tecnológicas, ha propiciado su desarrollo. Además, el modelo innovador de comercialización, basado en el pago por uso *(pay as you go)*, se asemeja al de servicios públicos tradicionales como luz, agua y gas.

Este enfoque comercial único obliga a las plataformas de CC a mantener la calidad de los servicios según lo acordado previamente. Esto subraya la importancia de analizar la arquitectura interna que posibilita la entrega consistente de estos servicios. Las innovaciones en este campo están impulsadas por una amplia gama de tecnologías subyacentes, como virtualización, granjas de servidores y servicios web, cuya madurez reciente permite ofrecer servicios con un nivel de calidad constante independientemente de la demanda de los usuarios.

El surgimiento de nuevas posibilidades tecnológicas ha dado lugar a la introducción de un concepto innovador conocido como **"elasticidad"**. Este concepto se fundamenta en el método de producción *just in time*, el cual se aplica a la producción de servicios informáticos y los recursos asociados. En este enfoque, los servicios generados reciben únicamente la cantidad de recursos necesarios para mantener un nivel constante de calidad, ajustándose a la demanda instantánea. En términos prácticos, esto se traduce en que los usuarios acceden a conjuntos de servicios a través de Internet que están siempre disponibles y, en principio, son infinitos.

Para los usuarios adheridos a este paradigma, el modelo de comercialización resulta beneficioso, ya que les exime de la responsabilidad de aprovisionarse con recursos informáticos adicionales para hacer frente a aumentos puntuales en la demanda de sus productos o servicios, así como de contar con la infraestructura necesaria para proporcionarlos.

Esta transformación permite convertir los gastos de capital en gastos

operacionales. No obstante, los proveedores deben ofrecer servicios de cómputo en la nube (CC) elásticos, gestionados mediante entornos de clústeres de computación de alto rendimiento (HPC), cuyo control y supervisión deben realizarse de manera automática, garantizando un acceso transparente para los usuarios finales.

El crecimiento exponencial de datos bajo el paradigma del Internet de las Cosas ha dado lugar a la aparición de dos nuevos enfoques computacionales: el cómputo en el borde *(edge computing, EC)* y el cómputo en la niebla *(fog computing, FC)*. En estos casos, no todo el procesamiento se lleva a cabo en la nube, evitando la transmisión masiva de datos y la centralización completa. En EC, el procesamiento se distribuye entre los nodos de la red, puertas de enlace cerca del borde o incluso en los propios dispositivos. Mientras tanto, en FC, este procesamiento se extiende a nivel de la arquitectura de red, teniendo lugar entre nodos de niebla distribuidos por la red o pasarelas IoT. El paradigma de cómputo en la nube se extiende hasta el borde de la red. Aunque esta aproximación ofrece beneficios, también plantea desafíos adicionales de seguridad al distribuir la inteligencia por la red. Para abordar este problema, se están considerando soluciones *peer-to-peer* como *blockchain* o grafos acíclicos dirigidos.

Es importante brindar a los usuarios un acceso a Internet que sea contextual, proactivo y personalizado. En lugar de depender únicamente de servicios reactivos, Internet debe permitir servicios proactivos que se adapten a las preferencias individuales, historial de uso y redes sociales de cada usuario. Este enfoque personalizado se sustenta en conceptos clave, como la conciencia de contexto, que busca una interacción adaptada a las circunstancias más amplias del usuario.

1.2.2 Atributos fundamentales y tecnologías base

El IoT representa una verdadera evolución de Internet, permitiendo que las aplicaciones accedan a información sobre las personas y su entorno, incluyendo su ubicación geográfica, actividades diarias y condiciones ambientales. Esta capacidad promete simplificar la vida en un futuro cercano

al hacer que las aplicaciones sean más proactivas y sensibles a las necesidades humanas. La expansión de IoT ha convertido a la red en un entorno sensorial, capaz de detectar una amplia gama de variables como temperatura, presión, luz y humedad, entre otras. Los sensores, debido a su tamaño y costo, son fácilmente integrables en hogares, lugares de trabajo y espacios públicos, convirtiendo prácticamente cualquier objeto en una fuente de datos. Esta transformación está remodelando los modelos de negocio, la administración pública y la vida cotidiana de millones de personas.

Aunque no se presentan como principios en sí mismos, existen directrices que orientan el desarrollo de aplicaciones dentro del marco del IoT. Estas directrices incluyen la comunicación y cooperación entre objetos conectados, la capacidad de direccionamiento para ubicar y configurar objetos remotamente, la identificación única de objetos para asociar información y contexto, la detección de información ambiental mediante sensores, la capacidad de actuar sobre el entorno mediante actuadores remotos, el procesamiento de información integrada en objetos inteligentes, la geolocalización y las interfaces de usuario adecuadas para interactuar con las personas. Estos principios han sido posibles gracias a la evolución de los procesadores, los sensores y las comunicaciones de bajo consumo, que han permitido el desarrollo y la implementación efectiva de la IoT en diversos ámbitos.

En el contexto de IoT, la necesidad de dispositivos más pequeños implica una evolución en la concepción de los **procesadores**. Estos deben reducir su tamaño y consumo, alejándose de la concepción clásica de los procesadores utilizados en ordenadores de sobremesa y portátiles. En este escenario, los procesadores en formato *System on a Chip (SoC)* de *smartphones* han desempeñado un papel clave al contribuir significativamente a la consecución de estos objetivos.

La arquitectura *Advanced RISC Machine (ARM)*, licenciada por *ARM Holdings*, cumple con los requisitos al ofrecer procesadores pequeños, potentes, económicos y de bajo consumo. Una ventaja adicional radica en

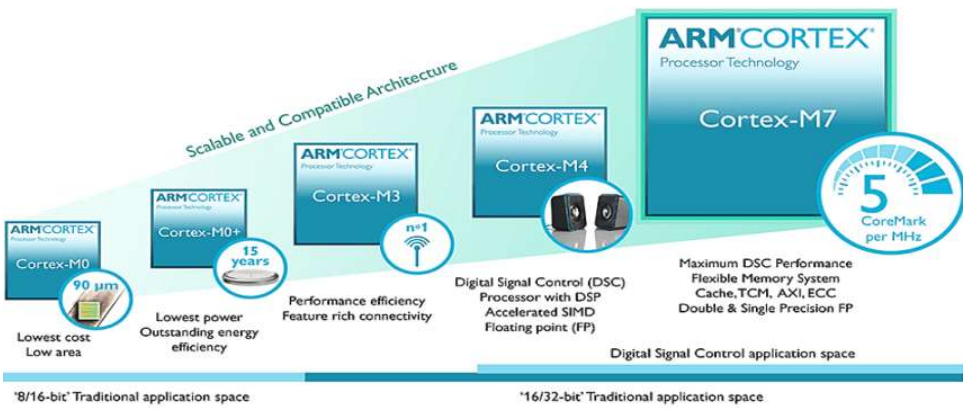
que *ARM Holdings* diseña los procesadores, pero no se encarga de su fabricación; en cambio, licencia su producción, facilitando así una rápida adopción en diversos dispositivos.

Actualmente, existen diversas familias de procesadores ARM, como ARM7, V8, ARM9, ARM 11, y *Cortex*, entre otras. En el ámbito del IoT, las arquitecturas Cortex destacan, siendo ejemplos notables *Cortex-R*, integrado en dispositivos como discos duros o en la industria automotriz, y *Cortex-M*, reconocidos por su utilidad en dispositivos finales más próximos al usuario, como termostatos, altavoces y dispositivos cuantificadores. La arquitectura *CORTEX de ARM* se integra en una amplia gama de objetos.

Aunque ARM ha liderado este sector, otras empresas con experiencia en el desarrollo de microprocesadores y microcontroladores también han lanzado sus propias arquitecturas. Intel presenta la arquitectura *Quark*, mientras que *Qualcomm* cuenta con líneas específicas de su gama *Snapdragon* dedicadas al IoT. En la Figura 1.5, que se presenta en la página siguiente, se ilustra la familia de procesadores ARM Cortex Serie M, destacando sus características y aplicaciones principales.

Figura 1.5

Familia de procesadores ARM Cortex serie



Fuente: (ARM, 2024)

Una característica fundamental del IoT reside en su capacidad de supervisión a través de **sensores**. Estos dispositivos destacan por su habili-

dad para observar y analizar el entorno en constante evolución. La utilización de sensores, elementos de hardware que actúan como intermediarios entre la tecnología y el entorno, resulta clave para capturar toda la información requerida por el software.

Actualmente, se encuentra en el mercado una amplia variedad de sensores, que abarcan desde opciones más simples, como ultrasonidos, sensores de luz o de distancia, hasta modelos más sofisticados como sensores táctiles, acelerómetros, de inclinación, potenciómetros, de humedad y temperatura, altitud, presión, entre otros. En otras palabras, para medir cualquier magnitud, es probable que exista un sensor correspondiente en el mercado.

La evolución de los sensores también ha sido necesaria para adaptarse a los requisitos impuestos por la IoT. Su principal transformación ha radicado en la facilidad para conectarse a través de Internet de manera ubicua y económica. La reducción de costos ha sido un factor clave en este proceso evolutivo. Es importante señalar que esta conectividad inalámbrica no se limita únicamente a los sensores, ya que diversos dispositivos de bajo coste, todos interconectados, enriquecen los datos básicos al agregar contexto, como la geolocalización, trascendiendo así la simple recopilación de datos.

Por otra parte, los **actuadores** tienen la capacidad de recibir instrucciones a través de Internet y generar cambios en el entorno mediante la activación de elementos como interruptores simples, solenoides, ajustes de equipos y transductores más avanzados. Estos últimos transforman las señales digitales en respuestas automáticas, adaptándose a las condiciones identificadas por el software que opera en las fuentes de datos del sensor. Aunque esta funcionalidad en sí misma no constituye una innovación radical, la mayor disponibilidad de dispositivos a un costo considerablemente menor, junto con una implementación más sencilla, facilita su adopción y aplicación.

Un nivel de automatización relativamente elevado ya se encuentra al alcance de pequeñas y medianas empresas que carecen de un equipo de

expertos técnicos. En el proceso de selección de sensores, diversos factores de gran impacto deben ser considerados, tales como la finalidad del sensor (temperatura, movimiento, etc.), su precisión, confiabilidad, rango, resolución y nivel de inteligencia para lidiar con interferencias y ruido.

Finalmente, las fuerzas impulsoras detrás del empleo de sensores IoT hoy en día están vinculadas a las tendencias emergentes en la tecnología, que están dando lugar a sensores más asequibles, inteligentes y compactos.

Todos estos elementos previamente citados requieren de **comunicaciones de bajo consumo** las tecnologías inalámbricas destinadas a dispositivos móviles, como GPRS/3G/4G/LTE, Wi-Fi o Bluetooth, requieren una integración con nuevas infraestructuras de red para hacer frente al crecimiento significativo de objetos conectados y aplicaciones M2M *(Machine To Machine)*. Específicamente, estas redes inalámbricas diseñadas para IoT deben cumplir con cuatro principios fundamentales:

a. Banda de frecuencia ultraestrecha para una capacidad de datos reducida.

b. Consumo eficiente de batería para garantizar una duración prolongada.

c. Alcance extenso para abarcar distancias considerables.

d. Costos reducidos de los módulos para fomentar la accesibilidad y la adopción generalizada.

En la tabla 1.1 se muestra las características de las redes LPWAN *(Low Power Wide Area)*.

Tabla 1.1

Requisitos/Características de una LPWAN

Requisito / Característica	Respuesta / Valor adecuados
Banda Ultra-Estrecha	200 bytes diarios y 50 Kbps de transferencia instantánea y pequeños paquetes de datos (de 12 a 255 bytes) la mayoría tráfico ascendente.

Bajo Consumo Energético	Varios años de batería (normalmente hasta 20 años).
Largo alcance o cobertura	0 - 5 Km. en áreas urbanas pobladas, 10-65 km. En áreas abiertas.
Hardware de bajo coste.	En torno a 1€ anual por mantenimiento del dispositivo.

Además de las mencionadas características, la propuesta destaca por su facilidad de instalación, su flexibilidad y capacidad de adaptación. Se presenta como una solución bidireccional, con una penetración notable, garantizando seguridad y encriptación. Esta propuesta se integra de manera complementaria con otras tecnologías disponibles.

Dentro del ámbito de las redes de área amplia de baja potencia (LPWAN), se encuentran diversas tecnologías que abordan distintos aspectos de la conectividad para aplicaciones de IoT.

LoRa *(Long Range).* - Es una especificación de LPWAN que ofrece tasas de datos bajas oscilando desde 0.3 kbps hasta 50 kbps, diseñada para facilitar comunicaciones bidireccionales. Su aplicación principal se centra en servicios de movilidad y localización en entornos de ciudades inteligentes.

***nWave.* -** Se trata de una tecnología propietaria diseñada específicamente para aplicaciones de IoT con altos volúmenes, buscando lograr una penetración efectiva en edificaciones extensas y un alcance considerable, al mismo tiempo que minimiza el consumo de energía de los dispositivos.

***OnRamp*/RPMA. -** Esta tecnología propietaria se orienta a proporcionar un servicio escalable de comunicación para sensores, priorizando una cobertura máxima y soluciones de geoposicionamiento efectivas.

***PicoWAN.* -** Basada en LoRa, su principal innovación radica en ofrecer un protocolo de red de radiofrecuencia mediante pico-puertas de enlace integradas en forma de enchufes inteligentes. Su enfoque se caracteriza por ser colaborativo, global, sin restricciones geográficas y accesible a un precio reducido.

***SigFox.* -** Se trata de una tecnología de IoT que opera con baja energía,

banda ultraestrecha y un enfoque similar al celular. Ampliamente adoptada, está licenciada por la empresa francesa del mismo nombre.

Weightless. - Este estándar abierto para IoT utiliza tecnología de banda ultraestrecha en la banda ISM (Industrial, Scientific and Medical), ofreciendo una opción versátil para la conectividad en este ámbito.

NarrowBand IoT (NB-IoT). - Este estándar LPWAN para IoT opera a velocidades de hasta 250 kbps y se centra principalmente en proporcionar cobertura en interiores, con un enfoque en la economía de costos, una larga duración de batería y la capacidad de conectar un gran número de dispositivos.

1.2.3 Normas y control

El IoT es un campo en expansión con repercusiones en diversos sectores, incluyendo la educación, las empresas, la industria, el entretenimiento, la transmisión, las infraestructuras y la asistencia sanitaria, entre otros. Para establecer un marco integral para el IoT que abarque dispositivos heterogéneos y cuente con respaldo tecnológico, se hace necesaria la interoperabilidad entre productos, aplicaciones y servicios evitando así bloqueos entre proveedores. En la era actual de la revolución digital, donde numerosos vendedores y compradores muestran un marcado interés, y donde investigadores y empresarios dedican esfuerzos significativos al desarrollo de soluciones, así como agencias gubernamentales se esfuerzan por conectar con sus ciudadanos, se vuelve imperativo que el mundo establezca un estándar común. Esta normalización no debería limitarse únicamente a los componentes de hardware, sino que también debería abarcar los aspectos de software mediante la creación de interfaces de programación estandarizadas y servicios de software. De esta manera, las aplicaciones futuras podrían implementarse en un entorno uniforme facilitando así la migración sin complicaciones entre sistemas.

La estandarización resulta imperativa para garantizar diversos aspectos fundamentales:

La **interoperabilidad** entre productos, aplicaciones y servicios, eliminando la dependencia de proveedores. La consecución de **economías** de escala, beneficiando a las tres secciones de la sociedad (desarrollador o investigador, gobierno o entidad reguladora, y usuario) en un plazo razonable. La **preservación** de la seguridad y **privacidad** de los datos y de los usuarios.

La **creación** de un espacio propicio para que los investigadores impulsen nuestra sociedad hacia niveles superiores. La **facilitación** de la interoperación a través de sistemas de comunicación física, sintaxis de protocolos, semántica de datos y conocimiento sobre el dominio.

El enfoque principal del IoT reside en la capacidad de controlar y supervisar diversos elementos a través de dispositivos informáticos interconectados mediante una red de conmutación de paquetes. Para lograr una implementación exitosa de la IoT, es necesario abordar ciertos impulsores tecnológicos clave que se beneficiarán considerablemente de la estandarización. Estos factores incluyen la mejora de la **conectividad** en aspectos como velocidad de datos, disponibilidad y costo; la **adopción** generalizada del Protocolo de Internet como el principal mecanismo de direccionamiento para los dispositivos conectados; la **miniaturización** de los dispositivos de cómputo y comunicación, acompañada de una disminución en los costos asociados; el progreso en el **análisis de datos**; y el aumento de la presencia de la **computación en la nube** simultáneamente con la reducción de costos en los sistemas de almacenamiento.

En consideración a lo anteriormente expuesto, se presenta una categorización de los desafíos asociados con la estandarización en el ámbito del IoT:

Conectividad. - La tarea de conectar miles de millones de dispositivos o elementos representa un desafío significativo. La conectividad influye en la escala del negocio, el margen de beneficio y el impacto social de las operaciones. A pesar de la predominancia de los despliegues basados en la nube en el mundo de IoT, los despliegues en los bordes están ganando terreno debido a la baja latencia, la facilidad de despliegue, una mayor seguridad y

privacidad, así como una alta agregación de datos.

Interoperabilidad. - Con el IoT expandiéndose en diversas direcciones y diferentes tecnologías desempeñando roles distintos, lograr una conectividad fluida entre dispositivos que operan con tecnologías diferentes se presenta como un desafío considerable. La interoperabilidad en las capas superiores de la pila de protocolos de red, con operaciones semánticas y específicas de dominio, constituye otro desafío relevante.

Análisis. - Uno de los aspectos fundamental de IoT consiste en obtener información y actuar en base a ella. En este sentido, el análisis de los datos de la IoT juega un papel importante. La utilización práctica de una plataforma analítica dentro de la arquitectura de IoT representa la principal problemática en cualquier despliegue. La toma de decisiones sobre la ubicación apropiada de las partes de la plataforma de análisis, considerando factores como el retraso las cuestiones reglamentarias, el costo, la escala y la facilidad de funcionamiento, resulta un aspecto base a considerar (Marjani, y otros, 2017).

Seguridad y privacidad. - Se ha observado que los despliegues de IoT enfrentan desafíos significativos en términos de seguridad y privacidad a nivel de dispositivo, borde y plataforma en la nube. Por tanto, la seguridad y privacidad de los datos, dispositivos aplicaciones y servidores deben ser consideradas al determinar la arquitectura de implementación adecuada. En lugar de ser consideradas como consideraciones secundarias, en la actualidad, la seguridad y privacidad son preocupaciones primordiales para cualquier tipo de despliegue.

Negocio o Retorno de la Inversión (ROI). - La decisión de despliegue puede impactar los mercados verticales, horizontales y de consumo de la industria del IoT, mientras se enfrenta a aspectos reglamentarios y legales. Según el uso del despliegue y la base de clientes, IoT se distribuye en categorías como IoT de consumo, industrial y comercial, cada una con su impacto específico en la sociedad.

Sociedad. - Los desafíos sociales desempeñan un papel fundamental en el

despliegue del IoT, ya que es necesario satisfacer las necesidades de clientes, desarrolladores y reguladores. Esto abarca aspectos como el estilo de vida, el consumo de energía, el impacto ambiental y social, entre otros.

En la actualidad, diversas industrias y ámbitos académicos han desarrollado soluciones propias, ejemplificadas por empresas líderes como CISCO, **Microsoft,** IBM, entre otras, con el propósito de abordar los desafíos previamente mencionados. No obstante, a nivel global los organismos de normalización se esfuerzan por colaborar en la búsqueda de una solución integral para la implementación sin inconvenientes del IoT.

Desde la perspectiva de la oferta tecnológica, los diversos empeños pueden ser divididos en dos categorías: genéricos y específicos de aplicación.

En la primera clasificación, los esfuerzos genéricos, representados por entidades como IEEE, IETF, 3GPP y *oneM2M*, han tradicionalmente desempeñado un papel importante en la formulación de estándares tecnológicos que abarcan el ámbito problemático en general. Estos organismos han delineado políticas o arquitecturas de referencia genéricas, proporcionando protocolos estándar para facilitar la comunicación. Además, especifican el ámbito tecnológico, como lo ejemplifica el IEEE con más de 110 nuevas normas relacionadas con IoT en diversas fases de desarrollo, junto con otras 40 normas en revisión. Paralelamente, los esfuerzos de desarrollo impulsados por organismos de normalización independientes, como la Organización Internacional de Normalización (ISO), están ganando gradualmente influencia.

Por último, surgen también organizaciones o alianzas con la finalidad de estandarizar tecnologías específicas para dominios particulares de aplicaciones. Estos esfuerzos se basan esencialmente en arquitecturas existentes y ofertas de protocolos con un enfoque genérico para establecer el modelo de comunicación. Dichas entidades generan estándares específicos para modelos de intercambio particularizados, colmando las brechas típicas en las ofertas estándar disponibles. Estas alianzas también promueven la

colaboración entre diferentes industrias, asegurando que las soluciones desarrolladas sean interoperables y puedan ser adoptadas globalmente.

1.3 Elementos y partes en la implementación de una red IoT

Este grupo de elementos se dispone en una estructura que permite la aplicación de diversas tecnologías específicas para cada una de las capas. Dentro de estas capas, algunas son consideradas transversales u horizontales, dado que impactan en todos los módulos que conforman la arquitectura en sí misma.

1.3.1 Atributos presentes en una implementación de Internet de las cosas (IoT)

Un despliegue de IoT comprende una amalgama de elementos tanto horizontales como verticales que son compartidos entre diversas plataformas de IoT, y que pueden ser implementados mediante tecnologías variadas. En primer lugar, se debe examinar las características y los requisitos que deben cumplir cada una de las capas involucradas. Estas capas incluyen la capa de dispositivos, que abarca sensores y actuadores; la capa de comunicación, que utiliza tecnologías como Wi-Fi, *Bluetooth* y redes celulares; y la capa de procesamiento, que involucra la recolección y análisis de datos en tiempo real. Adicionalmente, es crucial considerar la capa de aplicación, donde se desarrollan las interfaces de usuario y las funcionalidades específicas del sistema IoT. La interoperabilidad entre estas capas es esencial para garantizar un funcionamiento fluido y eficiente.

Entre estos requisitos, hay algunos específicos que se aplican exclusivamente a los dispositivos IoT o a los entornos que los respaldan. Sin embargo, también existen enfoques que se asemejan más a los diseños convencionales de productos de consumo que a los enfoques típicos de Internet. Naturalmente, hay una serie de mejores prácticas establecidas para el lado del servidor y la conectividad a Internet que deben tenerse en cuenta. En la Figura 1.6 se muestran los requisitos fundamentales que una plataforma de IoT debe poseer. proporcionando una visión clara de los componentes necesarios para un despliegue exitoso.

Figura 1.6

Requisitos de una Plataforma IoT

A continuación se describe cada uno de los requisitos:

Conectividad y Comunicaciones.- Los protocolos convencionales como HTTP desempeñan un papel fundamental en la funcionalidad de numerosos dispositivos, incluso aquellos con capacidades limitadas, como controladores de 8 bits, que pueden generar solicitudes GET y POST de manera sencilla. HTTP ofrece una conectividad unificada y uniforme. Sin embargo, la complejidad operativa inherente a protocolos como HTTP puede resultar en una carga excesiva para dispositivos con limitaciones de recursos, como memoria y capacidad de procesamiento.

Sin embargo, el principal desafío se encuentra en los requisitos energéticos. Para abordar este aspecto, se requiere un protocolo que sea sencillo y efi-

ciente, al mismo tiempo que permita la implementación de medidas de seguridad como cortafuegos y cifrado.

Al analizar las diversas opciones de implementación, se distinguen dispositivos que se conectan de manera directa y aquellos que requieren una pasarela intermedia. Los dispositivos que se vinculan a través de una pasarela potencialmente necesitan dos protocolos: uno para la conexión con la pasarela y otro para la comunicación desde la pasarela hacia la nube.

Por último, es importante que la arquitectura sea compatible con la diversidad de protocolos de transporte y conexión. Por ejemplo, se podría optar por un protocolo binario para la comunicación con el dispositivo, pero simultáneamente habilitar una API basada en HTTP para gestionar el acceso al dispositivo por parte de terceros.

La **gestión de dispositivos.-** Aunque actualmente muchos dispositivos de IoT operan sin una gestión unificada, esta situación puede no ser la más óptima. Se ha observado que la gestión unificada y proactiva de computadoras, teléfonos móviles y otros sistemas electrónicos está adquiriendo una creciente importancia. Es probable, y deseable, que esta misma tendencia se aplique a los dispositivos de IoT en el futuro. Dentro de la gestión de dispositivos existe unos requisitos específicos que se enlistan a continuación.

- Capacidad de desconectar un dispositivo en caso de robo o fraude, incluso sin tener acceso físico al mismo.
- Capacidad de actualizar el software de los dispositivos para garantizar su funcionamiento óptimo y la seguridad.
- Actualización periódica de las credenciales de seguridad para proteger los dispositivos contra amenazas cibernéticas.
- Capacidad de activar o desactivar ciertas funciones de hardware de forma remota según sea necesario.
- Capacidad de localizar dispositivos perdidos para facilitar su recuperación.

- Opción de eliminar de manera segura los datos almacenados en un dispositivo robado para proteger la información sensible.

- Posibilidad de reconfigurar los parámetros de comunicación de forma remota para adaptarse a diferentes escenarios.

Es importante destacar que esta lista no es una "camisa de fuerza" y que algunos de estos requisitos pueden no ser aplicables o necesarios en todos los casos, dependiendo del contexto y del tipo de dispositivo de IoT en cuestión.

La recolección, análisis y actuación de datos.-Algunos dispositivos de IoT pueden contar con una interfaz de usuario, pero su enfoque primordial radica en la provisión de sensores, actuadores o una combinación de ambos. La premisa fundamental es la capacidad de recopilar, almacenar y analizar una cantidad significativa de datos para luego emprender acciones correspondientes.

Una implementación estructurada de IoT está concebida para administrar una gran cantidad de dispositivos. Si estos dispositivos generan flujos continuos de datos, ello implica una considerable acumulación de información. Es importante contar con un sistema de almacenamiento escalable capaz de manejar datos diversos y volúmenes masivos.

Por otro lado, dado que se requiere que las acciones sean prácticamente instantáneas, surge una fuerte necesidad de análisis en tiempo real, e incluso de procesamiento de datos en flujo continuo a medida que se reciben. Por último, el dispositivo debe tener la capacidad de analizar y responder a los datos. En algunos casos, esta tarea puede ser simple, utilizando lógica básica integrada. Sin embargo, en dispositivos más potentes, se pueden emplear motores de procesamiento de eventos más sofisticados para llevar a cabo acciones más complejas.

La **escalabilidad.-** Se busca que cualquier desarrollo realizado en el servidor tenga la capacidad de adaptarse y manejar eficientemente una gran cantidad de dispositivos que interactúan constantemente con los datos.

Sin embargo, alcanzar altos niveles de escalabilidad implica una inversión significativa tanto en hardware como en software, además de requerir un nivel técnico complejo y personal altamente especializado. Un aspecto fundamental para la implementación es garantizar la capacidad de escalar desde un despliegue inicial pequeño hasta un número considerable de dispositivos. La capacidad de adaptación elástica y la opción de despliegue en una infraestructura en la nube se vuelven claves. Asimismo, la posibilidad de escalabilidad en servidores pequeños y económicos se convierte en un requisito obligatorio para hacer que esta arquitectura sea accesible tanto para despliegues de pequeña escala como para aquellos de mayor envergadura.

La **seguridad** representa un elemento fundamental en el ámbito del IoT. Los dispositivos IoT, al recolectar datos personales, intrínsecamente fusionan el mundo físico con el ciberespacio. Este contexto presenta tres categorías de riesgos. En primer lugar, los riesgos genéricos asociados a cualquier sistema en línea, los cuales pueden pasar desapercibidos para los diseñadores de productos IoT. Por ejemplos incluyen la falta de seguridad en puertos abiertos, como en el caso de una lavadora conectada a la red que pueda ser aprovechada para enviar spam debido a un servidor de correo no protegido.

En segundo lugar, existen riesgos específicos propios de los dispositivos IoT, vinculados a cuestiones de hardware. Por ejemplo, la posibilidad de que un dispositivo sea vulnerable a la lectura de información confidencial debido a una deficiente seguridad física, a pesar de contar con encriptación adecuada para las comunicaciones. Además, la ingeniería inversa puede ser empleada para identificar debilidades de seguridad y obtener acceso a contenido sensible.

Se debe considerar la seguridad para prevenir daños provocados por un uso inadecuado de los actuadores, como en el caso de un mal funcionamiento que resulte en daños físicos o económicos. Además de los aspectos previamente mencionados, también se presentan deficiencias en cuanto a la gestión de la identidad y el acceso. La identificación a menudo se ve

comprometida por prácticas inadecuadas, como el empleo de texto plano para contraseñas y el uso de codificación Base64 para autenticación de dispositivos y comunicación máquina a máquina.

En la actualidad, se recomienda optar por sistemas de *tokens* gestionados y otros modelos avanzados como el acceso basado en atributos y el uso de políticas. El estándar XACML es ampliamente reconocido en este sentido, según (Ammar, Malik, Rezgui, & Bertino, 2016). Estos métodos desvinculan las decisiones de control de acceso de la lógica codificada, permitiendo:

- Decisiones más contundentes y adecuadas.
- Podrían fundamentarse en variables como la ubicación, la red utilizada o el momento del día.
- La supervisión del acceso puede ser examinada y evaluada.
- Las directrices pueden ser modificadas y ajustadas, incluso de manera dinámica, sin necesidad de reprogramar o alterar dispositivos.

Dadas estas debilidades, nuestros requisitos de seguridad deben respaldarse en herramientas específicas:

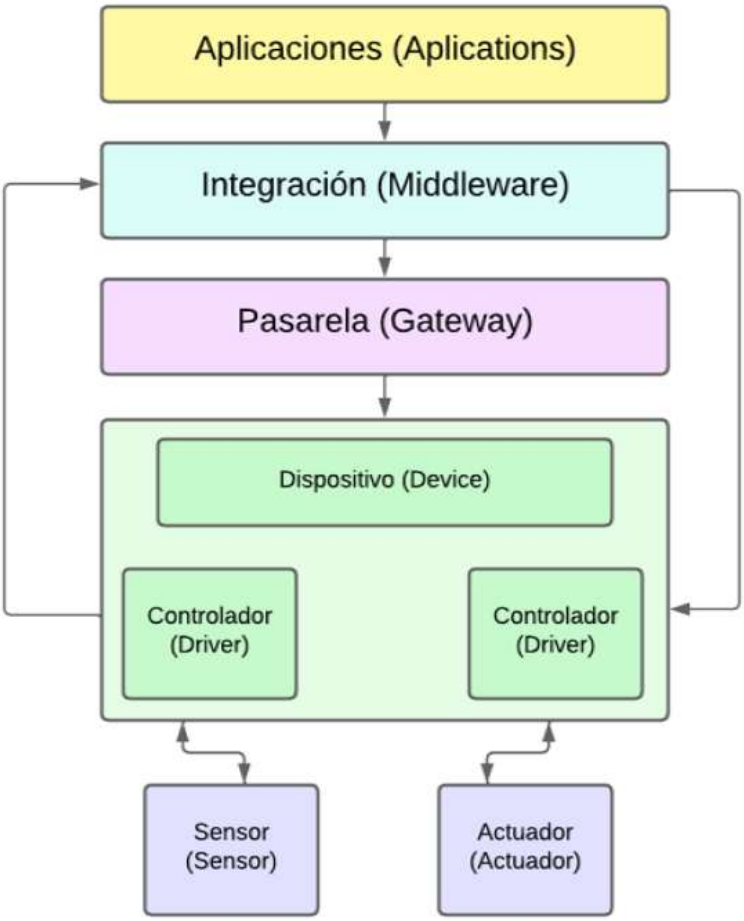
- Implementación de cifrado en dispositivos con suficiente potencia.
- Adopción de un moderno modelo de identidad basado en tokens en lugar de nombres de usuario y contraseñas.
- Gestión de claves y *tokens* de forma remota y sencilla.
- Utilización de un sistema de control de acceso basado en políticas gestionadas por el usuario, siguiendo el estándar XACML.

1.3.2 Capas y Componentes

Este apartado se enfoca en la configuración de un despliegue de IoT delineando los elementos más usuales que conforman el conjunto de capas existentes. En la Figura 1.7 se presentan las capas inmersas en un despliegue IoT.

Figura 1.7

Capas de despliegue IoT



A continuación, se describe cada uno de los elementos inmersos en las capas de un despliegue IoT desde el primer nivel donde están los sensores y actuadores hasta el nivel más alto que son las aplicaciones.

Un **sensor**, en términos de hardware, es un dispositivo que adquiere datos del entorno físico detectando estímulos como temperatura, luz, sonido, presión, magnetismo o movimientos específicos. Estos dispositivos transmiten la información recopilada a través de señales eléctricas hacia los dispositivos a los que están vinculados, pudiendo establecer esta conexión mediante cables o de manera inalámbrica. Aunque pueden configurarse mediante software, los sensores no son capaces de ejecutar dicho software de

forma autónoma.

Por otro lado, un **actuador** es un componente de hardware que posee la capacidad de alterar el entorno físico. Al recibir comandos del dispositivo al que está conectado, los actuadores transforman estas señales eléctricas en acciones físicas específicas. Al igual que los sensores, la conexión a los dispositivos puede ser cableada o inalámbrica, integrándose así en el dispositivo. Asimismo, aunque pueden ser configurados mediante software, los actuadores no pueden ejecutarlo por sí mismos.

Un **dispositivo**, como componente hardware, se conecta a sensores y/o actuadores, ya sea mediante cable o de forma inalámbrica, e incluso puede integrar otros elementos diversos. Equipados con un procesador y capacidad de almacenamiento, los dispositivos ejecutan software y se conectan al middleware de integración. De esta manera, actúan como el punto de entrada del mundo físico al mundo digital, pudiendo comunicarse directamente con el middleware si poseen la tecnología de comunicación adecuada, o a través de una pasarela en caso contrario.

El **controlador**, por su parte, es un software que opera en el dispositivo y facilita el acceso uniforme a sensores y actuadores de diferentes tipos. Los dispositivos pueden ser independientes o estar conectados a un sistema más amplio.

Una **pasarela** *(o gateway)* proporciona los recursos necesarios para traducir entre distintos protocolos, tecnologías de comunicación y formatos de datos.

El **middleware** sirve como una capa de integración para una variedad de sensores, actuadores, dispositivos y aplicaciones, gestionando la recepción, procesamiento y distribución de datos, así como la gestión de dispositivos y usuarios, y la agregación y utilización de datos recibidos.

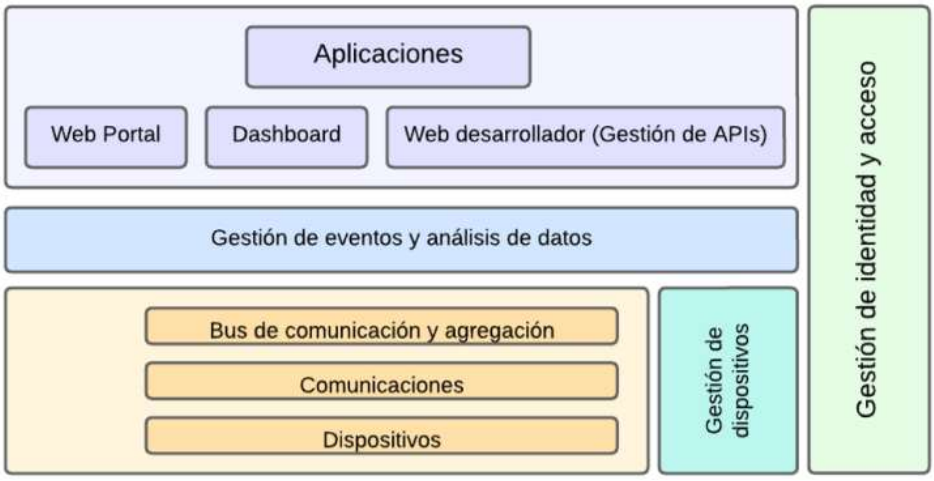
El componente de **aplicación** representa un software que utiliza el middleware de integración de IoT para obtener información del entorno físico o controlarlo, ya sea solicitando datos de sensores o manipulando ac-

ciones físicas a través de actuadores. Esta aplicación también puede funcionar como otro middleware de integración de IoT.

La Figura 1.8 muestra un modelo común de despliegue por capas para sistemas de IoT, que abarca los componentes principales de este tipo de infraestructura. Sin embargo, es importante destacar que no todos los despliegues incorporan necesariamente todos estos componentes, y es probable que también se agreguen otros según las exigencias específicas. La selección de los componentes a utilizar estará estrechamente ligada a los requisitos y circunstancias particulares de cada situación y aplicación como se ha mencionado anteriormente.

Figura 1.8

Desarrollo de un despliegue IoT por capas



Fuente: Adaptado de: (Fremantle, 2015)

De igual manera se describen a continuación cada uno de los elementos inmersos en este ejemplo de despliegue.

Los **dispositivos** en el contexto de IoT abarcan una variedad de tipos, pero para ser considerados como tales, deben ser capaces de facilitar algún modelo de comunicación que les permita conectarse a Internet, ya sea de forma directa o indirecta. Estos dispositivos alojan tanto sensores como, en ocasiones, actuadores, pudiendo inclusive formar una red inalám-

brica de sensores a la que se conectan. Cada dispositivo por lo general requiere una identidad, que puede manifestarse como un identificador único asociado a la electrónica del dispositivo, un UUID proporcionado por el subsistema de conexión, un *OAuth2 Refresh* mediante *Bearer Token* (que a su vez puede combinarse con las opciones anteriores), o un identificador almacenado en memoria no volátil.

En lo que respecta a las **comunicaciones**, la capa correspondiente facilita la conectividad entre los dispositivos y la nube. Existen múltiples protocolos potenciales para esta comunicación, destacándose tres combinaciones como las más utilizadas y prometedoras:

a. HTTP/HTTPS, con enfoques *RESTful* sobre estos. Aunque HTTP es ampliamente conocido y soportado por muchas bibliotecas, su protocolo basado en texto puede ser limitado para dispositivos más pequeños. Sin embargo, dispositivos de 32 bits más grandes pueden hacer uso de bibliotecas completas de cliente HTTP.

b. MQTT, un protocolo optimizado para IoT que opera sobre TCP. Basado en un modelo de publicación-suscripción, MQTT minimiza la sobrecarga y fue diseñado para redes con pérdidas y conexiones intermitentes.

c. CoAP, otro protocolo diseñado para IoT que trabaja sobre UDP. Aunque sigue un enfoque más tradicional cliente-servidor en comparación con MQTT, proporciona una sobrecarga más pequeña y un formato binario.

Aunque MQTT cuenta con un mayor soporte y bibliotecas disponibles en comparación con CoAP ambas opciones tienen sus propias fortalezas y debilidades que deben considerarse. Por lo tanto, la elección del protocolo de comunicación dependerá de las necesidades específicas de cada caso.

Para admitir MQTT, es necesario contar con un *broker* MQTT en el despliegue, así como con librerías específicas para integrar los dispositivos. Un aspecto clave en IoT es la bidireccionalidad de la comunicación, donde MQTT se destaca al seguir un modelo de intermediario que facilita

las conexiones tanto de publicadores como de suscriptores.

En el caso de una comunicación principal basada en HTTP, es importante considerar que el método tradicional de sondeo puede ser ineficiente y costoso en términos de tráfico de red y consumo de energía. Una alternativa moderna es el protocolo *WebSocket*, que permite actualizar una conexión HTTP a una bidireccional completa, actuando como un canal de socket entre el servidor y el cliente. En este sentido, MQTT también se beneficia al ser utilizado a través de *WebSockets*, siendo en algunos casos la única opción viable debido a su compatibilidad con cortafuegos y clientes de navegador/JavaScript puros.

Sin embargo, es importante tener en cuenta que el uso de WebSockets puede ser limitado en dispositivos de 8 bits debido al espacio de código disponible, por lo que se recomienda su implementación solo en dispositivos más grandes de 32 bits.

La implementación de un sistema de **comunicaciones y agregación** en un entorno de despliegue tecnológico se destaca por su relevancia en tres aspectos fundamentales. En primer lugar, esta capa es clave por su capacidad para sostener diversos sistemas de intermediación del lado del servidor, como servidores HTTP, *brokers* MQTT, entre otros. Estos sistemas facilitan la comunicación con dispositivos dentro de la red. En segundo lugar, esta capa permite la combinación y dirección de comunicaciones provenientes de distintos dispositivos hacia destinos específicos, posiblemente a través de una pasarela, lo que mejora la eficiencia y la gestión del flujo de datos.

Por último, la capa de agregación/bus desempeña un papel fundamental en la interoperabilidad entre diferentes protocolos, facilitando la conexión y la transformación de datos entre ellos, incluso en entornos que utilizan protocolos heredados.

Además de estas funciones principales, la capa de agregación/bus debe garantizar la seguridad del sistema en dos aspectos. Primero, actuando como servidor de recursos de autenticación, validando *tokens* portadores y controlando los alcances de acceso a recursos asociados. Segundo, funcio-

nando como punto de aplicación de políticas de acceso, donde las solicitudes de acceso son validadas por la capa de gestión de identidades y accesos, que actúa como punto de decisión política. posteriormente la capa de bus implementa los resultados de estas validaciones para permitir o denegar el acceso a los recursos según corresponda.

Procesamiento de eventos y capa de análisis, esta capa se encarga de gestionar los eventos del bus y ofrece la capacidad de analizarlos y actuar en consecuencia. Una funcionalidad central es la necesidad de almacenar los datos en una base de datos, lo cual puede llevarse a cabo de dos maneras distintas. En primer lugar, el enfoque tradicional implica asociar esta tarea a una aplicación en el servidor, aunque cada vez más se recurre a métodos más ágiles como el uso de plataformas robustas de análisis de datos en la nube. Estas plataformas, escalables y en la nube, admiten tecnologías como *Apache Hadoop, Spark, Tensorflow,* entre otras, para llevar a cabo análisis mediante técnicas como *MapReduce* y otras más complejas, con el fin de extraer conocimiento de los datos provenientes de los dispositivos.

Por otro lado, el segundo enfoque consiste en respaldar el procesamiento de eventos complejos para iniciar actividades y acciones casi en tiempo real, basándose en los datos de los dispositivos y del sistema en su conjunto, siguiendo un modelo de flujo de datos. Habitualmente, se pueden emplear distintos métodos, como el almacenamiento de datos altamente escalable basado en bases de datos no relacionales, sistemas de análisis basados en MapReduce u otro enfoque similar para el procesamiento a largo plazo orientado a lotes, así como el procesamiento de eventos complejos para una rápida respuesta en memoria, lo que posibilita acciones casi en tiempo real basadas en la información deducida de la actividad de los dispositivos y otros sistemas. Finalmente, esta capa puede soportar plataformas de procesamiento de aplicaciones tradicionales, como *Java Beans, lógica JAX-RS, node.js, PHP, Ruby o Python,* entre otras.

Capa de **aplicaciones**, el despliegue de sistemas debe incluir funcionalidades para facilitar la comunicación de los dispositivos más allá del entorno del sistema. Para cumplir con este propósito se identifican varias

necesidades clave

- Creación de interfaces y portales basados en web para permitir la interacción con los dispositivos y la capa de procesamiento de eventos.

- Desarrollo de cuadros de mando que presenten análisis y procesamiento de eventos de manera accesible.

- Integración con sistemas externos a través de comunicaciones M2M mediante APIs, las cuales requieren gestión y control mediante un sistema dedicado.

En lo que respecta al diseño del *front end* de la web, la estrategia predominante implica adoptar una arquitectura modular, como un portal, que facilita la rápida y sencilla composición de interfaces de usuario funcionales. Por otro lado, los *dashboards* representan sistemas reutilizables focalizados en la generación de gráficos y otras visualizaciones de datos derivados tanto de los dispositivos como de la capa de procesamiento de evento.

En cuanto a la gestión de APIs, se destacan tres funciones principales:

- Un portal centrado en el desarrollador, diferente al portal centrado en el usuario, donde los desarrolladores pueden descubrir, explorar y suscribirse a las APIs disponibles. También se brinda soporte para que los editores creen, versionen y administren las APIs.

- Una pasarela que administra el acceso a las APIs, llevando a cabo verificaciones de control de acceso para solicitudes externas y aplicando políticas de uso. Además, se encarga del enrutamiento y balanceo de carga.

- La pasarela también juega un papel fundamental al publicar los datos en la capa analítica, donde se almacenan y procesan para ofrecer informaciósobre el uso de las APIs.

La **administración de dispositivos** generalmente se lleva a cabo mediante dos componentes principales. Por un lado, está el sistema del lado

del servidor, también conocido como administrador de dispositivos, que se encarga de comunicarse con los dispositivos a través de varios protocolos y ofrece un control individual y masivo sobre ellos. Además, gestiona de manera remota el software y las aplicaciones instaladas en cada dispositivo, y puede llevar a cabo acciones como bloquear o limpiar un dispositivo si es necesario. Por otro lado, el administrador de dispositivos trabaja en conjunto con los agentes de gestión de dispositivos, los cuales son diversos debido a la amplia variedad de plataformas y tipos de dispositivos disponibles.

Una tarea importante del administrador de dispositivos es mantener una lista de identidades de dispositivos y asignarlas a sus respectivos propietarios. Esto implica trabajar con la capa de administración de acceso e identidades para gestionar los controles de acceso de los dispositivos. En cuanto a la clasificación de los dispositivos, se pueden distinguir tres niveles: totalmente gestionados, no gestionados y semigestionados.

Los dispositivos totalmente gestionados son aquellos que ejecutan un agente de gestión de dispositivos completo, el cual permite diversas funciones como la gestión de software, la habilitación o deshabilitación de funciones del dispositivo, el control de seguridad e identificación, la supervisión de la disponibilidad del dispositivo, el seguimiento de su ubicación y la capacidad de bloquearlo o limpiarlo de forma remota en caso de compromiso.

Los dispositivos no gestionados pueden conectarse a la red, pero no cuentan con ningún agente de gestión. Por lo general, estos dispositivos son aquellos que tienen limitaciones técnicas que no permiten la instalación del agente. A pesar de ello, el administrador de dispositivos puede mantener información sobre la disponibilidad y ubicación de estos dispositivos si es posible.

Los dispositivos semigestionados son aquellos que implementan algunas partes del sistema de gestión de dispositivos, pero por lo general no incluyen la gestión de software.

En la actualidad, no existe un estándar universal para la gestión de

dispositivos IoT, y muchos fabricantes optan por implementar sus propios protocolos de gestión. Sin embargo, tres protocolos son notablemente relevantes, siendo el más reciente (LWM2M) el que está ganando más importancia últimamente:

TR-069.- Este protocolo, también conocido como CWMP, es un estándar técnico del DSL Forum *(ahora Broadband Forum)* que define un protocolo de abstracción para el mantenimiento remoto de dispositivos de usuario final, especialmente adecuado para routers y dispositivos de red fija.

OMA-DM: Es un estándar definido por la *Open Mobile Alliance* (OMA) dirigido principalmente a terminales de telefonía móvil, aunque también puede aplicarse a dispositivos IoT más potentes.

LWM2M *(Lightweight Machine-to-Machine)***:** Sucesor de OMA-DM, este protocolo fue diseñado específicamente para ser ejecutado en dispositivos IoT con recursos limitados, y está ganando popularidad rápidamente en el ámbito de la gestión de dispositivos.

La capa final de sistema es la **gestión de identidades y accesos**, que despliega una serie de servicios fundamentales. Esto incluye la emisión y validación de tokens *OAuth2*, junto con otros servicios de identidad como SAML2 SSO y *OpenID Connect,* los cuales son compatibles con la identificación de solicitudes entrantes en la capa Web. Además, se integra un directorio de usuarios, por ejemplo, LDAP, y se establece un sistema de gestión de políticas para el control de acceso, que actúa como punto de control de políticas.

Es importante tener en cuenta que la capa de identidad puede requerir otros servicios específicos para la gestión de identidades y accesos, dependiendo de las necesidades particulares de cada instancia de despliegue de la aplicación de IoT. Además, es fundamental considerar aspectos como la seguridad, la escalabilidad y la integración con sistemas existentes. mbién se debe prestar atención a la conformidad con las regulaciones de privacidad y protección de datos, garantizando así un manejo ético y legal de la información de los usuarios.

1.3.3 Guía para seleccionar una plataforma IoT

Una vez que se han examinado detalladamente los componentes primordiales de las plataformas IoT surge la cuestión fundamental: ¿Cómo determinar cuál es la plataforma más idónea para una aplicación IoT específica?

En respuesta a esta interrogante, cada sector vertical (salud, industria, energía, banca, etc.) plantea requisitos y desafíos particulares a sus expertos en tecnología. Por consiguiente, la respuesta siempre será "depende". Veamos algunos ejemplos para entenderlo mejor:

La policía municipal y los servicios de bomberos necesitarán una plataforma que asegure la comunicación efectiva entre las operaciones en el campo y los centros de comando.

Las empresas de energía y transporte buscarán soluciones robustas que protejan sus activos en terreno de condiciones climáticas adversas.

Las plataformas para el sector bancario deberán demostrar fuertes capacidades de cifrado y seguridad para salvaguardar las comunicaciones y transferencias, tanto internas como entre consumidores.

En primer lugar, es importante distinguir entre las plataformas de IoT diseñadas para empresas y las dirigidas a consumidores finales. En el ámbito empresarial, un fallo en el sistema podría acarrear enormes riesgos, inclusive económicos o de vidas humanas. En cambio, en el caso de las plataformas para consumidores, un fallo podría ser simplemente un inconveniente para el usuario final. Sin embargo, a pesar de la amplia gama de aplicaciones IoT y sus variaciones, existen elementos comunes que son esenciales al evaluar la idoneidad de una plataforma para una aplicación específica:

- Estabilidad, se debe seleccionar una plataforma respaldada por soporte a largo plazo, ya que la inversión podría correr el riesgo de perderse si el proveedor de la plataforma desaparece.

- Escalabilidad y flexibilidad, se debe garantizar que la plataforma fun-

cione de manera consistente tanto para aplicaciones pequeñas como para grandes, permitiendo así el crecimiento empresarial en respuesta a la demanda.

- Adaptabilidad, para mantenerse al día con las tecnologías, protocolos y funciones en constante evolución. Las plataformas flexibles a menudo se basan en estándares abiertos. Asimismo, es importante que la plataforma sea agnóstica en términos de red, lo que significa que pueda integrarse y operar con todos los principales sistemas tecnológicos existentes.

- Experiencia previa del proveedor, en entornos similares a la aplicación IoT a construir suele ser un indicador confiable de su capacidad para satisfacer las necesidades específicas del sistema en cuestión.

- Transparencia en el modelo de precios, que el proveedor sea transparente en cuanto a su política de precios para garantizar una relación comercial clara y sin sorpresas.

- Seguridad integral, es un aspecto crítico en cualquier sistema IoT, por lo tanto, la plataforma seleccionada debe integrar políticas de seguridad en todos los niveles para proteger la integridad de los datos y la privacidad de los usuarios.

- Agilidad en el tiempo de comercialización, una plataforma IoT adecuada puede acelerar significativamente el tiempo necesario para llevar un producto al mercado. Evaluar una estimación realista del tiempo de lanzamiento y cómo el proveedor puede contribuir a este aspecto es fundamental.

- Análisis y gestión de datos, el valor en el contexto IoT reside en la capacidad de analizar y aprovechar los datos generados. La plataforma seleccionada debe ofrecer herramientas eficaces y sencillas para realizar análisis de datos que permitan obtener información procesable para mejorar las operaciones y la experiencia del usuario.

A continuación, en el siguiente código QR se presenta el enlace a un video explicativo complementario acerca de los fundamentos y princi-

pios básicos del funcionamiento en las redes IoT.

CAPÍTULO II:
HARDWARE EN EL IoT

2.1 Introducción y Objetivos del capítulo

Los dispositivos, en conjunto con los sensores, la conectividad y las plataformas, constituyen uno de los fundamentos del Internet de las Cosas (IoT). Estos dispositivos suelen estar integrados o vinculados a diversos objetos, convirtiéndolos en "cosas" dentro del ecosistema IoT. Su función principal radica en emplear sensores y actuadores para recopilar datos sobre el entorno y tomar acciones en función de dichos datos. Es fundamental que estos dispositivos puedan transmitir esta información a un servidor o realizar algún tipo de procesamiento interno para intervenir en el entorno de manera efectiva. Durante el desarrollo de un dispositivo o la implementación de una aplicación IoT, es fundamental interactuar con el entorno cercano para recopilar datos o ajustar el entorno según nuestras necesidades. Un sensor se encarga de convertir un fenómeno físico, como la temperatura o la presión, en una señal eléctrica. Tres cualidades básicas definen un sensor de calidad: debe ser sensible al fenómeno que está midiendo, no debe verse afectado por otros fenómenos físicos y no debe alterar el fenómeno que está midiendo durante el proceso de medición.

En base a esta introducción, luego de estudiar este capítulo se lograrán los siguientes objetivos:

- Conocer los elementos básicos de la electrónica presentes en un dispositivo IoT y comprender su sincronización para cumplir con los requisitos de captura, comunicación y acción.

- Distinguir entre microprocesadores y microcontroladores, lo que facilita la identificación del contexto de aplicación de cada uno según las necesidades específicas.

- Adquirir la capacidad de categorizar los dispositivos IoT según sus características internas.

- Comprender los distintos modelos de comunicación entre dispositivos

IoT y con la plataforma de análisis.

- Explorar las opciones disponibles para la programación de dispositivos IoT a nivel de hardware (firmware).

- Conocer los ***Single Board Computer*** y su aplicación en el contexto de IoT.

- Comprender sobre la naturaleza y las características fundamentales de los sensores.

- Profundizar el mecanismo operativo de un sensor, con el propósito de seleccionar el más idóneo para cada situación y variable física a ser medida.

- Reconocer la importancia de la calibración de los sensores, así como identificar los factores que inciden en su correcto funcionamiento.

2.2 Dispositivos: Características y partes

En la etapa inicial del desarrollo de dispositivos, se emplean numerosos recursos con el objetivo de allanar el camino hacia la ingeniería subsiguiente, orientada a la producción de un producto innovador. Muchas compañías optan por crear los primeros prototipos utilizando tecnologías que pueden ser fácilmente adaptadas a la producción, y que se fundamentan en circuitos de referencia suministrados por los fabricantes de microprocesadores y microcontroladores. Estas herramientas proporcionan un conjunto completo y robusto de funcionalidades para el desarrollo y la mejora del producto hasta su introducción en el mercado.

2.2.1 Categorización

Existen diversas maneras de categorizar los distintos tipos de dispositivos disponibles en el mercado. Por ejemplo, se puede clasificar según su nivel de complejidad tecnológica de la siguiente manera:

Dispositivos de gama baja o de nivel básico.- Estos dispositivos son simples y carecen de grandes capacidades de procesamiento o almacenamiento, lo que los hace incapaces de implementar protocolos complejos de cifrado

o ejecutar aplicaciones específicas para su gestión. Por lo general, estos dispositivos son gestionados por microcontroladores como ARM-M, Texas o PIC, entre otros.

Dispositivos de gama alta o de nivel avanzado.- Son dispositivos con una gran capacidad de procesamiento, capaces de ejecutar sistemas operativos completos como Linux o Windows. Estos dispositivos suelen ser gestionados por microprocesadores como Intel, AMD o ARM-A, y generalmente están conectados a la corriente eléctrica.

En base a esta clasificación inicial, se puede identificar dos arquitecturas de computación básicas en las que se fundamentan los dispositivos diseñados especialmente para el IoT. Por un lado, están los microprocesadores (de gama alta) y, por otro lado, los microcontroladores (de gama baja). En la siguiente sección se explorarán ambas arquitecturas de hardware. La elección entre una u otra aproximación suele depender de las necesidades de energía, así como del costo y los requisitos de procesamiento del dispositivo en cuestión.

Comparación entre Microcontroladores y Microprocesadores.

Los microprocesadores son circuitos digitales programables diseñados para facilitar la ejecución de sistemas operativos convencionales completamente funcionales. Estos chips tienen una alta capacidad de procesamiento al incluir uno o más núcleos, y, fundamentalmente, posibilitan el acceso a grandes cantidades de memoria RAM mediante buses externos de conexión.

En contraste, los microcontroladores son dispositivos que integran tanto el procesador como las principales memorias de programa (ROM/FLASH) y datos (RAM) en un único chip. Son soluciones compactas, económicas y fáciles de implementar en diversas situaciones, pero ofrecen un rendimiento menor y un consumo mucho más bajo.

Esta diferencia fundamental se traduce en que los microprocesadores, presentes en dispositivos como *smartphones, tablets* y PC, requieren

la conexión externa de abundantes recursos de memoria y consumen varios vatios de energía en su funcionamiento normal. Sin embargo, ofrecen una gran capacidad de procesamiento y pueden ejecutar sistemas operativos como Linux, Android, Windows o OS X, junto con todas las aplicaciones desarrolladas para estos sistemas.

Por otro lado, los microcontroladores no cuentan actualmente con cantidades suficientes de memoria para ejecutar sistemas operativos de propósito general como GNU/Linux o Windows. Por lo tanto, suelen trabajar sin sistema operativo o con sistemas operativos especiales que consumen menos recursos.

2.2.2 Elementos

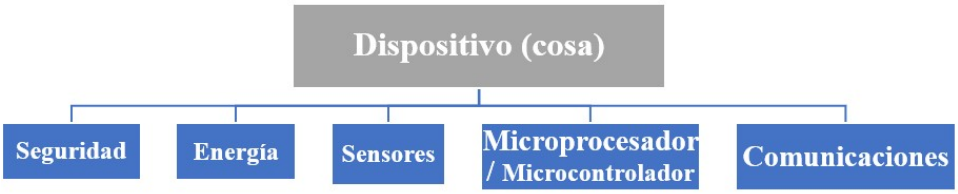
La estructura básica de cualquier objeto común, que ha sido mejorado mediante la incorporación de componentes electrónicos específicos para el IoT, guarda una gran similitud entre sí. Es decir, aunque los objetos puedan ser muy distintos en su apariencia, comparten componentes electrónicos similares desde la perspectiva del IoT. Por lo general, las diferencias radican en las características particulares de los componentes internos, como las magnitudes físicas a medir, las adaptaciones necesarias al entorno, los requisitos de procesamiento y la disponibilidad de fuentes de energía.

Estos componentes pueden incluir **sensores**, que a menudo se acompañan de circuitos para acondicionar las señales que reciben; **microcontroladores**, que integran memoria y gestión de energía, y en algunos casos microprocesadores adicionales si las demandas del sistema lo requieren y hay suficiente energía disponible; así como también sistemas de **comunicación**, ya sea inalámbrica o por cable, que permiten la transmisión de datos hacia una red local o recursos de computación en la nube. Además de los componentes esenciales ,que deben basarse en las necesidades específicas de la aplicación de IoT y a la arquitectura general del sistema, es vital asegurar la seguridad del dispositivo para evitar accesos no autorizados. Asimismo,garantizar una fuente de energía confiable para su funcionamiento eficiente. En la Figura 2.1, se muestra las características de un dispositivo

(Avnet, 2017).

Figura 2.1

Características de un dispositivo



Fuente: Adaptado de: (Avnet, 2017)

Junto con los tres componentes principales, es importante considerar también los dispositivos de acondicionamiento de señales y la gestión de energía. Estas consideraciones incluyen varios aspectos importantes:

Capacidad de procesamiento, esta determinación influye en la elección del procesador (de 8, 16 o 32 bits), la cantidad de memoria necesaria y la velocidad de reloj para ejecutar eficientemente el nodo IoT. Además, esta decisión tiene implicaciones en los requisitos de energía del dispositivo.

Método de comunicación, y dónde se almacenan los datos transmitidos desde el nodo del sensor remoto, existen opciones como *ZigBee, Bluetooth* de baja energía, Ethernet, entre otras, deben considerarse en función de las necesidades específicas del proyecto.

Resolución y frecuencia de muestreo, estos requisitos dependen de las características de los sensores y actuadores utilizados. Además, la magnitud a medir, la precisión del sensor y la necesidad de almacenamiento y gestión de datos influirán en la frecuencia de muestreo requerida y, por ende, en la elección del procesador y la memoria adecuados.

Microprocesadores.

La familia de procesadores ARM, que se destaca como una de las más relevantes en el panorama actual del IoT. ARM otorga licencias de sus CPU a fabricantes de circuitos integrados, quienes las incorporan junto con otros recursos periféricos para crear microcontroladores o microprocesa-

dores, dando lugar a lo que se conoce como *SoC (System on Chip)*. Por cada chip fabricado que incluye una de sus CPU, ARM recibe regalías que varían entre el 1.5% y el 2% del costo del chip. Dado que el modelo de negocio de ARM se centra en el diseño de las CPU y no en la fabricación física de microcontroladores o microprocesadores basados en sus diseños, existen numerosas implementaciones derivadas de los diseños de ARM que se utilizan en el ámbito del IoT.

ARM ofrece distintas categorías de procesadores, cada una adaptada para un propósito específico. Las tres familias más destacadas en la actualidad son las siguientes:

La familia Cortex-A, diseñada para funcionar como microprocesadores capaces de ejecutar sistemas operativos como Linux o Android.

La familia Cortex-R, optimizada para aplicaciones que requieren tiempos de respuesta estrictos en tiempo real, como aquellas utilizadas en entornos de alta fiabilidad para garantizar la seguridad de las personas.

La familia Cortex-M, desarrollada para microcontroladores y aplicaciones de bajo consumo energético. Estos microcontroladores son comunes en dispositivos embebidos utilizados para monitoreo y control. Es importante mencionar que un sistema o dispositivo embebido en el contexto de Internet de las Cosas (IoT), es un elemento especializado diseñado para realizar funciones específicas dentro de un sistema más grande. Estos sistemas están integrados en equipos electrónicos y están dedicados a tareas particulares, como recolección de datos, control de dispositivos, o interacción con el entorno físico. Los sistemas embebidos son importantes en IoT debido a su capacidad para gestionar y procesar datos localmente, interactuar con otros dispositivos y enviar información a plataformas en la nube, contribuyendo así a la automatización y eficiencia de los sistemas inteligentes.

Estos dispositivos son programados con lenguajes de bajo nivel, el cual es un lenguaje de programación que está más cercano al lenguaje de máquina o al código binario que entiende directamente el hardware de una computadora. Estos lenguajes están diseñados para aprovechar al máximo

las capacidades específicas de la arquitectura de la máquina, como el acceso directo a la memoria y a los registros del procesador. A menudo, los lenguajes de bajo nivel son difíciles de leer y de escribir para los humanos debido a su alta dependencia de la estructura interna del hardware. Ejemplos de lenguajes de bajo nivel incluyen el lenguaje ensamblador y el código máquina, los cuales son importantes para programar dispositivos embebidos y para realizar optimizaciones de rendimiento críticas en sistemas informáticos.

Es importante tener en consideración que al mencionar estas tres familias se está ofreciendo solo una introducción preliminar, ya que existe una amplia gama de subfamilias y diseños de procesadores específicos, así como múltiples implementaciones de los mismos.

Aunque todas las familias, como se ha señalado, son aplicables y de hecho se utilizan en el mundo del IoT, es la familia Cortex-M (microcontrolador) la más prevalente, principalmente debido a su eficiencia energética y a la diversidad de aplicaciones en las que se ha empleado hasta el momento.

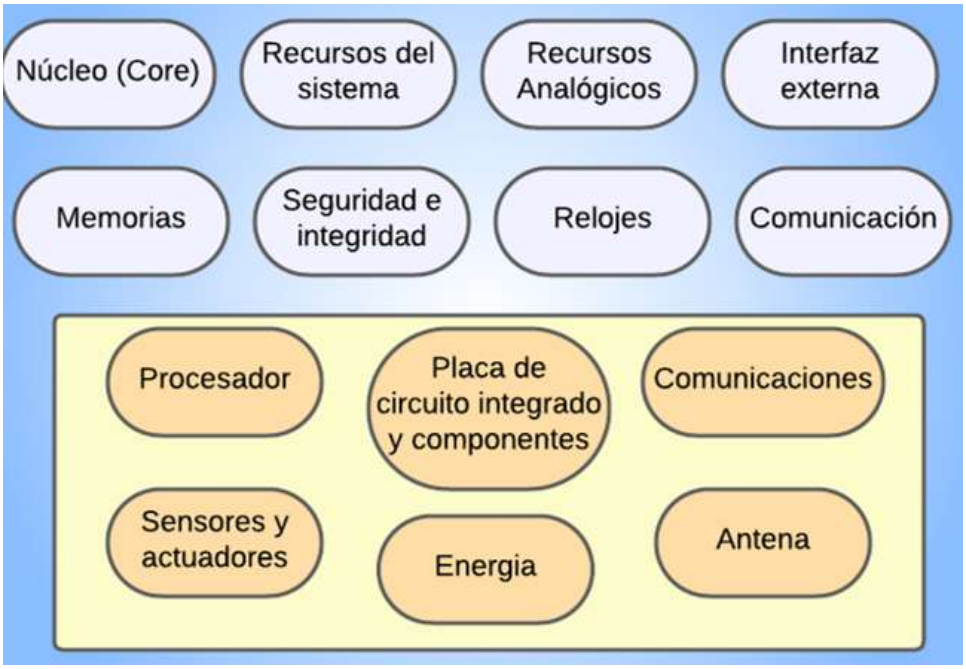
Microcontroladores.

Una situación común es el manejo de un dispositivo de IoT a través de un microcontrolador. Este componente, siendo un único circuito integrado, se encarga de ejecutar el código programado en él para llevar a cabo las funciones principales del dispositivo. Este chip cuenta con recursos internos de procesamiento, memoria y diversas opciones de conexión con otros componentes para facilitar la entrada y salida de datos, gestionar las comunicaciones externas, realizar la programación del microcontrolador, así como controlar el estado del dispositivo y sus parámetros de operación. Además, el microcontrolador puede interactuar con sensores y actuadores para recopilar datos del entorno y realizar acciones específicas. También puede incluir mecanismos de seguridad para proteger la integridad del sistema y asegurar la comunicación de datos.En algunos casos, estos microcontroladores están diseñados para ser energéticamente eficientes,

prolongando la vida útil del dispositivo. Finalmente, la capacidad de actualización remota permite mantener el sistema al día con las últimas mejoras y correcciones de seguridad.

Figura 2.2

Componentes de un microcontrolador/microprocesador



Fuente: Adaptado de: (Sanchez, 2022)

En la Figura 2.2 se muestra las partes de un microntrolador estándar, a continuación, una descripción de cada una.

Núcleo.- Este constituye el elemento central del microcontrolador, generalmente con un único núcleo y una frecuencia de funcionamiento baja, lo que permite un consumo energético reducido. Además de esto, contiene componentes estándar como controladores de interrupción, interfaces de programación y depuración, y unidad aritmético lógica, entre otros.

Recursos del sistema.- Incluyen componentes como el "perro guardián", que es un circuito diseñado para reiniciar el microcontrolador en caso de errores que causen bloqueos. También se encuentra la Unidad de Protección de Memoria, que impide el acceso no autorizado a ciertas áreas de la me-

moria, y el Acceso Directo a Memoria, que facilita las transferencias de datos entre la RAM y los periféricos sin necesidad de intervención de la CPU.

Memorias.- Se dividen en memoria de programa (FLASH), donde se almacena tanto código como datos de solo lectura, y memoria RAM, utilizada para almacenar variables y datos de programa.

Relojes.- Estos son fundamentales en dispositivos digitales, ya que controlan la velocidad de ejecución de las instrucciones del microcontrolador y los periféricos internos. Hoy en día, los relojes de los microcontroladores están compuestos por múltiples señales de diferentes frecuencias y usos adaptándose al rendimiento requerido por la aplicación. Se emplean recursos como PLL y FLL para generar frecuencias de reloj a partir de otras, osciladores para obtener frecuencias estables y referencias internas para reducir el consumo de energía cuando sea necesario.

Seguridad e integridad.- Son aspectos fundamentales para asegurar la precisión de los datos transmitidos o recibidos, así como para cifrar y descifrar la información. Ejemplos de estos elementos incluyen el Código de Redundancia Cíclica (CRC), que emplea un algoritmo reconocido para detectar errores en la transmisión de datos digitales. La presencia de este dispositivo resulta especialmente beneficiosa en interfaces de comunicación cableadas como Ethernet, que dependen ampliamente de este algoritmo para la detección de errores.

En cuanto a los **recursos analógicos**, estos facilitan la adquisición y generación de señales de tensión arbitrarias en un entorno digital. Entre ellos se encuentran el Convertidor Analógico/Digital (ADC), que transforma señales analógicas en valores digitales, y el Comparador Analógico, que compara tensiones en un pin con un valor de referencia determinado. Asimismo, el Convertidor Digital/Analógico (DAC) genera tensiones analógicas en función de valores digitales.

Las comunicaciones son fundamentales para permitir que un microcontrolador interactúe con dispositivos externos. Entre los dispositivos más co-

munes se encuentran:

- I2C: una interfaz de dos señales para conectar periféricos externos, útil para diversos sensores y con capacidad de conexión a múltiples dispositivos en el mismo bus.
- UART: un puerto serie simple para enviar caracteres entre dos puntos, comúnmente utilizado como consola para comandos y depuración.
- SPI: una interfaz para la conexión entre un maestro (generalmente el microcontrolador) y uno o más esclavos (generalmente periféricos).
- CAN: permite la conexión entre dispositivos sin necesidad de un dispositivo maestro, comúnmente usado en automoción.
- SDHC: para acceder a tarjetas de memoria.
- Ethernet: para comunicaciones de red hacia Internet.
- I2S: un bus para la transmisión de señales de audio.
- USB: permite la conexión del microcontrolador como dispositivo a un host, con capacidad de actuar como host para otros dispositivos USB.

Interfaces Exteriores.- Constan de entradas y salidas digitales de propósito general, como puertos USB, pines de conexión, conexión a monitor, entre otros.

Uno de los componentes principales entre todos ellos es la fuente de energía, responsable de alimentar tanto el microcontrolador como los demás elementos del circuito. Es fundamental proporcionar al microcontrolador una o más fuentes de tensión constante, regulada y estabilizada, dependiendo del contexto de uso. Las opciones incluyen la alimentación eléctrica directa, baterías recargables o no recargables.

La tendencia tecnológica actual se inclina hacia tensiones de alimentación más bajas, lo que permite reducir el consumo total del dispositivo. La tensión de 3.3V es comúnmente empleada en la actualidad, también para las señales que conectan el microcontrolador con los periféricos. Es importante evitar mezclar señales de 5V con microcontroladores de 3.3V y

viceversa, aunque muchos microcontroladores de 3.3V son tolerantes a señales de 5V, lo que permite utilizar periféricos de este voltaje con dichos microcontroladores (Sanchez, 2022).

Además de la alimentación, el dispositivo requiere sensores para detectar magnitudes físicas o químicas, conocidas como variables de instrumentación, y convertirlas en variables eléctricas. Los actuadores, por otro lado, transforman la energía eléctrica en acciones específicas para automatizar procesos. Estos elementos, junto con los módulos de comunicación, se integran en una placa de circuito impreso (PCB) que proporciona conexiones eléctricas y soporte mecánico para los componentes. En la PCB se encuentran también otros componentes como resistencias, condensadores y transistores, que son básicos para el funcionamiento del dispositivo.

2.2.3 Software de control (Firmware)

El firmware, siendo el programa fundamental que se integra en el hardware de un dispositivo determina su funcionamiento. Se sitúa entre el hardware, que no puede modificarse una vez fabricado y el software, el cual puede actualizarse con relativa facilidad. Desarrollar programas para el IoT conlleva un esfuerzo complejo, ya que implica dominar una amplia gama de lenguajes de programación. Esto se debe a que la IoT consiste en una red de dispositivos informáticos interconectados en diferentes capas, siguiendo una arquitectura de software que les confiere identificadores únicos y la capacidad de transferir datos a través de una red.

La selección del lenguaje de programación depende de la capacidad y el propósito específico del dispositivo. La IoT abarca una variedad de dispositivos, desde periféricos hasta pasarelas y servidores en la nube. Los lenguajes más comunes para este propósito incluyen Java, C, C++, Python, Javascript, Node.js, Assembler, PHP, C#, Lua, R, Go, Ruby, Swift, Rust, entre otros.

En dispositivos con microprocesadores y recursos limitados, se tiende a utilizar lenguajes como ensamblador o C, mientras que dispositivos con capacidades superiores pueden emplear lenguajes como Python,

Node.js y Java. En todos los casos, el objetivo primordial es minimizar el número de instrucciones y maximizar la velocidad de ejecución y la eficiencia en la gestión de recursos.

Cuando se desarrolla software para dispositivos en el IoT, es importante considerar una serie de características:

Escalabilidad.- Se debe emplear patrones apropiados que permitan distribuir la carga de manera dinámica y gestionar la presencia de múltiples dispositivos en el entorno.

Concurrencia.- Dado el volumen de comunicación en tiempo real entre millones de dispositivos y aplicaciones, se requiere la capacidad de manejar múltiples conexiones simultáneas de manera eficiente.

Coordinación.- Los lenguajes de programación deben brindar soporte para orquestar tanto de manera explícita (mediante control) como implícita (a través de datos) las operaciones de cada componente del sistema.

Tolerancia a fallos.- Las aplicaciones deben ser resilientes y capaces de recuperarse de fallos, así como de solventar problemas que puedan surgir durante su ejecución, como entradas erróneas o fallos de conectividad.

Huella ligera.- Es importante minimizar tanto el tiempo de ejecución como el esfuerzo de programación requerido para optimizar el rendimiento del sistema.

Soporte para latencia y sensibilidad.- En entornos distribuidos geográficamente, resulta beneficioso evitar concentrar todos los cálculos en la nube y en su lugar distribuir la carga mediante estrategias de programación adecuadas.

Otra característica a considerar es la disponibilidad de soporte para actualizaciones de firmware por aire *over the air* (OTA). Dado que el hardware no puede ser modificado, es importante que el firmware pueda ser actualizado, aunque este proceso no sea trivial. La capacidad de que los dispositivos puedan recibir actualizaciones de firmware de forma remota, lo que implica la posibilidad de actualizarlos a través de la red, en lugar de

requerir manipulación física, es de suma importancia, especialmente en escenarios donde los dispositivos están distribuidos en áreas extensas.

Las actualizaciones de firmware OTA representan una herramienta para abordar los problemas que puedan surgir durante el aprendizaje y la optimización, sin embargo, también pueden ocasionar problemas significativos. Si se contempla la implementación de una actualización de firmware para todos los sensores/dispositivos, es importante asegurarse de haber realizado pruebas en un pequeño conjunto de ellos previamente.

2.2.4 Conexiones

La conectividad de los dispositivos ofrece un medio seguro y eficaz para la transmisión de información entre cada componente individual. Es importante destacar que la comunicación se establece no solo entre dispositivos y redes, sino también de dispositivo a dispositivo, lo cual a veces requiere el uso de una pasarela o *gateway*. Dependiendo de cómo estén configuradas las aplicaciones específicas, pueden existir diversos patrones de interacción entre las entidades diversas de un sistema de IoT. Adicionalmente, es crucial asegurar la interoperabilidad entre diferentes fabricantes y estándares para maximizar la flexibilidad y la funcionalidad del sistema.

Los modelos comúnmente empleados son los siguientes:

- Comunicación directa entre dispositivos (D-D).- En este modelo, dos dispositivos pueden comunicarse entre sí sin necesidad de intermediarios.

- Comunicación entre el dispositivo y un servidor de aplicaciones en la nube (D-C).- Aquí, el dispositivo se comunica directamente con un servidor de aplicaciones en la nube. Si el dispositivo es un controlador que requiere información de control para ejecutar ciertas funciones, la obtiene de la aplicación correspondiente alojada en el servidor en la nube.

- Comunicación a través de una pasarela local (D-E-C).- Bajo este modelo, los dispositivos finales se conectan al servidor de aplicaciones en la nube a través de una pasarela local. Este enfoque permite una mayor diversidad por parte de los usuarios y es altamente escalable. Es especialmente

útil cuando los dispositivos no emplean protocolos estándar para proporcionar servicios locales, pero necesitan comunicarse con un servidor de aplicaciones en la nube que sí lo haga. En la tabla 2.1 Se muestra características según el tipo de conexión.

Tabla 2.1

Características según modelo de conexión

	D-D	D-C	D-E-C
Facilidad de despliegue	Muy bueno	Regular	Malo
Escalabilidad	Malo	Regular	Muy bueno
Heterogeneidad	Malo	Regular	Muy bueno
Variedad de aplicaciones	Malo	Aceptable	Muy bueno
Facilidad de actualización	Malo	Regular	Muy bueno
Costo	Muy bueno	Regular	Malo

Fuente: Adaptado de: (Sanchez, 2022)

Es fundamental considerar las diversas redes de comunicación comúnmente utilizadas en este contexto, las cuales pueden ser categorizadas según varios criterios, como se detalla a continuación:

Clasificación según su accesibilidad.

- Públicas.- Aquellas proporcionadas por un operador de red o proveedor de servicios de telecomunicaciones, ejemplificadas por 2G, 3G, LTE, Sigfox, entre otras.

- Privadas.- Instaladas directamente por el usuario o una empresa de manera específica, como Wi-Fi, LoRa, Bluetooth, 802.15.4, etc.

- Híbridas.- Compuestas por una combinación de ambas modalidades. Por ejemplo, un gateway que facilita la conectividad Bluetooth entre dispositivos cercanos, con salida a través de 3G.

Según el tipo de tecnología de acceso.

- Fijo. Como ADSL o fibra óptica.

- Móvil. Incluyendo 2G, 3G, LTE, entre otros.
- LPWA (Low Power Wide Area): EC-GSM, LTE-M, NB-IoT, SigFox, LoRaWAN, entre otros.
- Satélite u otras tecnologías WAN.
- Redes inalámbricas de corto o medio alcance, tales como Wi-Fi Bluetooth, ZigBee, etc.

2.2.5 Protección de los dispositivos

La proliferación de dispositivos IoT no solo implica una conexión a Internet, sino también la necesidad de intercambiar datos entre ellos según su entorno. Este cambio de paradigma no solo afecta a nuestra vida cotidiana, sino también a nuestra forma de aprender y trabajar. Sin embargo, junto con las oportunidades que brinda, también presenta riesgos significativos para la seguridad y la privacidad, ya que los hackers pueden comprometer tanto los sistemas como la información personal.

Si bien existen sectores en línea, como entidades financieras o el comercio electrónico, que han desarrollado sistemas seguros basados en algoritmos criptográficos avanzados, el desafío en el ámbito del IoT es aún mayor. La protección no solo debe garantizarse contra amenazas externas, sino también dentro de las redes privadas de los propios dispositivos IoT. Esto se complica por las limitaciones de potencia computacional y memoria, así como por la dependencia de baterías, lo que demanda soluciones energéticamente eficientes.

La introducción de dispositivos interconectados en entornos industriales plantea una serie de desafíos, incluyendo la seguridad, la privacidad y la confianza. Estos desafíos surgen de diversos aspectos, como la dificultad para implementar protocolos estándar debido a la minimización de datos intercambiados, la necesidad de asegurar un flujo bidireccional de información y las limitaciones de recursos hardware que dificultan la implementación de algoritmos criptográficos complejos. En consecuencia, se requiere una arquitectura de seguridad integral que abarque desde el inicio hasta el

final de la comunicación entre dispositivos IoT.

Protocolos basados de Internet para sistemas IoT.

La integración de tecnologías tradicionales de Internet dentro de los sistemas de IoT presenta una serie de beneficios básicos. Estos incluyen la utilización de protocolos homogéneos y probados, así como una arquitectura de seguridad que ha sido ampliamente validada en el entorno de Internet. Además, simplifica el proceso de desarrollo e implementación de servicios innovadores al aprovechar tecnologías previamente establecidas.

Sin embargo, al incorporar nuevos dispositivos a una red convencional como Internet, se enfrenta al desafío de la "expansión de la superficie de ataque". Este fenómeno implica que la conexión de estos nuevos nodos, que transmiten datos sensibles al contexto y se almacenan en la nube, introduce información adicional sobre el entorno de los dispositivos, generando nuevos puntos de vulnerabilidad y amenazas a la seguridad.

Con la fusión de las redes de objetos y el Internet, surge una alta probabilidad de nuevas vulnerabilidades de seguridad debido a la diversidad de protocolos y la incompatibilidad de las infraestructuras de seguridad. En consecuencia, los modelos de seguridad han seguido dos principios esenciales: mejorar la seguridad de aplicaciones y dispositivos específicos, y basar la seguridad en el control perimetral para proteger los dispositivos finales y los servidores.

Sin embargo, en el contexto de la IoT, los enfoques de seguridad centrados en el perímetro son menos relevantes debido a la extensa y heterogénea superficie de ataque que a menudo carece de límites claros.

La variabilidad en la transmisión de datos.

Una consideración crucial en la planificación de infraestructuras IoT es la capacidad de los dispositivos conectados para colaborar y generar valor mediante soluciones novedosas. Sin embargo, esta cualidad puede convertirse en un elemento de riesgo. Aunque ofrece una solución con un gran potencial en diversas situaciones avanzadas, también puede aumentar

considerablemente la complejidad operativa si no se integra adecuadamente con los procedimientos organizativos del contexto en el que se implementa. Además, es fundamental que los protocolos de seguridad se diseñen meticulosamente para sincronizarse con estos procesos dentro de la propia estructura organizativa teniendo en cuenta sus particularidades.

Seguridad en dispositivos livianos.

Esto plantea un dilema en los ecosistemas de IoT, donde encontrar un equilibrio entre el costo y la disponibilidad de recursos hardware destinados a la prevención de ataques es clave. Este consumo de recursos se traduce en un mayor gasto energético, especialmente dedicado a ejecutar algoritmos criptográficos y otros métodos para proteger el sistema.

El valor único de los ecosistemas de IoT radica en la variedad de dispositivos inteligentes que interactúan entre sí y con servicios en la nube. Tecnologías como IPv4 o IPv6, junto con servicios web, son fundamentales para estas aplicaciones. Al utilizar tecnologías de Internet, se aprovechan protocolos homogéneos, una arquitectura de seguridad probada y simplificaciones en el desarrollo y despliegue de servicios innovadores.

Seguridad en la Autenticación.

El proceso de inicio y autenticación regula el acceso de dispositivos IoT a una red. La autenticación en particular, es importante, siendo típicamente la primera operación ejecutada por un dispositivo al unirse a una nueva red. Por lo general, esta autenticación se lleva a cabo con un servidor remoto utilizando protocolos de acceso a la red como PANA *(Protocol for Carrying Authentication for Network Access)*, (Yegin, Chakratabarti, & Duffy, 2011), y para promover la interoperabilidad, también se puede emplear EAP *(Extensible Authentication Protocol)* (Vollbrtcht, Carlson, Blunk, Aboda, & Levkowetz, 2004). Una vez completada una autenticación exitosa, es posible establecer asociaciones de seguridad en niveles superiores, como IKE para IPSec, (Frankel & Krishnan, 2011) y desplegarlas entre el dispositivo recién autenticado y el agente de control de acceso en la red correspondiente.

Tanto el Internet *Key Exchange* (IKEv2)/IPSec como el HIP (Frankel & Krishnan, 2011) operan en o sobre la capa de red. Estos protocolos tienen la capacidad de llevar a cabo intercambios de claves autenticados y configurar transformaciones IPSec para asegurar la entrega de datos de manera segura.

Mecanismos de autorización.

Los servicios contemporáneos que operan en línea, tales como las plataformas de redes sociales, han confrontado y, en ciertas instancias, solventado dificultades vinculadas a la seguridad y la confidencialidad. Un caso común es el acceso a información personal por parte de entidades no autorizadas. En el porvenir, las aplicaciones de IoT podrían verse igualmente desafiadas por problemáticas similares, sin descartar otros dilemas específicos de su ámbito.

El protocolo OAuth *(Open Authorization)* ha sido desarrollado con el fin de abordar el desafío de permitir que terceros autorizados accedan a los datos personales de los usuarios sin necesidad de revelar credenciales no cifradas. En este sentido, OAuth 2.0 (Hardt, 2012), se presenta como un marco de autorización que posibilita a un tercero acceder a un recurso específico en nombre de un propietario determinado, sin requerir la entrega de credenciales en texto plano. Por ejemplo, consideremos el caso en el que un sensor de salud o una aplicación móvil necesiten acceder al perfil de un usuario en Facebook para publicar actualizaciones de estado. Mediante OAuth 2.0, no es necesario que la aplicación reciba las credenciales de acceso de Facebook. En cambio, el usuario inicia sesión en Facebook, otorgando así a la aplicación la autorización para utilizar la plataforma en su nombre. Este enfoque permite al usuario revocar dicha autorización en cualquier momento mediante la configuración de privacidad en Facebook.

El protocolo OAuth 2.0 establece cuatro roles fundamentales para su funcionamiento (Hardt, 2012).

- Propietario del recurso.- Se refiere a la entidad con capacidad para conceder acceso a un recurso protegido. Cuando este propietario es una per-

sona, se le denomina usuario final.

- Servidor de recursos.- Es el servidor que alberga los recursos protegidos y puede aceptar y responder a las solicitudes de fuentes protegidas mediante tokens de acceso. En el caso mencionado, este sería el servidor de Facebook.

- Cliente.- Es la aplicación que realiza las solicitudes de recursos protegidos en nombre del propietario del recurso y con su debida autorización. El término "cliente" no implica una implementación específica (por ejemplo, si la aplicación se ejecuta en un servidor, un escritorio u otros dispositivos).

- Servidor de autorización.- Es el servidor encargado de emitir los tokens de acceso al cliente después de autenticar con éxito al propietario del recurso y obtener su autorización. En el ejemplo, este sería el servidor de autorización de Facebook.

2.2.6 Procesador de placa única integrada (Single board computer)

La rápida evolución tecnológica de los últimos años ha dado lugar a la introducción de una gran cantidad de conceptos y términos novedosos. Sin embargo, hay excepciones como el término SBC, proveniente del inglés *single board computer*, que se traduce al español como ordenador de placa reducida o placa computadora. Este término ha estado presente desde 1976 (Sanchez, 2022), cuando fue introducido en la edición de mayo de la revista estadounidense Radio-Electronics. El avance tecnológico ha tenido un impacto significativo en las capacidades de los SBCs. Aunque en muchos aspectos no pueden igualar a los ordenadores convencionales actuales, sí son capaces de superar o igualar en rendimiento de procesamiento a los ordenadores portátiles o de escritorio fabricados entre hace cuatro y ocho años.

Para entender las ventajas adicionales ofrecidas por un SBC en comparación con las computadoras tradicionales, es necesario primero examinar una serie de características no funcionales de los SBC:

- Costo.- Una de sus principales ventajas es su costo de adquisición,

considerablemente más bajo que el de una computadora de escritorio con especificaciones similares.

- Consumo de energía.- Estos dispositivos tienden a consumir mucha menos energía que una computadora tradicional con características comparables.

- Tamaño.- Al ser una única placa que integra todos los componentes necesarios (procesador, memoria RAM, almacenamiento -generalmente en una tarjeta microSD-, puertos de entrada/salida, etc.), los SBC logran tener un tamaño considerablemente reducido, a menudo del tamaño de la palma de la mano, dependiendo del modelo.

- Conectividad.- Además de los puertos de entrada/salida estándar, como Wi-Fi, Ethernet o Bluetooth 4.0, suelen contar con una serie de pines de entrada/salida de propósito general (GPIO, por sus siglas en inglés), que permiten la conexión de diversos sensores o actuadores, establecer conexiones mediante puerto serie, suministrar energía a otros dispositivos, entre otras funciones.

- Sistema operativo.- Los SBC modernos son compatibles con una variedad de sistemas operativos, incluyendo varias distribuciones de Linux (generalmente optimizadas para mejorar el rendimiento), Windows (con una versión conocida como Windows 10 IoT Core) e incluso Android.

En la era actual, con la llegada del IoT y las amplias oportunidades que ofrece han surgido diversos tipos de SBC *(Single Board Computer)*. Aunque comparten características similares, tales como diseño, capacidad de procesamiento, consumo energético, conectividad y precio, es importante llevar a cabo un análisis preliminar antes de embarcarse en un nuevo proyecto con el fin de determinar cuál de ellos se ajusta mejor a las necesidades específicas.

A continuación, se enumeran algunos de los SBC más populares en la actualidad, presentando una variedad de modelos disponibles en el mercado.

Raspberry PI.

Raspberry Pi, (https://www.raspberrypi.org), reconocido como el SBC más prominente, ha reunido una amplia comunidad de seguidores desde que se presentó su primer modelo, el A, el 29 de febrero de 2012 (Foundation, 2024), un lanzamiento que llegó a sobrecargar sus servidores. Esta plataforma dispone de una abundante documentación, foros, tutoriales y proyectos en línea, lo que la convierte en una alternativa asequible para usuarios de diversas computadoras. En la Figura 2.3, se muestra la placa Raspberry PI en la versión 4.

Figura 2.3

Placa Raspberry Pi 4

Fuente: (Raspberry, 2024)

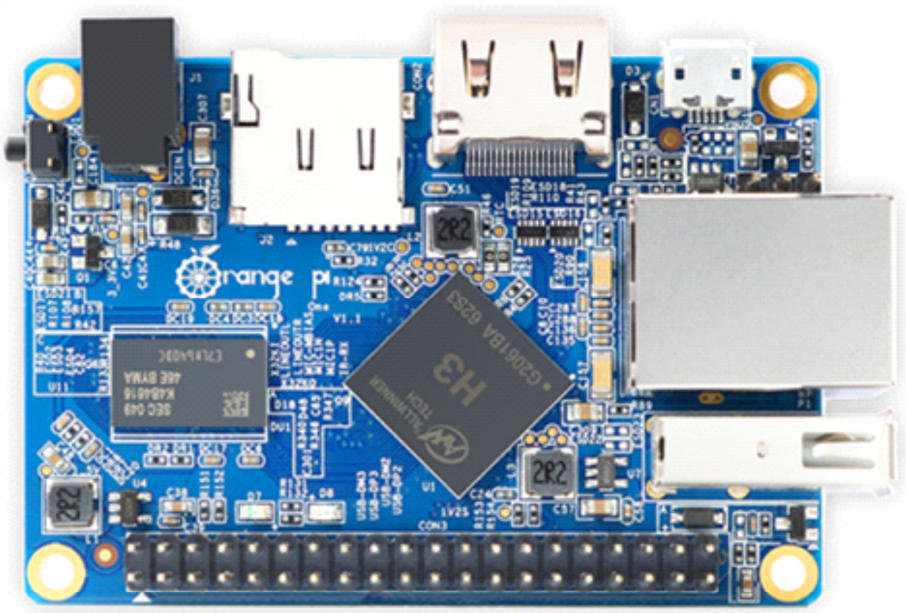
Orange PI.

Orange Pi, disponible en http://www.orangepi.org/, representa una alternativa a la popular Raspberry Pi, evidenciado incluso en su nombre. Destaca por su procesador ARM Cortex A7 de cuatro núcleos, que opera a 1.6 GHz, junto con 1 GB de RAM y un módulo Wi-Fi incorporado con antena. Todo esto se ofrece a un atractivo precio que oscila entre los 35 y 40

dólares americanos. Este proyecto de código abierto es compatible con diversos sistemas operativos, como Android, Ubuntu, Debian y Raspbian, ampliando así su versatilidad y utilidad.Cabe mencionar que la comunidad de Orange Pi es activa y ofrece soporte a través de foros y recursos en línea. En la Figura 2.4, se muestra la placa Orange Pi en el modelo One.

Figura 2.4

Placa Orange PI One



Fuente: (Orange, 2024)

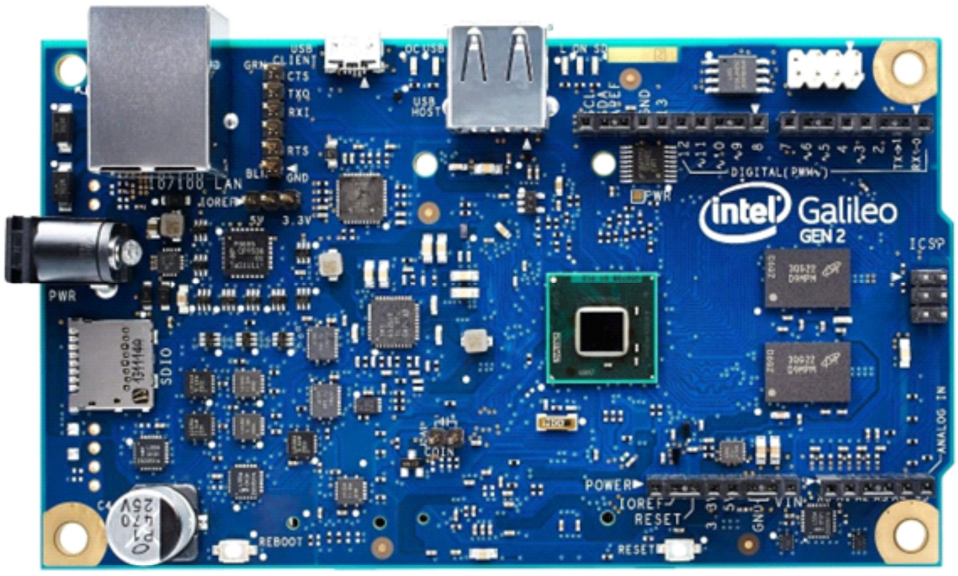
Intel Galileo Gen 2.

La placa Galileo Gen 2, (https://ark.intel.com/es-es/products/83137/Intel-Galileo-Gen-2Board) desarrollada por Intel, es un SBD *(Single Board Computer)* que se integra perfectamente con el software de Arduino. Este dispositivo está fundamentado en un *System on a Chip (SoC)* Intel Quark X1000 de 32 bits, funcionando a una velocidad de 400MHz. Con un costo que oscila entre los 50 y 60 euros, supera el precio habitual de las tarjetas de Arduino, sin embargo, su potencia superior y el respaldo de un fabricante como Intel justifican esta inversión. Además, esta placa ofrece una amplia gama de interfaces de entrada y salida, incluyendo

puertos USB, Ethernet y GPIO, lo que la hace muy versátil para diversos proyectos. También cuenta con soporte para tarjetas microSD, permitiendo una expansión de almacenamiento adicional. La comunidad de desarrolladores de Intel proporciona recursos y soporte continuo, facilitando el desarrollo y la implementación de proyectos innovadores.En la Figura 2.5 se muestra la placa Intel Galileo en el modelo Gen 2 (Generación 2).

Figura 2.5

Placa Intel Galileo Gen 2



Fuente: (Intel, 2024)

2.3 Sensores y Actuadores

Durante el desarrollo de un dispositivo o la implementación de una aplicación de IoT, es imperativo establecer interacciones con el entorno circundante. Estas interacciones pueden abarcar desde la recolección de datos hasta la modificación y adaptación del entorno conforme a las necesidades del usuario. En este contexto, los sensores desempeñan un papel fundamental al capturar diversos fenómenos físicos, como la temperatura o la presión, y convertirlos en señales eléctricas que pueden ser procesadas por el dispositivo o la aplicación.

2.3.1 Definición, atributos y categorización

Un sensor es un dispositivo que transforma una entrada que no es eléctrica en una señal eléctrica, la cual puede ser procesada por un circuito electrónico.Aunque un sensor por sí solo carece de utilidad su importancia radica en su integración dentro de un sistema electrónico, donde desempeña una función crucial. En esencia, un sensor se define como un componente con la capacidad de percibir y registrar cambios dentro de un determinado entorno (IEEE Standars, 2007). El complemento tecnológico de un sensor se conoce como actuador, un artefacto encargado de transformar una señal eléctrica en una acción, a menudo mediante la conversión de dicha señal en energía no eléctrica, como el movimiento. Un ejemplo básico de un actuador es un motor eléctrico que convierte la energía eléctrica en energía mecánica. Tanto los sensores como los actuadores son parte de una categoría más amplia de dispositivos electrónicos denominados transductores, los cuales se encargan de convertir una señal de una naturaleza física a otra señal con una naturaleza física diferente. En este contexto, nos centraremos en los transductores que operan con una magnitud física de interés y una señal eléctrica.

Clasificación.

En este segmento, vamos a introducir una variedad de sensores, clasificándolos según su naturaleza eléctrica. Destacan especialmente los sensores inteligentes o digitales, que ofrecen una amplia gama de opciones y funcionalidades ideales para aplicaciones de IoT. Sin embargo, otros tipos de sensores requieren un proceso de preparación y adquisición que afecta directamente a la calidad de los datos recopilados y su interpretación precisa.

Por otro lado, existen diversas taxonomías para clasificar los sensores, las cuales se fundamentan en diferentes criterios. Algunas de estas clasificaciones incluyen:

- Pasivos o activos.- Los sensores pasivos no dependen de una fuente externa de energía para monitorear su entorno, mientras que los sensores

activos sí la necesitan.

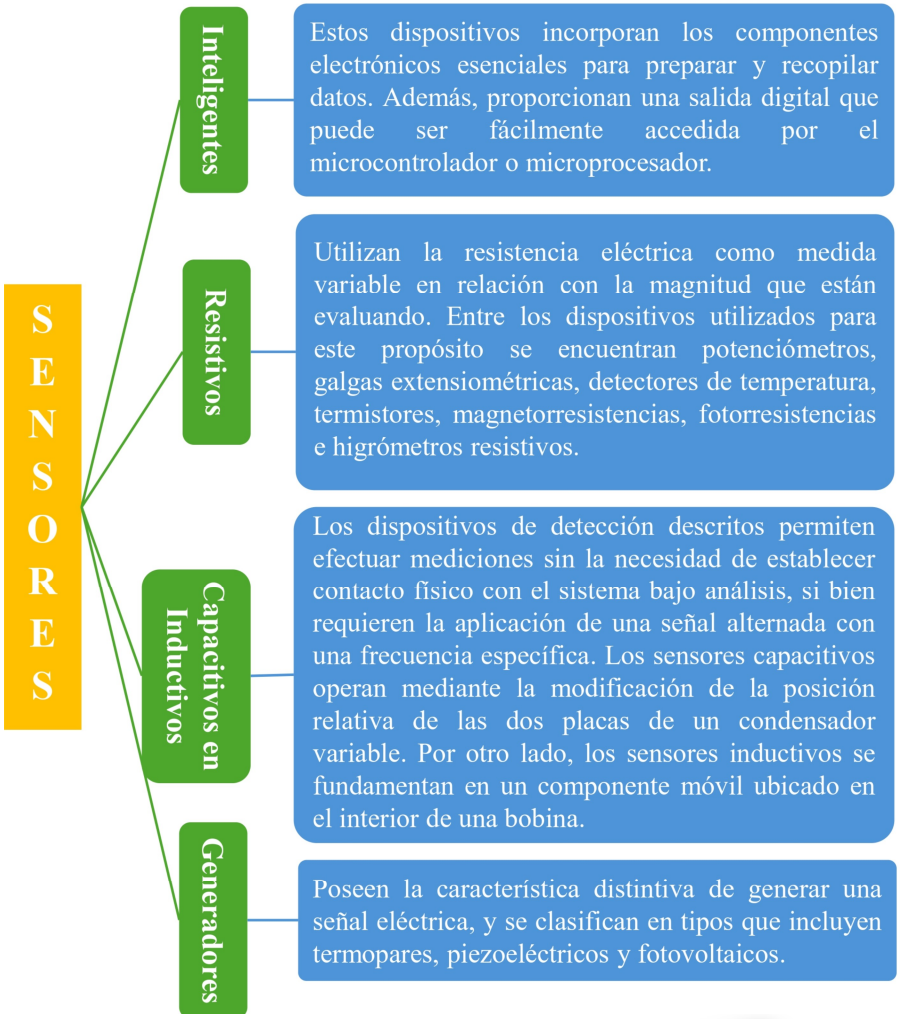
- Método de medición.- Otra clasificación se basa en los métodos utilizados para detectar y medir diversas propiedades (mecánicas, químicas, etc.).

- Analógicos y digitales.- Los sensores analógicos generan señales continuas, mientras que los sensores digitales generan señales discretas.

A continuación, se presenta una clasificación más amplia en función de la naturaleza eléctrica de los sensores.

Figura 2.6

Tipos de sensores según la naturaleza eléctrica



Los sensores **inteligentes** representan una fusión entre elementos sensoriales y la electrónica básica para el procesamiento y la recopilación de información. Esta combinación les confiere la capacidad de ofrecer una interfaz digital directamente compatible con microprocesadores o microcontroladores. Esta clase de sensores se ha vuelto de gran relevancia debido a la creciente diversidad de opciones disponibles en el mercado. Además de su capacidad para proporcionar datos digitales, estos sensores suelen ser flexibles en términos de ajustes internos, como el control de ganancia, rango y resolución lo que facilita su adaptación a diversas aplicaciones. También suelen integrar interfaces digitales serie (SPI) o intercircuitos (I2C), que permiten el acceso a registros internos de 8 bits para llevar a cabo operaciones de lectura, escritura, configuración y control de manera eficiente.

Los sensores **resistivos** son dispositivos que utilizan la resistencia eléctrica como variable, la cual varía en función de la magnitud física que están diseñados para medir. Son ampliamente utilizados y versátiles, permitiendo la medición de diversas magnitudes físicas. Todos estos sensores requieren de una fuente externa de energía para producir una señal eléctrica en forma de tensión o corriente.

Entre los tipos más comunes de sensores resistivos se encuentran:

- Potenciómetros.- Se trata de una resistencia con un contacto móvil, conocido como cursor que puede deslizarse o girar, permitiendo la medición de posición lineal o angular.

- Galgas extensiométricas.- Estos sensores se basan en el efecto piezorresistivo, que consiste en la variación de la resistencia debido a un esfuerzo mecánico. Suelen estar hechos de aleaciones metálicas y requieren amplificación debido a su baja salida de señal.

- Detectores de temperatura resistivos (RTD).- Funcionan midiendo la temperatura a través del cambio en la resistividad de los metales con la temperatura. Los más comunes son los de platino, como el Pt100, que tiene una resistencia de 100 ohmios a 0 ºC y puede medir temperaturas desde -200 ºC hasta +800 ºC.

- Termistores.- A diferencia de los RTD, están hechos de semiconductores, lo que hace que su relación entre resistencia y temperatura sea altamente no lineal. Existen dos tipos principales: PTC, que aumenta la resistencia con la temperatura, y NTC, que la disminuye. Son más sensibles, pero menos precisos que los RTD.

- Magnetorresistencias.- Se utilizan para medir campos magnéticos mediante la variación en la resistencia de un conductor por el que circula corriente. Esta relación es cuadrática y no lineal. Son empleadas, por ejemplo, en lectores de bandas magnéticas.

- Fotorresistencias.- Son resistencias cuya resistividad varía en función de la luz que absorben. Están hechas de semiconductores y se utilizan en aplicaciones como detectores de luz ambiental.

- Higrómetros resistivos.- Miden la humedad relativa mediante la variación de la resistencia de un material debido a la absorción de humedad. Pueden basarse también en la capacitancia.

Los sensores **capacitivos e inductivos** se destacan por su capacidad de realizar mediciones sin necesidad de contacto físico directo con el sistema bajo observación. Requieren una señal alterna de frecuencia específica, lo que impone un límite a la frecuencia máxima de la magnitud que se puede medir.

Los sensores capacitivos más comunes, como los condensadores variables, operan modificando la posición relativa de dos placas conductoras. Esto les permite medir una variedad de magnitudes que pueden traducirse en desplazamientos, como aceleración, presión, fuerza o torque. Son especialmente efectivos para medir niveles de líquidos, ya sean conductores o no conductores.

Por otro lado, los sensores inductivos suelen emplear un elemento móvil dentro de una bobina que lleva una corriente alterna. Estos sensores se utilizan principalmente para detectar la posición o la proximidad de objetos metálicos, entre otras aplicaciones.

Los sensores **generadores** tienen la capacidad única de producir una señal eléctrica observable sin requerir una excitación eléctrica externa. Se basan en efectos físicos reversibles y se utilizan principalmente como actuadores. Esta familia de sensores incluye termopares, piezoeléctricos y fotovoltaicos, cada uno con sus propias características y aplicaciones específicas.

- Los termopares generan una tensión en circuito abierto o una corriente en cortocircuito debido a las diferencias de temperatura entre dos metales distintos.

- Los sensores piezoeléctricos, por su parte, generan una tensión en respuesta a la presión mecánica ejercida sobre ellos, siendo utilizados en la medición de esfuerzos y vibraciones.

- Los sensores fotovoltaicos se emplean en la medición de luz y de magnitudes relacionadas con ella.

2.3.2 Variables físicas

La clasificación de los sensores también se puede realizar en función de magnitud física que se va a medir, a continuación, en la tabla 2.2 se presentan diferentes tipos de sensores según la magnitud a percibir.

Tabla 2.2

Lista de sensores en función de la variable física

Tipo Sensor	Detalle	Variable/ Magnitud
Potenciómetro Inclinómetro	Los sensores de posición tienen la capacidad de determinar la ubicación de un objeto de manera precisa, ya sea en relación con un punto de referencia fijo (como en el caso de los sensores de posición absoluta) o en relación con su posición anterior (como en los sensores de desplazamiento). Estos sensores se clasifican en lineales, angulares o multieje según el tipo de movimiento que miden.	Posición

Ultrasonidos Radar	Los dispositivos de detección identifican la presencia, mientras que los sensores de movimiento y ocupación responden al movimiento y a la presencia estática, respectivamente.	Ocupación y Movimiento
Acelerómetro Giroscopio	Los sensores de aceleración registran cambios en la velocidad de un objeto en movimiento lineal o angular.	Velocidad y Aceleración
Dinamómetro Viscosímetro Táctil	Observan la aplicación de una fuerza física y determinan si su intensidad excede un cierto límite.	Fuerza
Barómetro Piezómetro	Estos dispositivos, vinculados a los sensores de fuerza, cuantifican la fuerza ejercida por fluidos o gases, evaluando la presión según la fuerza por unidad de superficie.	Presión
Anemómetro Caudalímetro	Estos dispositivos, vinculados a los sensores de fuerza, cuantifican la fuerza ejercida por fluidos o gases, evaluando la presión según la fuerza por unidad de superficie.	Caudal
Micrófono Hidrófono Geófono	Evalúan los niveles acústicos y los transforman en señales digitales o analógicas.	Acústicos
Higrómetro Humedad	Los sensores detectan la presencia de humedad, que es la cantidad de vapor de agua presente en el aire o en una masa determinada. La medición de estos niveles de humedad puede realizarse a través de diversos métodos como la humedad absoluta, la humedad relativa, la relación de masa, entre otros.	Humedad

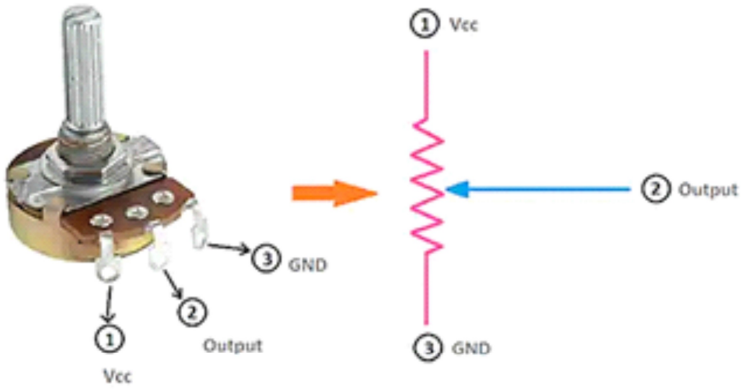
Infrarrojos Fotodetector Llamas	Se identifica la existencia de luz, ya sea perceptible por el ojo humano o no.	Luz
Contador Geiger-Müller	Identifican las emisiones radiactivas presentes en el entorno, las cuales pueden ser detectadas mediante dos métodos: el centelleo y la ionización.	Radiación
Termómetro Calorímetro	Los dispositivos de medición de temperatura evalúan la energía térmica de un sistema y se clasifican en sensores de contacto, que requieren contacto directo, y sensores sin contacto, que miden a través de convección y radiación.	Temperatura
Químicos	Los sensores químicos se encargan de evaluar la cantidad de sustancias químicas en un sistema determinado, mostrando preferencia por un tipo específico de sustancia al ser expuestos a una mezcla de productos químicos.	Glucosa
Pulso	Los biosensores tienen la capacidad de identificar diversos componentes biológicos, tales como organismos, tejidos, células, enzimas, anticuerpos y ácidos nucleicos.	Biológicos

A continuación, se describe en mayor detalle algunos de los diferentes sensores mostrados:

Potenciómetro.- Un dispositivo que se caracteriza por ser una resistencia ajustable manualmente. Estos componentes constan de tres terminales y son comúnmente empleados en circuitos de baja intensidad eléctrica. La medida de un potenciómetro se expresa en ohmios y representa la resistencia máxima que puede alcanzar, siendo su valor mínimo de 0 ohmios. Además, su diseño versátil permite su uso en aplicaciones como control de volumen, ajuste de brillo y sintonización de frecuencia.

Figura 2.7

Potenciómetro estándar con resistencia variable y eje giratorio

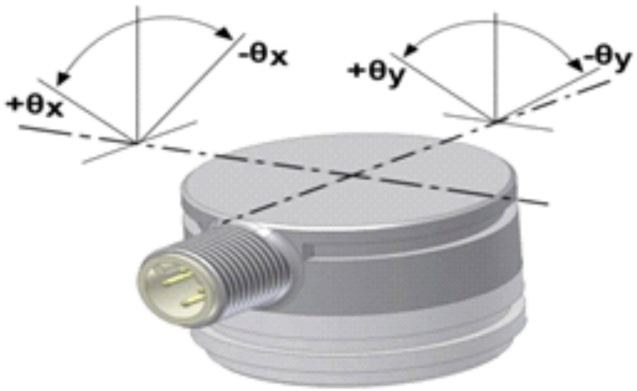


Fuente: (Schweber, 2021)

Inclinómetro.- Este dispositivo, tanto mecánico como eléctrico, es utilizado para detectar y medir los cambios en la inclinación o rotación de una superficie o estructura. Su funcionamiento se basa en el principio de la gravedad, registrando los movimientos de inclinación respecto a un eje vertical. Los primeros modelos de inclinómetros empleaban un péndulo simple que alteraba su dirección con los cambios de inclinación, los cuales luego eran evaluados ópticamente. Con el tiempo, se logró registrar estas variaciones de manera capacitiva, inductiva o electrónica. En la Figura 2.8 se muestra a un tipo de sensor que mide la inclinación.

Figura 2.8

Sensor Inclinómetro



Fuente: (Mecafenix, 2024)

Sensor de proximidad ultrasónico.- Los sensores de proximidad basados en ultrasonidos son dispositivos que detectan la presencia de objetos cercanos sin necesidad de contacto físico, utilizando ondas ultrasónicas. Estos sensores son capaces de detectar objetos a distancias cortas, aproximadamente hasta 8 metros. Funcionan emitiendo pulsos ultrasónicos que se reflejan en los objetos cercanos, y luego capturan y convierten estos reflejos en señales eléctricas. Estos sensores son efectivos en diversas condiciones, ya que pueden detectar objetos con diferentes formas, superficies y materiales, incluyendo sólidos, líquidos o granulados, siempre que puedan reflejar el sonido. La medición de la distancia se realiza midiendo el tiempo transcurrido entre la emisión del pulso ultrasónico y la recepción de su eco. En la Figura 2.9 se muestran dos tipos de sensores ultrasónicos para medir la proximidad de un objeto.

Figura 2.9

Sensores de proximidad ultrasónicos

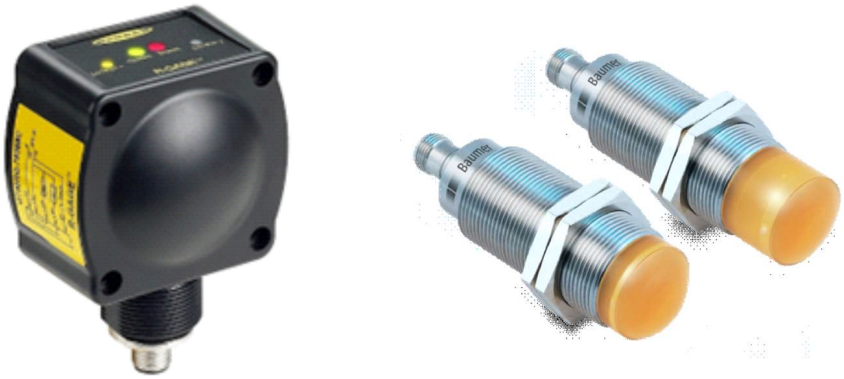
Fuente: (Sick, 2024)

Radar.- Los sensores de radar de movimiento son utilizados para identificar la presencia de movimiento humano en un área amplia con una gran zona de cobertura. Sin embargo, tienen limitaciones para detectar movimientos sutiles y para distinguir entre objetos en movimiento hacia adelante o hacia atrás. Su funcionamiento se basa en la detección de movimiento, lo que significa que pueden ser efectivos para detectar movimientos mínimos, pero no pueden detectar objetos estáticos. Además, dado que su capacidad de

detección se centra en el movimiento de acercamiento y alejamiento, a menudo resulta difícil o incluso imposible realizar tareas específicas, como contar el número de personas que ingresan o salen de una habitación. En la Figura 2.10 se muestra dos tipos de sensores radar.

Figura 2.10

Dos tipos diferentes de sensores radares

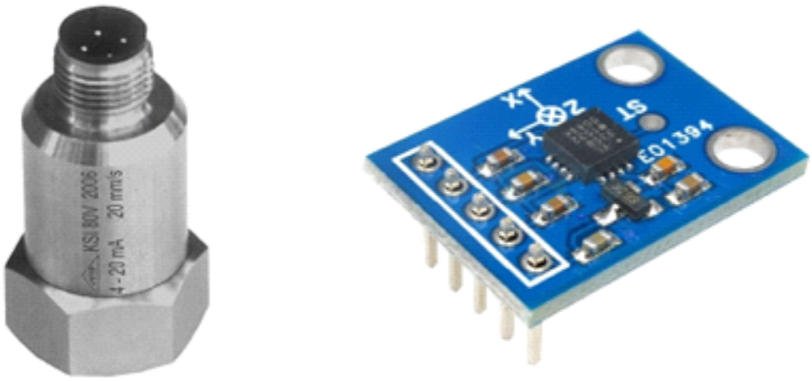


Fuente: (Mecafenix, 2024)

Acelerómetro.- Es un dispositivo diseñado para medir tanto la vibración como la aceleración de un objeto en movimiento. Su funcionamiento se basa en la conversión de la fuerza generada por la vibración o cambio en el movimiento (aceleración) en una carga eléctrica. Este proceso ocurre cuando la masa del dispositivo comprime el material piezoeléctrico, lo que a su vez produce una carga eléctrica proporcional a la fuerza aplicada sobre él. Dado que la carga generada es directamente proporcional a la fuerza y la masa del dispositivo se mantiene constante, la carga resultante también guarda una relación proporcional con la aceleración. Es crucial realizar un mantenimiento continuo y predictivo, donde se analizan las vibraciones para predecir y prevenir fallas en los equipos, programando el mantenimiento antes de que ocurran problemas. Además, existen diferentes tipos de acelerómetros, como los cilíndricos de metal o las placas de circuito con chips integrados, que son cruciales para la detección de movimiento en dispositivos móviles y la estabilización de cámaras. En la Figura 2.11 se muestra dos tipos acelerómetros.

Figura 2.11

Dos tipos de sensores acelerómetros

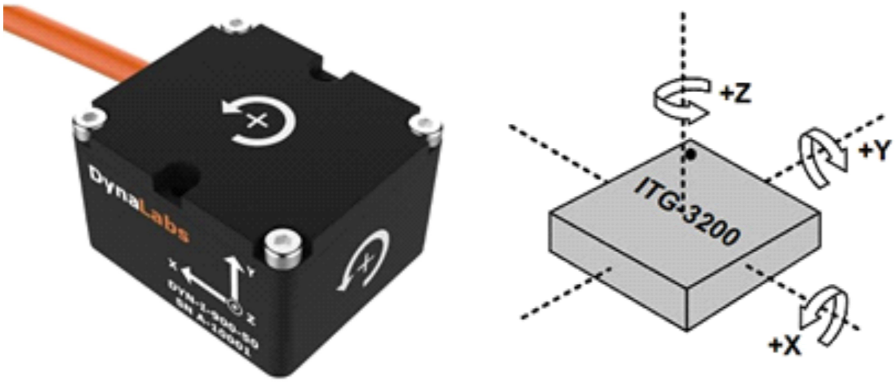


Fuente: (Sick, 2024)

Giroscopio.- Comúnmente emparejado con un acelerómetro, es un dispositivo sensorial utilizado para detectar y medir la rotación angular de un objeto en múltiples ejes. Al colaborar con el acelerómetro este sensor de movimiento determina la orientación del objeto. Su aplicación principal se encuentra en dispositivos móviles como los *smartphones*, donde facilita el desarrollo de una variedad de juegos, aplicaciones, así como la interacción con contenido multimedia en 360 grados. En la Figura 2.12 se muestra un sensor giroscopio y su capacidad para detectar y medir el entorno.

Figura 2.12

Sensor Giroscopio y su principio de funcionamiento



Fuente: (Sick, 2024)

Dinamómetro.- Un instrumento utilizado para la medición de fuerzas y el cálculo del peso de objetos, opera mediante el estiramiento de un resorte conforme a la ley de elasticidad de Hooke dentro de su rango de operación. Su funcionamiento se basa en un resorte interno que se extiende cuando se aplica una fuerza sobre él. Por lo general, presenta un indicador que muestra la fuerza aplicada de manera simultánea. En la Figura 2.13 se muestra dos tipos de sensores dinamómetros.

Figura 2.13

Dos tipos de sensores dinamómetros

Fuente: (Mecafenix, 2024)

Viscosímetro.- Es un dispositivo utilizado para determinar la viscosidad de un fluido en movimiento siendo capaz de analizar una amplia gama de fluidos, incluidos aquellos que no siguen el comportamiento newtoniano, como los geles. Aunque inicialmente se empleaban principalmente en entornos de laboratorio, su uso se ha extendido gradualmente a los procesos de control de calidad en diversas industrias. Dada su versatilidad, existen varios tipos de viscosímetros que se diferencian por los principios de funcionamiento en los que se basan, así como por su naturaleza analógica o digital siendo estos últimos capaces de calcular automáticamente el valor de viscosidad y proporcionarlo al usuario. Al seleccionar el viscosímetro adecuado debe considerar factores como la precisión requerida, el rango de viscosidad y las condiciones ambientales. En la Figura 2.14 se muestra una estación de monitoreo de líquidos con un sensor de viscosidad.

Figura 2.14

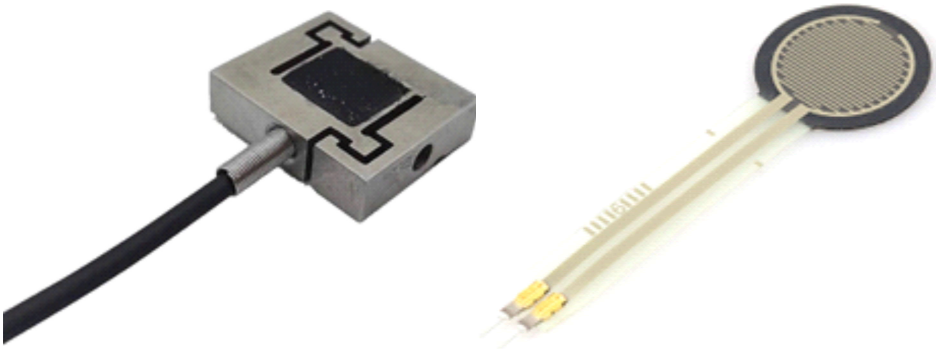
Sensor para medir viscosidad en líquidos

Fuente: (Mecafenix, 2024)

Sensor de presión táctil.- Responden al contacto físico, la fuerza o la presión ejercida sobre ellos. Funcionan como interruptores básicos: al tocar la superficie del sensor, se completa un circuito eléctrico y la corriente fluye; al retirar el contacto, el circuito se interrumpe.Estos sensores tienen una amplia gama de aplicaciones desde teléfonos móviles hasta mandos a distancia y paneles de control. En la Figura 2.15 se muestra dos tipos de sensores de presión táctil.

Figura 2.15

Dos tipos de sensores para medir la presión táctil

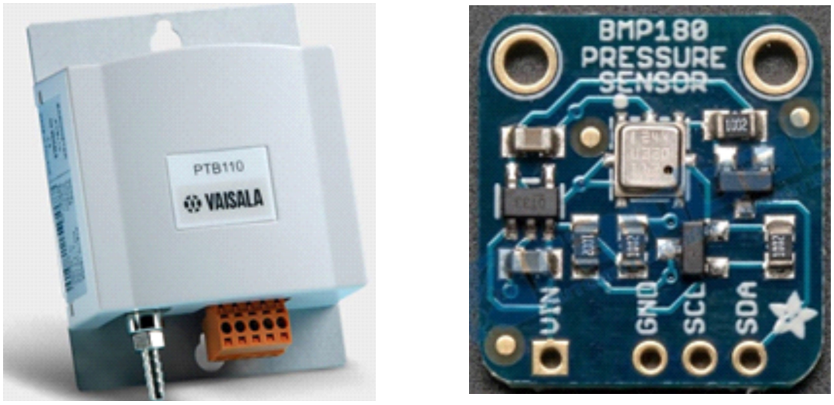


Fuente: (Sick, 2024)

Barómetro.- Es un dispositivo empleado en el ámbito de la meteorología con la finalidad de calcular la presión atmosférica. Más allá de su capacidad para cuantificar la presión del aire, los barómetros proporcionan indicios acerca de las previsiones meteorológicas. Por ejemplo, áreas de alta presión suelen asociarse con condiciones sin precipitaciones, mientras que aquellas de baja presión indican la posibilidad de lluvias y tormentas. En la Figura 2.16 se muestra dos tipos de sensores para medir la presión atmosférica.

Figura 2.16

Dos tipos de sensores barométricos



Fuente: (Vaisala, 2024)

Piezómetro.- Dispositivo sensorial diseñado para medir con precsión la presión del agua subterránea. Su aplicación abarca una variedad de contextos, incluyendo la ingeniería de diques sistemas de tuberías y otros conductos, donde desempeña un papel fundamental en la supervisión y regulación de la presión durante operaciones como excavaciones, sondeos o drenajes. Esta herramienta se considera fundamental para la ejecución segura y precisa de tales trabajos. Entre los diversos tipos de piezómetros disponibles, los más comúnmente empleados son de tubo abierto que miden la profundidad del nivel freático, mientras que los piezómetros de cuerda vibrante controlan tanto el nivel freático como las presiones intersticiales del terreno. No obstante, ambos son esenciales en la monitorización de agua subterránea y proyectos geotécnicos. En la Figura 2.17 se muestra un sensor para medir la presión del agua en el interior de la tierra.

Figura 2.17

Sensor piezómetro

Fuente: (Mecafenix, 2024)

Anemómetro.- Dispositivo utilizado para evaluar la velocidad o intensidad del viento. Aunque registra la velocidad instantánea del viento, este tipo de mediciones pueden ser alteradas por las ráfagas, por lo que la aproximación más precisa se obtiene al calcular el promedio de varias mediciones tomadas en intervalos de tiempo. En la Figura 2.18 se presentan dos tipos de sensores para medir la velocidad del viento.

Figura 2.18

Dos tipos de sensores anemómetros

Fuente: (Sick, 2024)

Caudalímetro.- Se utiliza para medir el flujo volumétrico o masa de un

fluido en una tubería. Estos dispositivos se instalan típicamente en línea con la tubería para monitorear el flujo. Hay variantes mecánicas y eléctricas disponibles. Por ejemplo, los calentadores de agua de paso y las lavadoras emplean caudalímetros eléctricos para determinar el flujo de agua circulante o para llenar el tanque a diferentes niveles. Por otro lado, un hidrómetro permite medir el flujo, la velocidad o la fuerza de los líquidos en movimiento, según su calibración y aplicación específica.En la Figura 2.19, se muestra dos tipos de sensores para medir la cantidad de líquido que pasa por un conducto en un determinado lapso de tiempo.

Figura 2.19

Dos tipos de sensores caudalímetro

Fuente: (Sick, 2024)

Micrófono.- Es un sensor de sonido, desencadena la conversión entre ondas sonoras y energía eléctrica, una función básica en los procesos de grabación y reproducción de audio. Básicamente consiste en un diafragma que responde a las vibraciones, modificando la corriente eléctrica en un circuito debido a las variaciones de presión. Esta transformación electroacústica permite amplificar transmitir y registrar el sonido en una señal eléctrica. En la Figura 2.20 se muestra un sensor acústico y su interior. A la izquierda, se observa el sensor montado en una placa de circuito, y a la derecha, un diagrama detallado del micrófono. Este sensor convierte las ondas sonoras en señales eléctricas, esenciales para aplicaciones de audio.

Figura 2.20

Sensor acústico y su interior (micrófono)

Fuente: (Mecafenix, 2024)

Hidrófono.- Un tipo especializado de dispositivos de captación de sonido son los hidrófonos diseñados para la detección de sonidos bajo el agua, permitiendo identificar la presencia y trayectoria de embarcaciones y determinados organismos marinos. En la Figura 2.21 se muestra un sensor para percibir sonidos bajo el agua.

Figura 2.21

Sensor hidrógrafo

Fuente: (Sick, 2024)

Geófono.- Es un dispositivo sensorial utilizado para capturar las vibraciones del suelo inducidas por actividades como explosiones y el paso de camiones vibradores, operando mediante la transformación de dichas vibraciones en

señales eléctricas. En la prospección sísmica en tierra, los geófonos más comúnmente utilizados son de naturaleza electromagnética.

Higrómetro.- Es un dispositivo utilizado en meteorología para detectar y medir la humedad relativa en el aire, plantas o suelo, expresando estos niveles en porcentaje de 0 a 100 %. La humedad relativa indica la proporción de vapor de agua en el aire respecto a la cantidad que podría saturarlo a una temperatura específica. Los modelos antiguos usaban sensores mecánicos, a menudo basados en el cabello humano por su sensibilidad a los cambios de humedad. Además, el higrómetro a menudo se combina con un sensor de temperatura para una evaluación más completa del ambiente. En la Figura 2.22 se muestran dos tipos de sensores para medir la humedad en el suelo.

Figura 2.22

Dos tipos de sensores higrómetros

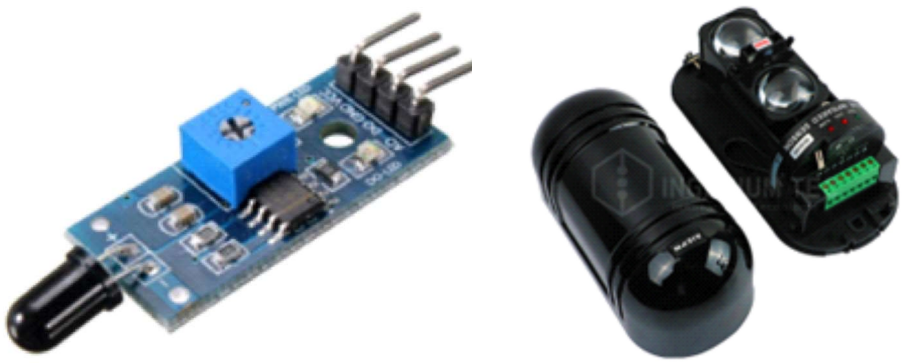
Fuente: (Sick, 2024)

Sensores de infrarrojos.- Es un dispositivo optoelectrónico con la capacidad de detectar la radiación electromagnética infrarroja emitida por los objetos dentro de su alcance visual. A pesar de que esta radiación es invisible para el ojo humano, los sensores infrarrojos pueden captarla eficientemente, ya que opera en el espectro justo por debajo de la luz visible. Estos dispositivos están específicamente diseñados para detectar, clasificar y posicionar objetos, así como para identificar formas, colores y variaciones en la superficie, incluso en condiciones ambientales adversas. En la Figura 2.23 se

muestran dos tipos de sensores infrarrojos para determinar la proximidad de objetos.

Figura 2.23

Dos tipos de sensores infrarrojos



Fuente: (Mecafenix, 2024)

Fotodetector.- Es un dispositivo sensorial que produce una corriente eléctrica en respuesta a la incidencia de luz o cualquier otra forma de radiación electromagnética que capta. Estos dispositivos pueden fundamentarse en diversos principios físicos, como el efecto fotoeléctrico, fotovoltaico fotoelectroquímico o fotoconductivo. En la Figura 2.24 se muestra dos tipos de sensores para determinar proximidad en base a fotoceldas.

Figura 2.24

Dos tipos de sensores fotodetectores

Fuente: (Sick, 2024)

Sensor de llamas.- Posibilita identificar la presencia de combustión mediante la radiación luminosa que esta genera. Esta radiación puede ser percibida por un sensor óptico y registrada. La llama constituye un fenómeno luminoso vinculado a los procesos de combustión. Se utiliza en aplicaciones como sistemas de detección de incendios y calefacción industrial.Además, existen diferentes tipos de sensores, como los de UV, que detectan la radiación emitida por las llamas durante la combustión, y los de IR, que son versátiles para varios tipos de combustiblesExisten diferentes tipos de sensores, como los de UV, que detectan la radiación emitida por las llamas durante la combustión, y los de IR, que son versátiles para varios tipos de combustibles En la Figura 2.25 se muestra un sensor para determinar la pre-sencia de fuego.

Figura 2.25

Sensor de llamas

Fuente: (Mecafenix, 2024)

Contactor de Geiger- Müller.- Es un instrumento diseñado para identificar la presencia de radiaciones ionizantes. Cuando las partículas ionizantes atraviesan el área sensible del detector generan iones que son impulsados por un campo eléctrico, lo que produce un impulso eléctrico que indica la presencia de radiación. Si la intensidad delcampo eléctrico es insuficiente, no se registra ningún impulso, mientras que, si es demasiado alta, se produce una descarga continua incluso sin presencia de radiación. En la Figura 2.26 se muestra un sensor de contactor de Geiger Müller y su estructura interna.

Figura 2.26

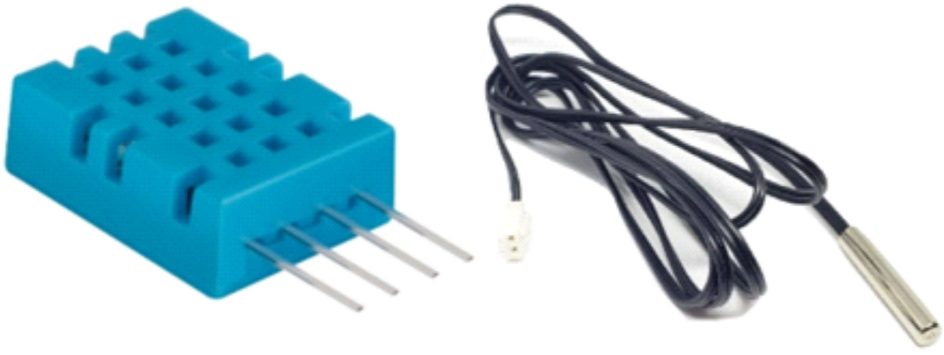
Sensor de Contactor de Geiger Müller y su estructura interna

Fuente: (Sick, 2024)

Termómetro.- Es un dispositivo sensorial diseñado para medir la temperatura, ha experimentado significativas transformaciones desde su concepción inicial, especialmente con el surgimiento y avance de los termómetros digitales. En la Figura 2.27 se presentan dos tipos de sensores para medir la temperatura ambiente.

Figura 2.27

Dos tipos de sensores termométricos



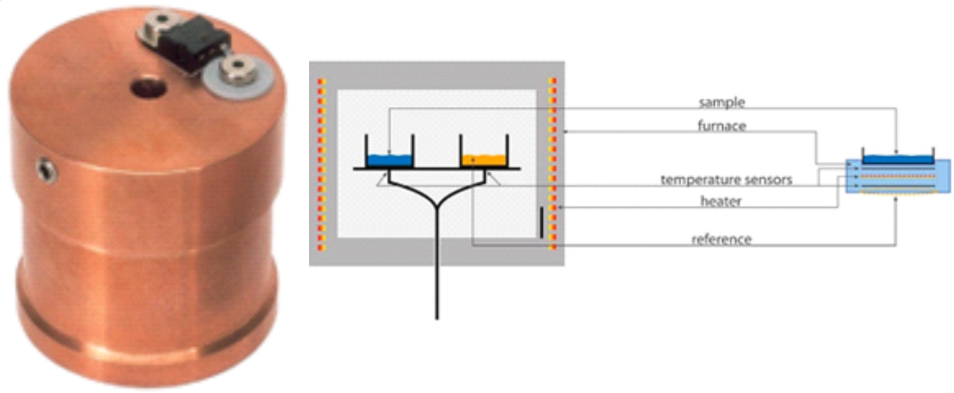
Fuente: (Mecafenix, 2024)

Calorímetro.- Es un dispositivo utilizado para cuantificar las cantidades de calor transferidas a o desde un objeto, se emplea con el propósito de cal-

cular su calor específico. Asimismo, posibilita la medición precisa de las cantidades de calor liberadas o absorbidas por los objetos en cuestión. Existen otros tipos de calorímetros, como la bomba calorimétrica, que mide la cantidad de calor en una reacción a volumen constante. En sistemas solares, de calefacción o refrigeración, el calorímetro desempeña un papel crucial al registrar la energía producida, consumida o transferida para una gestión eficiente de la energía. En la Figura 2.28 se muestra un sensor calorímetros y su estructura interna.

Figura 2.28

Sensor calorímetro



Fuente: (Mecafenix, 2024)

Sensor de glucosa.- Es un dispositivo de monitoreo continuo de glucosa se utiliza para realizar mediciones constantes de glucosa. Consiste en un sensor con un filamento flexible que se inserta debajo de la piel y dura entre 6 y 14 días, según el modelo. Este sensor se comunica con un transmisor que envía la señal a un receptor, como un monitor, proporcionando información sobre las lecturas. A diferencia de los medidores convencionales, que miden la glucosa en la sangre, estos dispositivos miden la glucosa en el tejido intersticial. Esto permite obtener una visión más completa y continua de los niveles de glucosa a lo largo del día, incluso durante el sueño y las actividades diarias. Además, al no requerir punciones frecuentes en los dedos, mejoran la comodidad y la calidad de vida de los pacientes. En la Figura 2.29 se muestra un sensor para medir la cantidad de glucosa en la

sangre.

Figura 2.29

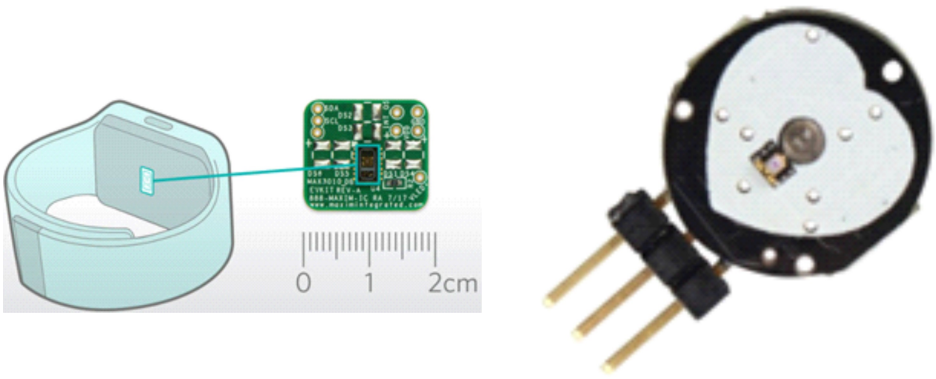
Sensor de glucosa y su aplicación móvil de monitore

Fuente: (Sick, 2024)

Sensor de pulso.- La finalidad del sensor de pulso es monitorear el ritmo cardíaco. Emplea una combinación de amplificación y filtrado de ruido para asegurar la fiabilidad y estabilidad de la señal que registra la actividad cardíaca. Su correcto funcionamiento depende del contacto directo con puntos como el pulgar, la yugular, la muñeca, el brazo y el pecho. En la Figura 2.30 se muestran dos tipos de sensores para medir el pulso humano y su ubicación en un reloj inteligente.

Figura 2.30

Sensor de pulsos y una de sus aplicaciones



Fuente: (Sick, 2024)

2.3.3 Características de un sensor

Un sensor se caracteriza por diversas propiedades que influyen en su elección para una aplicación concreta la magnitud a medir, ya sea posición o movimiento, suele ser el factor principal en la selección del sensor adecuado. Sin embargo, hay varios factores genéricos que determinan la idoneidad de un sensor para una aplicación específica, entre ellos:

a. Exactitud.- La precisión con la que el sensor informa la señal, evidenciada por la ausencia de error.

b. Error.- La discrepancia entre la lectura del sensor y el valor verdadero de la magnitud.

c. Precisión.- La consistencia en las mediciones ante estímulos idénticos, reflejando la repetibilidad y reproducibilidad.

d. Alcance.- El rango de señales dentro del cual el sensor puede operar con precisión, más allá del cual pueden surgir señales inactivas y daños potenciales.

e. Ruido.- Las fluctuaciones no deseadas en la señal de salida, originadas tanto por el sensor como por el entorno externo.

f. Resolución.- El cambio mínimo en la señal de entrada necesario para que el sensor detecte y comunique un cambio en la salida.

g. Selectividad.- La capacidad del sensor para identificar y comunicar selectivamente una señal específica, como en el caso de un sensor de oxígeno que distingue el O_2 entre otros gases.

h. La propiedad de linealidad se refiere a un sensor cuya respuesta es proporcional a la señal de entrada, lo cual elimina la complicación de ajustes no lineales y facilita la calibración.

i. En cuanto a la velocidad, un sensor que pueda proporcionar lecturas precisas de manera más rápida es altamente deseable en circunstancias similares.

Los diversos factores mencionados pueden incidir en la confiabili-

dad de los datos que se obtienen, lo que a su vez influye en la calidad de la información misma. Es importante diferencias claramente entre los conceptos de exactitud, resolución y precisión para una mejor comprensión se presenta a continuación un ejemplo.

Supongamos que tenemos conocimiento de que la temperatura registrada por un dispositivo es de 24,6 ºC, mientras que un termómetro con una resolución de 0,2 ºC nos indica una lectura estable de 25,5 ºC. La precisión del termómetro se sitúa en torno a ± 0,05 ºC o incluso mejor, ya que proporciona una lectura constante, sin variaciones significativas entre mediciones consecutivas, al menos con un grado decimal. Es importante distinguir entre precisión y exactitud en este contexto. Mientras que la temperatura real es de 24,6 ºC, la discrepancia de 0,9 ºC entre esta y la lectura del termómetro representa un error en la medición. La resolución del instrumento es de 0,2 ºC, lo que indica el cambio mínimo que puede detectar. Por ende, no se observará ningún cambio en la lectura del termómetro hasta que la temperatura real varíe en ± 0,2 ºC, es decir, hasta que alcance los 24,4 ºC o los 24,8 ºC.

Las principales cualidades que destacan en un sensor son las siguientes:

Precisión, que se refiere a la capacidad del sensor para generar consistentemente la misma respuesta ante una entrada dada.

Resolución, la cual indica la habilidad del sensor para detectar con fiabilidad incluso los cambios más mínimos en el parámetro que está midiendo.

2.3.4 Configuración y calibración de sensores

La calibración implica ajustar y caracterizar un sensor o instrumento de medición mediante la comparación con un estándar de referencia. Durante este proceso, el sensor o instrumento se somete a señales de entrada conocidas, y sus medidas se contrastan con las de un dispositivo de referencia. Esta comparación permite corregir y ajustar el sensor para que se asemeje lo más posible al estándar utilizado en la calibración. La necesidad de calibración surge debido a que ningún sensor es perfecto con problemas

de precisión, ruido y otros desafíos comunes.

Los problemas comunes que requieren calibración incluyen:

a. Variaciones de fabricación.- Incluso sensores de la misma serie pueden dar lecturas ligeramente diferentes debido a diferencias entre lotes de producción.

b. Diseño del sensor.- Sensores diferentes pueden reaccionar de manera distinta en condiciones similares, especialmente los sensores indirectos que calculan mediciones basadas en parámetros relacionados pero diferentes.

c. Influencias ambientales. Factores como calor, frío, golpes o humedad durante el almacenamiento, transporte o montaje pueden afectar la respuesta del sensor.

d. Envejecimiento tecnológico.- La respuesta de algunos sensores puede cambiar con el tiempo debido al envejecimiento natural de la tecnología, lo que requiere recalibración periódica.

Además, es importante considerar que el sensor constituye únicamente un elemento adicional dentro del conjunto del sistema de medición.

- En sistemas con sensores analógicos, la conversión de la señal a digital se integra dentro del proceso de medición, contribuyendo así a la variabilidad inherente del sistema.
- Las mediciones de temperatura pueden ser influenciadas por gradientes térmicos entre el sensor y el punto de medición, lo que afecta su precisión.
- Sensores de luz y color pueden experimentar interferencias debido a diversos factores como la distribución espectral, luz ambiental, reflexión, y otros fenómenos ópticos.
- Sensores inerciales frecuentemente presentan errores de traslación inicial y son sensibles a la alineación con el sistema de referencia durante la medición.

Los dos factores más relevantes que afectan a la precisión de un sensor al momento de medir son:

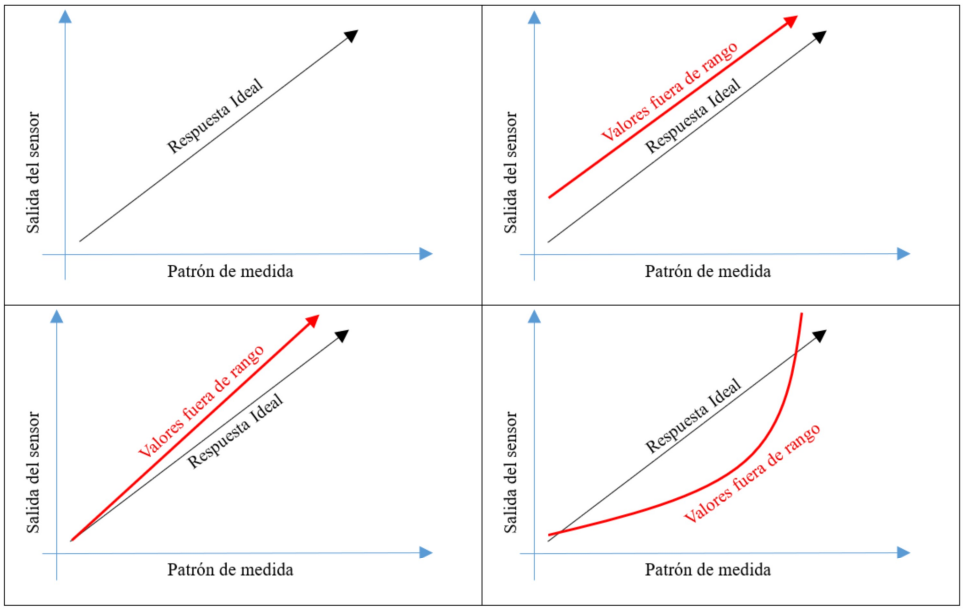
Ruido.- Es una presencia inevitable en todos los sistemas de medición,

hasta cierto punto. En aquellos sistemas donde la relación entre la señal y el ruido es baja, es probable que surjan dificultades para obtener mediciones consistentes de manera repetida. Por otro lado, la **histéresis** es un fenómeno observado en ciertos tipos de sensores, caracterizado por la tendencia del sensor a mostrar lecturas más bajas cuando la señal está aumentando y más altas cuando la señal está disminuyendo. Esta inconsistencia es especialmente prominente en muchos sensores de presión.

Calibración en sensores inteligentes.- En cierta medida, los sensores digitales (inteligentes) son calibrados durante el proceso de fabricación. No obstante, su precisión sigue siendo influenciada por las condiciones variables de fabricación y funcionamiento. Para garantizar mediciones precisas en situaciones críticas, es importante calibrar el sistema en su totalidad. En la Figura 2.31 se muestran los gráficos con los tipos de calibración de un sensor.

Figura 2.31

Tipos de calibración



Fuente: Adaptado de: (Adafruit, 2018)

La calibración de un sensor implica contrastar su medición con otra considerada como precisa. Esta comparación puede realizarse utilizando

diversas referencias, como un **sensor previamente calibrado** reconocido por su exactitud y precisión, o estándares físicos reconocidos, como los proporcionados por el Instituto Nacional de Normas y Tecnología (NIST). Otro patrón puede ser un **punto de referencia físico convencional**, es decir se pueden emplear estándares físicos con precisión adecuada como puntos de referencia para ciertos tipos de sensores.

Estos estándares suelen contar con documentación detallada que incluye la referencia específica utilizada en su calibración, así como cualquier corrección necesaria para asegurar la precisión de la salida del sensor.

Usualmente, cada sensor exhibirá una curva característica que describe su respuesta ante una entrada específica. El procedimiento de calibración busca alinear esta respuesta con una respuesta lineal ideal. El enfoque óptimo para lograrlo varía según la naturaleza de la curva característica, la cual está influenciada por varios factores:

- **Offset.-** Un desfase implica que la salida del sensor es mayor o menor que la salida ideal. Estos desajustes pueden corregirse fácilmente mediante una calibración de un solo punto.

- **Sensibilidad o pendiente.-** Las disparidades en la pendiente indican que la respuesta del sensor cambia a una velocidad diferente de la ideal. La calibración de punto doble puede subsanar estas diferencias de pendiente.

- **Linealidad.-** La mayoría de los sensores no presentan una curva característica completamente lineal. Aunque algunos son lo suficientemente lineales dentro de su rango de medición como para no suponer un problema, otros requieren cálculos más complejos para linealizar su salida.

2.3.5 Elementos que influyen en la incorporación

Los avances en la tecnología de sensores se ven impulsados por tres factores clave: el **precio**, la **capacidad** y el **tamaño**. A medida que estos dispositivos se vuelven más asequibles, más sofisticados y más compactos, su utilidad se amplía considerablemente (French & Jung, 2016). Por ejemplo, el costo promedio de un acelerómetro ha disminuido significativamente

en los últimos años, pasando de 2 dólares en 2006 a tan solo 40 céntimos en la actualidad. Esta tendencia a la baja en los **precios** permite que los sensores sean viables para una variedad de aplicaciones comerciales. Además, la evolución de los microprocesadores ha contribuido a la mejora de la **inteligencia** de estos dispositivos, lo que los hace parte fundamental de sistemas más complejos. Asimismo, el **tamaño** de los sensores ha experimentado una reducción notable, lo que ha facilitado su integración en dispositivos cotidianos como teléfonos inteligentes y prendas de vestir. Por ejemplo, la cantidad de sensores en un smartphone ha aumentado significativamente en los últimos años, lo que abre nuevas posibilidades tanto en el ámbito del consumidor como en el de la salud, con la aparición de biosensores que pueden ser usados e incluso ingeridos.

2.3.6 Desafíos y propuestas de solución

Aunque los sensores pueden ser compactos, eficientes y asequibles, todavía se enfrentan a diversos desafíos. Estos incluyen el consumo de energía, la protección de datos y la compatibilidad, aspectos que son comunes en los dispositivos de Internet de las cosas.

En términos de consumo energético, los dispositivos que alojan los sensores pueden ser alimentados de dos maneras: a través de una conexión constante a la red eléctrica o mediante baterías. Las fuentes de alimentación ofrecen una energía constante, aunque a menudo pueden resultar poco prácticas o costosas. Por otro lado, las baterías pueden ser una alternativa conveniente, pero su vida útil limitada y la necesidad de recargarlas periódicamente, especialmente en áreas remotas, pueden presentar desafíos significativos.

Por tanto, existen dos aspectos principales a considerar en cuanto al consumo energético:

a. Eficiencia.- A pesar de los avances en la tecnología de baterías y el uso de materiales como el silicio algunos sensores pueden funcionar con una sola carga durante más de 10 años, lo que facilita su implementación al reducir la necesidad de reemplazo. Sin embargo, estos beneficios pueden

ser contrarrestados por la creciente demanda de sensores para capturar la información requerida por los sistemas de IoT. En consecuencia, el consumo total de energía puede no disminuir e incluso aumentar en algunos casos.

b. Fuente de energía.- Aunque los sensores dependen principalmente de baterías, el aprovechamiento de fuentes de energía alternativas, como la solar, es una opción viable, al menos como respaldo durante los cambios de batería. No obstante, la instalación de estas fuentes de energía sigue siendo costosa, lo que desalienta a muchas empresas debido a la falta de fiabilidad asociada con su suministro.

La **seguridad** de los sensores se presenta como uno de los desafíos más importantes en la actualidad generando una preocupación significativa en el campo. Abordar esta problemática desde su origen se muestra como una estrategia lógica, aunque se encuentran obstáculos importantes. A pesar de la posibilidad de implementar algoritmos criptográficos complejos para garantizar la integridad de los datos, las limitaciones de potencia de procesamiento, memoria y consumo energético en los dispositivos pueden restringir la efectividad de esta medida de seguridad. Es importante que las empresas sean conscientes de estas limitaciones al planificar sus implementaciones de IoT.

Por otro lado, la **interoperabilidad** también surge como un desafío significativo, con la probabilidad de que persistan problemas en este ámbito. Esto se debe a que la mayoría de los sistemas de sensores actualmente en funcionamiento son propietarios y diseñados para aplicaciones específicas, lo que conlleva a problemas de interoperabilidad en términos de comunicación, intercambio almacenamiento y seguridad de datos, así como escalabilidad. Se requiere el establecimiento de protocolos de comunicación que faciliten la interoperabilidad entre sistemas de sensores heterogéneos. Dadas diversas limitaciones técnicas como la baja potencia de procesamiento capacidad de memoria y disponibilidad energética a nivel de sensor, es importante recurrir a estándares y protocolos ampliamente aceptados para reducir los problemas de interoperabilidad que puedan surgir.

A continuación, en el siguiente código QR se presenta el enlace a un video explicativo complementario acerca de los sensores, actuadores y el hardware inmerso en las redes IoT.

CAPÍTULO III:
PROTOCOLOS Y REDES DE COMUNICACIÓN

3.1 Introducción y Objetivos del capítulo

Los sensores y otros dispositivos se integran en redes que emplean una variedad de dispositivos de red, como *hubs, gateways, routers*, puentes de red y conmutadores, según lo requiera la aplicación específica. En el contexto del Internet de las Cosas, la conectividad presenta una amplia gama de alternativas: desde conexiones móviles, satelitales, *Wi-Fi, Bluetooth*, RFID y NFC hasta redes de baja energía y *Ethernet*, entre otras.

El Internet de las cosas se basa principalmente en tecnologías de redes inalámbricas, siendo el 5G la opción destacada en la actualidad. Esta nueva generación de tecnología móvil promete incrementar la velocidad de conexión y minimizar la latencia, lo que resultará en una proliferación exponencial de dispositivos conectados. Dicho de otro modo, el 5G habilitará una conectividad constante y veloz entre dispositivos, permitiendo una interacción fluida. Además del 5G, también se emplean otras tecnologías inalámbricas como las LPWAN, diseñadas para transmitir pequeñas cantidades de datos a grandes distancias con un consumo energético mínimo. En base a este contexto se establecen los siguientes objetivos a ser alcanzados en el presente capítulo.

- Adquirir un entendimiento de las diversas clasificaciones de protocolos de comunicación destinados específicamente para el IoT.

- Desarrollar la capacidad de discernir las características fundamentales que permiten clasificar cada protocolo IoT, facilitando así la identificación del más apropiado para cada situación sin verse limitado por una tecnología específica.

- Conocer el funcionamiento interno y la estructura de los sistemas de comunicación entre máquinas diseñados especialmente para IoT.

- Comprender las distintas partes que conforman las jerarquías de comunicación diseñadas específicamente para el paradigma IoT.

- Investigar las principales tecnologías IoT disponibles en el mercado y determinar su óptima aplicación en diversos contextos.

3.2 Protocolos de comunicación

El ideal de comunicación óptima sería aquella que requiera un mínimo de energía, tenga un alcance amplio y pueda transmitir grandes volúmenes de datos, es decir, un ancho de banda significativo. Lamentablemente, tal sistema de comunicación perfecta no está disponible en la realidad. Cada forma de comunicación implica un equilibrio entre estos tres aspectos. La conectividad juega un papel importante en el IoT, por lo tanto, comprender las opciones disponibles es fundamental para el desarrollo fluido y económico de un proyecto.

3.2.1 Generalidades y Clasificación

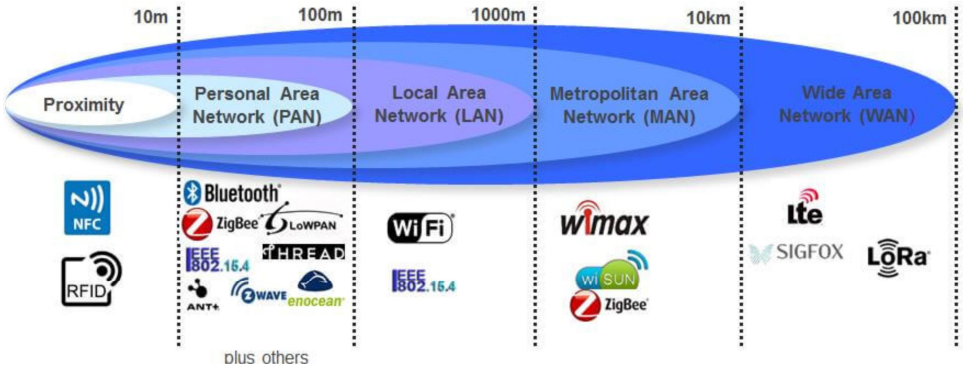
La interacción entre dispositivos similares se denomina comunicación máquina a máquina, abreviada como M2M. Los protocolos de red constituyen un conjunto de normativas que especifican el modo en que los distintos dispositivos y máquinas se identifican y se comunican entre sí. La selección de una tecnología de red se ve influenciada en gran medida por la ubicación geográfica que se pretende abarcar.

Clasificación de las redes según el alcance.- Cuando se trata de transmitir datos en distancias cortas como dentro de un entorno como una habitación, los dispositivos suelen recurrir a tecnologías de redes de área personal (PAN). Ejemplos comunes de tecnologías inalámbricas utilizadas en este contexto incluyen Bluetooth y ZigBee, mientras que el uso de cables puede implicar tecnologías como Universal Serial Bus (USB). En contraste, para la transferencia de datos en áreas más extensas, como una oficina, se recurre a tecnologías de redes de área local (LAN). Entre las opciones de LAN, se encuentran las conexiones por cable Ethernet y las conexiones inalámbricas, como Wi-Fi. Por último, para la transmisión de datos en áreas más amplias, que pueden extenderse más allá de los límites de edificios y ciudades, se establece una red de área extendida (WAN) que conecta múltiples redes de área local a través de dispositivos como *routers*. Internet y

las tecnologías asociadas son ejemplos destacados de una WAN. Como se muestra en la Figura 3.1.

Figura 3.1

Tecnologías, protocolos y alcance según las redes



Fuente: (Crespo, 2014)

Clasificación de redes según el tipo de protocolo.- Existen diversas categorías de clasificación que permiten categorizar las distintas clases de redes y las tecnologías asociadas. Por un lado, los protocolos de red pueden dividirse en dos grupos: propietarios y abiertos. Los protocolos de red **propietarios o patentados** posibilitan la interacción identificación y validación de máquinas con un conjunto específico de hardware y software, lo que simplifica la personalización y brinda a los fabricantes la oportunidad de destacar en un mercado sumamente competitivo. Por otro lado, los protocolos **abiertos** facilitan la interoperabilidad entre dispositivos de distintas características, lo que favorece la escalabilidad del sistema.

Clasificación por el tipo de medio de transmisión.- Las tecnologías de red se pueden agrupar en dos categorías principales: cableadas e inalámbricas. Las redes **inalámbricas** proporcionan conveniencia al permitir una conectividad prácticamente continua, lo que se ajusta perfectamente a las necesidades modernas de movilidad y ubicuidad tanto para usuarios como para dispositivos. Por otro lado, las conexiones **por cable** siguen siendo relevantes y altamente efectivas, especialmente para rutas de red que requieren mayor fiabilidad, seguridad y capacidad de transferencia

de datos.

Clasificación de las redes protocolos y tecnologías según el propósito.- Protocolos de **propósito general**, ampliamente adoptados como IP y SNMP que han sido fundamentales en la gestión, supervisión y configuración de dispositivos de red, así como en el establecimiento de conexiones de comunicación, han sido pilares durante muchos años. Por otro lado, protocolos más **livianos** como CoAP han sido diseñados específicamente para cumplir con las demandas de dispositivos con recursos limitados y hardware reducido. Además, existen protocolos y APIs **específicos** de ciertos dispositivos o proveedores, los cuales suelen requerir un entorno de desarrollo específico y un conjunto particular de herramientas.

La selección de una tecnología de red para una aplicación específica implica considerar tanto las velocidades de transferencia de datos como los requerimientos de energía. Por ejemplo, tecnologías como 4G (LTE, LTE-A) y 5G son preferibles para aplicaciones de IoT debido a su capacidad para transferir datos a alta velocidad. Por otro lado, tecnologías como *Bluetooth Low Energy* y *Low Power Wi-Fi* son más adecuadas para dispositivos que necesitan un consumo energético bajo. A continuación, se llevará a cabo un análisis de los aspectos clave que han facilitado el desarrollo de IoT en términos de protocolos y tecnologías de red. Asimismo, se identificarán los desafíos que aún persisten y requieren ser superados en la actualidad.

Durante las últimas tres décadas, hemos sido testigos de un notable aumento en las **velocidades** de transmisión de datos, evolucionando desde los modestos 2 Kbps hasta alcanzar la asombrosa cifra de 1 Gbps en la actualidad. Este progreso ha revolucionado la transferencia de archivos pesados y ha habilitado una amplia gama de modelos de comunicación avanzados, como la transmisión de datos multimedia. La transición entre distintas generaciones de redes inalámbricas, desde GSM hasta LTE y actualmente 5G, ha marcado un salto cualitativo en cada etapa, abriendo nuevas posibilidades de comunicación e interacción tanto entre usuarios como con dispositivos.

En el ámbito de las **tarifas de acceso a Internet**, el precio que cobran los proveedores por transferir datos entre puntos de la red es fundamental. Dado el alcance global de la red, estos proveedores dependen en gran medida de interconexiones y pasarelas para la transmisión eficiente de datos.

La **eficiencia energética** ha cobrado una importancia creciente con el incremento del número de dispositivos conectados. Ejemplificando este avance, el protocolo *Bluetooth* de baja energía consume aproximadamente un 50% menos de energía que su contraparte clásica, lo que resulta fundamental en un entorno donde la optimización de recursos es importante.

La **adopción de IPv6** ha sido impulsada por su vasto espacio de direcciones, lo que lo convierte en el protocolo preferido para dispositivos nuevos. Las empresas están migrando sus dispositivos de IPv4 a IPv6 para aprovechar sus ventajas. El crecimiento en la capacidad para IPv6 es evidente, con un aumento del 33% en sitios web habilitados para IPv6.

Desafíos y propuestas de soluciones.

A pesar de los avances en las tecnologías de red, que han incrementado las velocidades de transferencia de datos y han reducido los costos asociados, persisten desafíos significativos en este ámbito. Entre ellos se encuentran:

La **interconexión** de dispositivos, donde la Ley de *Metcalfe* establece que el valor de una red es proporcional al cuadrado del número de dispositivos compatibles, lo que implica que el crecimiento del ecosistema IoT depende de la cantidad de dispositivos conectados. Sin embargo, conectar nuevos dispositivos puede resultar costoso y complejo, ya que suele requerir pasarelas adicionales, y puede aumentar la dificultad en la gestión de la seguridad.

La **penetración de la red** es otro desafío, especialmente en el contexto de IoT de banda ancha, donde tecnologías como LTE y LTE-A tienen una penetración limitada, y el despliegue de 5G aún está pendiente. Los altos cos-

tos involucrados han llevado a los operadores de red a seguir un enfoque gradual en la creación de una infraestructura adecuada para soportar el crecimiento masivo de dispositivos IoT, aprovechando las inversiones previas en tecnología.

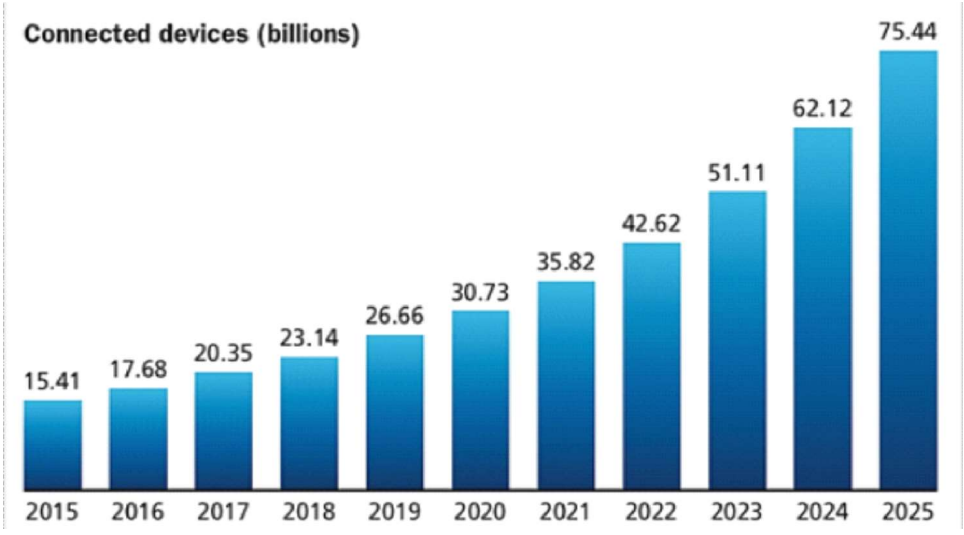
La **seguridad** representa una preocupación creciente, con la proliferación de dispositivos conectados a la red, lo que requiere una autenticación y control de acceso efectivos. Aunque IPv6 incluye una capa de seguridad llamada IPSec, los riesgos de seguridad persisten, comprometiendo la privacidad y generando problemas adicionales.

El **consumo de energía** es crucial para dispositivos conectados. La gestión de la energía puede mejorar mediante la implementación de protocolos que consideren el consumo energético y la gestión automatizada de encendido y apagado, lo que puede optimizar la eficiencia energética de las redes. Estos protocolos determinan rutas eficientes y permiten estados latentes sin afectar la funcionalidad.

En la Figura 3.2 se muestra la cantidad de dispositivos conectados a internet y la proyección de crecimiento a futuro.

Figura 3.2

Cantidad de dispositivos conectados a internet



Fuente: (Corning, 2019)

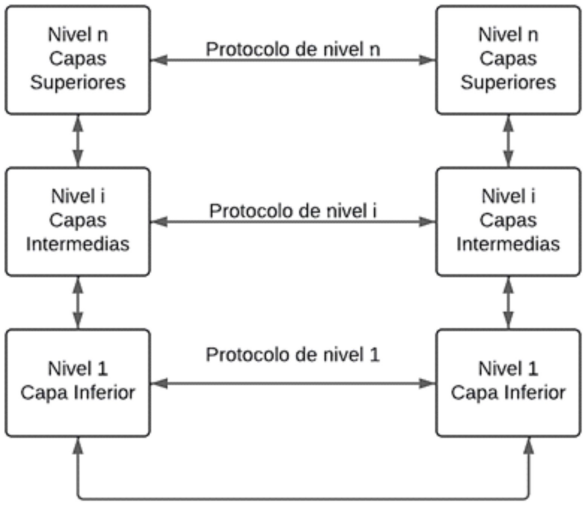
3.2.2 Prototipo en base a segmentos

Los protocolos de red desempeñan un papel fundamental en la administración de la comunicación entre dispositivos. Al hablar de la arquitectura de red, se refiere a un conjunto de tecnologías, servicios y protocolos diseñados para facilitar el intercambio de información entre puntos específicos dentro de una red de computadoras o dispositivos en general. La configuración de una arquitectura de red típicamente se caracteriza por tres elementos principales: la **topología**, que describe la disposición física de los dispositivos; el **método de acceso a la red**, pertinente cuando se comparte un medio de transmisión; y los **protocolos de comunicación**, que establecen las normas y reglas para la transmisión de datos y la corrección de errores.

En la actualidad, las redes se estructuran en distintos niveles o estratos para simplificar su diseño. Cuando dos dispositivos se comunican, los protocolos en el mismo nivel coordinan el proceso. Estos protocolos, llamados "protocolos de nivel n", aseguran que ambos dispositivos sigan las mismas pautas de transmisión. El nivel 'n' se refiere a la posición de los procesos en cada máquina, ya sea local o remota. En la Figura 3.3 se muestra el modelo genérico de una red de comunicación.

Figura 3.3

Modelo genérico de una red

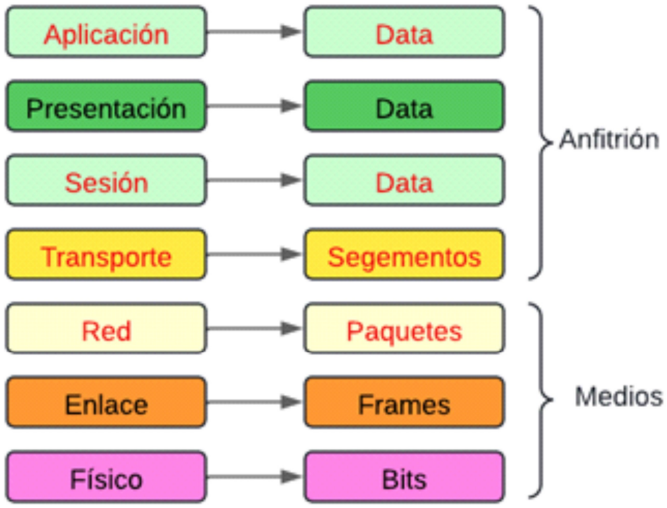


Por otra parte, el modelo *Open Systems Interconnection* (OSI) ha desempeñado un papel fundamental como una arquitectura de referencia en el ámbito de los sistemas de comunicación de información. Fue desarrollado por la Organización Internacional de Estandarización (ISO) en 1983 y ha sido ampliamente utilizado desde entonces. El estándar OSI se estructura en siete niveles, que abarcan desde la interacción física básica entre dispositivos hasta la comunicación avanzada entre aplicaciones utilizadas por los usuarios finales. Este marco incluye capas dedicadas a funciones específicas, como el enrutamiento y gestión de conexiones. Aunque el modelo OSI no define una topología específica ni protocolos de comunicación, establece las funciones necesarias para lograr la interoperabilidad entre sistemas heterogéneos y sirve como una guía para desarrollar cualquier modelo de red aplicable a diversas tecnologías. Los principios teóricos de esta capa se describen a continuación:

- Cada capa de la arquitectura debe desempeñar un conjunto específico de funciones bien definidas.
- El número de niveles debe ser suficiente para evitar la agrupación de funciones distintas, pero no tan grande como para que la arquitectura sea poco manejable.
- Debe crearse una nueva capa cuando se requiera realizar una función diferente del resto.
- El flujo de información entre las capas debe mantenerse al mínimo para simplificar la interfaz.
- Se deben minimizar las posibles repercusiones de las actualizaciones o cambios en funciones o protocolos en una capa determinada en las capas contiguas.
- Es importante aprovechar la experiencia de protocolos anteriores.
- Cada nivel solo debe interactuar con los niveles adyacentes.
- Las funciones de cada capa deben basarse en protocolos estandarizados internacionalmente.

Figura 3.4

Capas del modelo OSI



Por otra parte, el paradigma predominante en el ámbito de Internet en la actualidad es indudablemente el protocolo TCP/IP, concebido en 1973 por el Departamento de Defensa de los Estados Unidos como parte de un programa de investigación en tecnologías de comunicación y transmisión de datos. A lo largo de la década de los ochenta, este protocolo se expandió a nivel global, fusionando una variedad de protocolos preexistentes y amalgamando sus principales capas, adoptando los nombres de estas, es decir, TCP e IP.

Su propósito fundamental radica en facilitar la interconexión entre redes heterogéneas, permitiendo la tolerancia a fallos sin pérdida de datos y posibilitando la utilización de diversas aplicaciones. Este objetivo condujo al desarrollo de una red con una topología irregular, donde la información se descompone en paquetes que siguen rutas diferentes hacia su destino. Como resultado, surgieron dos redes distintas: ARPANET, orientada a la investigación, y MILNET, destinada al uso militar.

El sistema se estructura en cuatro estratos:

Capa de Subred o Acceso a Red.- Esta capa se encarga de la conexión de cada dispositivo a la estación de red, facilitando la comunicación entre dis-

positivos dentro de una misma red.

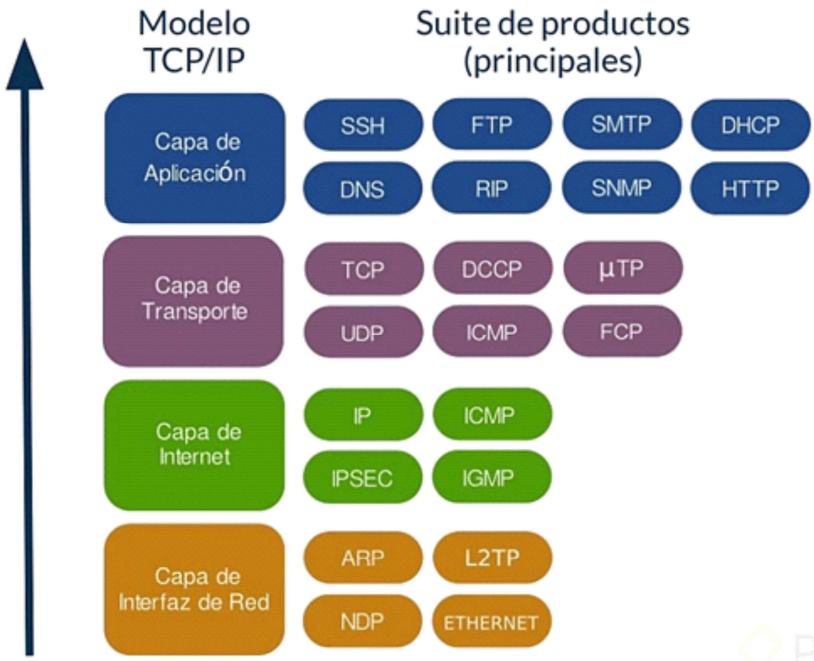
Capa de Inter-Red o Internet.- Aquí, los dispositivos pueden enviar datos a la estación de red, que luego los reenvía a otros dispositivos en redes distintas. Los paquetes atraviesan diversas redes de manera no secuencial.

Capa de Transporte (Punto a Punto).- Esta capa facilita la comunicación entre el origen y el destino, además de gestionar tareas de control de errores y ordenamiento de paquetes. Los protocolos clave en este nivel incluyen TCP (Protocolo de Control de Transmisión), que es confiable y orientado a la conexión, y UDP (Protocolo de Datagramas de Usuario), que es no confiable y no orientado a la conexión, pero mejora el rendimiento en situaciones donde la corrección de errores no es crucial.

Capa de Aplicación.- Facilita la comunicación de alto nivel entre aplicaciones. Aquí se encuentran protocolos importantes como HTTP/S, S/FTP, TELNET/SSH, SMTP, NFS, entre otros.

Figura 3.5

Modelo TCP/IP



Fuente: (Meza, 2021)

Arquitectura de redes IoT.

La efectiva interconexión entre diversos dispositivos representa un requisito fundamental para el IoT. La velocidad, confiabilidad y durabilidad de las conexiones de red influyen considerablemente en la experiencia global. Desde una perspectiva de red y comunicación el IoT se puede concebir como una amalgama de varias redes, que incluyen redes móviles como 3G 4G, CDMA, entre otras, así como redes convencionales como WLAN, WSN, y redes móviles. Con la llegada de redes móviles de alta velocidad como 5G, y la proliferación de protocolos de comunicación para redes locales y urbanas como *Wi-Fi, Bluetooth* y *WiMax*, la creación de una red interconectada de objetos es ya una realidad. Sin embargo, la gestión y la identificación adecuada de los diversos protocolos de comunicación que facilitan la conexión entre estos objetos, así como su función específica, continúan siendo un desafío considerable en la actualidad.

La comunicación *Machine-to-Machine* (M2M) tiene como objetivo facilitar la integración de objetos físicos y virtuales en entornos domésticos y empresariales a nivel global, permitiendo la automatización sin intervención humana. La presión competitiva ejercida por numerosas empresas para maximizar su cuota de mercado y sus ingresos ha resultado en una amplia gama de tecnologías disponibles. Esta diversidad ha generado una alta fragmentación y una baja coherencia en el campo. Por lo tanto, es importante fomentar una estrecha colaboración entre las diferentes capas de comunicación, y considerar los diversos enfoques utilizados por los dispositivos existentes en cuanto al almacenamiento, el intercambio de mensajes, entre otros aspectos.

A continuación, se presentan los principales protocolos y estándares de comunicación que se utilizan comúnmente:

- RFID, representado por la serie ISO 18000, que comprende cinco clases y dos generaciones abarcando tanto las etiquetas RFID activas como las pasivas.

- IEEE 802.11 (WLAN), IEEE 802.15.4, ZigBee, *Near Field Commu-*

nication (NFC) y IEEE 802.15.1 *(Bluetooth)*.

- Estándares de redes inalámbricas de área personal de baja potencia (6LoWPAN) definidos por el IEFT *(Internet Engineering Task Force)*.
- Protocolos M2M tales como MQTT y CoAP.
- Tecnologías de la capa de Internet, como IPv4, IPv6, entre otras.

La elección de los protocolos apropiados durante la etapa de desarrollo puede presentar desafíos y resultar en una tarea de gran complejidad. Esto se debe a varios factores, como la consideración del soporte futuro, la facilidad de implementación y la universalidad de acceso. En esta elección, es fundamental considerar las especificaciones del dispositivo en cuestión, tales como memoria capacidad de procesamiento, almacenamiento y duración de la batería. Estas características influyen en la selección de los medios de comunicación y los protocolos pertinentes. Además, aspectos como la seguridad y el rendimiento requeridos también son determinantes para el despliegue y la ejecución exitosa. La consideración de todos estos aspectos añade complejidad a la identificación de los protocolos y tecnologías de comunicación más adecuados para cada caso específico.

La ausencia de estandarización en aplicaciones y protocolos específicos agrega un riesgo significativo cuando se toman decisiones deficientes en la selección de tecnologías y protocolos. Este desajuste puede dar lugar a errores estratégicos que resultan costosos de rectificar en el futuro. Por consiguiente, para fomentar una adopción más amplia, resulta importante garantizar una documentación y una estandarización, o al menos un proceso encaminado hacia ella, de los protocolos de comunicación.

Por ejemplo, el paradigma de publicación/suscripción se ha convertido en una opción común para la transferencia de mensajes en entornos distribuidos, ya que su simplicidad ha impulsado su adopción en protocolos de comunicación M2M populares como MQTT. Este enfoque resulta eficiente en escenarios dinámicos donde los nodos se unen o abandonan la red con regularidad, y donde las transferencias continuas son necesarias para

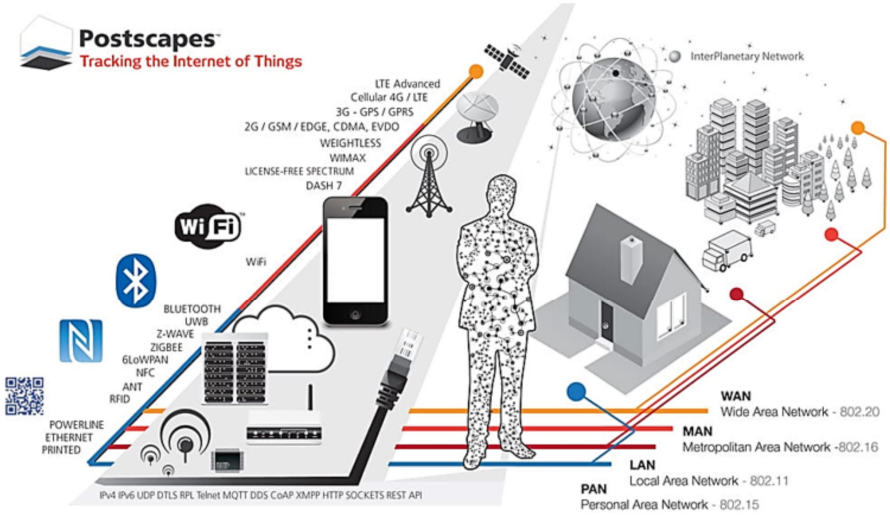
mantener las conexiones activas. Esto se logra mediante notificaciones basadas en *"push"* y el mantenimiento de colas para la entrega de mensajes diferida.

Por otro lado, protocolos como HTTP/REST y CoAP solo admiten el paradigma de petición/respuesta, donde se utiliza un mecanismo de solicitud para obtener nuevos mensajes de la cola. CoAP, además, emplea los protocolos IPv6 y 6LoWPAN en su capa de red para la identificación de nodos.

A pesar del progreso gradual hacia la madurez de estos protocolos, todavía persisten esfuerzos para fusionarlos y normalizarlos, con el objetivo de respaldar tanto los modelos de publicación/suscripción como los de solicitud/respuesta.

Figura 3.6

Tecnologías y protocolos en IoT



Fuente: (Harwood, 2019)

3.2.3 Tecnologías y modelos base

Cuando se elige una tecnología de comunicación, es importante considerar las capas arquitectónicas disponibles en cualquier red, para poder seleccionar la tecnología más apropiada para cada una. Un desafío significativo radica en la falta de interoperabilidad entre tecnologías, lo que difi-

culta la evolución de una pila tecnológica de protocolos seleccionada para las comunicaciones en el IoT.

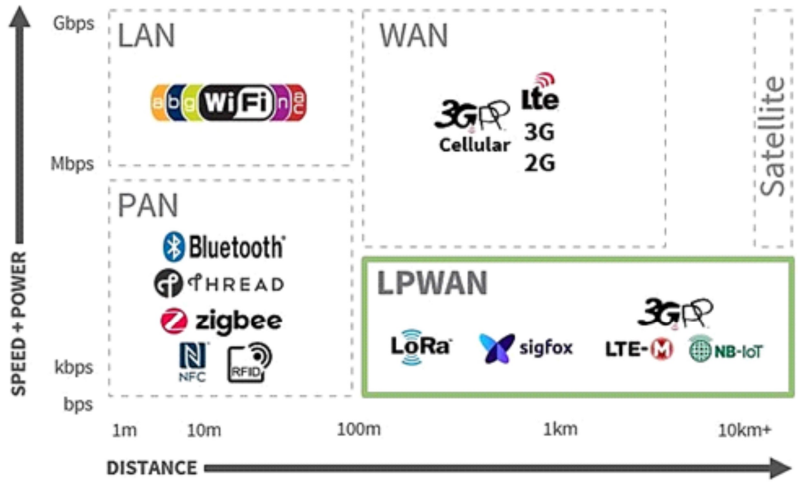
Por lo tanto, se sigue un orden específico de análisis de estas capas arquitectónicas. En primer lugar, se examinan los niveles inferiores que establecen la conexión entre los dispositivos. Los criterios principales a tener en cuenta suelen ser el consumo energético, el ancho de banda y el alcance. Según estas variables, en el mercado se pueden identificar dos grupos principales:

- Tecnologías con bajo alcance, bajo consumo y bajo ancho de banda. Este grupo comprende una variedad de protocolos como *z-wave, Bluetooth* y *ZigBee*, entre otros. Sin embargo, estos protocolos presentan el problema de una falta de interoperabilidad desde su concepción, al ser desarrollados como protocolos propietarios por diferentes entidades empresariales y organismos internacionales independientes.

- Tecnologías con mayor o gran alcance, mayor consumo y mayor ancho de banda. Este grupo incluye revisiones de estándares ampliamente utilizados como *Wi-Fi*, así como redes móviles como LTE, junto con estándares más nuevos y específicos como *Sigfox* o *LoRa/LoRaWAN.*

Figura 3.7

Cuadro comparativo entre protocolos IoT

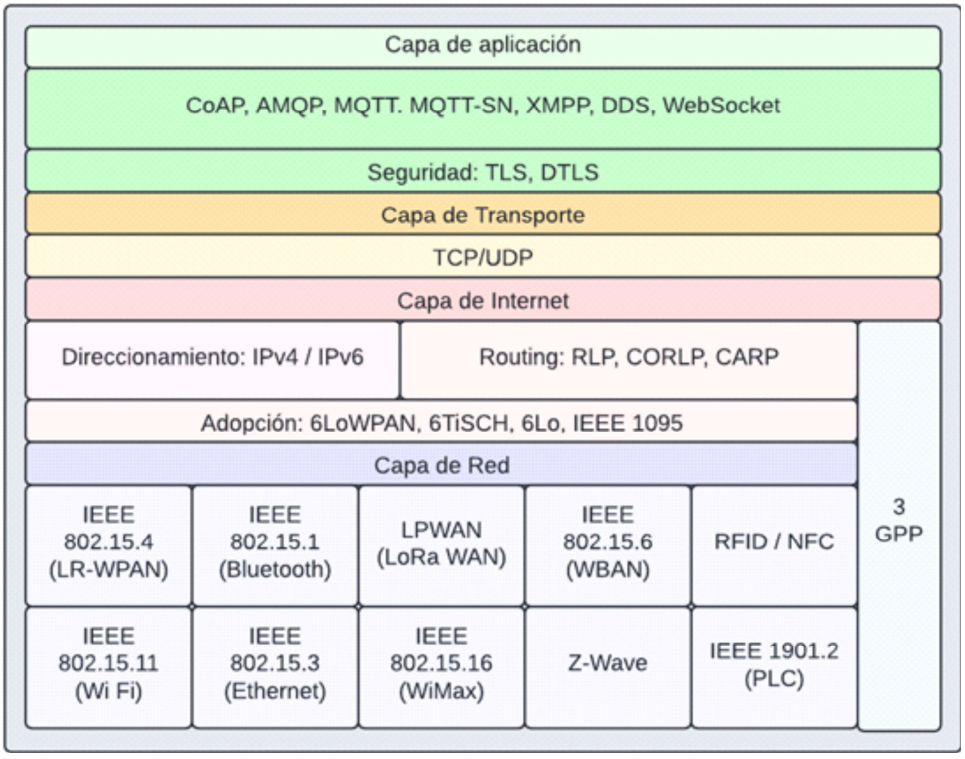


Fuente: (Bassi, 2021)

En lo que respecta a las capas intermedias o de red, comúnmente se distinguen dos categorías de protocolos. Por un lado, se encuentran los protocolos de **enrutamiento**, los cuales facilitan la conexión a Internet tanto de forma directa desde los dispositivos como a través de pasarelas. Por otro lado, están los protocolos de **encapsulación**, que ajustan las tramas IPv6 para que puedan ser empleadas por dispositivos ligeros que utilizan protocolos más simples en las capas de enlace. En cuanto a las capas superiores, por lo general, el IoT hace uso de TCP y UDP en la capa de transporte, aunque existen varios protocolos significativos a considerar en la capa de sesión, entre los que destacan MQTT y, más recientemente, CoAP.

Figura 3.8

Protocolos IoT según capa



Fuente: Adaptado de: (Čolaković & Hadžialić, 2018)

Tecnologías y protocolos en capas inferiores.

Esta estrata alberga una serie de protocolos fundamentales en el ám-

bito tecnológico, los cuales son empleados para la conexión física entre dispositivos, y en ocasiones, también abarcan el acceso a redes. Sin embargo, existen numerosos protocolos adicionales que pueden ser empleados con este propósito, como PLC, WBAN, Ethernet, entre otros.

Tecnologías y protocolos en capas intermedias.

Esta sección aborda diversos protocolos empleados comúnmente en el enrutamiento de aplicaciones de IoT. Dentro de estas categorías de protocolos, se distinguen aquellos que facilitan el enrutamiento desde los dispositivos hasta la red y los que posibilitan la encapsulación de tramas y la conversión entre protocolos. A continuación, se presentan las tecnologías clave en uso en la actualidad.

Los Protocolos de **Enrutamiento** son fundamentales para dirigir los datos desde los dispositivos hacia Internet. En el ámbito de IoT, los principales protocolos de enrutamiento son los siguientes:

Protocolo de Enrutamiento para Redes de Baja Potencia y con Pérdidas (RPT).- Se trata de un protocolo de vector de distancia capaz de adaptarse a una amplia gama de protocolos de capas inferiores, incluyendo aquellos discutidos anteriormente. Utiliza un grafo acíclico dirigido orientado a destino para el enrutamiento, garantizando una única ruta desde cada nodo de hoja hasta la raíz.

Protocolo de Enrutamiento Consciente del Canal (CARP).- Diseñado para la comunicación subacuática, este protocolo distribuido es adecuado para aplicaciones de IoT debido a su eficiencia en el manejo de paquetes. Evalúa la calidad del enlace basándose en datos históricos de transmisión recopilados de sensores cercanos para seleccionar los nodos de reenvío. Sin embargo, su principal limitación radica en su incapacidad para reutilizar datos previamente recopilados, lo que puede no ser beneficioso para aplicaciones que requieren datos solo en casos de cambios significativos.

Protocolos de encapsulación.

El principal estándar en esta área es conocido como 6LoWPAN, que

significa IPv6 sobre Red de Área Personal Inalámbrica de Baja Potencia. Este estándar, tanto pionero como el más prevalente en su categoría, eficientemente encapsula los encabezados largos de IPv6 en paquetes pequeños IEEE802.15.4, limitados a 128 bytes. Su especificación es adaptable, permitiendo la compatibilidad con diversas longitudes de direcciones, ancho de banda reducido, variadas topologías como estrella o malla, así como también facilita la gestión del consumo de energía, bajos costos, escalabilidad de redes, movilidad, falta de fiabilidad y largos tiempos de espera. Este estándar proporciona herramientas como compresión de encabezados para minimizar la sobrecarga de transmisión fragmentación para ajustarse a la longitud máxima de trama de 128 bytes en IEEE802.15.4, y soporte para entrega multipunto. Además de 6LoWPAN, existen otros estándares como IPv6 para Bluetooth de Baja Energía, 6Lo, entre otros.

Tecnologías y protocolos en capas superiores.

En principio, se destaca la prevalencia del uso de TCP o UDP en la capa de transporte de la mayoría de las aplicaciones, incluidas las relacionadas con el IoT. No obstante, en el ámbito de IoT, existen diversos protocolos estandarizados en la capa de sesión, los cuales serán resumidos en esta sección.

La elección del protocolo de capa de sesión adecuado depende en gran medida de la naturaleza de la aplicación específica. Es relevante mencionar que MQTT es ampliamente preferido en IoT debido a su eficiencia en términos de consumo de energía y baja sobrecarga.

MQTT, fue concebido por IBM en 1999 y estandarizado por OASIS en 2013. Su función principal radica en facilitar la conectividad embebida entre las aplicaciones y el *middleware*. Adopta un modelo de **publicación/suscripción**, conformado por editores, suscriptores y un intermediario *(broker)*.

Desde la perspectiva del IoT, los editores corresponden a los sensores ligeros que se conectan al broker para transmitir datos, mientras que los suscriptores son las aplicaciones interesadas en información específica pro-

veniente de los dispositivos. Los *brokers* clasifican los datos en temas y los envían a los suscriptores correspondientes.

Por otro lado, el Protocolo Avanzado de Colas de Mensajes **(AMQP)** constituye otro protocolo de capa de sesión diseñado inicialmente para el sector financiero. Opera sobre TCP y sigue un modelo de publicación/suscripción similar al de MQTT. No obstante, en este caso, el *broker* se divide en intercambiadores y colas, siendo el primero responsable de recibir y distribuir los mensajes a las colas según criterios predefinidos.

El Protocolo de Aplicación *Constrained* **(CoAP)** representa otra alternativa en el ámbito de los protocolos de capa de sesión. Desarrollado por el grupo de trabajo IETF *Constrained RESTful Environment*, tiene como objetivo ofrecer una interfaz *RESTful* ligera sobre HTTP. Mientras que REST constituye la interfaz estándar entre clientes HTTP y servidores, para aplicaciones de IoT con restricciones de energía, CoAP surge como una solución más adecuada, al emplear UDP en lugar de TCP y ofrecer un mecanismo liviano para la comunicación.

La arquitectura CoAP se estructura en dos subcapas principales: la de **mensajería** y la de **solicitud/respuesta**. La primera se encarga de la fiabilidad y la duplicación de los mensajes, mientras que la segunda facilita la comunicación. CoAP utiliza peticiones *GET, PUT, PUSH* y *DELETE* similar a HTTP, para realizar acciones como recuperar, crear, actualizar y eliminar datos.

Por otro lado, el *Data Distribution Service* **(DDS)** es un protocolo de publicación/suscripción desarrollado por el *Object Management Group* (OMG) para comunicaciones M2M. Su principal ventaja radica en la calidad de servicio y la fiabilidad que ofrece, basada en una arquitectura sin intermediarios adaptada a IoT y M2M. DDS proporciona 23 niveles de calidad de servicio que abarcan aspectos como seguridad, urgencia, prioridad, durabilidad y fiabilidad.

DDS se compone de dos subcapas: la de **suscripción** de publicaciones, centrada en la entrega de mensajes a los suscriptores, y la de **re-**

construcción de datos locales, opcional y facilitadora de la integración de DDS en la capa de aplicación. La capa de editores se encarga de distribuir datos sensoriales, mientras que los escritores de datos acuerdan los datos y cambios a enviar a los suscriptores. Los abonados son receptores de datos que deben entregarse a la aplicación IoT, mientras que los lectores de datos se encargan de leer los datos publicados y entregarlos a los suscriptores. Los temas representan los datos que se están publicando, y los escritores y lectores de datos asumen responsabilidades similares a las de un intermediario en arquitecturas de este tipo.

3.3 Redes inalámbricas y 5G

En este apartado se aborda las características de las diferentes redes inalámbricas que se pueden utilizar en un sistema IoT, de manera especial la red inalámbrica 5G por ser la que brinda más beneficios.

3.3.1 Sistemas de comunicación inalámbrica y tecnología 5G

Las principales tecnologías utilizadas en el ámbito del Internet de las Cosas se centran en las redes inalámbricas, destacando en la actualidad el 5G. Esta última representa una innovación en las comunicaciones móviles al incrementar la velocidad de conexión y minimizar la latencia, lo que resultará en un significativo aumento en la cantidad de dispositivos conectados.

3.3.2 Tecnologías 5G

La adopción de la tecnología 5G promete una mejora significativa en la conectividad y una reducción notable en la latencia, transformando la manera en que nos comunicamos. Este avance, en combinación con el crecimiento y desarrollo del IoT, llevará a una integración más profunda de los objetos cotidianos, como electrodomésticos y vehículos, en nuestra red de comunicaciones en tiempo real. Este cambio tecnológico no solo impactará en la vida diaria, sino que también abrirá nuevas posibilidades en campos como la medicina, la automoción y la agricultura, permitiendo intervenciones quirúrgicas remotas, el despliegue de vehículos autónomos

y el monitoreo agrícola a través de sensores distribuidos en campos de cultivo.

La designación "5G" hace referencia a la quinta generación de redes móviles, marcando un hito en la evolución de la telefonía móvil. Desde sus inicios, las redes móviles han experimentado un progreso notable, desde la limitada capacidad de hablar en los primeros teléfonos de tecnología 1G hasta la introducción de mensajes de texto y conexiones web con la tecnología 2G, seguida por la llegada más fluida a Internet con el 3G, y finalmente, la posibilidad de streaming de video, realidad aumentada y comunicaciones rápidas con baja latencia gracias al 4G.

El principal avance del 5G radica en su velocidad, que alcanza hasta 10 GBps, diez veces más rápida que las principales ofertas de fibra óptica disponibles en el mercado. Esta velocidad permite descargas instantáneas, como la de una película completa en cuestión de segundos. Además, la latencia, es decir el tiempo de respuesta de la red, también experimenta un avance significativo, alcanzando un mínimo teórico de 1 milisegundo, prácticamente imperceptible para los usuarios. Esto posibilita una conexión prácticamente en tiempo real, lo que se traduce en interacciones instantáneas con Internet o la nube.

La combinación de velocidades de descarga ultrarrápidas y una latencia mínima permite una experiencia de interacción instantánea. Por ejemplo, abrir una foto almacenada en la nube es tan rápido como si estuviera en la memoria del dispositivo. Esta mejora tiene un impacto revolucionario en aplicaciones móviles, especialmente en áreas como la telemedicina para operaciones quirúrgicas remotas o la seguridad en vehículos de conducción autónoma. La capacidad del 5G para manejar una mayor cantidad de dispositivos conectados simultáneamente mejora la eficiencia y la confiabilidad de las redes, representa un salto significativo en términos de velocidad, latencia y capacidad de conexión, lo que abre nuevas posibilidades en áreas como la Internet de las cosas, la automatización industrial y la comunicación móvil avanzada. Además, busca reducir el consumo de energía en comparación con tecnologías anteriores. La Tabla 4 ofrece una comparativa

detallada entre las propiedades del 5G y las tecnologías anteriores.

Tabla 3.1

Velocidad y latencia según las tecnologías inalámbricas

Característica	1G	2G	3G	4G	4G+	5G
Velocidad máxima de descarga (Mbps)	0.0024	0.064	2	200	1200	10000
Tiempo de latencia mínimo (milisegundos)	500-700	500	100-250	100	20	1

En resumen, la evolución de las tecnologías móviles desde 1G hasta 5G ha supuesto un aumento significativo en la velocidad máxima de descarga y una reducción considerable en el tiempo de latencia. La tecnología 1G ofrecía una velocidad máxima de descarga de solo 0.0024 Mbps y una latencia de entre 500 y 700 milisegundos, mientras que la 2G mejoró ligeramente a 0.064 Mbps y una latencia de 500 ms. Con 3G, la velocidad aumentó a 2 Mbps y la latencia se redujo a un rango de 100 a 250 ms. La llegada de 4G trajo una velocidad de hasta 200 Mbps y una latencia de 100 ms, y 4G+ mejoró aún más la velocidad a 1200 Mbps y la latencia a 20 ms. Sin embargo, 5G representa un salto cuántico, alcanzando velocidades de hasta 10,000 Mbps y una latencia mínima de solo 1 ms, lo que permite aplicaciones en tiempo real y una conectividad masiva, abriendo la puerta a innovaciones como el Internet de las Cosas (IoT), la realidad aumentada y la telemedicina.

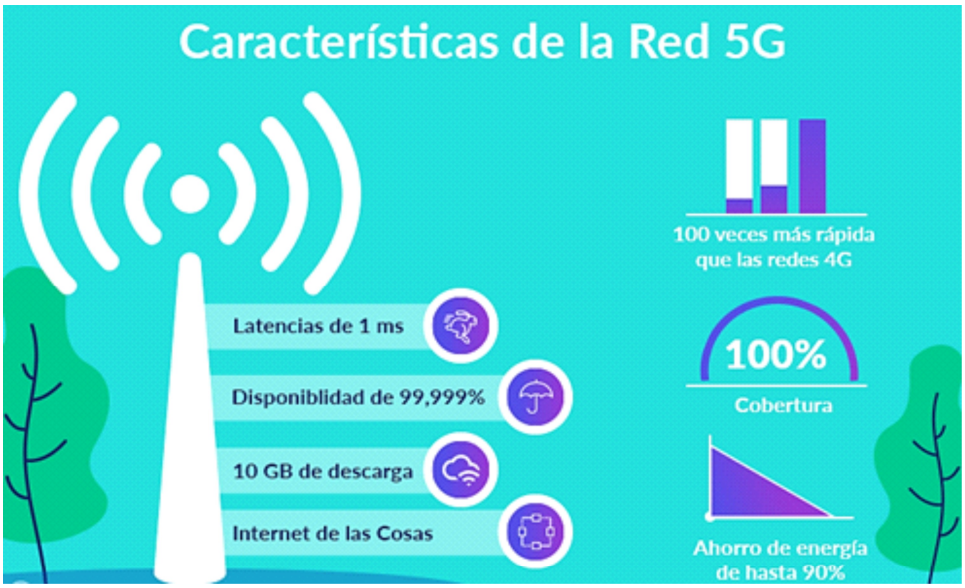
Características de la tecnología 5G.

- Tasa de descarga de datos de hasta 10Gbps, mejorando entre 10 y 100 veces la capacidad de las redes 4G y 4,5G.
- Latencia reducida a 1 milisegundo.
- Banda ancha 1000 veces más rápida por unidad de área.
- Conexión de hasta 100 dispositivos adicionales por unidad de área en comparación con las redes 4G LTE.

- Disponibilidad del 99,999%.
- Cobertura total del 100%.
- Reducción del 90% en el consumo de energía de la red.
- Duración de batería de hasta 10 años para dispositivos IoT de baja potencia.

Figura 3.9

Características de la red 5G



Fuente: (Acuña, 2019)

Adopción de la tecnología 5G.

La proyección de la tasa de adopción de la tecnología 5G contrasta notablemente con las generaciones anteriores de redes móviles, como el 3G y el 4G. Mientras que estas últimas se vieron impulsadas principalmente por el crecimiento del uso de Internet móvil y la popularidad de diversas aplicaciones se anticipa que la 5G será impulsada en gran medida por nuevas aplicaciones de IoT, como los vehículos de conducción autónoma, según (Ericsson, 2019). Se prevé que para el año 2024, la tecnología 5G alcance una cobertura de población del 45 % y 1900 millones de suscripciones, lo que, si se cumplen estas predicciones, la convertiría en la generación de

redes móviles más rápida en ser implementada a nivel mundial.

Asimismo, al igual que la tecnología 4G, la 5G es considerada una tecnología de banda ancha celular y una red de redes. El conocimiento y la experiencia de los operadores de redes móviles en la construcción y gestión de infraestructuras de red serán fundamentales para el éxito de la 5G.

La implementación de redes 5G mientras se mantienen en funcionamiento las redes 3G y 4G probablemente planteará nuevos desafíos en cuanto a la capacidad de frecuencia en el espectro especialmente ante el previsible aumento masivo en dispositivos IoT. Los operadores de redes móviles necesitarán desplegar nuevos espectros en el rango superior a 1 GHz, lo que implicará inversiones significativas en la infraestructura de red. Además, para alcanzar el objetivo de latencia de 1 ms, las redes 5G requerirán conectividad para las estaciones base a través de fibras ópticas.

Desde una perspectiva de reducción de costos, se prevé que las redes 5G sean capaces de soportar ciertas redes virtuales, como las de bajo rendimiento y bajo costo (LPLT), destinadas a IoT económico (aunque actualmente esto sigue siendo una incógnita). A diferencia de la situación actual, donde las redes LORA abordan esta necesidad de forma independiente a la tecnología 4G.

Para los consumidores, la llegada del 5G implica no solo una conectividad móvil más rápida, sino principalmente la conectividad a Internet de una multitud de objetos más allá de lo que se ve hoy en día. Los vehículos autónomos y los hogares totalmente conectados son solo dos ejemplos de la inminente revolución del IoT, respaldada por las redes y la tecnología 5G. Desde 2019, ya están disponibles teléfonos inteligentes y tarjetas SIM compatibles con la tecnología 5G.

Por último, es importante señalar que muchas aplicaciones de IoT, como la domótica y algunas aplicaciones en ciudades inteligentes, solían depender de la conexión inalámbrica Wi-Fi para su despliegue. A pesar de sus ventajas, el Wi-Fi es una tecnología de red de área local con limitaciones en cuanto a alcance operativo, velocidad y latencia. Por lo tanto, la adopción

generalizada de la tecnología 5G resultará en que los servicios de IoT que requieren mayor ubicuidad, movilidad y rendimiento en términos de velocidad y tiempo de respuesta se beneficien considerablemente de las capacidades que ofrece esta tecnología de comunicación.

3.3.3 Redes inalámbricas de largo alcance

La introducción de la tecnología 5G promete transformar el panorama del Internet de las Cosas gracias a su capacidad para ofrecer conexiones en tiempo real y una rápida transmisión de datos con baja latencia. Sin embargo, hay escenarios donde se prioriza el ahorro energético o económico, lo que plantea desafíos para el despliegue de aplicaciones masivas de IoT que involucren numerosos dispositivos.

En tales casos, recurrir a redes inalámbricas de largo alcance y bajo consumo, conocidas como LPWAN *(Low Power Wide Area Network)*, puede ser una alternativa viable. LPWAN, cuyo nombre descompuesto explica su funcionamiento, se destaca por su capacidad para proporcionar conectividad en áreas extensas con un consumo de energía reducido.

El término *"Network"* subraya la necesidad de una infraestructura de red estandarizada para conectar dispositivos IoT de distintos fabricantes. Por otro lado, *"Wide Area"* señala la capacidad de LPWAN para abarcar distancias considerablemente mayores que las redes locales, como el Wi-Fi. Finalmente *"Low Power"* destaca la eficiencia energética de esta tecnología, fundamental para dispositivos alimentados por batería.

El ajuste de estos tres elementos permite a LPWAN adaptarse a aplicaciones donde se requiere alcance extendido y eficiencia energética, aunque la transferencia de datos sea moderada. Ejemplos incluyen la monitorización de humedad del suelo o la gestión de plazas de estacionamiento, donde los cambios son gradualmente previsibles. Sin embargo, actividades que demanden una alta velocidad de transferencia de datos, como la telemetría en competiciones automovilísticas de alta velocidad excederían las capacidades de las redes LPWAN.

3.3.4 Protocolo LoRa y red LoRaWan

LoRaWAN, una tecnología inalámbrica relativamente nueva según (Lauridsen, Vejlgaard, Kovács, Nguyen, & Mogensen, 2017), ha sido concebida para redes WAN (*Wide Area Network*, o Red de Área Amplia) con un rango extenso y consumo energético reducido, además de ser económicamente viable. Esta tecnología ofrece movilidad, seguridad y comunicación bidireccional para aplicaciones de IoT. Se trata de un protocolo eficientemente diseñado para redes inalámbricas escalables, capaces de soportar millones de dispositivos, con capacidad de operar redundante y sin depender de ubicación específica, todo ello manteniendo bajos costos y consumo energético.

LoRa, la tecnología de modulación patentada por *Semtech* (*https://www.semtech.com)*, se ha consolidado como una de las principales en el ámbito de las redes inalámbricas de largo alcance y bajo consumo. Respaldada por una amplia alianza de importantes empresas tecnológicas, LoRa facilita la conexión a larga distancia en aplicaciones de IoT, especialmente en entornos como ciudades inteligentes o áreas con cobertura celular limitada, así como en redes privadas de sensores o actuadores. LoRaWAN, el protocolo asociado que utiliza la tecnología LoRa para la comunicación y gestión de dispositivos, se basa principalmente en dos componentes: **gateways** y **nodos**. Los gateways actúan como intermediarios entre los nodos y la red, mientras que los nodos son los dispositivos finales que envían y reciben datos a través de los gateways. Entre las características principales de LoRaWAN se incluyen:

Topología en estrella, un alcance de 10 a 15 km en línea de visión, encriptación AES 128, soporte para 3 clases de nodos, administración de dispositivos, compatibilidad con redes públicas y privadas, bajo consumo y largo alcance, así como una capacidad de transferencia de datos reducida de hasta 242 bytes.Además, LoRaWAN permite la implementación de soluciones IoT en áreas rurales y remotas donde otras tecnologías de comunicación no son viables, proporcionando una cobertura amplia y fiable. Esta tecnología también es ideal para aplicaciones que requieren una transmisión de datos

poco frecuente pero crítica, como el monitoreo ambiental, la gestión de recursos hídricos y la agricultura de precisión.

Figura 3.10

Aplicaciones con la tecnología LoRa empleando la red LoRaWAN

Fuente: (Kuan, Moko Smart, 2019)

La tecnología LoRa cuenta con las siguientes características:

- Alta tolerancia a las interferencias, con un presupuesto de enlace que disminuye gradualmente a medida que aumenta la distancia entre el emisor y el receptor, siendo esta reducción más moderada en comparación con otras tecnologías, incluso en presencia de obstáculos como muros o árboles.
- Alta sensibilidad para recibir datos (-168dB).
- Basado en modulación *"chirp"*.
- Bajo consumo energético, con una duración de hasta 10 años con una sola batería.
- Alcance teórico de 10 a 20 km, especialmente si se transmite la señal a través de un satélite LoRa, aunque en condiciones normales este alcance se reduce considerablemente debido a obstáculos físicos, alcanzando solo algunos centenares de metros.

- Baja tasa de transferencia de datos, con un máximo de 255 bytes por segundo.

- Conexión punto a punto.

- Frecuencias de trabajo, 868 MHz en Europa, 915 MHz en América y 433 MHz en Asia, siendo necesario verificar la compatibilidad de los dispositivos con la frecuencia deseada antes de su adquisición.

Actualmente, estas frecuencias están disponibles de forma gratuita, sin necesidad de licencias ni suscripciones. La comunidad TTN *(The Things Network)* proporciona una plataforma útil para acceder a los gateways LoRa más cercanos o instalar uno propio. Sin embargo, en algunos países, las compañías de telecomunicaciones están incorporando *gateways* LoRa a sus infraestructuras de comunicaciones móviles para ofrecer servicios mediante suscripción, ampliando así las opciones de conectividad para los usuarios.

3.3.5 Tecnologías inalámbricas adicionales

Además de LoRa y la tecnología 5G, hay una variedad de tecnologías inalámbricas disponibles.

RFID.

La Identificación por Radiofrecuencia es una forma de comunicación que permite el seguimiento e identificación de objetos de manera inalámbrica. Ampliamente utilizada en diversas aplicaciones, desde el seguimiento de productos en la cadena de suministro hasta el control de peajes y la gestión de pacientes en hospitales, la tecnología RFID se ha integrado significativamente de manera casi imperceptible.

Las etiquetas RFID son similares a los códigos de barras, pero con capacidades adicionales, ya que no solo pueden ser leídas sino también actualizadas, modificadas y bloqueadas. Esta tecnología comprende etiquetas y lectores. Las etiquetas pueden ser activas, alimentadas por batería y capaces de transmitir señales independientemente del lector, o pasivas, que se activan cerca de un lector y aprovechan la energía transmitida por este último. Las etiquetas pasivas operan en diferentes frecuencias, como baja

frecuencia (LF), alta frecuencia (HF) y ultra alta frecuencia (UHF).

DASH7.

El protocolo de comunicación inalámbrica DASH7, una variante de RFID según (Weyn, Ergeerts, Wante, Vercauteren, & Hellinckx, 2013), se caracteriza por su operatividad en la banda ISM *(Industrial Scientific Medical)*, accesible a nivel mundial, y su idoneidad para IoT. Este protocolo está especialmente diseñado para ofrecer una cobertura exterior escalable y de largo alcance, con una alta velocidad de transmisión de datos. Además, se destaca por ser una solución de bajo costo que integra funciones de encriptación y admite direccionamiento IPv6. Su arquitectura maestro/esclavo facilita un tráfico ligero, asincrónico y en ráfagas. Las características de DASH7 según lo señalado por (Cetinkaya & Akan, 2015), pueden resumirse de la siguiente manera:

- Filtrado. Las tramas entrantes pasan por tres procesos de filtrado: verificación de redundancia cíclica (CRC), aplicación de una máscara de subred de 4 bits y evaluación de la calidad de los enlaces entre dispositivos. Solo se procesan las tramas que superan estos tres controles.

- Direccionamiento. DASH7 emplea dos tipos de direcciones: el identificador único, conocido como ID EUI-64, y el identificador de red dinámico, que es una dirección de 16 bits designada por el administrador de la red.

- Formato de trama. Las tramas tienen una longitud variable, con un máximo de 255 bytes, e incluyen información como direcciones, subredes, potencia estimada de la transmisión y algunos campos opcionales adicionales.

NFC.

Near Field Comunication (NFC por sus siglas en inglés), en español, Comunicación de Campo Cercano es un protocolo de comunicación basado en radiofrecuencia, desarrollándose como un subconjunto del protocolo de RFID aunque con notables distinciones. Se ha consolidado como una tecnología muy demandada, siendo incluida en aproximadamente el 90% de

los smartphones disponibles en el mercado actualmente. Esta popularidad ha propiciado la proliferación de sistemas de pago sin contacto como *Apple Pay y Google Wallet*.

Los dispositivos NFC intercambian datos al acercarse físicamente entre sí, lo que facilita la transferencia de información como contactos, imágenes o datos de sensores. Además, se emplea en diversas aplicaciones como el desbloqueo de automóviles y la interacción con anuncios publicitarios que requieren la interacción del usuario con su smartphone para acceder a contenido adicional o descargar aplicaciones.

Concebido para comunicaciones de corto alcance, típicamente unos pocos centímetros, NFC se distingue por su eficiencia energética y opera en la banda de 13,56 MHz, compartida con la RFID de alta frecuencia, lo que le permite leer etiquetas HF RFID.

En cuanto a su arquitectura, los dispositivos NFC se dividen en dos tipos: iniciador y objetivo. Sin embargo, a diferencia de otros sistemas, un mismo dispositivo puede desempeñar ambos roles, actuando como etiqueta o lector según sea necesario.

El **iniciador** es el dispositivo que inicia la comunicación, generando activamente un campo de radio mientras que el **objetivo** es el receptor de la información, pudiendo ser pasivo, como en etiquetas NFC simples, o activo, como en smartphones en comunicación directa.

IEEE 802.15.4e.

El estándar IEEE 802.15.4, figura como uno de los pilares fundamentales en el panorama del IoT, particularmente en las capas de conexión física entre dispositivos. Este estándar establece un marco que incluye el formato de las tramas, las cabeceras que contienen direcciones de origen y destino, así como las pautas para la comunicación entre nodos (Zheng & Lee, 2006).

Sin embargo, las estructuras de trama típicas en las redes convencionales no son idóneas para las redes de baja potencia usuales en el IoT,

debido a su carga excesiva. Por ello, en 2008, se instauró el grupo de trabajo IEEE802.15.4e, con el propósito de ampliar el alcance de IEEE802.15.4 para abarcar las comunicaciones de baja potencia comúnmente empleadas en el ámbito del IoT. La versión más reciente de este estándar fue ratificada en 2012.

Según (Gaglio & Lo Re, 2014) las características de IEEE 802.15.4e son:

- Bajo consumo energético. Se enfoca en ciclos de trabajo muy bajos para aumentar la eficiencia energética, importante en aplicaciones de IoT donde los dispositivos pueden tener niveles variables de actividad.

- Elementos de información. Permite intercambiar información a nivel de capa de enlace extendiendo un concepto ya presente en estándares anteriores.

- *Beacons* mejorados. Introduce *beacons* extendidos que ofrecen mayor flexibilidad y mejoran la estructura de *beacons* existente.

- Tramas multiusos. Proporciona un formato de trama flexible capaz de manejar diversas operaciones a nivel de enlace basado en *beacons*.

- Métricas de desempeño a nivel de enlace. Ofrece retroalimentación sobre la calidad del canal para ayudar en la toma de decisiones a niveles superiores de la red.

- Asociación rápida *(FastA)*. Introduce un mecanismo que permite la asociación de dispositivos en un tiempo reducido, priorizando la latencia sobre la eficiencia energética en aplicaciones críticas en tiempo.

El estándar también establece una serie de modos a nivel de enlace diseñados para facilitar su implementación en el IoT:

- *Blink* (Parpadeo) de RFID, orientado a aplicaciones como la identificación, localización y seguimiento de objetos y personas.

- Adaptación Multicanal Asincrónica (AMCA), dirigida a sectores donde se requieren despliegues a gran escala, como la automatización y

control de procesos o la monitorización de infraestructuras.

- Extensión Multicanal Determinista y Sincrónica (DSME), destinada a respaldar aplicaciones industriales y comerciales con requisitos estrictos de puntualidad y fiabilidad.

- Red Determinista de Baja Latencia (LLDN), diseñada para aplicaciones que demandan una latencia mínima, como la automatización de fábricas o el control de robots.

- Salto de Canales con Ranuras de Tiempo (TSCH), adecuado para entornos de automatización de procesos.

IEEE 802.11ah.

IEEE 802.11ah, según (Adame, Bel, Bellalta, Barceló Vicens, & Riera, 2014), representa una variante optimizada y de bajo consumo del conocido estándar de acceso inalámbrico IEEE 802.11 comúnmente conocido como Wi-Fi. Este estándar, ampliamente utilizado en entornos inalámbricos, ha sido adaptado específicamente para satisfacer las demandas de IoT priorizando la eficiencia energética. En comparación con su predecesor, IEEE 802.15.4e, se destaca por una serie de mejoras significativas.

La omnipresencia de IEEE 802.11 a nivel global ha resultado en su implementación generalizada en diversos entornos, como hogares, oficinas, áreas urbanas y campus universitarios. En estos contextos una amplia gama de dispositivos, desde teléfonos inteligentes hasta computadoras portátiles y tabletas, dependen de esta tecnología como su principal medio de conexión a Internet.

Es importante señalar que las versiones actuales del estándar IEEE 802.11, como 802.11 a/b/g, n o ac, no fueron diseñadas inicialmente para su aplicación en sistemas de IoT. De hecho, los estándares Wi-Fi presentan limitaciones significativas para este propósito, como una alta sobrecarga de trama y un consumo energético elevado. Consciente de esta brecha, el grupo de trabajo IEEE 802.11 ha lanzado la iniciativa 802.11ah para desarrollar un estándar que aborde específicamente estas necesidades, ofreciendo una

comunicación de baja sobrecarga y consumo energético adecuado para dispositivos con sensores (Hasan & Hossain, 2013).

- Operando en el rango de frecuencia de 900MHz, esta tecnología funciona a frecuencias muy bajas, lo que resulta en longitudes de onda más largas y una cobertura más amplia.

- El nuevo estándar ofrece anchos de canal de 4, 8 y 16MHz para aplicaciones de alta velocidad, aunque los anchos de canal de 1MHz y 2MHz son más comunes.

- Las pruebas iniciales han arrojado un ancho de banda de 150Kbps.

- Diseñado para soportar miles de nodos sin problemas de saturación, optimizando al máximo el uso del espectro.

Bluetooth low energy.

El Bluetooth de baja energía, también conocido como *Smart Bluetooth* según (Gomez & Oller, 2014) es un protocolo de comunicación de corto alcance muy utilizado en redes. A diferencia del Bluetooth clásico, este protocolo consume considerablemente menos energía, hasta diez veces menos, aunque su latencia puede ser hasta 15 veces mayor. Sin embargo, su alcance es similar al del Bluetooth original. Este nuevo protocolo no se centra en la transferencia de archivos como su predecesor, sino que está especialmente diseñado para la transmisión de pequeños fragmentos de datos, como los necesarios en dispositivos de IoT. Su principal ventaja radica en su amplia integración en smartphones y otros dispositivos móviles. Es importante señalar que las versiones más recientes del estándar permiten la conexión directa del dispositivo a Internet mediante conectividad 6LoWPAN o LTE.

Z-Wave.

Según (Hasan & Hossain, 2013), se presenta como un protocolo de conectividad física de bajo consumo especialmente diseñado para aplicaciones en el ámbito de la domótica, aunque también se emplea en la comunicación de dispositivos IoT. Su enfoque principal recae en entornos de

hogares inteligentes y pequeñas empresas. Este protocolo facilita la comunicación punto a punto, siendo óptimo para la transmisión de mensajes breves en aplicaciones de IoT, tales como el control de iluminación, gestión energética, dispositivos de salud portátiles, entre otros. Operando en la banda de 868 MHz, evita la congestión de emisiones presentes en la banda de 2,4 GHz, y alcanza velocidades de hasta 40 kbit/s, con un alcance teórico de hasta 30 metros en condiciones óptimas. Utiliza el protocolo CSMA/CA para evitar colisiones y mensajes de confirmación para asegurar una transmisión fiable. Z-Wave adopta una arquitectura cliente/servidor, donde un nodo maestro dirige a los nodos esclavos, emitiendo comandos y gestionando la programación de la red en su totalidad. Su topología de red es de tipo malla, donde cada elemento funciona como un nodo capaz de recibir o retransmitir mensajes.

Zigbee Smart Energy

(Han & Lim, 2010), dice que este estándar ha sido diseñado para abarcar una amplia variedad de aplicaciones dentro del IoT, tales como sistemas para hogares inteligentes, control remoto, y soluciones en el ámbito socio-sanitario. Este protocolo es compatible con diversas topologías de red, incluyendo configuraciones en estrella, punto a punto, y en árbol. En esta arquitectura, un coordinador desempeña el papel central y puede ubicarse en cualquier punto de la red.

En términos de estándares, *ZigBee Smart Energy* utiliza IEEE 802.15.4 como base para sus capas inferiores, y se estructura sobre esta base mediante la definición de componentes para las capas superiores. La especificación de ZigBee abarca dos perfiles de pila: *ZigBee* y *ZigBee Pro*. Ambos perfiles admiten redes con topología de malla completa y son compatibles con una variedad de aplicaciones, lo que facilita la implementación en dispositivos con limitaciones de memoria y capacidad de procesamiento. *ZigBee Pro* ofrece funcionalidades adicionales, como seguridad a través del intercambio de claves simétricas, escalabilidad mediante la asignación de direcciones de forma estocástica, y un rendimiento mejorado gracias a mecanismos de enrutamiento eficientes de varios a uno.

G.9959.

Según, (Badenhop, Fuller, Hall, Ramsey, & Rice, 2015), éste estándar representa un protocolo de enlace, concebido por la UIT (Unión Internacional de Telecomunicaciones), con el propósito de facilitar una comunicación inalámbrica confiable, de semidúplex y de bajo ancho de banda y coste. Su diseño se orienta hacia aplicaciones en tiempo real donde la puntualidad es importante, la confiabilidad es fundamental y se exige una eficiencia energética notable.

- Este protocolo abarca una serie de atributos que comprenden:
- Identificadores de red únicos, permitiendo que hasta 232 nodos se integren a una red.
- Implementación de mecanismos para evitar colisiones.
- Establecimiento de un tiempo de espera en caso de colisión.
- Funcionalidad de retransmisión automática para asegurar la integridad de la comunicación.
- Incorporación de un patrón de despertar dedicado, que autoriza a los nodos a entrar en estado de reposo cuando no están activamente comunicándose, lo que contribuye al ahorro de energía.
- Adicionalmente, el protocolo ofrece acceso exclusivo al canal, validación de tramas, reconocimientos y retransmisiones.

LTE-A.

LTE-A, un conjunto de estándares concebidos para adaptarse a las exigencias de las aplicaciones de comunicación M2M e IoT en entornos de redes móviles, representa un protocolo escalable y más económico en comparación con alternativas celulares. En su funcionamiento, LTE-A emplea OFDMA (Acceso Múltiple por División de Frecuencia Ortogonal) como tecnología de acceso en la capa de enlace, dividiendo la frecuencia en múltiples bandas, cada una de las cuales puede ser utilizada de manera independiente. Su arquitectura se compone de una red central, una red de acceso

radioeléctrico y los nodos móviles. Mientras la red central se encarga de controlar los dispositivos móviles y rastrear sus direcciones IP, la red de acceso se responsabiliza de establecer los planos de control y datos, así como de gestionar la conectividad inalámbrica y el control del acceso radioeléctrico (Dahlman, Parkvall, & Sköld, 2014).

SigFox.

Es una empresa con sede en Francia, se posiciona como líder en la provisión de redes para el IoT, con la ambición de convertirse en el principal proveedor a nivel mundial en este campo. Ofrece la infraestructura, tecnología y ecosistema necesarios para que las empresas y organizaciones aprovechen al máximo las aplicaciones del IoT (Lauridsen, Vejlgaard, Kovács, Nguyen, & Mogensen, 2017).

Al igual que LoRa, *SigFox* utiliza redes LPWAN para la comunicación, aunque se diferencia en la falta de una comunidad similar a TTN que facilite el acceso gratuito y abierto a la red.

La empresa proporciona un estándar para la recopilación de datos de sensores y dispositivos, con un conjunto único de API basadas en estándares. Su tecnología está diseñada para permitir un servicio global, con una mayor duración de la batería y a un costo reducido.

Las características destacadas de la tecnología tomadas del sitio web de la empresa, incluyen:

- Banda ultraestrecha. Utilización de una banda de 192KHz para la transmisión de mensajes, con una modulación de banda ultraestrecha. Cada mensaje tiene un ancho de 100 Hz y se transfiere a velocidades de datos de 100 o 600 bits por segundo, según la región.

- Acceso aleatorio. Los dispositivos pueden acceder de forma aleatoria a la red, lo que garantiza una alta calidad de servicio. Esto se logra mediante la transmisión en frecuencias aleatorias y el envío de réplicas en diferentes frecuencias y tiempos, conocido como "diversidad de tiempo y frecuencia".

- Cooperación en la recepción. Los dispositivos no están vinculados a

una estación base específica, sino que cualquier estación base cercana puede recibir los mensajes, involucrando en promedio a tres estaciones base en el proceso, lo que se denomina "diversidad espacial".

- Mensajes pequeños. Los mensajes transmitidos son de tamaño reducido, variando entre 0 y 12 bytes.

- Comunicación bidireccional. La tecnología permite la comunicación en ambas direcciones.

A continuación, en el siguiente código QR se presenta el enlace a un video explicativo acerca de los protocolos y redes de comunicación dentro del IoT.

CAPÍTULO IV:
TRATAMIENTO Y ESTUDIO DE DATOS EN LAS VERTICALES DE IoT

4.1 Introducción y Objetivo del capítulo

La evolución de nuevos casos de aplicación en el ámbito del IoT continúa impulsando el progreso tecnológico y la adopción de nuevos enfoques para superar los desafíos existentes. Los sistemas IoT generan una gran cantidad de datos, que provienen de diversas fuentes, tales como: datos públicos proporcionados por entidades gubernamentales organizaciones estatales y comunidades. Estos datos se pueden emplear para ofrecer servicios tanto a organismos públicos como privados. Ejemplos de estos datos incluyen información meteorológica y datos demográficos. Además, se obtienen datos de dispositivos físicos como dispositivos móviles (como *smartphones, tablets* y *smartwatches*), vehículos equipados con sistemas de posicionamiento GPS y sensores que recopilan información sobre diversos parámetros como el nivel de llenado de contenedores, la concentración de partículas contaminantes en el aire y el nivel de luminosidad en las calles. También se accede a datos comunitarios, los cuales son extraídos de fuentes no estructuradas en entornos sociales en línea, como redes sociales y sitios web donde se comparten opiniones sobre productos o se realizan encuestas.

Este segmento ofrece una visión de las diversas aplicaciones dentro del ámbito del Internet de las Cosas. Sin embargo, es importante tener en cuenta que estas muestras siempre serán parciales, dado que constantemente surgen nuevas áreas de aplicación y casos de uso en este campo. Algunas de estas aplicaciones, actualmente en implementación en diversos entornos, incluyen la automatización y control remoto de edificios, sistemas de seguridad, gestión de energía inteligente, atención médica, domótica, así como servicios en sectores como ventas y turismo. Es evidente que los entornos industriales representan el próximo gran avance para el Internet de las Cosas, impulsando lo que se conoce como la próxima revolución industrial, enfocada en la captura de datos, el mantenimiento predictivo, y la optimi-

zación de procesos, entre otros aspectos clave.

En base a este contexto se proponen alcanzar los siguientes objetivos en este capítulo final.

- Comprender la distinción entre la manipulación de datos en lotes *(batching)* y en tiempo real *(streaming)*, discerniendo sus respectivas aplicaciones y ventajas en el procesamiento de información.

- Adquirir un conocimiento profundo sobre los conceptos de flujo de datos, identificando las características esenciales de una infraestructura analítica diseñada específicamente para abordar este tipo de datos dinámicos y continuos.

- Familiarizarse con las diversas plataformas disponibles para el análisis de datos en el contexto del IoT, así como comprender los componentes fundamentales que conforman estas soluciones tecnológicas.

- Identificar ejemplos destacados de aplicaciones para el análisis de datos bajo el paradigma de Big Data, tanto en el procesamiento por lotes como en tiempo real, ilustrando cómo estas metodologías pueden ser implementadas efectivamente en diferentes contextos y sectores industriales.

- Identificar algunas de las principales áreas de aplicación de los sistemas IoT.

- Determinar si un sistema puede ser clasificado como IoT según sus características.

- Fomentar la actitud crítica del estudiante para que pueda identificar otras posibles áreas de aplicación de sistemas dentro del ámbito de IoT.

4.2 Proceso y estudio de la información

En la actualidad, la creación de una plataforma IoT requiere la capacidad de manejar una gran cantidad de datos provenientes de una variedad de dispositivos diversos. Para abordar este desafío, es crucial adoptar un enfoque distribuido en el análisis de estos datos. Además, en el ámbito del big data, se reconocen dos enfoques principales para extraer información

de manera eficiente: el procesamiento por lotes y el procesamiento en tiempo real. Estos métodos permiten una extracción valiosa a partir de datos en bruto en períodos de tiempo reducidos.

4.2.1 Ruta de recorrido de los datos

En el ámbito del procesamiento de datos por lotes, se posibilita el análisis de extensas colecciones de datos en bruto, recopiladas previamente a lo largo del tiempo, sin requerir supervisión directa del usuario. Este enfoque, altamente escalable, permite la adición dinámica de nuevos nodos de procesamiento conforme aumenta el volumen de datos, utilizando un enfoque distribuido y paralelo. En los inicios del procesamiento de datos, el enfoque predominante era el procesamiento cíclico en lotes, gestionado por sistemas como *Apache Hadoop*, que incluían herramientas como YARN *(Yet Another Resource Manager)* y HDFS *(Hadoop Distributed File System)* para la gestión de recursos y la persistencia de datos.

Por otro lado, el procesamiento en tiempo real es importante en la actualidad para analizar grandes volúmenes de datos de manera instantánea, con frecuencias de actualización en milisegundos. Esto permite satisfacer las demandas de información en entornos como el IoT.

El procesamiento de datos en *streaming* (tiempo real) ha ganado importancia en los últimos años al ofrecer una ventaja competitiva al reducir los tiempos entre la adquisición y el análisis de los datos. Además, ofrece beneficios como la detección de anomalías, fallos y la actualización dinámica de modelos de aprendizaje automático. Es en este contexto donde surge el término *"fast data"*, que implica el aprovechamiento eficiente de grandes cantidades de datos mediante sistemas de procesamiento relativamente económicos en relación con el beneficio que se obtiene.

Un método de procesamiento adecuado deberá cumplir con características como ser tolerante a fallos, flexible ante el volumen de datos y capaz de proporcionar un alto rendimiento de procesamiento sin generar excesiva latencia a partir de los datos de entrada.

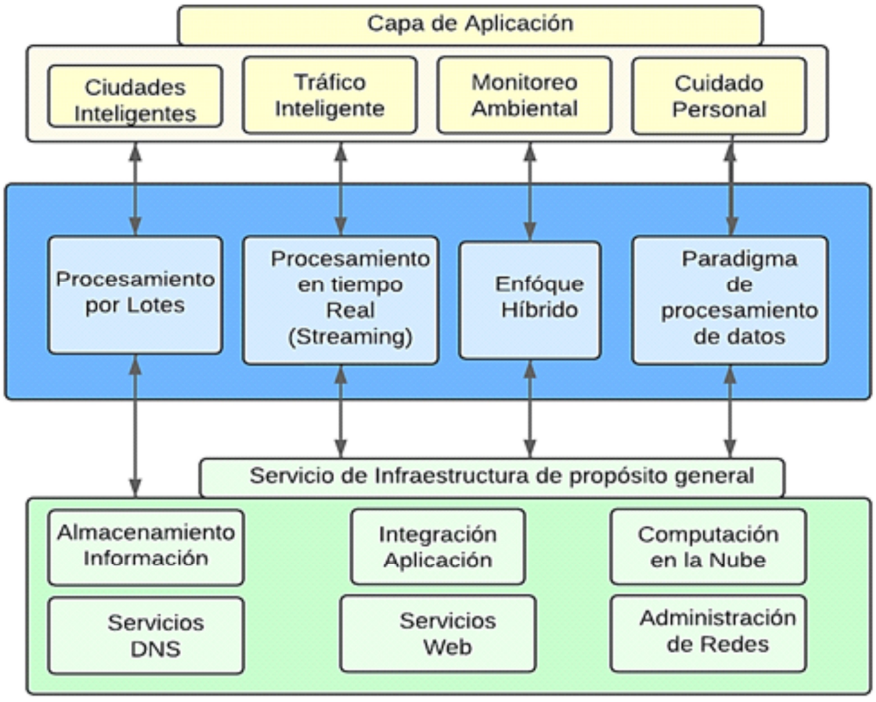
Un método de procesamiento adecuado deberá poseer las siguientes cualidades:

- Ser resistente a fallos.
- Ser adaptable al volumen de datos a gestionar.
- Ser capaz de ofrecer una alta capacidad de procesamiento sin generar una latencia excesiva a partir de los datos de entrada.

El procesamiento en tiempo real siempre ha sido esencial en el contexto del IoT, dado que posibilita la implementación de soluciones que son escalables, altamente disponibles y capaces de tolerar fallos. Estas soluciones son necesarias para gestionar grandes volúmenes de datos que se generan de forma continua.

Figura 4.1

Flujo de datos en el procesamiento de la información



La razón primordial detrás de esta adopción radica en el cambio en la dinámica de generación de datos, la cual ha evolucionado hacia un pro-

ceso cada vez más activo. Anteriormente, en contextos convencionales, la generación de datos resultaba en acciones mayormente pasivas o en acciones que dependían de la intervención directa del usuario. Sin embargo, en la era actual, el IoT posibilita la generación automática y masiva de datos, haciendo que el enfoque tradicional de generar datos en lotes carezca de la capacidad necesaria para satisfacer las demandas del entorno.

En cuanto a su enfoque metodológico, el procesamiento de *streaming* se posiciona principalmente como un enlace entre la capa de aplicación, la capa de servicios y el middleware. Este modelo facilita que la lógica de nivel superior haga un uso efectivo de los servicios de infraestructura subyacente de propósito general, como se ilustra en la Figura 4.1.

Flujo de *Stream.*

Un *stream* o flujo de datos se define como una sucesión cronológica de elementos de información que puede comprender diversas señales discretas, registros de eventos o cualquier otra combinación de datos relacionados con series temporales. Estos flujos suelen originarse a partir de los datos recopilados por los sensores de dispositivos y se transmiten a través de un canal específico para su análisis en tiempo real.

Cada elemento dentro de un flujo de datos está acompañado de una marca de tiempo explícita, la cual desempeña un papel importante en la organización secuencial de los datos. Formalmente, un flujo de datos se representa como una serie de pares: Elemento-Tiempo (s, Δ), donde "s" representa la secuencia de datos disponibles para el sistema de procesamiento. Aunque "s" puede abarcar varios atributos, generalmente se trata de un elemento atómico, ya que estos atributos están intrínsecamente vinculados entre sí para mantener la coherencia lógica.

Los componentes habituales abarcan tanto conjuntos de datos inmutables, como tuplas de categorías similares, así como eventos heterogéneos provenientes de diversas fuentes. Estos datos suelen ser generados por redes de sensores que operan con intervalos de monitoreo o actualización muy específicos, o bien surgen de eventos del mundo real.

La variable Δ representa una secuencia de marcas temporales que indican el orden y la secuencia de los elementos en el flujo de información. La utilización de esta marca temporal resulta imperativa, dado que los datos pueden agregarse de forma desordenada debido a los procedimientos distribuidos de recolección, e incluso durante la transmisión misma.

Resulta importante emplear una marca temporal que facilite la reconstrucción de la secuencia lógica para las etapas posteriores de análisis.Las marcas temporales no solo pueden ordenar los eventos cronológicamente, sino que también son cruciales para evaluar las propiedades en tiempo real de un sistema de procesamiento en *streaming*. Esto es escencial para verificar la precisión y oportunidad de los resultados obtenidos durante el analisis. Al utilizar marcas temporales, se puede determinar si los datos se procesan y entregan dentro de los límites especificados, garantizando así la eficiencia y fiabilidad del siste. Además, permiten identificar y corregir posibles retrasos y errores en la transmisión de datos, mejorando la robustez del sistema.

Las marcas temporales se pueden aplicar de dos maneras distintas:

- Utilizando una serie de valores temporales absolutos, lo que, si bien requiere una cantidad considerable de recursos para su generación, simplifica la tarea de los desarrolladores al permitirles crear algoritmos coherentes que puedan aplicarse a flujos separados en tiempo real, a medida que estos se van incorporando.

- Empleando una secuencia de intervalos positivos en tiempo real, donde únicamente se registra el orden relativo de los datos dentro de un mismo flujo. Este enfoque resulta en marcas temporales más compactas, lo que facilita la comunicación, pero a su vez dificulta la reorganización de eventos recibidos a través de múltiples flujos o dispositivos en redes de sensores, dado que la reconstrucción precisa del orden puede ser más compleja.

Los datos en flujo poseen una naturaleza intrínsecamente constante, fluyen en una dirección y son procesados en tiempo real. Las características primordiales de estas secuencias de datos son las siguientes:

a. Disponibilidad e instantaneidad. Es importante asegurar que el flujo de datos esté siempre disponible, lo que implica recopilar, transferir y procesar los datos en tiempo real. Esto se debe a que la relevancia de los datos puede disminuir con el tiempo. Por lo tanto, en un sistema IoT, de debe procesar los datos tan pronto como se reciben, manteniendo el orden de llegada y actualizando continuamente los resultados.

b. Aleatoriedad e imperfección. Estas características son inherentes a la naturaleza dinámica de los flujos de datos en IoT. Varias variables impredecibles pueden influir en el proceso de datos. Por ejemplo, la generación de datos en las fuentes puede ser aleatoria debido a la diversidad de entornos en los que están instaladas. Además, los modelos de transmisión de datos a través de redes públicas pueden introducir desorden debido a retrasos o pérdidas en la transmisión de la señal.

c. La continuidad de los flujos. Implica que los dispositivos IoT generarán datos de manera constante mientras sus sensores estén activos, lo que demanda una plataforma robusta capaz de procesarlos sin interrupciones. Por ende, es fundamental que esta plataforma cuente con características de alta disponibilidad para evitar cualquier tipo de interrupción que pueda ocasionar retrasos, garantizando así un procesamiento en tiempo real.

d. Volatilidad. Dado que la mayoría de los datos generados serán descartados una vez procesados. Incluso en algunos casos, esta eliminación de datos puede ser un requisito legal, especialmente cuando se trata de datos crudos que contienen datos sensibles que deben ser anonimizadas durante el análisis. De esta manera, solo se retiene la información relevante una vez que ha sido debidamente anonimizada.

e. Irrepetibilidad. Es decir, imposibilidad de replicar exactamente la secuencia de datos enviada inicialmente, esto es un desafío inherente cuando se solicita la retransmisión de datos desde los dispositivos de origen. Este proceso de retransmisión puede resultar en una presentación alterada de los resultados del procesamiento debido al reprocesamiento de los datos. Además, se reconoce que los datos en flujo son dinámicos y heterogéneos lo

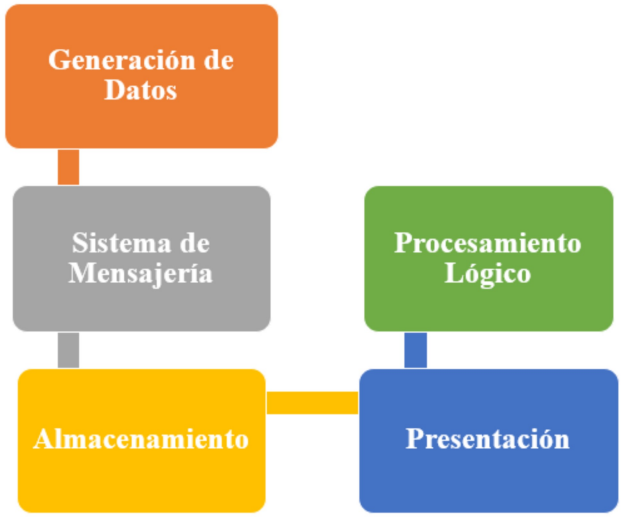
que implica variaciones tanto en volumen como en calidad y credibilidad a lo largo del tiempo.

4.2.2 Plataformas de manejo de la información

En su primer aspecto, una plataforma de procesamiento debe contar con una secuencia de actividades destinadas al tratamiento de datos, abarcando todas las etapas desde su creación hasta su utilización.

Figura 4.2

Fases en el procesamiento de un flujo



En la Figura 4.2, se muestra una vista panorámica de las partes del proceso que debe abordar una plataforma diseñada para el procesamiento de flujos, ajustada específicamente a las características del entorno IoT. Dentro de este diseño arquitectónico, se han reconocido los componentes siguientes:

La generación de datos.- Es una parte importante en este sistema, que se nutre de una amplia gama de fuentes que proporcionan constantemente materia prima en forma de datos para su procesamiento. Estos datos pueden categorizarse en tres tipos:

- Datos estáticos. Se refieren a información de largo plazo que ya está almacenada en infraestructuras o ubicaciones remotas. Estos datos, en su

mayoría, representan conocimiento estable y no se actualizan con frecuencia. Son adquiridos regularmente por el sistema de procesamiento en flujo y actúan como puntos de referencia durante el análisis.

- Datos de flujo centralizado. Constituyen un tipo especial de flujo que proviene de una sola fuente. Aunque pueden procesarse en el lugar de origen, carecen de una visión general agregada. Este tipo de datos es poco común en entornos de procesamiento en tiempo real, ya que generalmente la información requerida para el análisis proviene de múltiples fuentes.

- Datos de flujo distribuido. Son los más comunes en aplicaciones de IoT. Proceden de diversas fuentes dispersas y son altamente heterogéneos. El volumen y la temporalidad de estos datos distribuidos determinan los requisitos de rendimiento en el procesamiento de flujos.

Sistema de mensajería.- Cumple el rol de intermediario en la transmisión de información a lo largo de toda la cadena de procesamiento de datos. Su función principal es recolectar y consolidar distintos tipos de datos.

Estos sistemas pueden encontrarse de manera independiente en los dispositivos de los clientes o en pasarelas, con el propósito de dirigir los datos hacia los canales de transmisión para su posterior almacenamiento en un entorno centralizado de alta disponibilidad. Este entorno se encarga de reunir datos provenientes de diversos flujos centralizados. Existen dos tipos principales de sistemas de mensajería:

- Aquellos basados en temas o *"topics"*, los cuales ofrecen una mayor configurabilidad específica y variable.

- Los sistemas basados en colas, los cuales están más optimizados para brindar un mejor rendimiento, aunque tienen menos flexibilidad en cuanto a configuración.

Capa de almacenamiento.- Desempeña un papel fundamental en el despliegue de sistemas, ya que se encarga de mantener un registro de datos históricos que no requieren procesamiento inmediato. Estos datos suelen incluir información que debe conservarse, conocimientos previamente ge-

nerados o datos que pueden guiar futuros procesamientos.

Capa de presentación.- Actúa como un componente de apoyo adicional al proporcionar una interfaz para visualizar los datos que han sido procesados. Además, esta capa facilita la recepción de actualizaciones de comandos de búsqueda o consultas de usuarios, lo que permite una adaptabilidad y una capacidad de respuesta mejoradas del sistema.

Procesamiento lógico.- Por su importancia será discutida en detalle en la sección siguiente.

Despliegues para el procesamiento de datos.

Como mencionado previamente, con el continuo avance del paradigma del IoT, se experimenta un crecimiento constante en la generación de datos, lo que conlleva a una creciente demanda de análisis para extraer valor de este flujo de información. Por ende, se requiere el establecimiento de nuevos modelos arquitectónicos capaces de abordar los diversos escenarios de uso presentes en el ecosistema del IoT.

La necesidad imperante de procesamiento ha sido abordada mediante metodologías específicas respaldadas por sistemas de procesamiento y almacenamiento distribuido. Dentro de este espectro, *Hadoop* ha sobresalido consistentemente, haciendo uso de *MapReduce* como su herramienta central de procesamiento. Este enfoque paradigmático se estructura en dos fases fundamentales:

- Mapeo *(Map)*: Esta etapa se encarga de aplicar una función a los datos de entrada generando una serie de pares (clave-valor) y agrupándolos según su clave respectiva.

Ejemplo: *Map*(clave1, valor1) -> lista(clave2, valor2)

- Reducción (*Reduce)*: Aquí, se realiza un proceso paralelo sobre la salida del mapeo combinando los resultados para obtener el resultado final deseado.

Ejemplo: *Reduce*(clave2, lista(valor2)) -> lista(clave3, valor3)

Apache Hadoop se fundamenta en el *Hadoop Distributed File System* (HDFS), un sistema de archivos distribuido, escalable y portable desarrollado en Java. Originalmente concebido para integrarse con *Hadoop*, HDFS sirve como la base para este marco de trabajo de código abierto destinado al desarrollo de aplicaciones distribuidas. Su concepción se inspira en los conceptos propuestos por *Google,* específicamente en el *Google File System* y el paradigma *Map-Reduce*.

Además de la infraestructura consolidada de *Apache Hadoop* y su conjunto de herramientas (como *Hadoop, Hive y HBase*), es importante resaltar el papel fundamental desempeñado por *Apache Spark* en la progresión de estas plataformas de datos distribuidos. *Spark* representa un motor de procesamiento de datos distribuidos que permite la gestión eficiente de enormes volúmenes de información. Se puede conceptualizar como una evolución de Hadoop proporcionando varias ventajas significativas respecto al ecosistema anterior:

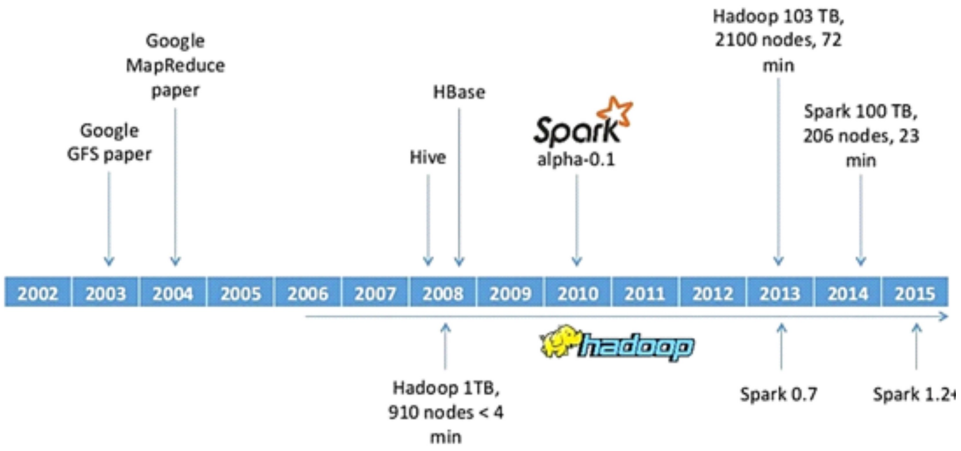
- Operación en memoria, a diferencia de *Hadoop* que basa su almacenamiento en disco. Esta característica impulsa una mayor velocidad a expensas de un consumo de recursos más elevado y costoso.
- Capacidades de procesamiento en tiempo real.
- Inclusión de componentes como *MLib*, que incorpora algoritmos de aprendizaje automático.
- Compatibilidad con una variedad de lenguajes de programación.

Con el propósito de contextualizar la llegada de *Hadoop* y otras plataformas estrechamente vinculadas, se muestra la Figura 51 la cual incorpora dos letras griegas (*lambda* y *kappa*, en los años 2012 y 2014, respectivamente). Estas designaciones aluden a dos categorías de métodos que se detallarán posteriormente y que ostentan una significativa importancia en el ámbito de los sistemas de procesamiento de datos en tiempo real. La evolución de estas plataformas ha permitido el desarrollo de aplicaciones más eficientes y ha abierto nuevas posibilidades en campos como la inteli-

gencia artificial y el aprendizaje automático. Además, la introducción de tecnologías como Spark ha revolucionado la forma en que se manejan grandes volúmenes de datos, mejorando significativamente el rendimiento y la velocidad de procesamiento.

Figura 4.3

Línea de tiempo de las plataformas de procesamiento



Fuente: (Málaga, 2024)

Método Lambda.

Se trata de un enfoque metodológico que respalda tanto los paradigmas de procesamiento en lotes como en tiempo real. El método *lambda* está estructurado en tres niveles y se fundamenta en el procesamiento de datos inmutables de manera continua.

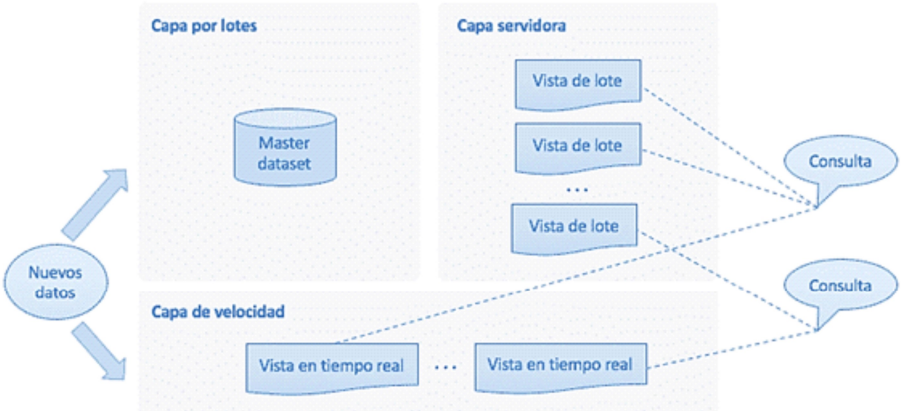
Estos tres niveles se definen de la siguiente manera:

- La capa de procesamiento, responsable de la transformación inicial de grandes volúmenes de datos para la generación de vistas.
- La capa de velocidad, encargada de procesar los datos en tiempo real con el propósito de cubrir la brecha entre el momento actual y el último procesamiento en lotes.
- La capa de presentación, destinada a atender las consultas relacionadas con las vistas generadas en las dos capas anteriores.

En la Figura 4.4 que se presenta a continuación, se muestra la arquitectura del método *Lambda*.

Figura 4.4

Arquitectura del método Lambda



Fuente: (Calvo, 2017)

El método *lambda* se caracteriza por varios aspectos fundamentales:

- La información nueva capturada por el sistema se dirige tanto a la capa de lotes *(batch)* como a la capa de *streaming* para su procesamiento rápido.

- En la capa de lotes *(batch)*, los datos se manejan en su forma original, sin alteraciones, y se agrega a los datos existentes. Luego, se somete a un proceso de tratamiento en lotes que produce las vistas en lotes, las cuales se utilizan en la capa de servicio para ofrecer información transformada externamente.

- La capa de servicio indexa las vistas en lotes generadas previamente para que puedan ser consultadas con una baja latencia.

- La capa de *streaming* (tiempo real) compensa la alta latencia de las operaciones de escritura en la capa de servicio y solo considera los datos nuevos.

- La respuesta a las consultas se genera combinando los resultados de las vistas en lotes y las vistas en tiempo real generadas en etapas anterio-

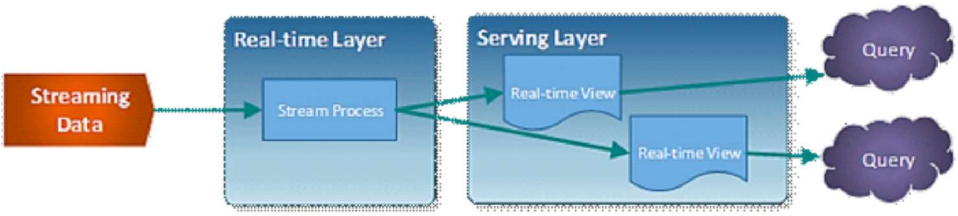
res.

Método Kappa.

Los métodos *Kappa*, introducidos en 2014 como una evolución de los métodos *lambda* representan un enfoque en el procesamiento de datos que elimina la necesidad de una capa *batch* enfocándose exclusivamente en el procesamiento en *streaming*. En este contexto, el procesamiento *batch* se considera una instancia específica de procesamiento en *streaming*, dado que puede conceptualizarse como un flujo limitado de datos. En los métodos *Kappa*, al prescindir de la capa *batch*, el proceso de procesamiento no tiene un inicio ni un final definidos temporalmente, sino que opera de manera continua, incorporando nuevos datos a medida que se reciben.

Figura 4.5

Arquitectura del método Kappa



Fuente: (Dominguez, 2018)

El método descrito se caracteriza por los siguientes puntos clave:

- Se adopta un enfoque de flujo continuo para todas las operaciones, ya que las operaciones por lotes se consideran como un subconjunto de las operaciones en *streaming*. Esto permite que todo el proceso se maneje como un flujo continuo de datos.

- Los datos originales permanecen intactos, almacenados sin modificaciones, mientras que las vistas se generan a partir de ellos. Esto asegura que el estado inicial de los datos se conserve, lo que facilita la recalculación de estados específicos en cualquier momento sin alterar la información original.

- Se mantiene un único flujo de procesamiento, lo que simplifica signi-

ficativamente el código, el mantenimiento y las actualizaciones del sistema. Esto se traduce en una gestión más eficiente y menos propensa a errores.

- La capacidad de relanzar el procesamiento es una característica fundamental, ya que permite ajustar configuraciones específicas y modificar procesamientos particulares para obtener resultados variados a partir de los mismos datos de entrada. Esto otorga una flexibilidad para adaptarse a diferentes necesidades y escenarios.

Ejemplo de método clásico.

Apache Hadoop, una plataforma de software de código abierto, se emplea para llevar a cabo el procesamiento en lotes de volúmenes masivos de datos, a la vez que ofrece un sistema de archivos distribuido, conocido como HDFS a través de conglomerados de nodos de computación.

Sus rasgos principales engloban una notable escalabilidad y eficiencia en el manejo y almacenamiento de grandes cantidades de información. Cada nodo dentro del conjunto puede almacenar, procesar y analizar estos datos, haciendo hincapié en su naturaleza de código abierto lo cual limita los costes al hardware utilizado. Asimismo, su flexibilidad radica en la capacidad para almacenar datos en diversos formatos y sin estructura definida, gracias al empleo de un sistema de archivos distribuido en lugar de depender de una base de datos convencional.

Además, se distingue por su resiliencia frente a fallos, donde la caída de un nodo en el conglomerado no compromete el proceso global, dado que la tarea se redirige automáticamente a los nodos restantes. La información almacenada en HDFS se replica en múltiples nodos asegurando así una mayor tolerancia a fallos y una mayor disponibilidad de datos.

Apache Hadoop se basa en HDFS, concebido para el almacenamiento eficiente de archivos voluminosos en múltiples nodos de un clúster implementado en el lenguaje Java e inspirado en el *Google File System*. Diseñado para operar en hardware económico, destaca por su escalabilidad y su capacidad de mantener la integridad de los datos incluso ante fallos.

Las características primordiales del HDFS incluyen la detección rápida y la recuperación automática de fallos, un rendimiento óptimo en el acceso a datos, especialmente apto para gestionar grandes volúmenes de información. Además, admite conjuntos de datos extensos con un ancho de banda elevado y puede expandirse hasta involucrar cientos de nodos dentro del clúster. Adopta el modelo de "escribir una vez, leer muchas veces", lo que asegura la coherencia de los datos al evitar su modificación después de ser creados, escritos y cerrados.

Por otro lado, gracias a su capacidad para manejar grandes conjuntos de datos, el HDFS permite llevar a cabo cálculos directamente sobre estos datos en lugar de trasladarlos hasta el nodo de cálculo. Esto no solo mejora el rendimiento de las aplicaciones, sino que también evita congestiones en la red. Para facilitar esta funcionalidad, el HDFS ofrece interfaces que permiten a las aplicaciones desplazarse al nodo donde residen los datos o a su cercanía.

Ejemplo del método moderno.

Apache Spark es una herramienta completa para el procesamiento distribuido de datos que abarca desde el almacenamiento y la supervisión hasta el análisis y la distribución de datos. Ofrece la capacidad de trabajar con una variedad de fuentes, incluidos sistemas de archivos, bases de datos estructuradas o no estructuradas, así como buffers de varios protocolos y servicios.

El núcleo de *Spark* radica en la implementación de RDDs, (Conjuntos de Datos Distribuidos Resilientes). Estos RDDs están diseñados sobre el concepto de almacenamiento en memoria para mejorar el rendimiento al evitar pérdidas de datos durante la comunicación. La principal ventaja de este enfoque es que, al mantener los datos en memoria, se reducen significativamente las latencias asociadas con la entrada y salida de datos. Este es un beneficio importante especialmente para algoritmos iterativos que requieren el acceso recurrente a subconjuntos de datos, y particularmente en entornos con sistemas de archivos distribuidos, superando

así una de las limitaciones principales del paradigma *Map-Reduce*.

Los RDDs, o Conjuntos de Datos Resilientes, son estructuras de datos de solo lectura almacenadas en la memoria, que representan una muestra inmutable y particionada de los datos, adecuada para ser procesada mediante acciones y transformaciones. Estos se generan directamente a partir de un conjunto de datos o mediante la aplicación de transformaciones sobre otros RDDs.

Una alternativa cada vez más utilizada en *Spark* para desarrollar funcionalidades es el empleo de *DataFrames*. Estos constituyen un conjunto de datos distribuido en columnas *(tuplas o frames).* Su principal ventaja sobre los RDDs radica en el uso de .*SparkSQL* para la gestión de datos estructurados. *SparkSQL* hace uso de la información estructural de los datos y optimiza la ejecución de los procesos, lo cual resultaría difícil de lograr de otra manera.

En consecuencia, los datos son accesibles mediante consultas SQL básicas, métodos más complejos como HiveQL, o mediante operaciones definidas en la API. Esto permite a los usuarios interactuar con los datos de manera flexible, adaptándose a sus necesidades específicas de análisis y procesamiento. Además, la posibilidad de utilizar diferentes lenguajes y herramientas de consulta facilita la integración con diversas aplicaciones y sistemas. Así, los datos pueden ser explotados tanto por analistas con conocimientos avanzados como por aquellos que prefieren métodos más sencillos y directos. Esta versatilidad en el acceso y manipulación de datos contribuye significativamente a la eficiencia y efectividad en la toma de decisiones informadas.

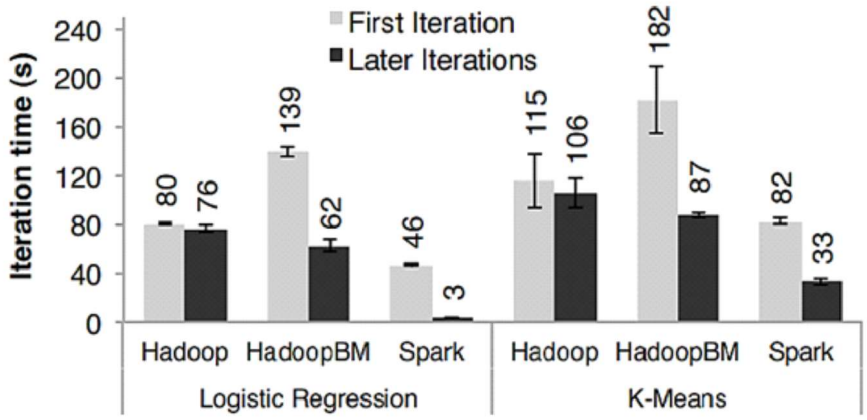
Comparativa final de Spark Vs Hadoop.

Hadoop, como predecesor de **Spark**, se centra en procesos de tipo **MapReduce** que siguen una aproximación basada en lotes. En constrate, *Spark* permite una obtención de resultados más dinámica al gestionar datos distribuidos en tiempo real mediante el procesamiento en memoria, lo que posibilita tiempos de procesamiento mucho menores para el manejo de

grandes subconjuntos de datos. En particular, *Spark* reduce significativamente los tiempos de iteración en algoritmos como la regresión logística y K-Means, demostrando así su eficiencia superior, como se muestra en la Figura 4.6.

Figura 4.6

Duración de la primera y última iteración en Hadoop y Spark utilizando 100 GB de datos en un clúster de 100 nodos



Fuente: (Zaharia, y otros, 2012)

4.3 Industrias Específicas en el Internet de las Cosas

Actualmente, diversas aplicaciones están siendo implementadas en diversos contextos, tales como la automatización y el control remoto de edificios, sistemas de seguridad, gestión energética inteligente, atención médica domiciliaria, así como en sectores comerciales como ventas y turismo. Es innegable que los entornos industriales representan el próximo gran avance para el IoT, impulsando lo que se reconoce como una nueva revolución industrial. Este enfoque se centra en la recopilación de datos, el mantenimiento predictivo y la optimización de procesos, entre otros aspectos.

A continuación, se detalla una amplia gama de sistemas IoT cuya implementación se relaciona con diversos ámbitos, según (Minoli, 2013).

Servicios públicos y ciudades inteligentes.

- Utilización de telemetría en diferentes aplicaciones como contadores

inteligentes, contadores de estacionamiento y máquinas expendedoras.

- Desarrollo de sistemas inteligentes para el transporte y la gestión del tráfico.

- Facilitación de la conexión de los consumidores y ciudadanos con la infraestructura pública de transporte.

- Automatización de procesos en edificios, así como en la infraestructura municipal y regional.

- Mejora en la gestión de servicios al ciudadano, abarcando áreas como el control de tráfico, peajes automáticos y prevención de incendios.

- Implementación de sistemas para la gestión de la red eléctrica, incluyendo redes de energía inteligentes.

Figura 4.7

Algunos servicios en ciudades inteligentes

Fuente: (Fernández, 2022)

La automoción, la gestión de flotas y el seguimiento de activos.

- Los vehículos eléctricos ofrecen una plataforma versátil que abarca múltiples funciones, como navegación, seguridad vial y control de tráfico, entre otras.

- Se prioriza la seguridad del conductor y se ofrecen servicios de emergencia para garantizar un viaje seguro y protegido.

- Los sistemas de gestión y monitorización de flotas son esenciales para optimizar la eficiencia operativa y el rendimiento de los vehículos en circulación.

- La integración de dispositivos de entretenimiento en los vehículos añade valor al viaje, proporcionando comodidad y entretenimiento a los ocupantes.

- Los servicios de localización mediante GPS permiten un seguimiento preciso de la ubicación de los vehículos y activos en tiempo real.

- Se ofrecen diversas aplicaciones de seguimiento, incluyendo el rastreo de activos, cargas y pedidos, que mejoran la visibilidad y la gestión de la cadena de suministro.

Figura 4.8

IoT en la automoción, la gestión de flotas y el seguimiento de activos

Fuente: (Kuan, Moko Smart, 2023)

Aplicaciones en entornos industriales, sociales y comerciales.

- Supervisión y gestión de operaciones industriales.

- Implementación de servicios interconectados en contextos comerciales.

- Regulación de procesos industriales.

- Optimización y automatización de tareas de mantenimiento.
- Recolección automatizada de datos de contadores y gestión de carga.
- Desarrollo de sistemas de seguridad nacional, abarcando riesgos químicos, biológicos radiológicos, y nucleares mediante sensores inalámbricos.
- Despliegue de sensores inalámbricos para monitorear condiciones ambientales en diferentes entornos, como terrestres, aéreos y marítimos, así como aplicaciones en agricultura.
- Utilización en el ámbito financiero, tales como terminales de punto de venta y sistemas de venta de boletos.

Aplicaciones vinculadas a la seguridad.

- Monitoreo en espacios públicos y protección individual.
- Dispositivos de detección para propósitos militares.

Dispositivos domésticos y de oficina inteligentes que forman parte de sistemas integrados de red.

- Electrodomésticos inteligentes que permiten controlar la potencia y la iluminación, así como funciones como temporización de calefacción, entre otros.
- Implementación de sistemas de control y gestión de bajo consumo energético.
- Utilización de contadores inteligentes para promover la eficiencia energética.
- Desarrollo de servicios de e-Health que ofrecen asistencia médica y de vida en el hogar, incluyendo monitorización y diagnóstico a distancia.
- Implementación de servicios de seguridad y emergencia, tales como sistemas integrados de monitoreo y asistencia remota.

A continuación, se expondrán varias soluciones comúnmente utili-

zadas de IoT en diversos contextos, sin focalizarse específicamente en el entorno industrial, sino en el uso generalizado de IoT.

4.3.1 Metrópolis avanzadas desde el punto de vista tecnológico

Los dispositivos genéricos utilizados en entornos urbanos abarcan una variedad de sensores ambientales, que comprenden desde mediciones térmicas y de viento hasta la detección de sonido, gases, partículas, luminosidad y actividad sísmica. Esta amalgama de sensores permite, en ciertas ocasiones, la monitorización en tiempo real de diversas actividades urbanas, como la presión en las calles o la detección de vehículos y la disponibilidad de espacios de estacionamiento.

A continuación, se detallan algunas de las aplicaciones más destacadas en el contexto de las ciudades inteligentes.

Gestión de tráfico en combinación con control dinámico de semáforos.

La gestión del tráfico en áreas urbanas se ve influenciada por una variedad de factores, que incluyen el volumen de vehículos en las vías, la hora del día, las condiciones climáticas actuales y previstas, el estado actual del tráfico, los incidentes viales y el mantenimiento de las carreteras entre otros aspectos. Los sensores de tráfico son fundamentales para recopilar datos precisos sobre estas condiciones, los cuales se integran en un sistema central de gestión del tráfico. Este sistema analiza la información en tiempo real y ejecuta estrategias para optimizar los flujos vehiculares, ya sea reduciendo la congestión o desviando el tráfico hacia rutas menos transitadas.

Para comunicar esta información a los conductores, se utilizan paneles de datos dinámicos que advierten sobre congestiones y rutas bloqueadas, mientras que las señales de tráfico también pueden ajustarse dinámicamente para dirigir el flujo de vehículos de manera eficiente. Además el sistema de gestión del tráfico puede interactuar con semáforos inteligentes, prolongando o acortando el tiempo de luz verde según el volumen de tráfico, lo que contribuye a optimizar la circulación en áreas de alta den-

sidad vehicular.

La implementación de estos modelos de gestión de tráfico, junto con señalización dinámica y semáforos inteligentes, ofrece una forma más eficiente de manejar el flujo vehicular en entornos urbanos. Además, se observan beneficios adicionales, como la reducción del consumo de combustible y la contaminación atmosférica, lo que resulta importante para mejorar la calidad de vida en las ciudades modernas.

Control de luminarias.

A pesar de las apariencias, las luminarias en las calles urbanas o interurbanas no necesitan brillar constantemente con la misma intensidad para garantizar la seguridad. La luminosidad del entorno está sujeta a diversas condiciones, como la luz lunar y las condiciones atmosféricas. La adaptación dinámica de la intensidad de las luminarias no solo permite reducir el consumo energético, sino que también facilita el control del gasto por parte de las autoridades municipales.

Estas luminarias son gestionadas en grupos por un controlador central, similar a un gateway en el IoT. Cada grupo de luminarias está conectado al sistema central de gestión y control del municipio, a menudo de manera inalámbrica. Además, mediante sensores específicos que recopilan información local, como la luminosidad y las condiciones atmosféricas, junto con datos meteorológicos actuales y pronósticos, es posible encender o apagar segmentos específicos de luminarias, así como ajustar su intensidad de manera dinámica.

Sistema de información al pasajero para el transporte público.

Los servicios de transporte público, tales como autobuses, metro y trenes de cercanías, operan según horarios susceptibles a influencias externas, lo que conlleva cierta variabilidad en comparación con un horario estándar. No obstante, es importante para los usuarios conocer la disponibilidad de sus próximas conexiones, no solo para estimar tiempos de llegada, sino también para tomar decisiones informadas ante posibles

retrasos prolongados, ya sea por cuenta propia o mediante un sistema automatizado de análisis que sugiera alternativas de conexión.

En este contexto, la ubicación actual de los diferentes vehículos de transporte público se comunica al sistema central, el cual puede relacionarla con la ubicación planificada en cada momento o en puntos de control específicos. Utilizando estos datos, el sistema calcula el retraso actual y estima la hora de llegada en las siguientes paradas, ajustando así la información para los usuarios.

Para determinar la ubicación del vehículo, se pueden emplear puntos de control a lo largo de la ruta habitual o dispositivos de rastreo que combinan tecnología GPS con conexiones móviles de bajo ancho de banda, como GPRS, para proporcionar actualizaciones de posición en intervalos regulares. Además, la combinación de puntos de control y sistemas GPS/GPRS permite integrar tanto vehículos ferroviarios (como metro y tranvías) como vehículos terrestres (como autobuses) brindando así un sistema completo de atención al usuario.

4.3.2 Bienestar y estado físico

Las aplicaciones *e-health* representan sistemas de IoT que fusionan el ámbito de la salud y el mantenimiento físico. En la actualidad, se está desarrollando un entorno específico de IoT que incorpora una variedad de sistemas móviles e inalámbricos diseñados para monitorear la salud de manera fluida y coherente. Este ecosistema tiene como objetivo principal reducir el tiempo entre la aparición de síntomas médicos en un individuo y el diagnóstico de la enfermedad subyacente, aprovechando así el modelo basado en IoT.

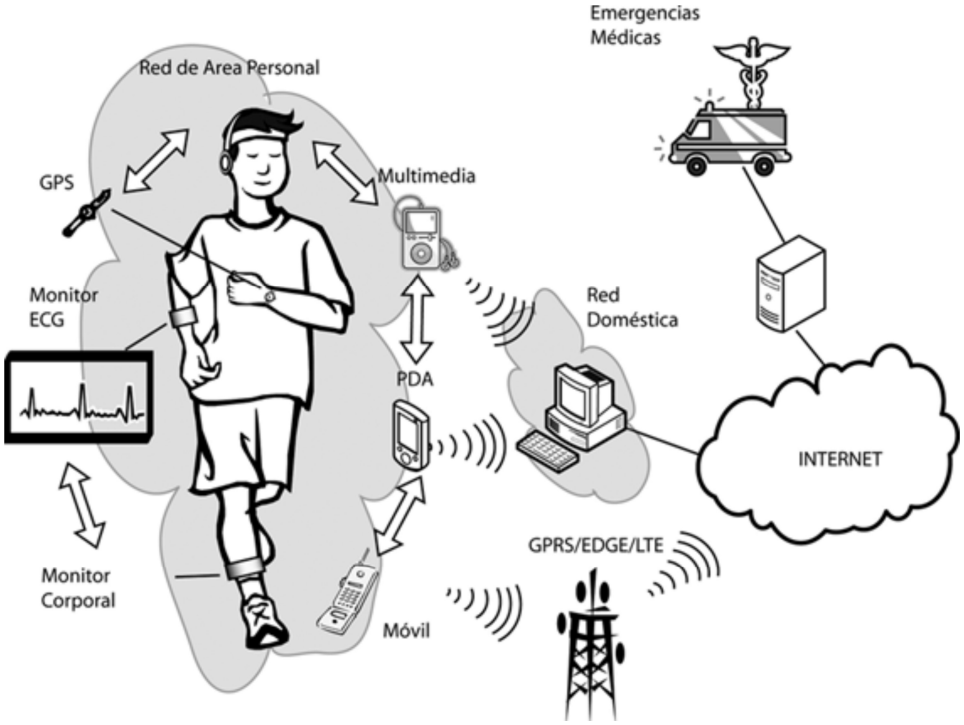
Estas aplicaciones emplean biosensores que se colocan en el cuerpo humano, posibilitando la transmisión de datos relacionados con las constantes vitales. En otras palabras, permiten la monitorización constante y remota de un conjunto específico de parámetros fisiológicos. Estos sensores inalámbricos liberan a los pacientes de los cables que, de otra manera, los limitarían a un lugar fijo en casa o a una cama de hospital. Por lo general,

estos sensores son ligeros y se conectan de forma inalámbrica, lo que otorga al paciente una considerable movilidad. Los dispositivos pueden consistir en varias unidades de sensores corporales portátiles, cada una de las cuales contiene un biosensor, una radio, una antena y funciones de control y cálculo integradas.

Cuando un paciente utiliza múltiples sensores, estos generalmente se comunican con una unidad central también ubicada en el cuerpo. Estos sistemas de sensores corporales, que incluyen los sensores y la conectividad, se conocen como redes inalámbricas de área corporal *(WBAN)* o alternativamente, como redes médicas de área corporal *(MBAN)*. La Figura 4.9 muestra un ejemplo visual de este tipo de redes de sensores.

Figura 4.9

Sensores IoT en el cuerpo humano para monitoreo de estado de salud



Fuente: (Betancur, 2011)

La tecnología de Red de Área de Cuerpo Médica (MBAN, por sus siglas en inglés) se compone de dispositivos diminutos y de bajo consumo

energético que se colocan en el cuerpo humano para recopilar datos clínicos, tales como la temperatura corporal, la función respiratoria y otros indicadores vitales. Estos sensores se emplean con el fin de monitorear y analizar patrones para identificar, evaluar la evolución, remisión y estado físico de enfermedades. Durante el proceso de recuperación, los MBAN permiten a los pacientes moverse dentro del centro médico mientras continúan siendo vigilados para detectar cualquier problema de salud que pueda surgir.

Los MBAN constan de dos dispositivos complementarios, uno o varios sensores colocados en el cuerpo y otro dispositivo, denominado *"gateway"*, ubicado en el cuerpo o en su proximidad. Algunos de estos sensores son desechables y tienen un tamaño y forma similares a un apósito estos sensores desechables cuentan con un transmisor de radio de baja potencia. Por lo general estos sensores registran la temperatura corporal, el pulso, los niveles de glucosa en sangre, la presión arterial y la salud respiratoria del paciente. Los beneficios para el paciente son evidentes ya que facilitan una mayor movilidad, una atención médica más eficiente y reducen los costos asociados.

A continuación, se enumeran algunos de los sensores específicos más comúnmente empleados en este contexto:

- Medidor de glucosa. Este dispositivo se utiliza para medir de manera aproximada la concentración de glucosa en la sangre, principalmente en aplicaciones relacionadas con el control de enfermedades crónicas como la diabetes.

- Oxímetro de pulso. Se trata de un dispositivo que evalúa de forma indirecta la cantidad de oxígeno en la sangre de un paciente, es decir, su nivel de saturación de oxígeno.

- Electrocardiógrafo. Este equipo registra y analiza la actividad eléctrica del corazón a lo largo del tiempo, proporcionando información relevante para evaluar su funcionamiento.

- Dispositivos de alarma social. Estos dispositivos permiten a las per-

sonas alertar y comunicarse con un cuidador en situaciones de emergencia. El cuidador puede ser un centro de salud, un equipo médico o un miembro de la familia. Además de funciones básicas de alerta, estos dispositivos a menudo incluyen características adicionales como detectores de caídas y transmisores de pánico integrados en colgantes o pulseras.

Los estándares proporcionan ventajas en términos de eficiencia económica para los componentes y también facilitan la gestión y supervisión de pacientes en entornos hospitalarios, centros de atención y domicilios. La e-Salud y la m-Salud se sustentan en conjuntos de dispositivos interconectados, entre los que se incluyen aquellos que se vinculan con teléfonos inteligentes convencionales u otros nodos utilizando tecnologías de radiocomunicación de corto alcance y baja potencia, como *Bluetooth*, *Zigbee* o NFC. Estas tecnologías permiten una integración fluida y segura de los datos médicos, mejorando la precisión y la rapidez en la toma de decisiones clínicas. Además, la interoperabilidad entre dispositivos facilita la recopilación continua de datos de salud, proporcionando a los profesionales médicos información en tiempo real para un monitoreo más eficaz.

Los datos recabados por estos dispositivos se transmiten de manera segura a una ubicación central con el fin de facilitar la toma de decisiones, analizar tendencias y almacenar información. La supervisión del bienestar personal puede aplicarse en los siguientes contextos:

- En el ámbito del seguimiento de la actividad de personas mayores, se focaliza en observar su actividad diaria y rutinas. Este tipo de aplicaciones utiliza sensores o dispositivos médicos portátiles para vigilar los signos vitales (como el ritmo cardíaco, la temperatura corporal, etc.), así como sensores ambientales no médicos.

- En cuanto a la supervisión de la seguridad, se trata de vigilar la seguridad del entorno doméstico. Se monitorea el ambiente del hogar en busca de riesgos como gases tóxicos fugas de agua e incendios. Además, se lleva a cabo la monitorización de los signos vitales de las personas que habitan en el hogar, tales como el ritmo cardíaco y la temperatura corporal.

4.3.3 Viviendas Automatizadas (Hogares inteligentes)

Desde sus inicios, la domótica ha sido objeto de considerable interés por parte de IoT. En el contexto de las casas automatizadas, las funciones básicas abarcan la capacidad de gestionar remotamente una variedad de sistemas, como la calefacción, la iluminación y hasta los electrodomésticos. Además, los contadores inteligentes y las soluciones para la eficiencia energética están experimentando un notable crecimiento recientemente. La integración de asistentes virtuales y la conectividad con dispositivos móviles también están revolucionando la forma en que interactuamos con nuestros hogares. Esto no solo mejora la comodidad y seguridad, sino que también optimiza el consumo de recursos, contribuyendo a una vida más sostenible.

Se anticipa que los sistemas IoT desempeñarán un papel importante en los hogares, ya que transforman elementos cotidianos en facilitadores del confort, la salud, la seguridad y la eficiencia energética. Esta evolución promete elevar tanto la calidad de vida como la experiencia residencial en general. Los dispositivos inteligentes, como termostatos, luces y electrodomésticos conectados, pueden ser controlados de manera remota y automatizada, ofreciendo un nivel de conveniencia sin precedentes. Además, los sensores IoT pueden monitorear la salud y el bienestar de los residentes, alertando sobre posibles problemas antes de que se conviertan en emergencias. La seguridad también se ve mejorada con sistemas de vigilancia y alarmas inteligentes, que proporcionan una protección robusta y proactiva. Finalmente, la optimización del uso energético contribuye a la sostenibilidad y a la reducción de costos, haciendo que los hogares sean más ecológicos y económicos.

Las diversas utilidades de las aplicaciones de domótica residencial abarcan una amplia gama de funciones, entre las cuales se pueden mencionar:

- Gestión de la iluminación.
- Regulación de la temperatura y control de calderas.

- Control de electrodomésticos conectados.
- Seguridad mediante cerraduras en puertas y ventanas.
- Detección de movimiento para seguridad.
- Sistema de alerta ante incendios o humo.
- Monitoreo de bebés.
- Dispositivos de asistencia médica personal, como colgantes de emergencia.

Figura 4.10

Aplicaciones en los hogares inteligentes

Fuente: (Mainframe, 2024)

En la Figura 4.10, se observa algunas de las aplicaciones del IoT en los hogares.

La optimización del consumo energético en los hogares es una aplicación de gran relevancia por su potencial de ahorro para los usuarios. Por ejemplo, los sensores de ocupación tienen la capacidad de identificar la presencia de personas en una habitación, permitiendo que las luces se apaguen automáticamente cuando está vacía, contribuyendo así a la reducción de la

energía consumida para iluminación y climatización. Otros tipos de sensores pueden controlar el uso energético de distintos dispositivos, como sistemas de calefacción, televisores, entre otros.

Estos sensores y actuadores pueden operar de manera independiente, como en el caso de los sensores de luz, o estar conectados a un centro de control, también conocido como nodo o *gateway*. Al consolidar los datos recopilados por diversos sensores, este nodo puede llevar a cabo un análisis interno y enviar instrucciones pertinentes a los actuadores correspondientes. Gracias a este sistema de IoT, es posible ajustar automáticamente el uso de los dispositivos del hogar en respuesta a diferentes situaciones a corto plazo, como la presencia o ausencia de personas en las habitaciones, así como a situaciones a largo plazo, como periodos prolongados de ausencia, como vacaciones o fines de semana fuera de casa.

4.3.4 Industria automotriz

Las utilidades de IoT en el campo de la industria automotriz y el transporte se enfocan en garantizar la seguridad, protección, navegación y otros servicios asociados a los vehículos, tales como seguros y la tarificación de peajes. Además, se destacan aplicaciones destinadas a brindar asistencia en situaciones de emergencia, la gestión de flotas y la administración de la recarga de vehículos eléctricos, junto con otros aspectos que contribuyen a optimizar el flujo del tráfico. Estas aplicaciones comúnmente incorporan módulos de comunicación IoT que se integran en los vehículos mismos o en otros componentes del equipo de transporte.

Se plantean desafíos técnicos, especialmente en relación con la gestión de la movilidad y las consideraciones ambientales vinculadas al hardware. La gestión de la movilidad requiere soluciones avanzadas para mantener la conectividad y el rendimiento óptimo en dispositivos que se desplazan constantemente. Esto incluye el desarrollo de algoritmos eficientes para el traspaso de redes y la optimización del consumo de energía. En cuanto a las consideraciones ambientales, es crucial diseñar hardware que no solo sea potente y eficiente, sino también sostenible. Esto implica el uso

de materiales reciclables y la reducción de residuos electrónicos. Además, es necesario implementar prácticas de fabricación que minimicen la huella de carbono y promuevan la reutilización de componentes. Enfrentar estos desafíos es esencial para el avance sostenible de las tecnologías IoT.A continuación, se proporciona una breve reseña de las aplicaciones existentes en este dominio.

Figura 4.11

Aplicaciones del IoT en un automóvil

Fuente: (Locke, 2020)

Llamada automática en caso de avería o accidente.

Esta aplicación especializada facilita la comunicación de la ubicación actual de un vehículo en situaciones de avería o accidente. Esta funcionalidad simplifica la coordinación de los distintos recursos necesarios en tales circunstancias, tales como servicios de asistencia técnica, atención médica, fuerzas de seguridad y gestión del tráfico.

Normalmente, el sistema de alerta de esta aplicación se activa mediante un interruptor que el usuario acciona manualmente para solicitar ayuda. Sin embargo, también puede activarse automáticamente si se detecta un accidente. Además de la simple transmisión de la ubicación en caso de emergencia o avería, algunos servicios avanzados pueden incluso enviar información diagnóstica del vehículo junto con la posición.

Seguimiento de vehículos robados.

Una aplicación fundamental en el ámbito de las comunicaciones IoT para la industria automotriz es el seguimiento de activos móviles, ya sea para la gestión de flotas de vehículos o para la recuperación de bienes sustraídos. La finalidad principal de esta tecnología es facilitar la localización y recuperación de un vehículo en caso de robo. En este sistema, el vehículo transmite regularmente datos de su ubicación a una unidad de control telemática instalada en el vehículo mismo, la cual puede interactuar directamente con las autoridades policiales. Esta unidad también puede estar programada para enviar alertas automáticas en caso de detectar movimientos sospechosos o intrusiones en el vehículo. Adicionalmente, la información recopilada puede ser utilizada para optimizar rutas y mejorar la gestión operativa de las flotas, proporcionando un valor añadido más allá de la seguridad.

Además, esta unidad de control telemática puede estar conectada al sistema de gestión del motor del vehículo, permitiendo la posibilidad de inmovilizar o reducir la velocidad del vehículo de forma remota. Estas aplicaciones suelen estar compuestas por diversos dispositivos IoT integrados, los cuales pueden comunicarse con el GPS para obtener la ubicación del vehículo y transmitir esta información a través de una red móvil hacia un servidor centralizado.

En el caso específico de las aplicaciones para el rastreo de robos, es común que el dispositivo IoT esté ubicado en un lugar discreto o inaccesible para evitar su desactivación por parte de posibles ladrones. El servidor de seguimiento, por otro lado, es operado por el propietario del activo o el proveedor de servicios, y su función principal es recibir, procesar y registrar la información de ubicación y velocidad proporcionada por los dispositivos IoT instalados en los vehículos.

Diagnóstico a distancia.

Los servicios de diagnóstico remoto pueden ser clasificados en varias categorías principales:

- Gestión de mantenimiento. Este sistema monitorea el kilometraje del vehículo y notifica al propietario o al concesionario designado cuando es necesario un servicio proporcionando alertas sobre la necesidad de mantenimiento.

- Evaluación del estado general del vehículo. Este sistema recopila datos sobre el estado general del vehículo de manera regular o a solicitud del propietario. La información recopilada se puede enviar al propietario, al concesionario designado o al fabricante del vehículo. Además, si se detecta un problema en algún sistema del vehículo el dispositivo es capaz de enviar la información relevante al concesionario o al fabricante.

- Respuesta a emergencias. En caso de una avería o accidente, estos dispositivos pueden enviar datos de ubicación y estado del vehículo al servicio de asistencia en carretera o al fabricante para una intervención oportuna.

Gestión de flotas.

El dueño de una flota de vehículos típicamente busca monitorear sus activos de cerca. Esta supervisión implica la obtención de información actualizada, como la ubicación y la velocidad de los vehículos, con el fin de planificar y mejorar las operaciones comerciales. Una aplicación de gestión de flotas se basa en la premisa de que los vehículos de la flota están equipados con dispositivos de IoT que les permiten:

- Conectar con los sensores del vehículo para obtener datos como la velocidad.

- Interactuar con dispositivos capaces de detectar la posición geográfica.

- Establecer comunicación con una red de telecomunicaciones móviles utilizando credenciales de acceso, lo que permite al dueño de la flota recibir, recopilar y analizar los datos de seguimiento de la flota, proporcionando así información relevante sobre los vehículos.

Los dispositivos de IoT integrados en los vehículos de una flota pueden ser programados para iniciar la comunicación de manera automatizada

con el servidor mediante una red móvil. Esta comunicación puede ocurrir en intervalos regulares, en momentos predeterminados o en respuesta a eventos específicos, como la entrada a una zona geográfica determinada.

Comunicación directa entre vehículos.

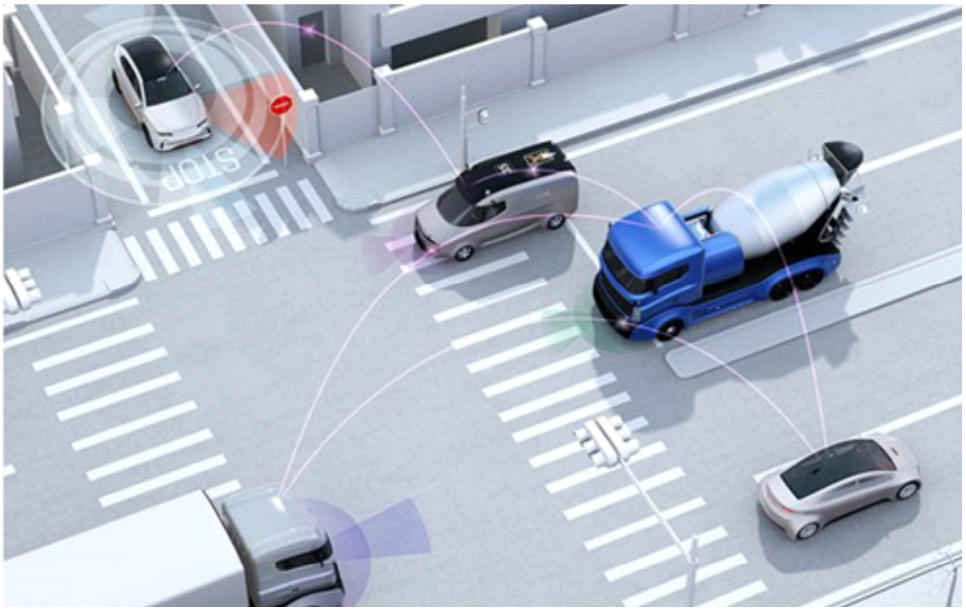
La aplicación IoT en cuestión representa una innovadora solución destinada a fortalecer la seguridad en el ámbito vehicular mediante la facilitación de la comunicación entre los distintos vehículos. Esta tecnología se fundamenta en la integración de dispositivos IoT en los vehículos, los cuales posibilitan la interacción con el sistema GPS y establecen comunicación a través de una red de telecomunicaciones móviles. Dichos dispositivos se conectan a un servicio centralizado con el propósito de potenciar la seguridad del tráfico, generando así un entorno más seguro y eficiente en las vías de circulación. Además, esta solución permite la detección temprana de posibles colisiones y la emisión de alertas en tiempo real a los conductores, mejorando la capacidad de respuesta ante situaciones de emergencia. Con la implementación de esta tecnología, se espera una reducción significativa en el número de accidentes de tráfico y una optimización en la gestión del flujo vehicular.Adicionalmente, la recopilación de datos sobre el comportamiento de conducción y las condiciones de la carretera puede proporcionar información valiosa para futuras mejoras en la infraestructura y en la regulación del tráfico.

Asimismo, la aplicación puede integrarse con sistemas de gestión de tráfico urbano para proporcionar datos en tiempo real sobre la densidad del tráfico y las condiciones de las carreteras. Esto no solo ayuda a los conductores a elegir rutas más seguras y rápidas, sino que también permite a las autoridades de tráfico tomar decisiones informadas para mejorar la infraestructura vial. La capacidad de recopilar y analizar grandes volúmenes de datos también abre la puerta a futuras innovaciones en la conducción autónoma y la movilidad inteligente. Además, la integración con otros sistemas de transporte público puede optimizar la coordinación entre diferentes modos de transporte, promoviendo una movilidad más eficiente y sostenible en las ciudades. Esta sinergia entre tecnologías no solo mejora la experien-

cia del usuario, sino que también contribuye a una planificación urbana más efectiva y a la reducción de la congestión vehicular.

Figura 4.12

Vehículos conectados entre sí



Fuente: (Locke, 2020)

Los dispositivos de IoT incorporan diversas funcionalidades en el contexto vehicular, lo que les habilita para ejecutar una variedad de tareas:

- Comunicarse con el sistema encargado de medir la velocidad y los impactos externos del vehículo.
- Interactuar con dispositivos equipados con tecnología GPS para determinar su ubicación precisa en tiempo real.
- Establecer conexiones con redes de telecomunicaciones móviles para acceder a servicios y datos externos.
- Transferir información relacionada con el tráfico y la seguridad hacia o desde un servidor especializado.

Estas aplicaciones facilitan la comunicación de eventos ocurridos en un vehículo, como un impacto externo o una falla del motor, al servidor

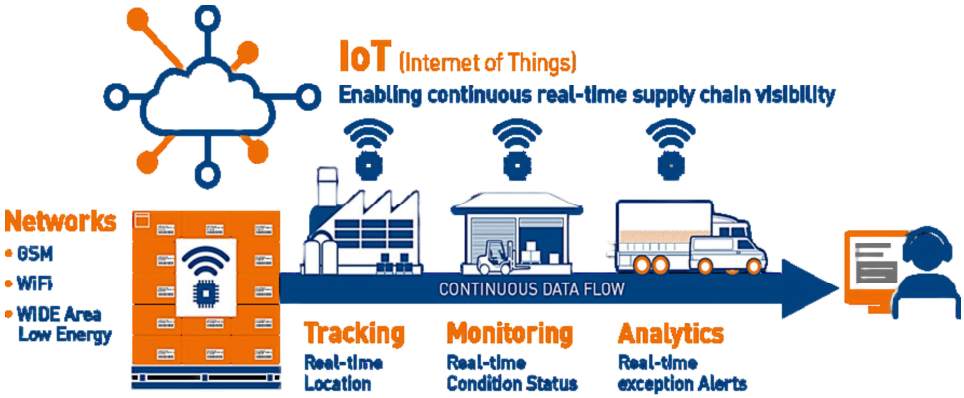
de información de tráfico. Esta transferencia de datos posibilita la toma de decisiones centralizadas y coordinadas respecto a las acciones a emprender en cada situación.

4.3.5 Gestión de la cadena de suministro y transporte de mercancías

Las aplicaciones de seguimiento y localización son comunes tanto en la industria automotriz como en la logística de movimientos de mercancías en entornos de producción, distribución y ventas al por menor. En estos últimos, es común el uso de etiquetas RFID. En el ámbito automotriz, estas aplicaciones se enfocan en garantizar la seguridad física de las personas, especialmente en situaciones de emergencia, en el rastreo de activos para prevenir robos o para propósitos de aplicación de la ley, y en la gestión de flotas para mejorar la eficiencia operativa. Además, estos servicios suelen ofrecer funcionalidades adicionales como diagnóstico remoto, sistemas de navegación, entre otros.

Figura 4.13

IoT en la logística y distribución



Fuente: (Zetes, 2024)

En estas aplicaciones, los componentes de IoT deben operar en ambientes desafiantes debido a las condiciones ambientales adversas en las que se ubican, que incluyen fluctuaciones extremas de temperatura y humedad, entre otros elementos. Además, están sujetos a vibraciones intensas o impactos debido al medio de transporte utilizado, como vehículos moto-

rizados. Por otra parte, el espacio disponible suele ser muy limitado, lo que requiere que el tamaño de los módulos IoT se reduzca al mínimo posible. El seguimiento de vehículos, contenedores, personas, mascotas, etc., se realiza mediante un dispositivo IoT que integra una aplicación de comunicaciones que trabaja en conjunto con un módulo de GPS.

A continuación, en el siguiente código QR se presenta el enlace a un video explicativo complementario acerca de las áreas y aplicaciones del mundo real donde se aplica la tecnología emergente del IoT.

CONCLUSIONES

En el Capítulo I se proporciona los fundamentos básicos para entender la tecnología emergente del Internet de las Cosas, destacando la integración de objetos cotidianos en una red inteligente. Se mostró que esta evolución no solo amplía las posibilidades de interacción y comunicación, sino que también redefine la funcionalidad de los objetos, dándoles una "nueva vida digital". La comprensión de estos fundamentos es importante para apreciar la magnitud y el impacto potencial del IoT en diversos ámbitos de la vida e industria.

En el Capítulo II se enfatizó la importancia del hardware, especialmente los microprocesadores microcontroladores, sensores y actuadores, en una red IoT. Se mostró las características que debe tener un sensor, así como también la capacidad de estos dispositivos para recopilar y procesar datos del mundo físico. Se mostró que los avances en tecnología de sensores y la integración efectiva del hardware permiten que los objetos inteligentes interactúen con su entorno de mejor manera, lo cual es importante para el desarrollo y la implementación de aplicaciones IoT avanzadas.

En el Capítulo III se destacó cómo la conectividad y las redes de comunicación es una parte importante para el funcionamiento del IoT. Se evidenció la diversidad de tecnologías de red, desde el 5G hasta las LPWAN, mostrando las características, ventajas y desventajas de cada una. Se dio tip's para elegir la mejor opción de comunicación en función de la aplicación, facilitando así la comprensión y la selección adecuada de los protocolos de comunicación para diseñar sistemas IoT que sean robustos y capaces de manejar grandes volúmenes de datos.

En el Capítulo IV se presentaron algunas de las aplicaciones del IoT en diferentes sectores, subrayando su impacto y potencial para transformar industrias enteras. Estas aplicaciones no solo ilustran la versatilidad del IoT, sino que también ofrecen directrices valiosas para desarrollar posibles temas de tesis en ingeniería. Al explorar casos de uso concretos y sectores verticales, este capítulo sirve como una fuente de inspiración y un marco de re-

ferencia para futuras investigaciones y desarrollos en el campo del IoT.

BIBLIOGRAFÍA

Acuña, M. (25 de Junio de 2019). *EvirtualPlus*. Obtenido de EvirtualPlus: https://www.evirtualplus.com/red-5g-futuro-educacion/

Adafruit, I. (2018). *Calibraciónn de sensores*. Obtenido de Adafruit Industries: https://cdn-learn.adafruit.com/downloads/pdf/calibrating-sensors.pdf

Adame, T., Bel, A., Bellalta, B., Barceló Vicens, J., & Riera, M. (2014). IEEE 802.11AH: the WiFi approach for M2M communications. *Institute of Electrical and Electronics Engineers (IEEE)*, 144-52.

Ammar, N., Malik, Z., Rezgui, A., & Bertino, E. (2016). IEEE 32nd International Conference on Data Engineering (ICDE). *IEEE Xplore*, 70-71.

arm. (2024). *arm.* Obtenido de arm: https://www.arm.com/products/silicon-ip-cpu/cortex-m/cortex-m7

Avnet. (29 de Marzo de 2017). *Avent.* Obtenido de Avnet: https://www.avnet.com/wps/portal/us/resources/article/nxp-intro-to-iot-components/

Badenhop, C., Fuller, J., Hall, J., Ramsey, B., & Rice, M. (2015). Evaluating ITU-T G.9959 Based Wireless Systems Used in Critical Infrastructure Assets. *SpringerLink*, 209-227.

Bassi, A. (27 de Febrero de 2021). *GotoIoT*. Obtenido de GotoIoT: https://www.gotoiot.com/pages/articles/iot_protocols_intro/index.html

Betancur, L. (2011). Redes de área corporal. Una perspectiva al futuro desde la investigación. *Researchgate*, 11-30.

Calvo, D. (15 de Noviembre de 2017). *Diego Calvo*. Obtenido de Diego Calvo: https://www.diegocalvo.es/arquitectura-lambda-combinacion-de-procesamiento-batch-y-stream/

Cetinkaya, O., & Akan, Ö. (2015). A DASH7-based power metering system. *Semantic Scholar*.

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review

of enabling technologies, challenges, and computer network. *sciencedirect*, 17- 39.

Corning. (2019). *CORNING*. Obtenido de CORNING: https://www.corning.com/catalog/coc/documents/articles/The-Practical-Internet-of-Things.pdf

Crespo, E. (14 de Noviembre de 2014). *Aprendiendo Arduino*. Obtenido de Aprendiendo Arduino: https://aprendiendoarduino.wordpress.com/2018/11/11/tecnologias-iot/

Dahlman, E., Parkvall, S., & Sköld, J. (2014). 4G: *LTE/LTE-Advanced for Mobile Broadband*. Ámsterdam: Elsevier.

Dominguez, J. (16 de Abril de 2018). *Paradigma*. Obtenido de Paradigma: https://www.paradigmadigital.com/techbiz/de-lambda-a-kappa-evolucion-de-las-arquitecturas-big-data/

Ericsson, M. R. (2019). 5G momentum continues.

Fernández, S. (21 de Octubre de 2022). *Las Smart Cities y el papel de los Data Centers*. Obtenido de DCD: https://www.datacenterdynamics.com/es/features/las-smart-cities-y-el-papel-de-los-data-centers/

Foundation, R. P. (19 de marzo de 2024). *Raspberry Pi Foundation*. Obtenido de Raspberry Pi Foundation: https://www.raspberrypi.org

Frankel, S., & Krishnan, S. (Febrero de 2011). *datatracker*. Obtenido de datatracker: https://datatracker.ietf.org/doc/html/rfc6071

Fremantle, P. (Octubre de 2015). *A Reference Architecture For The Internet of Things*. Obtenido de WS02: https://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things/

French, A., & Jung, S. (2016). The Digital Revolution: Internet of Things, 5G and Beyond. *ResearchGate*, 840-850. Obtenido de The Digital Revolution: Internet of Things, 5G and Beyond.

Gaglio, S., & Lo Re, G. (2014). *Advances onto the Internet of Things*. Pa-

lermo: SpringerLink.

Gomez, C., & Oller, J. (2014). Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *Sensors*, 11734-53.

Han, D., & Lim, J. (2010). Smart home energy management system using IEEE 802.15. 4 and zigbee. *IEEE Transactions on Consumer Electronics*, 1403-10.

Hardt, D. (Octubre de 2012). *Datatracker*. Obtenido de Datatracker: https://datatracker.ietf.org/doc/html/rfc6749

Harwood, T. (11 de 01 de 2019). *Postscapes*. Obtenido de Postscapes: https://www.postscapes.com/internet-of-things-technologies/

Hasan, M., & Hossain, E. (2013). Random Access for Machine-to-Machine Communication in LTE-Advanced Networks: Issues and Approaches. *IEEE Communications Magazine*, 86-93.

IEEE Standars, A. (2007). IEEE Standars Association. Obtenido de The IEEE 1451.4 Standard for Smart Transducers: https://standards.ieee.org/wp-content/uploads/import/documents/tutorials/1451d4.pdf

Intel. (4 de Mayo de 2024). Intel. Obtenido de Intel: https://www.intel.la/content/www/xl/es/products/sku/78919/intel-galileo-board/specifications.html

Kuan, F. (29 de Junio de 2023). *Moko Smart*. Obtenido de Moko Smart: https://www.mokosmart.com/es/fleet-management-technologies/

Lauridsen, M., Vejlgaard, B., Kovács, I., Nguyen, H., & Mogensen, P. (2017). Interference Measurements in the European 868 MHz ISM Band with Focus on LoRa and SigFox. *IEEE Wireless comunication and networking conference*, 16.

Locke, J. (17 de Junio de 2020). *DIGI Connect with Confidence*. Obtenido de DIGI Connect with Confidence: https://es.digi.com/blog/post/what-is-connected-vehicle-technology-and-use-cases

Mainframe. (4 de Mayo de 2024). *Mainframe Telecomunicaiones*. Obtenido de Mainframe Telecomunicaiones: https://mainframeltda.com/tendencias-hogares-inteligentes/

Málaga, U. (17 de Febreo de 2024). *Universidad de Málaga*. Obtenido de Universidad de Málaga: https://www.bigdata.uma.es/apache-spark-un-poco-de-historia/

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Targio, I., Siddiqa, A., & Ibrar, Y. (2017). Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. IEEE Xplore, 5247-5261. Obtenido de *IEEE Xplore*.

Mecafenix, I. (4 de Mayo de 2024). *Mecafenix, Ingeniería*. Obtenido de Mecafenix, Ingeniería: https://www.ingmecafenix.com/automatizacion/sensores/inclinometro/

Meza, Q. (2021). *Platzi*. Obtenido de Platzi: https://platzi.com/clases/2225-redes/35584-modelo-tcpip/

Minoli, D. (2013). *Building the Internet of Things with IPv6 and MIPv6*: *The Evolving World of M2M Communications*. John Wiley & Sons.

Orange, P. (4 de mAYO de 2024). *Orange PI*. Obtenido de Orange PI: http://www.orangepi.org/html/hardWare/computerAndMicrocontrollers/details/Orange-Pi-One.html

Raspberry, P. (4 de Mayo de 2024). *Raspberry Pi*. Obtenido de Raspberry Pi: https://www.raspberrypi.com

Sanchez, F. S. (2022). *Sensores y redes*. La Rioja: Universidad Internacional de la Rioja.

Schweber, B. (19 de Mayo de 2021). *DigiKey*. Obtenido de DigiKey: https://www.digikey.es/es/articles/the-fundamentals-of-digital-potentiometers

Sick. (4 de Mayo de 2024). *Sick Sensor Inteligence*. Obtenido de Sick Sensor Inteligence: https://es.rs-online.com/web/b/sick/

Tech&Business, i. (Septiembre de 2019). *itUser Tech&Business*. Obtenido de itUser Tech&Business: https://www.ituser.es/actualidad/2019/09/el-numero-de-dispositivos-conectados-crecera-a-un-ritmo-anual-del-12-hasta-2024

Vaisala. (4 de mayo de 2024). *Vaisala*. Obtenido de Vaisala: https://store.vaisala.com/en/products

Vergara, C., & Ocampo, M. (14 de Noviembre de 2017). Energub. Obtenido de Energub: https://energub.com/el-internet-de-las-cosas-iot-y-la-cuarta-revolucion-industrial/

Vollbrtcht, J., Carlson, J., Blunk, L., Aboda, B., & Levkowetz, H. (Junio de 2004). *Datatracker*. Obtenido de Datatracker: https://datatracker.ietf.org/doc/rfc3748/

Weyn, M., Ergeerts, G., Wante, L., Vercauteren, C., & Hellinckx, P. (2013). Survey of the DASH7 Alliance Protocol for 433 MHz Wireless Sensor Communication. *Sage Journals Home*, 12.

Yegin, A., Chakratabarti, S. O., & Duffy, P. (agosto de 2011). *Datatracker*. Obtenido de Datatracker: https://datatracker.ietf.org/doc/rfc6345/

Zaharia, M., Chowdhury, M., Das, T., Dave, A., Ma, J., McCauley, M., & Michael J. Franklin, S. S. (2012). Resilient Distributed Datasets: A Fault-Tolerant Abstraction for In-Memory Cluster Computing. I*n Proceedings of the 9th USENIX c*, 9.

Zetes. (4 de Mayo de 2024). Zetes. Obtenido de Zetes: https://www.zetes.com/es/tecnologias-y-productos/el-iot-en-la-cadena-de-suministro

Zheng, J., & Lee, M. (2006). A Comprehensive Performance Study of IEEE 802.15.4. S*ensor network operations*, 1-14.

SEMBLANZA DE AUTORES

Isaac David Torres Paredes

Ingeniero en Sistemas Informáticos por la Escuela Superior Politécnica de Chimborazo (ESPOCH) Máster Universitario en la Industria 4.0 por la Universidad Internacional de La Rioja y Especialista en Data y Business Analytics por la Universidad de Miami. Técnico Docente en la ESPOCH durante tres años y contando, gerente propietario de la empresa Servicios Industriales Torres SEINTO S.A. Además, es autor de varios libros y artículos sobre las TIC.

Narcisa de Jesús Salazar Álvarez

Doctora en Matemática y Master en Informática Aplicada por la ESPOCH. Con más de 30 años de experiencia en la ESPOCH, se ha desempeñado como docente en áreas como sistemas inteligentes, simulación matemática y análisis estadístico. Ha coordinado programas de maestrías y actualmente coordina la carrera de telemática en la ESPOCH. Además, es autora de varios libros y artículos científicos sobre matemáticas, estadística y TIC.

Alex Ricardo Guamán Andrade

Ingeniero en Electrónica y Control por la Politécnica Nacional y Magíster en Electricidad con Mención en Sistemas Eléctricos de Potencia por la Universidad Politécnica Salesiana. Actualmente, se desempeña como docente en la Escuela Superior Politécnica de Chimborazo (ESPOCH), donde contribuye con su experiencia en el diseño de instalaciones eléctricas y en la docencia universitaria.

Escuela Superior Politécnica de Chimborazo

Universo IoT, ofrece una visión detallada sobre el Internet de las Cosas (IoT), destacando su capacidad para transformar la relación entre los entornos digital y físico. El libro está estructurado en cuatro capítulos que abarcan desde los conceptos básicos hasta las aplicaciones del IoT, proporcionando un enfoque integral de esta tecnología emergente. En el Capítulo I, "Fundamentos, Capas y Componentes del IoT", se presentan los principios básicos y la arquitectura de una red del IoT. Se describe cómo esta tecnología ha integrado objetos cotidianos a la red, transformándolos en entidades inteligentes capaces de comunicarse e interactuar. El Capítulo II, "Hardware en el IoT", se centra en los dispositivos que forman una red IoT, como son sensores, actuadores, microcontroladores y microprocesadores que recopilan y procesan datos del entorno. El Capítulo III, "Protocolos y Redes de Comunicación", aborda la integración de los dispositivos en diversas redes de comunicación. Se destacan tecnologías como el 5G, que promete una conectividad rápida y fiable, y las LPWAN, que son ideales para transmitir pequeños datos a largas distancias con bajo consumo energético. Además, se discuten otras tecnologías como LoRa, RFID, DASH7, y NFC, que forman parte de la infraestructura de conectividad del IoT. El Capítulo IV, "Tratamiento y Estudio de Datos en las Verticales del IoT", explora las aplicaciones prácticas del IoT en diferentes sectores. Se evidencia cómo el IoT genera enormes cantidades de datos de diversas fuentes, incluyendo datos públicos, dispositivos móviles y/o sensores ambientales. Se muestra que las aplicaciones del IoT abarcan la automatización de edificios, la gestión inteligente de la energía, la atención médica, la domótica entre otros.

SOLUZIONINNOVATIVE S.A.S.

ISBN: 978-9942-7294-5-3

9 789942 729453