MONOGRAFÍA INTERNET DE LAS COSAS: MODELOS DE COMUNICACIÓN, DESAFÍOS Y APLICACIONES

160003421 MARYEN CAROLINA MORA PERALTA
160003435 KAREN GISETH URREGO GAITÁN

UNIVERSIDAD DE LOS LLANOS
FACULTAD DE CIENCIAS BASICAS E INGENIERIA
ESCUELA DE INGENIERIAS
PROGRAMA DE INGENIERIA DE SISTEMAS
VILLAVICENCIO, COLOMBIA
2018

MONOGRAFÍA INTERNET DE LAS COSAS: MODELOS DE COMUNICACIÓN, DESAFÍOS Y APLICACIONES

160003421 MARYEN CAROLINA MORA PERALTA
160003435 KAREN GISETH URREGO GAITÁN

Trabajo de grado presentado como requisito parcial para optar al título de
Ingeniero de Sistemas

Director:
Ingeniero Electrónico, M. Sc en Teleinformática, de la Universidad Distrital Francisco José De Caldas, PhD. en Ingeniería de la Universidad de Dakota del Norte (U.S.A.)
Héctor Iván Reyes Moncayo

UNIVERSIDAD DE LOS LLANOS
FACULTAD DE CIENCIAS BASICAS E INGENIERIA
ESCUELA DE INGENIERIAS
PROGRAMA DE INGENIERIA DE SISTEMAS
VILLAVICENCIO, COLOMBIA
2018

Nota de Aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Ingeniero Juan Fajardo
Jurado

_____
Ingeniero Héctor Iván Reyes
Director

_____

Ciudad y fecha

Tabla de contenido

Lista de Tablas

Lista de Gráficas

Lista de Ilustraciones

LISTA DE ACRÓNIMOS

4G: 4 generación.

5G: 5 generación.

6LOWPAN: IPv6 over Low power Wireless Personal Area Networks.

AIDC: Automatic identification and data capture.

AMQP: Advanced Message Queuing Protocol.

API: Interfaz de programación de aplicaciones.

ARPA: Agencia de proyectos de investigación avanzada.

ARPANET: Red operativa de internet global.

CoAP: Constrained Application Protocol.

CSMA/CD: Carrier sense multiple access with collision detection.

D2D: Dispositivo a Dispositivo.

DdoS: Distributed Denial of Service.

DDS: Data Distribution Service.

DSSS: Direct Sequence Spread Spectrum.

DTLS: Datagram Transport Layer Security.

ECG: Electrocardiograma.

ENISA: Agencia Europea de Seguridad de las Redes y de la Información.

EPC: Código Electrónico De Producto.

FBI: Federal Bureau of Investigation.

GHZ: Gigahertz**.**

H2M: Humano a Máquina.

HEW: High Efficiency WLAN.

HF: High Frequency.

HTTP: Hypertext Transfer Protocol.

HVAC: Heating, Ventilating and Air Conditioning.

IaaS: Infraestructura como Servicio.

IBSG: Internet Business Solutions Group.

IEC: International Electrotechenical Commissoion.

IETF: Internet Engineering Task Force.

IETF: Internet Engineering Task Force RFCs.

IIoT: Internet Industrial de las Cosas.

IoT: Internet of Things (Internet de las cosas).

IP: Internet Protocol.

IPv4: Internet Protocol Versión 4.

Ipv6: Internet Protocol Versión 6.

ISM: Industrial, Scientific and Medical.

ISO: International Organization for Standardization.

ITS: Sistemas Inteligentes de Transport.

LAN: Local Area Network.

LF: Low Frequency.

LPWAN: Low Power Wide Area Network.

LTE: Long Term Evolution.

M2M: Máquina a Máquina.

MHz: Megahertz.

MIT: Massachusetts Institute of Technology.

MQTT: Message Queue Telemetry Transport.

MTU: Maximum Transmission Unit.

NFC: Near Field Communication.

OMG: Object Management Group.

PaaS: Plataforma como Servicio.

PREPA: Puerto Rican Electric Power Authority.

QoS: Calidad de Servicio.

RF: Radiofrecuencia.

RFID: Radio Frequency Identification.

SaaS: Software como Servicio.

SIG: Special Interest Group.

STOMP: Simple/Streaming Text Oriented Messaging Protocol.

TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet.

TCP: Transmission Control Protocol.

TI: Tecnologías de la Información.

TIC: Tecnologías de la Información y la Comunicación.

UDP: User Datagram Protocol.

UHF: Ultra High Frequency.

UIT: Unión Internacional de Telecomunicaciones.

V2V: Vehicle to Vehicle.

VSCP: Very Simple Control Protocol.

W3C: World Wide Web Consortium.

WPAN: Wireless Personal Área Network.

WWW: World Wide Web.

XEP: Extensiones de protocolo.

XMPP: Extensible Messaging and Presence Protocol.

INTRODUCCIÓN

Cuando la Internet llegó como servicio de comunicación a organizaciones y ciudadanos del común, se abrieron nuevos mercados en el desarrollo del internet de las cosas (IoT). Este concepto se refiere generalmente a escenarios en los que la conectividad de la red y la capacidad de cómputo se extiende a objetos, sensores y artículos de uso cotidiano [1], estos dispositivos generan y procesan datos, intercambian información dinámicamente y requieren la mínima intervención humana, es decir, las comunicaciones entre las personas y los objetos que se conectan a Internet se hicieron más sencillas, transformando el mundo de los negocios y la calidad de vida.

IoT se convirtió en un ecosistema tecnológico dominante no sólo en las fábricas sino en los diferentes sectores sociales hasta llegar a la comodidad del hogar, por ello este libro presenta una visión global de los modelos y protocolos de comunicación afines con el paradigma IoT, además expone los sectores de aplicación e incidentes de seguridad IoT reales con el fin de comprender los desafíos de seguridad, los focos de riesgo y posibles ataques.

OBJETIVOS

1.1 OBJETIVO GENERAL

Exponer una visión global sobre el paradigma del Internet de las cosas, partiendo desde el nacimiento del concepto y los activos que lo comprenden como un ecosistema inteligente, hasta los desafíos que afronta el mercado en el despliegue de servicios IoT.

1.2 OBJETIVO ESPECIFICOS

- Proporcionar una visión general sobre los componentes de un ecosistema inteligente.
- Presentar los modelos de comunicación que soportan el paradigma IoT.
- Describir los principales protocolos de comunicación y hacia qué tipo de servicios están dirigidos.
- Presentar los campos de aplicación del internet de las cosas, para generar iniciativas de investigación y desarrollo en la facultad de ciencias básicas e ingeniería.
- Indicar los diferentes desafíos de interoperabilidad y seguridad que afronta IoT como ecosistema tecnológico de comunicación dominante.

PLANTEAMIENTO DEL PROBLEMA

DEFINICIÓN DEL PROBLEMA

El suministro de Internet de banda ancha más el desarrollo de tecnologías de la información y los dispositivos inteligentes de bajo costo y abiertos al público general, han impulsado el crecimiento comercial de servicios IoT. Estos servicios se encuentran presentes en casi todos los sectores de la sociedad y se han convertido en un ecosistema de comunicación dominante entre el hombre y una amplia red de dispositivos, edificios, sensores, maquinas industriales y electrodomésticos que están conectados a internet de manera continua, de ahí que en tiempo real se recolectan datos bidireccionalmente de usuarios y componentes electrónicos embebidos con el fin de medir, analizar y optimizar procesos con la más mínima intervención humana. Actualmente no hay una estandarización en el despliegue de dichos servicios y dispositivos por ello es necesario conocer ¿Cuáles son los potenciales riesgos a considerar en el internet de las cosas como ecosistema dominante? y ¿hacia qué tipo de servicios IoT están dirigidos los distintos protocolos de comunicación existentes?

El propósito de esta monografía es informar sobre los aspectos más relevantes del internet de las cosas, los activos que la componen, la arquitectura, los protocolos de comunicación por capas, los sectores de aplicación y los desafíos que enfrenta como sistema de comunicación de avanzada.

JUSTIFICACIÓN

El despliegue masivo de diversos servicios y dispositivos IoT, resulta ser un caos si no se conocen las redes y protocolos de comunicación adecuados, pues no sólo se compromete la interoperabilidad sino además la integridad y seguridad de los datos de usuarios y dispositivos, actualmente hay más dispositivos que personas conectadas, estos dispositivos inteligentes son detectables y configurables de manera remota por medio de un software que de no tener las medidas de seguridad adecuadas se puede convertir en un punto de acceso para agentes malintencionados.

La consultora Gartnet In, una empresa dedicada a la investigación tecnológica con sede en Stamford, público que China, Norteamérica y Europa Occidental representan el 63 % de dispositivos IoT conectados en el año 2017, una cifra cercana a 8.380,6 millones de unidades y se espera que para finales de 2018 esta cifra llegue a los 11.196,6 millones de unidades[2]. Teniendo en cuenta dicha expansión tecnológica, se busca suministrar un libro como herramienta base que contenga las definiciones técnicas que constituye la panorámica del internet de las cosas, como referencia para futuras implementaciones de proyectos similares en Colombia y/o en la región.[2]

MARCO CONTEXTUAL

¿Qué es Internet?

Es un sistema de redes informáticas interconectadas que ha revolucionado el uso de la computadora y dispositivos electrónicos, se distingue por hacer uso de la familia de protocolos TCP/IP para conectar los dispositivos a nivel global. Nació en 1969 y fue creada por un grupo de investigadores de Defensa de los Estados Unidos con la finalidad de implementar un sistema de comunicación con otros entes gubernamentales. Internet ofrece al mercado una amplia gama de servicios y recursos en la que los usuarios pueden acceder a él con un solo clic, debido a que es una instalación pública, cooperativa y autosostenible.[3]

Internet de las cosas

La definición de IoT, se está diversificando alrededor de una multiplicidad de elementos, cosas, objetos o dispositivos inteligentes de uso cotidiano, como sensores, etiquetas de identificación por radiofrecuencia, actuadores, etc., que están interconectados entre sí y así permitir la comunicación e intercambio información a través de internet.[4]

La implementación de esta tecnología en el escenario de comunicaciones inalámbricas ha tenido un gran impacto, y ha integrado una nueva dimensión en el campo de las TIC (Tecnologías de la Información y Comunicación) y en la calidad de vida de las personas porque transforma, simplifica, innova y optimiza los servicios ya presentes en el mercado que necesitan grandes volúmenes de almacenamiento y necesiten procesar la información en tiempo real de manera autónoma.[4]

Dispositivos IoT

Con la aparición de termino de internet de las cosas, se han impulsado en el mercado múltiples dispositivos que interactúan entre sí y con los usuarios por medio de internet o redes de comunicación dedicadas, para recopilar, procesar información del entorno. La tendencia de estos dispositivos cada vez es de menor tamaño.[5]

IoT hace uso de dispositivos electrónicos que sean capaces de recopilar y detectar ciertos parámetros externos, por ejemplo, temperatura, humedad, energía, actividad, variables fisiológicas (presión arterial, frecuencia cardiaca, saturación de oxígeno, etc.) de manera automática y sin la interacción del ser humano, estos datos son emitidos a un repositorio por medio de señales eléctricas para un posterior análisis y toma de decisiones en tiempo real.[5]

Algunos dispositivos usados en IoT son:

Sensores

Es un dispositivo que está especialmente diseñado para detectar o medir una magnitud física de un entorno que se requiere medir o controlar, los datos recolectados son emitidos mediante una señal eléctrica u óptica en tiempo real a una pantalla, smartphone, actuador o son enviados a la nube a un repositorio Back-End. Los sensores se han convertido en un elemento indispensable para trasladar el mundo físico al mundo digital.[6]

En el mercado existen una amplia gama de sensores, que son ofrecidos para complementar ciertas aplicaciones que mejoran la calidad de vida y tareas cotidianas de los usuarios, algunos de estos son [6]:

Sensores de Información ambiental (temperatura y humedad):

Estos sensores se pueden usar en casi todos los ambientes de uso de IoT, permiten monitorear, obtener información y controlar el clima de un entorno.[7]

Sensores de presencia

Estos sensores responden al movimiento físico de un cierto lugar, estos se encuentran generalmente en sistemas de seguridad, control de iluminación en una infraestructura, abrir automáticamente las puertas de una tienda.[7]

Sensor de proximidad:

Son usados para detectar el movimiento de un objeto, o personas que se encuentran cerca del sensor, son usados para monitorear la disponibilidad de lugares en los parqueaderos indicando al conductor que espacio se encuentra disponible.[7]

Sensor de presión:

Estos son utilizados especialmente en la agricultura, ya que ayudan a evitar el desperdicio de agua en el riego usando tácticas que determinan el flujo de agua por las tuberías, al igual se usan en vehículos inteligente y aviones para indicar la fuerza y la altitud apropiada.[7]

Sensores de nivel:

Detectan el nivel de líquidos y otros fluidos, son usados para la gestión inteligente de residuos, medición de tanques, de combustible Diesel, control de irrigación, entre otros.[7]

Actuadores

Estos dispositivos tienen como finalidad recibir la señal de un controlador o regulador, y transformarla en una acción en base a dicha señal, causando un efecto en conjunto sobre un proceso automatizado, estas ejecuciones se fundamentan de acuerdo a ciertas especificaciones ya programadas.[8]

Existen tres tipos de actuadores utilizados en el ecosistema IoT:

Hidráulicos:

Estos dispositivos se utiliza para la presión ejercida por fluidos comúnmente por algún tipo de aceite, se usan para máquinas de gran tamaño que usualmente requieren potencia.[8]

Neumáticos:

Estos actuadores usan la energía de aire comprimido de alta presión para para convertirlo en trabajo mecánico por medio de un movimiento lineal de vaivén.[8]

Eléctricos:

Son accionados por medio de corrientes eléctricas, son usados en sistemas de control de temperatura del agua, controlar el encendido y apagado de sistemas de calefacción y refrigeración.[8]

RED

Una red es un conjunto de dispositivos interconectados entre sí, para compartir recursos e información, y siguen las reglas de los protocolos de la comunicación.[9]

Clasificación de una red

Las redes de comunicación, se pueden dividir en diversas categorías. Algunas de ellas son:

Topología de red

Una topología de red define la estructura física y lógica, en la que varios elementos se conectan a una red. En IoT se utilizan las siguientes topologías.[10]

Estrella: En esta topología de red cada nodo se comunica a un solo nodo central, es decir los nodos extremos no pueden comunicarse directamente. El nodo central actúa como un servidor comúnmente se utiliza como puerta de enlace a internet, en este tipo de red se pueden añadir o eliminar nodos sin interrumpir la red. Un ejemplo de una topología estrella es una red Wifi.[10]

Malla: Esta topología de red es aquella en la que cada nodo se comunica con uno o más nodos a la vez, una red malla ofrece una gran redundancia en la comunicación, es decir, en caso de que un nodo falle los demás pueden seguir intercambiando información usando otro camino logrando una mejor confiabilidad. El beneficio que aporta esta topología es que puede ampliar el rango de alcance a través de múltiples saltos, y a la vez maneja una potencia baja de transmisión[10]. Un ejemplo de una red en malla es Zigbee Light LinkTM, es un control de iluminación inteligente, permitiendo a los consumidores cambiar la luminosidad de manera remota y además administrar el uso de la energía convirtiendo las infraestructuras en edificaciones más ecológicas.[11]

Rango de alcance

La aplicación de estas redes se verá reflejadas en el capítulo de protocolos, y se clasifica de la siguiente manera [12]:

Red inalámbrica de área personal (*Wireless Personal Area Network,* WPAN): esta red tiene un rango de alcance de 10m, son las más básicas y se emplean para conectar dispositivos que estén a cortas distancias, son usadas comúnmente para la transmisión de información emitida por sensores, o de dispositivos, como un smartphone conectado a un auricular a través de Bluetooth.[12]

Red inalámbrica de área personal (*Wireless Local Area Network,* WLAN): Estas redes generalmente cuentan con un rango de alcance de 100m hasta 1Km de cobertura con la ayuda de repetidores, un ejemplo del uso de esta red es una red Wifi doméstica, que proporciona acceso a internet a los smartphones, Tablet, Smart tv, termostatos, etc.[12]

Red de área metropolitana (*Metropolitan Area Network,* WAN): Estas redes tienen un rango de alcance de 50km de cobertura, son ofrecidas por un operador de comunicaciones a través de redes de fibra óptica, en este tipo de red se encuentra Ethernet.[12]

Red de área amplia (*Wide Area Network,* WAN): Es la unión de dos o más redes, proporcionan una cobertura ubicua, este tipo de red es proporcionada por proveedores de internet para cubrir la necesidad de conexión de una zona muy amplia, permitiendo la transmisión a largas distancias de datos, videos, voz imágenes y videos. Hacen uso de satélites, cables interoceánicos, etc., un ejemplo es las redes 4G y 5G.[13]

1. INTERNET DE LAS COSAS

Las personas actualmente se encuentran ocupadas casi todo el día, priorizando el trabajo, el estudio o algún pasatiempo, esto ha llevado a delegar muchas de las pequeñas obligaciones cotidianas a aparatos inteligentes, el ser humano siempre busca la comodidad y con el avance tecnológico y la era digital ya es posible aprovechar al máximo los lapsos de tiempo entre las diversas ocupaciones que exige el ritmo de vida actual. los dispositivos que se conectan a internet son cada vez más accesibles para el público en general, pues ya no son recursos tecnológicos con los que solo contaban las grandes industrias, sino que ya están presentes en hogares y demás sectores económicos.

El internet de las cosas hace referencia a objetos del mundo real que cuentan con una dirección única y se pueden comunicar entre sí, usando como puente la internet
los dispositivos inteligentes (Tablet, Smartphone, Laptop) están conectados todo el tiempo a internet y funcionan como una llave no física, que brinda acceso remoto a los diferentes mercados que ofrece IoT (Internet of Things), desde encender una cafetera y las luces del hogar sin estar presente en el sitio, hasta llamar automáticamente una ambulancia en caso de un ataque cardiaco o manejar un tractor de manera remota.

Los servicios emergentes de IoT tienen como objetivo suministrar calidad de servicio entre los tiempos de solicitudes y respuestas, reduciendo la complejidad y optimizando el manejo de recursos como pueden ser la comunicación en la nube y protocolos de enrutamiento.[14]

1.1 HISTORIA DEL INTERNET DE LAS COSAS

Antes de iniciar con la historia del internet de las cosas, se debe conocer al origen del Internet, dado que gracias a este medio de comunicación y su evolución a través del tiempo se dio el acceso e interconexión a múltiples servicios.

1.1.1 Breve historia sobre el origen del internet

Internet comenzó como un proyecto de defensa de los Estados Unidos por ARPA (Agencia de proyectos de investigación avanzada), quienes crearon ARPANET (red operativa de internet global), su misión consistía en mantener las comunicaciones con diferentes entidades académicas entre ellas universidades y centros de investigación, el 29 de octubre de 1969 envía su primer mensaje; y crea una red de información descentralizada el 21 de noviembre entre 4 universidades, Stanford, Utah, Santa Bárbara y Los Ángeles, su crecimiento fue exponencial y en 1983 ya tenía 500 computadoras enlazadas y en promedio cada 20 días se establecía comunicación con una nueva computadora. [15]–[17]

Debido a la alta concentración de computadoras conectadas y la incompatibilidad que presentaban entre ellas por convertirse en una red de redes, en 1981 se implementó el Protocolo De Control De Transmisión/Protocolo De Internet (TCP/IP), que determina cómo se envía la información desde el remitente hasta el destinatario. [18]

En 1990 Berners-Lee llevó a cabo la primera comunicación exitosa entre un servidor, y un cliente llamado World Wide Web (WWW) que se basa en un sistema de hipertextos interconectados y accesibles vía internet, en este mismo año desaparece ARPANET. Un año después se creó la primera página web con dominio y nombre propio, donde las empresas publicaban sus servicios en sitios web. A partir de 1994 el comercio electrónico hace su aparición y a finales de siglo XX aparece por primera vez el término internet de las cosas y se mantiene en auge hasta hoy en día. [16]

1.1.2 Acontecimientos destacados en la historia del Internet de las cosas

I. "El término internet de las cosas fue utilizado por primera vez en 1999 por el británico Kevin Ashton para describir un sistema en el que los objetos en el mundo físico podrían ser conectados a Internet por sensores ". [1]

En 1999, Ashton lo dijo mejor en esta cita de un artículo en el RFID Journal (Radio Frequency Identification): *"Si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiese saberse de cualquier cosa –usando datos recolectados sin intervención humana– seríamos capaces de hacer seguimiento detallado de todo, y poder reducir de forma importante los costes y malos usos. Sabríamos cuando las cosas necesitan ser reparadas, cambiadas o recuperadas, incluso si están frescas o pasadas de fecha. El Internet de las Cosas tiene el potencial de cambiar el mundo como ya lo hizo Internet. O incluso más."* [19]

II. En el 2005 IoT alcanzó otro nivel cuando la Unión Internacional de Telecomunicaciones (UIT) de la ONU publicó su primer informe sobre el tema.

"Una nueva dimensión al mundo de las tecnologías de la información y la comunicación (TIC): desde *cualquier momento*, la conectividad de *cualquier lugar* para *cualquier persona*, ahora tendremos conectividad para *todo*. Las conexiones se multiplicarán y crearán una red dinámica de redes completamente nueva: Internet de las Cosas". [20]

III. Según Cisco Internet Business Solutions Group (IBSG), Internet of Things nació entre 2008 y 2009 simplemente en el momento en que más "cosas u objetos" estaban conectados a Internet, que las personas. [21]

IV. En el 2009 Kevin **Ashton**, profesor del MIT, usó la expresión *Internet of Things (IoT)* de forma pública por primera vez, y desde entonces el crecimiento y la

expectación alrededor del término ha ido en aumento de forma exponencial. [22]

V. En el 2010 el Primer ministro chino Wen Jiabao considera a IOT una industria clave para China. [23]

VI. En 2011 se lanzó el nuevo **protocolo IPV6**. Con este nuevo protocolo de Internet se pueden identificar instantáneamente todos los objetos, otorgando 340 sextillones de direcciones IP suficientes para que IoT pueda disponer de estas a gran escala.[20]

VII. En el año 2020, se espera que más de 20.400 millones de dispositivos estén conectados.[15]

1.2 DEFINICIONES DE INTERNET DE LAS COSAS

Con respecto al termino de internet de las cosas, es necesario abordar los diferentes conceptos que han tenido impacto en la sociedad tecnológica.

"El término "Internet de las cosas" (IoT) denota una tendencia donde una gran cantidad de dispositivos integrados emplean servicios de comunicación ofrecidos por los protocolos de Internet. Muchos de estos dispositivos, a menudo llamados "objetos inteligentes ", no son operados directamente por los seres humanos, sino que existen como componentes en edificios o vehículos, o se extienden en el medio ambiente." [24]

"Internet of Things (IoT) es un framework en el que todas las cosas tienen una representación y presencia en Internet. Más específicamente, Internet of Things tiene como objetivo ofrecer nuevas aplicaciones y servicios que conectan los mundos físicos y virtuales, entre las comunicaciones de máquina a máquina

(M2M) representando la comunicación en línea que permite las interacciones entre cosas y aplicaciones en la nube." [25]

"El Internet de las cosas es un nuevo concepto que completa la evolución de las comunicaciones y la informática, aplicándola a los objetos, que facilita una mejor interacción con ellos. Se refiere a una red de objetos cotidianos interconectados a través de Internet". [26]

"El Internet de las cosas (IoT) es un paradigma de comunicación reciente que prevé un futuro cercano, en el que los objetos de la vida cotidiana estarán equipados con microcontroladores, transceptores para la comunicación digital y apilamientos de protocolos adecuados que los harán capaces de comunicarse entre ellos. y con los usuarios, convirtiéndose en una parte integral de Internet." [27]

"IoT (Internet of things/Internet de las cosas) es una arquitectura emergente basada A la cadena de suministro y que tiene un impacto importante en la seguridad y privacidad de los actores involucrados." [28]

1.3 ACTIVOS EN EL ECOSISTEMA IOT

La esencia del internet de las cosas es mantener una comunicación oblicua y permanente entre los activos, es decir, los recursos como las redes y protocolos de comunicación, objetos inteligentes, sensores, actuadores, intermediarios, servicios de administración, servicios de minería de datos, servicios en la nube y demás elementos, de ahí nace el termino ecosistema IoT, ya que está compuesto de una variedad de activos.

A continuación, se expone en la tabla 1, una panorámica de los activos indispensables en cualquier ecosistema IoT.

ACTIVOS	ELEMENTOS	DESCRIPCIÓN
Dispositivos IoT	Hardware	Conjunto de componentes físicos de un dispositivo electrónico.
	Software	Conjunto de programas y aplicaciones que pertenecen a un sistema específico.
	Sensores	Estos dispositivos son utilizados para detectar estímulos y acciones externas del medio, por ejemplo, la humedad, temperatura de una infraestructura.
	Actuadores	En IoT estos dispositivos tienen como función realizar una acción en conjunto, en caso de que se sobrepase un límite que está parametrizado.
Otros dispositivos presentes en ecosistemas IoT	Dispositivos intermediarios	Son dispositivos que funcionan como interfaz de comunicación, dentro de un ecosistema IoT determinado.
	Dispositivos de administración	Son dispositivos cuya especialidad es la administración de redes de manera remota.
	Sistemas embebidos	Son sistemas que realizan unas pocas funciones dedicadas, su objetivo es ejecutar tareas de control.
Comunicaciones	Redes	Hace referencia a un conjunto de dispositivos conectados entre sí y que comparten recursos.
	Protocolos	Es un conjunto de reglas definidas para comunicaciones especiales.
Infraestructura	Routers	Un enrutador se encarga de definir la conectividad de los dispositivos a nivel de red.

	Gateways	Funciona como puerta de enlace y se encarga de traducir la información de un protocolo.
	Power supply	Se encarga de suministrar energía a los dispositivos IoT y a sus componentes.
	Activos de seguridad	Están encargados de la protección de las redes, dispositivos e información, para ello se implementan diversos aplicativos de seguridad.
Plataformas Back-end	Servicios basados en web	Utilizan un conjunto de estándares y protocolos, para el intercambio de información entre aplicaciones.
	Infraestructura y servicios en la nube	Los servicios back-end se encargan de almacenar y procesar los datos que son subidos a la nube por distintos dispositivos.
Toma de decisiones	Minería de datos	Hace referencia a los algoritmos que se encargan de filtrar y procesar los datos recopilados por diversas fuentes.
	Procesamiento de datos e informática	Tras el análisis de los datos, se optimizan y automatizan procesos sistemáticos.

Tabla 1 Activos presentes en un ecosistema IoT.[29]

2. MODELOS DE COMUNICACIÓN

En marzo de 2015 la Junta de Arquitectura de Internet (Internet Architecture Board), dio a conocer un documento (RFC 7452) que describe cuatro modelos de comunicación estandarizados para la conectividad de objetos inteligentes[1].

Ilustración 1 Conectividad IoT.
Tomado de BICS, Soluciones integrales de conectividad IoT global.[30]

2.1 MODELO DE COMUNICACIÓN DISPOSITIVO A DISPOSITIVO

Comúnmente conocido como D2D (Dispositivo a Dispositivo), es un modelo de comunicación que permite la conexión entre dos dispositivos o más en tiempo real y de manera remota, para recibir o transmitir información y desencadenar una

acción sin disponer de un servidor de aplicaciones que opere como intermediario, funciona a través de una red o un enlace directo para el intercambio de información.

Entre las tecnologías que implementan el modelo de comunicación D2D se encuentran Bluetooth, Z-Wave y ZigBee, ya que se caracteriza por soportar una baja tasa de transmisión de datos y puede operar en diferentes topologías de red.

Su principal uso es en la domótica en servicios de control de iluminación, temperatura y sistemas de seguridad que deben soportar varios nodos de comunicación, por medio de redes inalámbricas enlazadas a dispositivos de bajo consumo energético. [31][1]

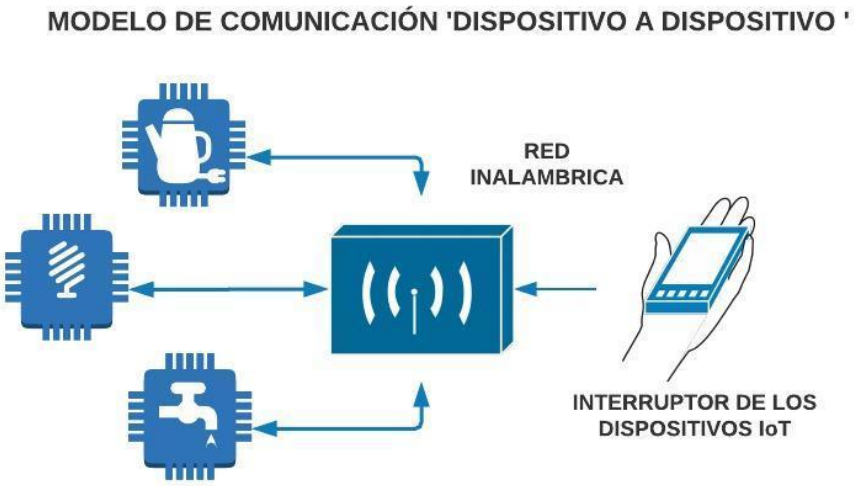


Ilustración 2 Modelo de comunicación dispositivo a dispositivo.[32]

Este modelo de comunicación es ideal en el uso de redes celulares ya que funciona con una latencia ultra baja para la comunicación entre los dispositivos, además puede operar en un espectro de frecuencia de uso privativo (con licencia) o libre (sin licencia). Actualmente este paradigma de comunicación se enfoca en cubrir la exigencia de una transferencia de datos diligente en cuanto a

información tipo multimedia, así mismo, mejorar la calidad de llamadas de voz, según sea el tipo servicio IoT.[1]

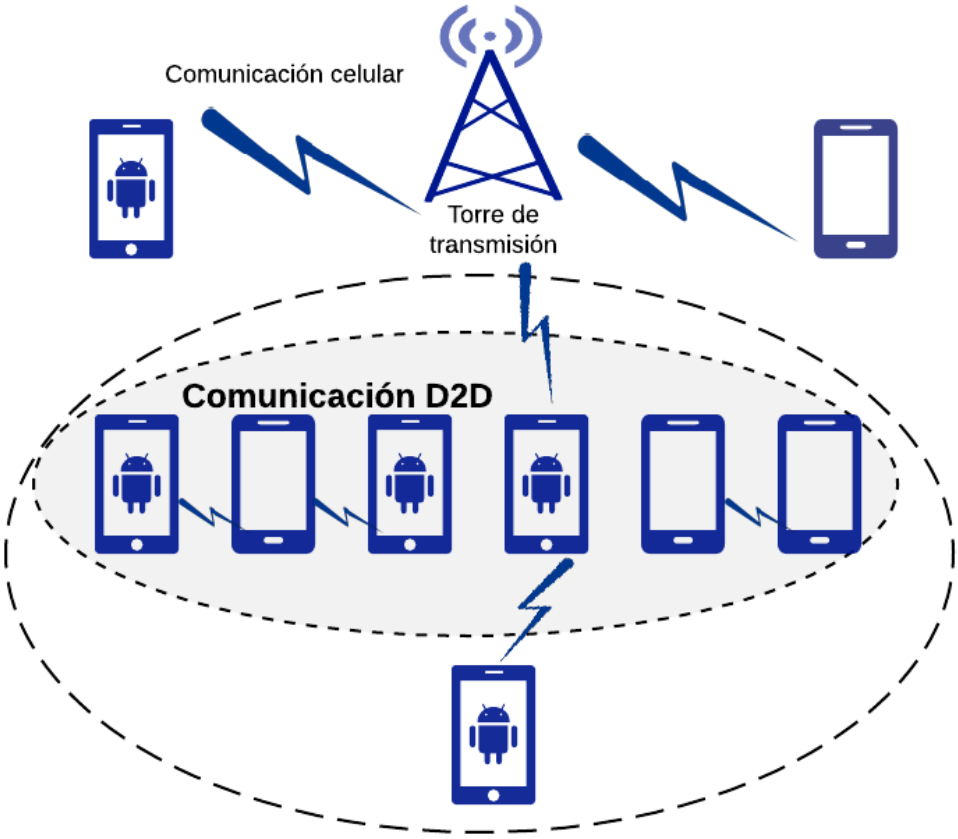


Ilustración 3 Comunicación celular y comunicación D2D. Se muestran las redes de un solo salto y multisalto formadas por enlaces D2D. [33]

Para qué un dispositivo actúe como un punto de acceso debe poseer una conexión previa con un segundo dispositivo, esto hace posible la comunicación entre los nodos y el suministro de servicios que cada nodo (dispositivo) tiene asignado, de esta manera se conoce el volumen de transferencia de datos. [34]

2.1.1 Escenarios de caso de uso del paradigma D2D

Servicios de datos locales

Por medio de transmisiones unicast, groupcast y broadcast, se establecen comunicaciones D2D de calidad para brindar servicios IoT con datos locales, sirve de ejemplo el intercambio de información y la descarga de datos.[33]

Extensión de cobertura

Debido al crecimiento de servicios IoT, es indispensable extender el rango de cobertura, pues existen casos como los fallos de cobertura en los bordes o bloqueos de la señal por factores ambientales, para ello se implementan relés que habilitan multisalto en los nodos y así extender la cobertura del servicio de red celular, *otra forma de aumentar la potencia de la señal en un receptor es retransmitirlo a través de múltiples rutas paralelas, cada una compuesta de dispositivos de colaboración.*[33]

Comunicación máquina a máquina (M2M)

Es una tecnología habilitada para IoT, se comunica de manera autónoma y en tiempo real, esta permite a los dispositivos (máquinas) de baja potencia establecer comunicación con dispositivos de alto nivel computacional que hacen parte de la misma red, para ser más específicos el último se encarga de supervisar el flujo de datos mediante una aplicación determinada para el sistema IoT que se suministra, transmitiendo información de su funcionamiento o anomalías en el mismo. [33]

2.2 MODELO DE COMUNICACIÓN DE DISPOSITIVO A LA NUBE

Este modelo conecta directamente los dispositivos IoT a servicios de almacenamiento y procesamiento de algoritmos en la nube, los mismos deben poseer un hardware capaz de establecer comunicación a internet por medio de cableado ethernet o wifi, además estos dispositivos deben tener recursos de

procesamiento de una pila TCP/IP para disponer de un intercambio de datos eficiente entre el dispositivo y la red IP. [1][31]

El usuario controla el dispositivo remotamente enviando comandos desde un aplicativo web alojado en el teléfono celular, tablet o computadora, por ejemplo, un termostato como dispositivo IoT envía información a una base de datos en la nube, estos se pueden analizar para optimizar el consumo de energía en el hogar (Ver Ilustración 3).[1]

Se debe tener en cuenta que al suministrar un servicio IoT que utiliza este modelo de comunicación, se hace necesario contar con el mismo proveedor de dispositivos y de servicios a la nube, para garantizar que la conexión entre los mismo sea activa y segura, pues así se promete un buen servicio, a esto se le conoce como bloqueo de proveedor. [1], [31]

Ilustración 4 Modelo de comunicación dispositivo a la nube [32]

Los datos almacenados por el dispositivo se llaman Telemetría, esta tecnología proporciona información acerca de la medición y monitorización automática que comúnmente son recopilados por los sensores o dispositivos IoT, para

posteriormente ser enviados al proveedor de aplicaciones en la nube. Los datos de telemetría son lecturas tomadas sobre el medio ambiente.[35]

En el modelo de comunicación dispositivo a la nube, los dispositivos IoT deben conectarse directamente a un servicio a la nube para garantizar el intercambio de información y a su vez controlar el tráfico de mensajes, por ello deben contar con un proveedor de servicios de aplicaciones. Los servicios en la nube, proporcionan diversos modelos de aplicación dependiendo si es para un cliente individual o es para uso comercial, estos modelos son un Servicio de Arquitectura Orientada (SOA); que define distintos niveles de abstracción que ofrecen las empresas para clientes comerciales [36]. Estos modelos de servicio son los siguientes:

Software como servicio (SaaS): en este tipo de modelo el proveedor de servicios de aplicaciones, posibilita a un cliente usar diversas aplicaciones de software a través de Internet y que accedan a distintas aplicaciones como por ejemplo, Google Apps y SalesForce, por medio de sus teléfonos, computadoras, IPad, etc. [37]

Plataforma como servicio (PaaS): permite al cliente ejecutar, desplegar y gestionar aplicaciones que proporcionan los proveedores de servicios a la nube. A diferencia de SaaS que provee al cliente aplicaciones completas, PaaS permite al cliente desarrollar, diseñar y usar aplicaciones directamente a la nube, de esa forma el cliente controla el ciclo de vida del software, un ejemplo de un proveedor de PaaS es Windows Azure.[37]

Infraestructura como Servicio (IaaS): en este modelo se suministra al cliente un conjunto de servicios virtualizados (ancho de banda de red, capacidad de almacenamiento, memoria, potencia de procesamiento) en la nube, permitiendo reducir o escalar los recursos con rapidez para ajustarlos a la demanda y pagar por el uso de los mismos. Su objetivo principal es hacer que los recursos sean más accesibles para las aplicaciones, por consiguiente, brinda servicios de

demanda para una infraestructura básica. Ejemplo de proveedores IaaS son Dropbox y Amazon web service. [38]

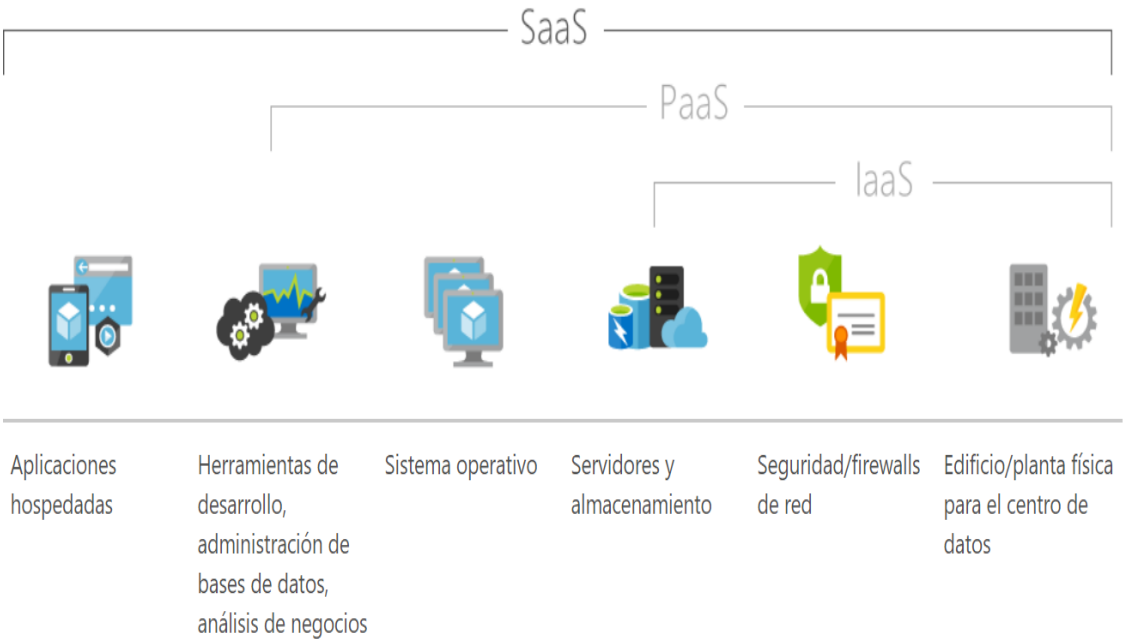


Ilustración 5 Infraestructura de las plataformas de servicios

Tomado de Microsoft Azure IoT[39]

Un ejemplo de comunicación de dispositivo a la nube es Microsoft Azure IoT, este es un proveedor de servicios y de tecnologías a la nube, que ofrece aplicaciones y servicios de tipo PaaS y SaaS [40], además están especialmente diseñadas para conectar, supervisar y controlar múltiples recursos IoT con la ayuda de IoT Hub, que es un servicio administrado y controlado desde la nube, el cual opera como un centro de mensajes para la comunicación bidireccional entre aplicaciones y dispositivos IoT que se están administrando. [41]

Guía de comunicación dispositivo a la nube de Microsoft Azure IoT

	Mensajes de dispositivo a nube	Propiedades notificadas del dispositivo gemelo	Cargas de archivos
Escenario	Serie temporal de telemetría y alertas. Por ejemplo, lotes de datos del sensor de 256 KB enviados cada cinco minutos.	Funcionalidades disponibles y condiciones. Por ejemplo, el modo actual de conectividad del dispositivo, como móvil o Wifi. Sincronización de flujos de trabajo de ejecución prolongada, como configuración y actualizaciones de software.	Archivos multimedia. Lotes de telemetría (generalmente comprimidos) de gran tamaño.
Almacenamiento y recuperación	Almacenados temporalmente por IoT Hub, hasta 7 días. Solo lectura secuencial.	Almacenados por IoT Hub en el dispositivo gemelo. Recuperables mediante el lenguaje de consulta de IoT Hub.	Almacenadas en la cuenta de Azure Storage proporcionada por el usuario.
Tamaño	Mensajes de hasta 256 KB.	El tamaño máximo de las propiedades notificadas es 8 KB.	Tamaño máximo de archivo admitido por Azure Blob Storage.
Frecuencia	Alta.	Mediana.	Baja.

Protocolo	Disponible en todos los protocolos.	Disponible con MQTT o AMQP.	Disponible cuando se usa cualquier protocolo, pero hace falta HTTPS en el dispositivo.

Tabla 2 Guía de comunicación dispositivo a la nube Tomada de guía de desarrollador, Microsoft Azure IoT. [42]

2.3 MODELO DE DISPOSITIVO A PUERTA DE ENLACE

La puerta de enlace se traduce como un dispositivo tipo smart que posee un software que hace de intermediario entre internet y un servidor de aplicaciones, establece una conexión a diversos servicios en la nube, esta puerta garantiza una interoperabilidad en la trasmisión de datos bidireccionalmente.[1]

En otras palabras, utiliza el paradigma ALG o Application Layer Gateway, es un componente de software que gestiona protocolos de aplicación específicos, tales como SIP (Session Initiation Protocol) y FTP (File Transfer Protocol).[31]

Al presentarse en el mercado una amplia variedad de servicios IoT, al igual que diversos dispositivos smart, no se cuenta con la capacidad nativa de conectarse directamente a la nube, de allí que es necesario poseer el software que otorga el proveedor del servicio, para no tener complicaciones en la traducción de protocolos y datos.[1], [31]

Ilustración 6 Modelo de comunicación dispositivo a puerta de enlace. [32]

El software se convierte en la puerta de enlace al dispositivo IoT, y se encarga de cerrar la brecha semántica entre los datos sin procesar que son recolectados por el sensor, y filtrarlos de los datos que se deben observar en el nivel de aplicación, dicho de otra manera, en lugar de tratar directamente con los datos en bruto, su principal objetivo es acceder y consultar de una manera fácil e intuitiva los dispositivos y/o sensores y los datos producidos por los mismos, de no filtrarlos se podrían observar datos privados y de configuración, como la ubicación del sensor y el modo de operación del mismo.[43]

En el nivel de aplicación se ejecutan reglas y comandos de forma remota sobre los dispositivos que hacen parte de una red local, para mantener una comunicación con sistemas en la nube, por otra parte, la puerta de enlace puede contener funciones de enrutamiento, firewall, y servicios de proxy. De lo anterior se puede decir que es fácil integrar sistemas de gestión de la privacidad y seguridad de los datos, que se mantienen locales y los que se publican.[44]

Como ejemplo de comunicación de dispositivo a puerta de enlace se hablará de Azure IoT Edge.

Azure IoT Edge se puede usar para satisfacer todas las necesidades de una puerta de enlace de IoT, admite sistemas operativos como Linux y Windows, y lenguajes como Java, .NET Core 2.0, Node.js, C y Python, además opera sin conexión o con una conexión intermitente con el servicio alojado en la nube. Azure IoT Edge también permite implementar el procesamiento de eventos complejos, el aprendizaje automático, el reconocimiento de imágenes y otros tipos de inteligencia artificial de gran valor sin necesidad de escribirla internamente, además funciona en dispositivos que implementen cualquiera de los protocolos MQTT, AMQP o HTTP.[45]

Ilustración 7 Aplicaciones de Azure IoT Edge
Tomado de ownCloud 9.0 Enables Full Federation. [46]

Compañías que han implementado servicios de Azure IoT Edge para mejorar sus servicios productivos.

Ilustración 8 Empresas que usan servicios Azure IoT
Tomado ownCloud 9.0 Enables Full Federation [46]

Existen tres patrones para usar un dispositivo IoT Edge como puerta de enlace: transparente, traducción del protocolo y traducción de la identidad:

- Transparente

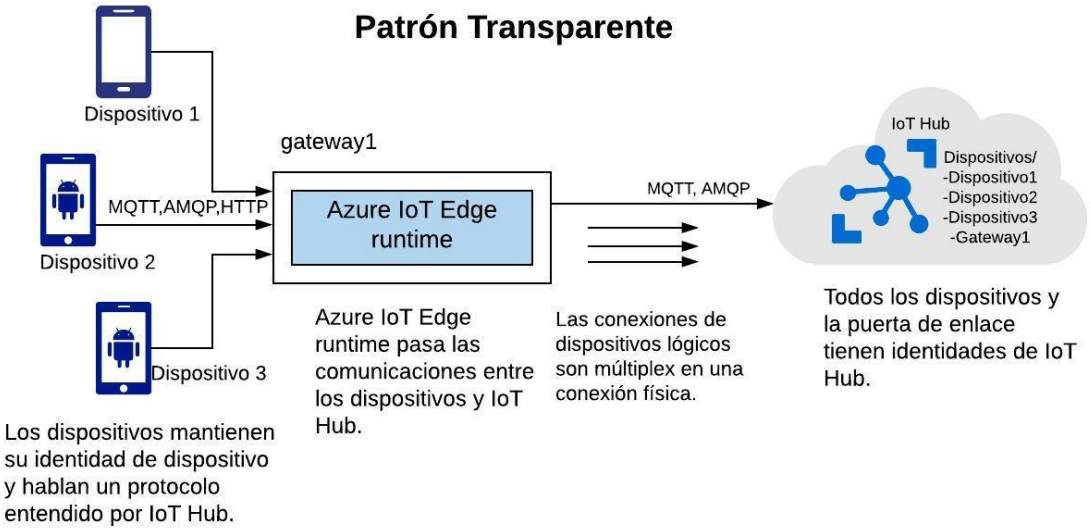


Ilustración 9 Patrón de Transparente[45]

La puerta de enlace es transparente para el usuario que se comunica con los dispositivos IoT Hub, ya que no sabe que hay un intermediario entre el dispositivo y los servicios alojados en la nube.[45]

- Traducción del protocolo

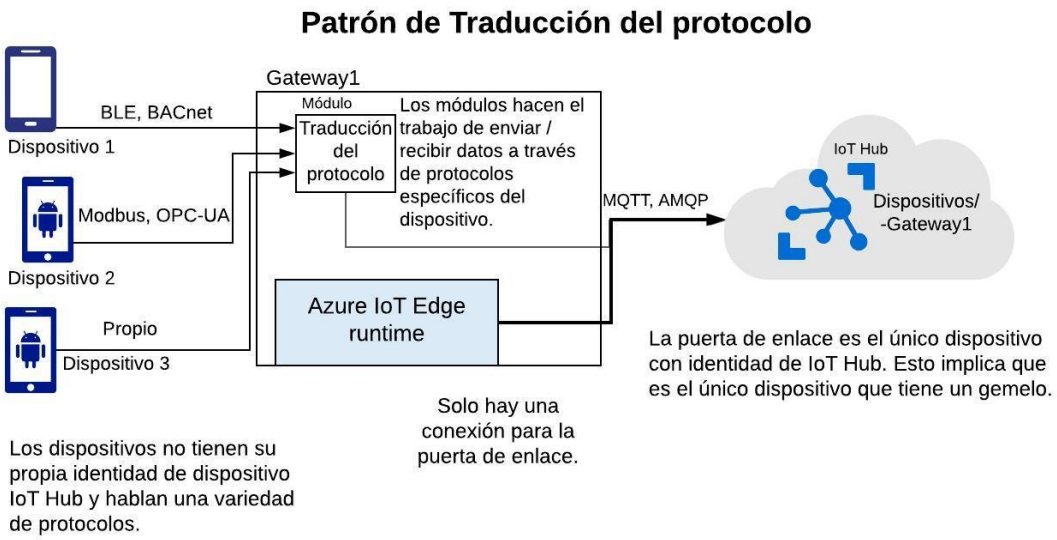


Ilustración 10 Patrón de Traducción del protocolo[46]

Los dispositivos que no admiten MQTT, AMQP o HTTP usan un dispositivo de puerta de enlace para enviar datos a IoT Hub. La puerta de enlace es lo suficientemente inteligente como para comprender ese protocolo utilizado por los dispositivos de nivel inferior; sin embargo, es el único dispositivo que tiene identidad en IoT Hub. Toda la información parece proceder de un dispositivo, es decir, la puerta de enlace.[45]

- Traducción de identidad

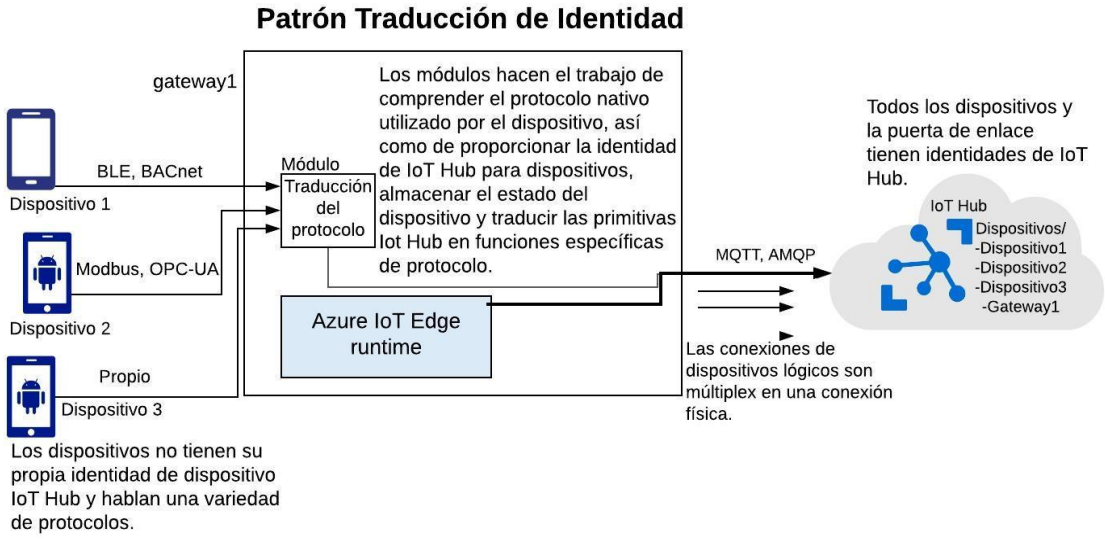


Ilustración 11 Patrón Traducción de identidad [46]

La puerta de enlace traduce el protocolo implementando por los dispositivos de nivel inferior que no se pueden conectar a IoT Hub, por ello les otorga una nueva identidad, de ahí que en IoT Hub se visualizan como dispositivos de primera clase.[45]

2.4 MODELO DE INTERCAMBIO DE DATOS A TRAVÉS DEL BACK-END

Este modelo extiende la comunicación del modelo de comunicación dispositivo a la nube, y se caracteriza por permitir el acceso a los datos recolectados por dispositivos smart que exportan información por medio de sensores a la nube, estos flujos obtenidos por toda una gama de dispositivos IoT en un entorno específico pueden ser accedidos y analizados por parte de terceros, esto quiere decir que ya no se presentan silos de datos por cada dispositivo; a través de back-end permite al usuario trasladar sus datos si llegan a cambiar de servicio IoT. [1]

El modelo de intercambio de datos a través del back-end sugiere que, para lograr la interoperabilidad de los datos de dispositivos inteligentes alojados en la nube, se requiere un enfoque de servicios federados o interfaces de programación de aplicaciones (Apis) en la nube.[47]

¿Pero qué es un back-end? es aquella tecnología que se encarga de interactuar con las bases de datos, permitiendo procesar solicitudes, al igual que generar y enviar respuestas al cliente. Para realizar este proceso se necesita tres componentes [48]:

- Almacenamiento de los datos: la información puede ser almacenada en la nube por el usuario o la aplicación, para que pueda ser recuperada de manera rápida.[48]
- Servidor de aplicaciones: se conecta con un servicio a la nube, este involucra una cantidad de servidores, en donde cada uno de ellos está diseñado para ejecutar diferentes funciones, y a su vez estar disponibles para el cliente por medio de una interfaz.[48]
- Nodos de control: se usan principalmente para mantener todo el sistema, además, monitorear la demanda del cliente y el flujo de tráfico de información, para asegurar que el sistema funcione sin ningún problema. [48]

El dispositivo IoT realiza el envío de datos por medio back-end, esta información es alojada en múltiples tipos de bases de datos, de acuerdo a la función que se desee realizar. Existen diversas formas para la conexión a la nube, que puede soportar back-end, como por ejemplo que sea por medio de una conexión de red remota, a través de M2M o Wifi.[48]

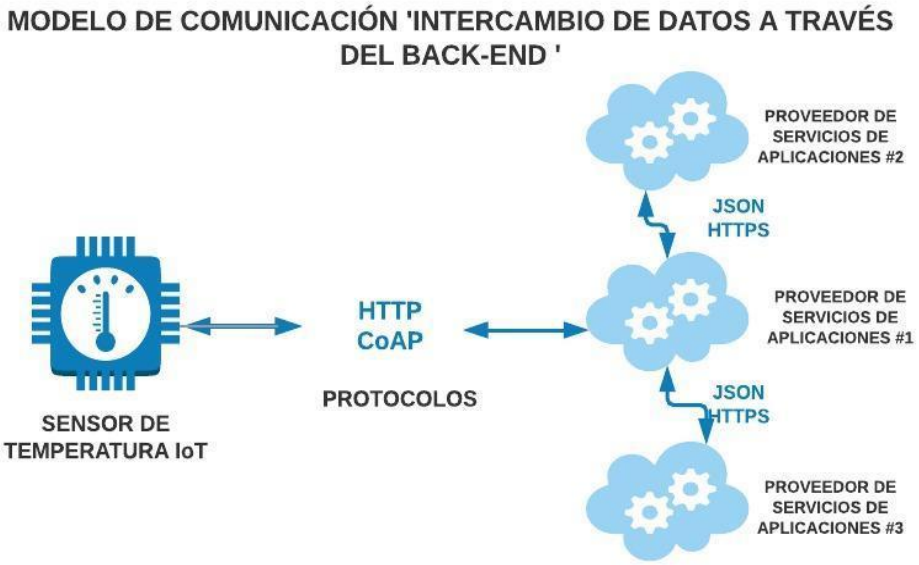


Ilustración 12 Modelo de comunicación de intercambio de datos a través del back-end [32]

Un ejemplo de aplicación de comunicación por medio de back-end, es en Smart Cities que otorgan cobertura a los servicios asociados a front-end (es la capa de presentación, que actúa como la interfaz con el usuario) como servicios IoT orientados a transporte, energía, sanidad, educación, entre otros, que necesitan de la tecnología back-end, para permitir la recolección de datos, el análisis y almacenamiento de los mismos. [49]

Ilustración 13 Aplicación de back-end en las Smart cities Tomado de El front-end y el back-end de las Smart Cities, Equipo Altran. [49]

Otro ejemplo, es IEI Smart Fitness Solution, es un servicio que ofrece equipos de acondicionamiento físico personalizados y equipos de rehabilitación tipo IoT, con el propósito de crear un mejor entorno de entrenamiento y ofrecer una experiencia de alta calidad a sus clientes, a estos se les proporciona una interfaz estándar, que también puede ser personalizada. Los datos son recolectados por los equipos de entrenamiento y clasificados para un posterior análisis de la condición física de cada cliente.[50]

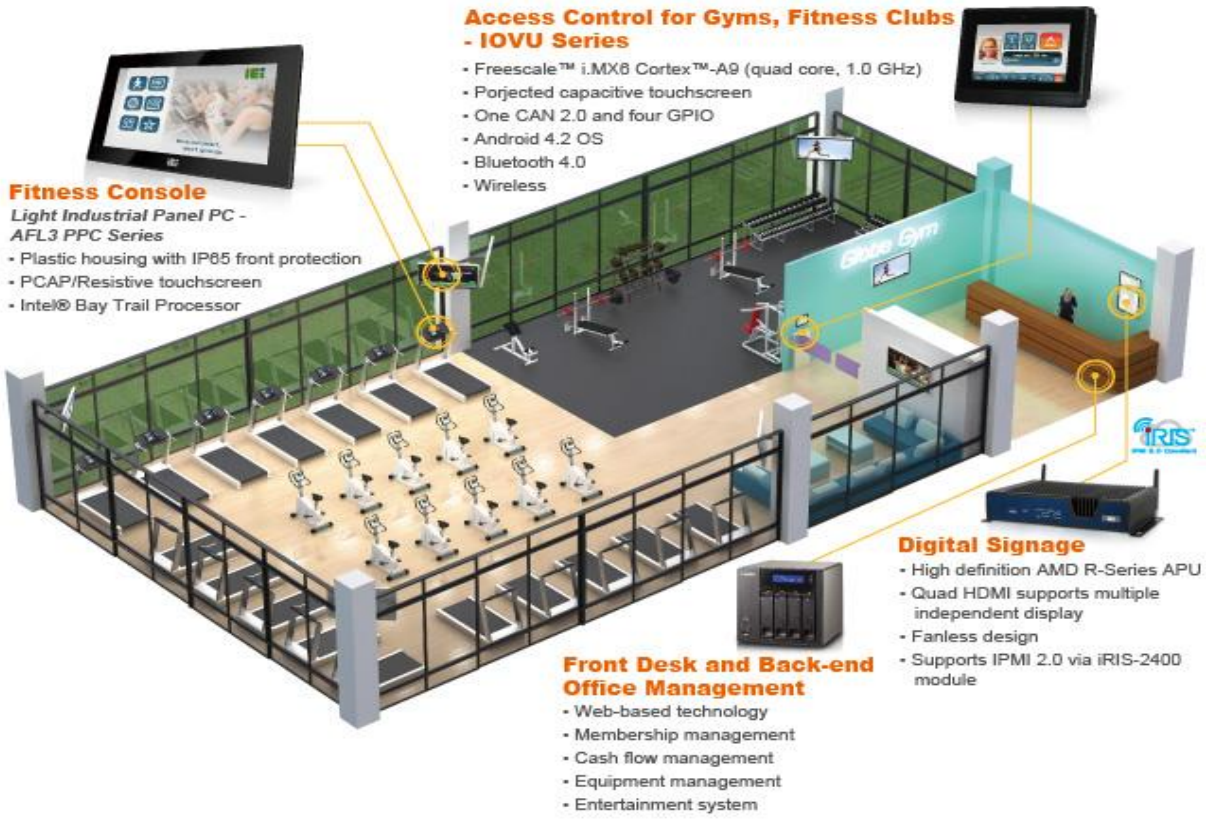


Ilustración 14 Centro de acondicionamiento físico personalizado usando servicios IoT y el modelo de comunicación back-end Tomado de Fitness Solution. [50]

3. PROTOCOLOS DE COMUNICACIÓN PARA IOT

Para garantizar una comunicación confiable y eficiente entre diversos dispositivos IoT, que están situados en sistemas diferentes, se adoptan protocolos que se definen y utilizan dependiendo de la necesidad o requerimientos del servicio que se suministra. Los protocolos presentan una arquitectura en capas, donde cada una brinda una funcionalidad que está condicionada por un conjunto de reglas, para el envío y recepción de datos entre dispositivos que estén conectados a una red.

Los elementos que caracterizan un protocolo son [51]:

- ***La sintaxis:*** Incluye aspectos tales como el formato de los datos y los niveles de señal.
- ***La semántica:*** Incluye información de control para la coordinación y el manejo de errores.
- ***La temporización:*** Incluye la sincronización de velocidades y la secuenciación.

CAPAS	MODELO OSI	MODELO TCP/IP	MODELO IoT
1	APLICACIÓN	APLICACIÓN	APLICACIÓN
2	PRESENTACIÓN		
3	SESIÓN		
4	TRANSPORTE	TRANSPORTE	INTERNET
5	RED	INTERNET	
6	ENLACE DE DATOS	ACCESO A LA RED	PERCEPCIÓN
7	FÍSICA		

Tabla 3 Comparación de los Modelos OSI, TCP/IP y IoT.[52][53]

<table>
<tr><th>CAPAS OSI</th><th>CAPAS IoT</th><th colspan="15">TECNOLOGÍAS Y PROTOCOLOS</th></tr>
<tr><td>APLICACIÓN</td><td rowspan="3">APLICACIÓN</td><td>HTTP</td><td>COAP</td><td>XMPP</td><td>MQTT</td><td>AMQP</td><td>VSCP</td><td>STOMP</td><td>DDS</td><td colspan="2">OpenWire</td><td rowspan="5">Z-Wave</td><td rowspan="5">Zigbee</td><td rowspan="4">THREAD</td></tr>
<tr><td>PRESENTACIÓN</td></tr>
<tr><td>SESIÓN</td></tr>
<tr><td>TRANSPORTE</td><td colspan="2" rowspan="2">UDP</td><td colspan="2" rowspan="2">TCP</td><td colspan="2" rowspan="2">6LowWPAN</td><td colspan="2" rowspan="2">IPv6</td><td>IPv4</td><td rowspan="4">Sigfox</td></tr>
<tr><td>INTERNET</td><td>INTERNET</td></tr>
<tr><td>ENLACE</td><td rowspan="2">PERCEPCIÓN</td><td rowspan="2">Wifi</td><td>LoRaWAN</td><td rowspan="2">Bluetooth</td><td rowspan="2">RFID</td><td rowspan="2">NFC</td><td rowspan="2">Ethernet</td><td rowspan="2">IEEE 802.15.4</td><td rowspan="2">4G</td><td rowspan="2">5G</td></tr>
<tr><td>FISICA</td><td>LoRa</td></tr>
</table>

Tabla 4 Tecnologías y Protocolos presentes en el modelo IoT.[54]

3.1 PROTOCOLOS Y TECNOLOGÍAS EN LA CAPA DE PERCEPCIÓN

3.1.1 Wifi

Esta tecnología permite la interconexión de distintos dispositivos, de manera inalámbrica, por medio de radiofrecuencias e infrarrojos, que son usados para la difusión de información.[55]

WIFI es una tecnología de comunicación inalámbrica, basada en el estándar IEEE 802.11, esta especificación determina las normas o protocolos de operabilidad de una red de área local, en consecuencia la tecnología wifi, garantiza la compatibilidad e interoperabilidad en los dispositivos certificados bajo este estándar.[56]

Para el funcionamiento de la tecnología Wifi, se requiere obligatoriamente el uso de un enrutador o router que esté conectado a internet, para que este emita la señal de forma inalámbrica en un radio de alcance determinado.[55]

Actualmente existen diferentes tipos de comunicación Wifi basados en el estándar **IEEE 802.11**, distinguiéndose las siguientes: **802.11b**, se emite a 11 Mbit/seg, **IEEE 802.11g** ofrece una velocidad de 54 Mbit/s, **IEEE 802.11n** que cuenta con una velocidad de hasta 300 Mbit/s, todas ellas operan con una banda de frecuencia universal de 2,4 GHz, por este motivo se convierte en una tecnología perfecta para el acceso a internet, de forma inalámbrica, y por ultimo está el estándar **IEEE 802.11ac** que opera únicamente en la banda de 5 GHz y trabaja a una velocidad máxima de 1.300 Mbit/s. Normalmente el radio de cobertura es de 5 a 150 metros, esto depende del tipo de dispositivo emisor se esté usando para transmitir dicha señal. [57]

Wifi es una alternativa apropiada para aplicaciones IoT, pero debido a ciertas limitaciones en los requisitos para la conectividad de dispositivos IoT, han

encaminado a la alianza wifi a crear nuevas especificaciones, que solucionen las restricciones tanto en eficiencia energética y alcance.[58]

Una de las nuevas tecnologías diseñadas es **Wifi Halow**, se lanzó al mercado para resolver problemas de potencia y de alcance de IoT, opera con una banda de 900 MHz, por esta razón es apropiado para pequeños paquetes de datos y dispositivos con bajo consumo de energía[58]. Otra especificación que se lanzará al mercado para el 2019 es el estándar **HEW** (High Efficiency WLAN), que poseerá características amigables para IoT, que permitirá un mayor ahorro de energía y evitar colisiones. **HEW** está implementado para operar con ancho de banda de 2,4 GHZ y 5 GHZ, y se centrará esencialmente en las velocidades de los dispositivos individuales, para así proporcionar que los clientes obtengan un mayor rendimiento alcanzando velocidades en Gigabits. [59]

3.1.2 LoRa

Es una tecnología de comunicación inalámbrica de largo alcance, ideal para dispositivos de bajo consumo, y ofrece seguridad en la transmisión de datos, por consiguiente, es una opción predominante para aplicaciones IoT.[60]

Las redes que utilicen esta tecnología tienen la ventaja de proporcionar una cobertura de mayor alcance con un rango de 15 km o más, otra característica es la vida útil de la batería que puede ser hasta de 20 años, y usa un cifrado integrado de extremo a extremo. Los chips de LoRa se transmiten con un espectro de radiofrecuencias sin licencia, usando la banda ISM (Industrial, Scientific and Medical), que son bandas para uso no comercial para áreas industriales, científicas y médicas.[60], [61]

Con la finalidad de impulsar LoRa al mercado, se diseñó **LoRaWAN** este protocolo fue desarrollado por LoRa Alliance, esta especificación permite la comunicación a un gran alcance de cobertura y de baja potencia entre los sensores remotos y puertas de enlace que están conectadas a la red, y además es el encargado de coordinar las frecuencias de comunicación,

potencia de los dispositivos y velocidad de los datos. LoRaWAN está diseñado para cumplir los requisitos IoT, conforme a la movilidad, interoperabilidad, comunicación bidireccional segura y servicios de localización sin el uso de GPS. Esta especificación usa una topología estrella, y las velocidades de datos van desde los 0,3 Kbps hasta 50 kbps, está basado en el estándar LPWAN (Low Power Wide Area Network).[62]

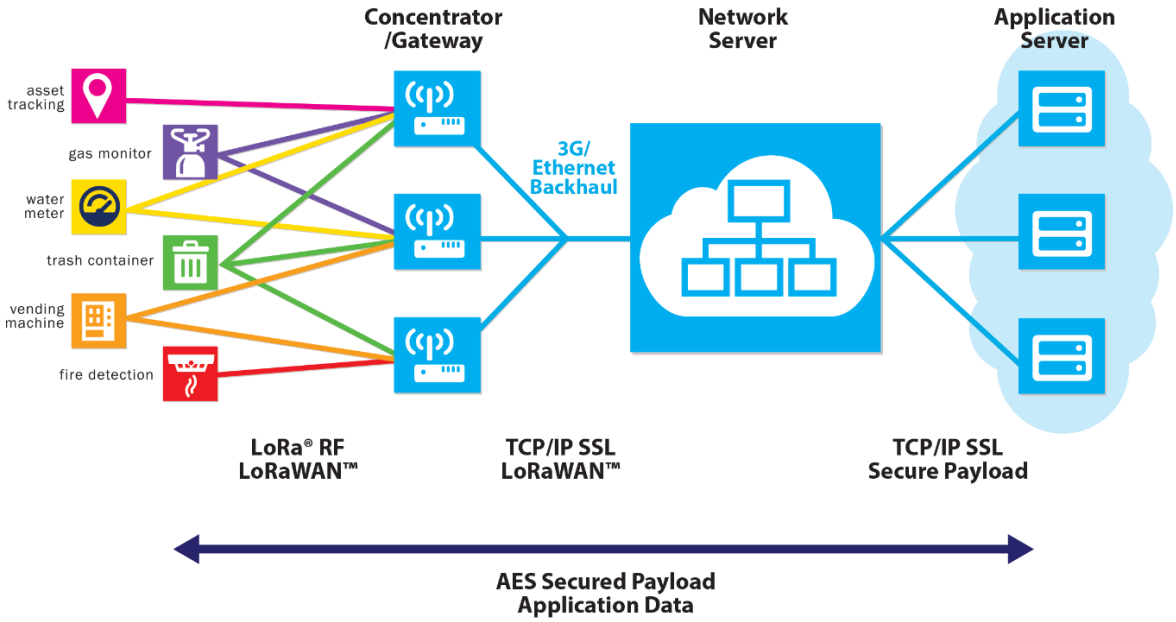


Ilustración 15 Diagrama de la Red LoRaWAN. Tomado de LoRa Alliance, "What is the LoRaWAN TM Specification." [60]

LoRa ofrece múltiples aplicaciones e implementaciones para IoT, por ejemplo, ofrece a los viñedos controlar y gestionar la humedad del suelo, en la domótica monitorea la contaminación y calidad del aire, en las granjas permite rastrear y detectar anomalías en el comportamiento del ganado, LoRa juega un papel importante en la agricultura de precisión, también apoya a la salud con el monitoreo de detección de caídas en adultos mayores, entre otras.[60]

Ilustración 16 Sistema de arquitectura LoRa con InteliLIGHT. Las soluciones de alumbrado público basadas en LoRaWAN se hacen realidad con los nuevos controladores inteliLIGHT. Tomado de inteliLIGHT®. [63]

3.1.3 Sigfox

Es una alternativa en la comunicación inalámbrica ideal para conexiones en aplicaciones masivas IoT, ya que ofrece un largo ciclo de vida de la batería del dispositivo, bajo costo del dispositivo, bajo costo de conectividad, alta capacidad de red y largo alcance. La industria Sigfox provee dispositivos, servicios y certificaciones de módems para asegurar la compatibilidad y conectividad con un alto nivel de calidad de servicio entre los mismos, la red se basa en la topología estrella e implementa una conectividad LPWA (baja potencia y largo alcance, del inglés Low Power Wide Area) en zonas rurales con una cobertura de 30 a 50 km, mientras que en zonas urbanas debido a los obstáculos este rango se reduce de 10 a 25 km, opera en bandas libres, además es compatible con Bluetooth, GPS 2G / 3G / 4G y Wifi.[64]

Los objetos IoT envían una señal de tipo mensaje de enlace, que va hasta los 12 bytes y en promedio tarda 2 segundos en el aire, hasta llegar a las estaciones base que monitorean el espectro en busca de señales en su rango

de alcance, esta base (transmisora/receptora) se encarga de enviar el mensaje a la nube.[64]

Actualmente está presente en 45 países, la red atiende a 803 millones de personas y cubre 3,8 millones de km^2 y se caracteriza por operar en las bandas de radio ISM (bandas de radio industriales, científicas y médicas).[64]

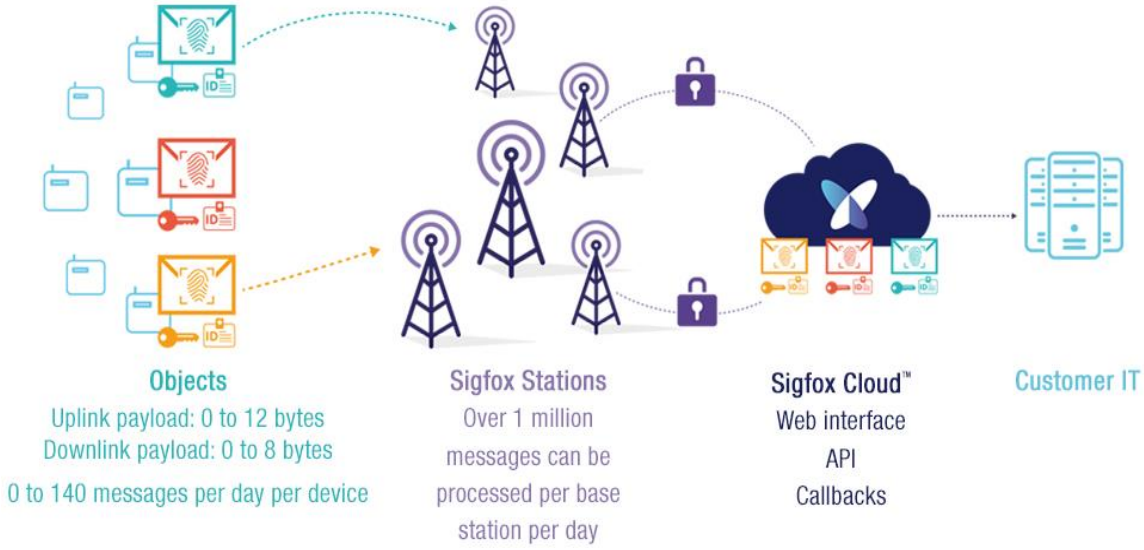


Ilustración 17 Arquitectura de la red Sigfox.
Tomado de "Sigfox Technology Overview". [64]

3.1.4 Bluetooth

Es una tecnología inalámbrica, que permite la comunicación entre dispositivos a través de ondas de radio de corto alcance, y utiliza una banda de radiofrecuencia de 2,4 a 2,8 GHz. Las ondas de radio Bluetooth usualmente solo pueden viajar con un rango óptimo de 100m o menos usando un canal de comunicación máximo de 720 kbit/s, aunque el rango depende de la clase de potencia que tenga integrado el dispositivo.[65]

Bluetooth posee varias clases de potencia, por ejemplo, la clase 1 opera un rango óptimo de 100 metros, a diferencia de la clase 2 que su alcance máximo es de 10m, y la clase 3 cuenta con una potencia máxima de transmisión de 1m.

Esta tecnología fue creada en 1994 por Ericsson, y posterior a ello en 1998 se unieron varias empresas como IBM, Intel, Toshiba y Nokia, para conformar la asociación privada sin ánimo de lucro **Bluetooth Special Interest Group (SIG), Inc.**[66]

Bluetooth es un protocolo que opera sobre una frecuencia sin licencia, se creó para redes PAN (Personal Area Networks – Redes de área personal), y usa topologías de red punto a punto o punto-multipunto; está tecnología es de pequeña escala, bajo costo y cuyo objetivo principal es facilitar el intercambio de datos entre dispositivos. Actualmente la tecnología Bluetooth se puede encontrar en smartphones, tablet, auriculares, smart tv, impresoras, entre otros. [67]

Bluetooth se conecta y se comunica de forma inalámbrica por medio de redes ad-hoc de rango de corto alcance, distinguidas como Piconet (picoredes) estas se establecen en forma automática y dinámica cuando los dispositivos entran o salen del radio de proximidad. Una piconet está conformada por un nodo maestro y hasta 7 nodos esclavos activos, y además tiene la capacidad de extender la red por medio de Scatternet (es un grupo de piconets interconectadas que comparten, aunque sea un dispositivo bluetooth en común). [68]

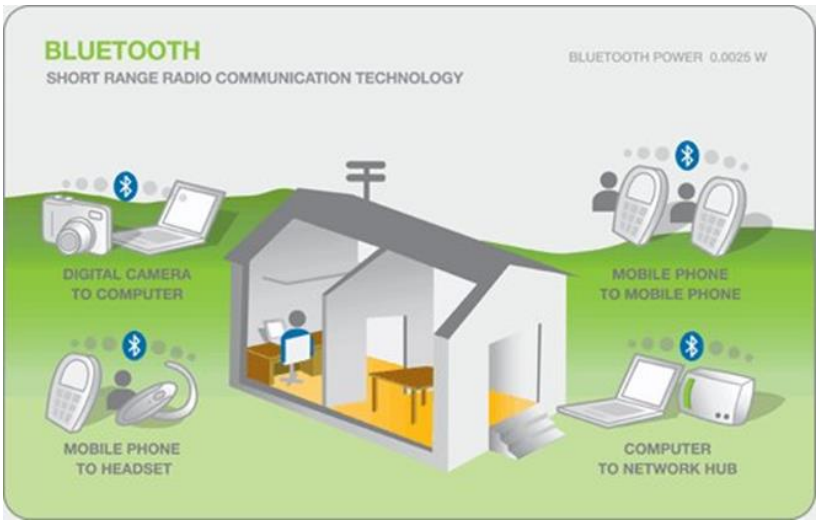


Ilustración 18 Aplicación de Bluetooth en el hogar Tomado de B. Borowicz, The Internet of Things and Bluetooth [69]

Bluetooth ha jugado un papel muy importante en las tecnologías de comunicación, y se espera que sea un componente clave para aplicaciones IoT. Con la aparición del nuevo estándar llamado **Bluetooth Low Energy**, se espera optimizar y perfeccionar la operabilidad de los dispositivos, permitiendo que la comunicación sea más rápida y a su vez ampliar el rango de la señal hasta cuatro veces mayor que una red Wifi [70]. Convirtiéndolo en un método de comunicación más confiable y segura para conectar numerosos dispositivos en el hogar.[71]

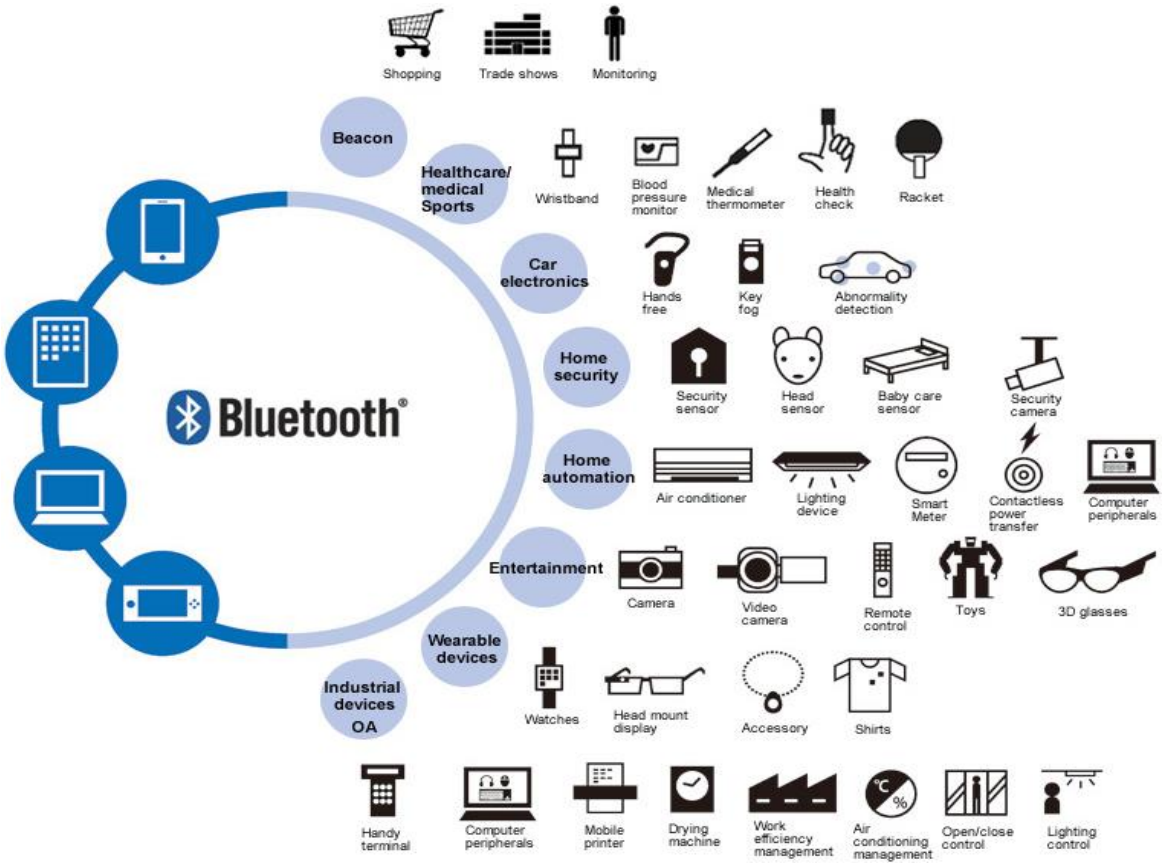


Ilustración 19 Aplicación de Bluetooth® low energy.
Tomado de Bluetooth® low energy modules with an embedded antenna smaller than current small-type modules are developed. [70]

3.1.5 RFID (Radio Frequency Identification)

La tecnología RFID tiene como objetivo principal transmitir la identidad de un producto u objeto a distancia, al tener incorporado un chip o etiqueta en su sistema, con la ayuda de ondas de radio, sin necesidad de intervención

humana, ni línea de visión directa, por esta característica pertenece a la gama de tecnologías de identificación automática y captura de datos (AIDC), que usa un método para la recopilación de los datos y los ingresa directamente a los sistemas de información, debido a estas particularidades es considerada una tecnología de identificación remota e inalámbrica.[72]

Esta tecnología utiliza diferentes frecuencias de trabajo atendiendo el tipo de necesidad, distinguiéndose en las siguientes: LF (Low Frequency) usa una banda de 125 kHz y un rango hasta de 50 cm, HF (High Frequency) opera con un rango de 80 cm y una banda de frecuencia de 13,56 MHz y es la más utilizada en la industria, UHF(Ultra High Frequency) trabaja con un rango de 3 a 10 m y una banda de frecuencia de 400 MHz a 1000 MHz, y por último las microondas poseen un mayor rango de alcance de 10 o más metros con una banda de frecuencia de 1,45 GHz a 5,4 GHz.[73]

Sin embargo RFDI no es una tecnología nueva, su primera aparición fue en 1940, durante la primera guerra mundial, era utilizada para la identificación por radiofrecuencia de aviones con el objetivo de reconocer si eran aliados o enemigos y a través de los años esta idea se empleó para un seguimiento más reducido.[74]

RFID usa un código electrónico de producto (EPC), que es un número único que permite la identificación y seguimiento de cualquier objeto en tiempo real [73], el funcionamiento de esta tecnología se basa en una señal de radio generada por una etiqueta que está adherida o incorporada a un objeto, en la cual anticipadamente se han guardado los datos, posteriormente un lector es el encargado de recibir la información de dicho producto, para así transmitirla a un middleware, que es un software que sirve como intermediario entre el lector y las aplicaciones empresariales. [75]

RFID juega un papel muy importante en IoT, porque está tecnología habilita la comunicación entre dispositivos con la finalidad de transmitir, intercambiar y

monitorizar los datos. Actualmente RFID se encuentra aplicado en un entorno muy amplio, por ejemplo, ofrece la identificación electrónica de mascotas, pago automático de peajes, seguimiento e identificación de pacientes en centros de salud usando brazaletes RFID, control de acceso a un recinto (habitaciones de hotel, zonas residenciales, plantas industriales) que requieran seguridad, monitorización de ganado en las explotaciones ganaderas, gestión del tráfico de entrada y salida de préstamos de libros en una biblioteca, etc.[76].

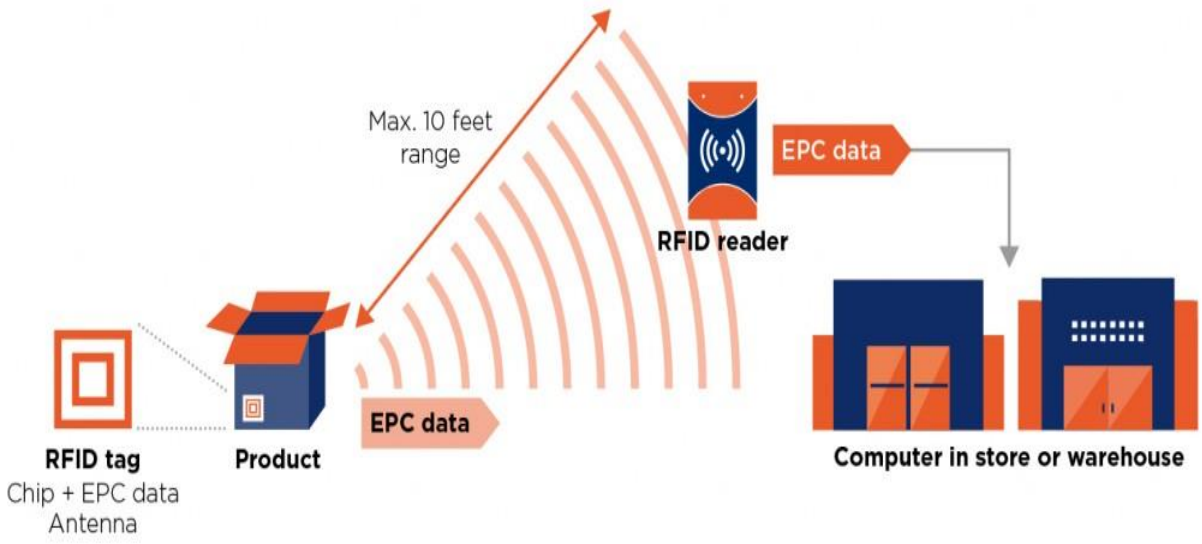


Ilustración 20 Aplicación de RFID en la una Empresa de correos. Tomado de GS1 Spain, "EPC / RFID". [77]

3.1.6 NFC (Near Field Communication)

Hace parte de las tecnologías de comunicación inalámbricas de corto alcance, es decir, distancias hasta 10 cm, en consecuencia, posee un alto grado de seguridad, funciona usando el modelo pasarela entre dispositivos que emiten una señal de radiofrecuencia y son receptores/transmisores, es una extensión de la tecnología RFID, fue aprobada como el estándar ISO 18092 en el año 2003, y en el 2004 las empresas Sony, Nokia y Philips dan origen a *NFC-Forum*, una organización encargada de regular y determinar las características y estándares de *NFC, actualmente tiene como miembros a* Google, Visa, Dell,

Intel, Microsoft, Samsung, At&t, Paypal [78]. *A* partir del año 2013 la tecnología NFC se popularizó entre los fabricantes de dispositivos móviles razón por la cual la gran mayoría de dispositivos de alta gama posee dicha cualidad [79].

NFC utiliza la banda de los 13.56 MHz que se caracteriza por ser libre, es decir, no necesita licencia para su uso, solo puede transferir un flujo de datos pequeño ya que su tasa de transferencia solo llega los 424 kbit/s, en consecuencia, es ideal para el reconocimiento y validación de dispositivos por proximidad, como tarjetas NFC, smartphones, tablet y smartwatches. Es implementado por su alta velocidad de intercambio de datos en bancos y organizaciones que adoptaron esta tecnología en sus sistemas de pago, identificación de usuarios, acceso a servicios y transferencia de información. [79]

Actualmente las etiquetas NFC son fáciles de conseguir en el mercado tecnológico, además son fáciles de implementar, las etiquetas se activan al entrar al campo magnético del dispositivo receptor o emisor, en otras palabras, no dependen de una fuente de alimentación directa, al ser una pegatina es fácil de anexar a cualquier artículo como puede ser una pulsera o un llavero. NFC es fácil de usar con su funcionalidad "tap-and-go" y proporciona una serie de opciones de seguridad, razón por la cual puede impulsar el crecimiento de sistemas IoT a gran escala como hogares inteligentes, sistemas de transporte urbano e intercambio de contenido digital, con un simple toque les permite a los usuarios finales realizar transacciones rápidas y seguras. [80]

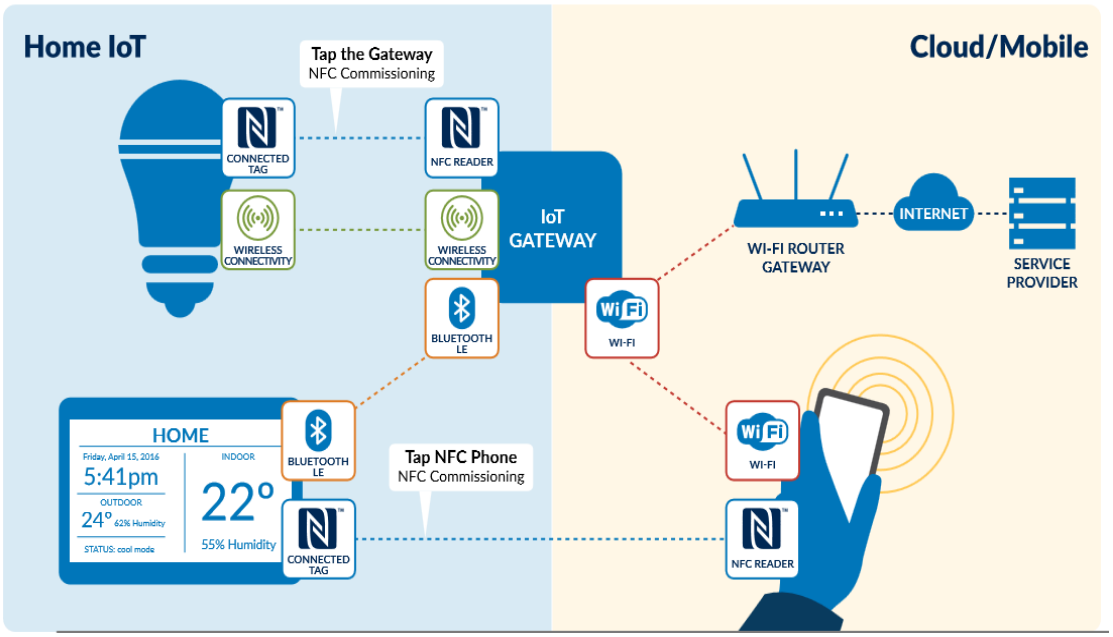


Ilustración 21 Aplicación de NFC en un sistema Smart Home.
Tomado de NFC forum, Why The Internet Of Things needs NFC[80]

3.1.7 Ethernet

Es el estándar para redes LAN (Local Area Network) más usado, que determina las singularidades físicas y eléctricas que debe tener una red cableada. Ethernet se ha caracterizado por ser el protocolo principal en el nivel de enlace para el modelo OSI, y también es el encargado de especificar los formatos de las tramas de datos. Ethernet sirvió como base para la especificación IEEE 802.3.[81]

Esta tecnología se caracteriza por adecuarse perfectamente para aquellas aplicaciones que deben transportar tráfico de datos de manera esporádica y eventualmente muy pesadas, a velocidades muy altas. El rango máximo de transmisión de ethernet puede alcanzar alrededor de los 5000 metros y contar una velocidad de 1000 Mbit/s, gracias al uso de la fibra óptica; estas características se definen dependiendo el tipo de tecnología que se esté utilizando.[81]

Ethernet utiliza el método CSMA/CD (Carrier sense multiple access with collision detection / accesos múltiples con detección de portadora y detección de colisiones) que es un algoritmo de acceso al medio compartido, en CSMA/CD es necesario que los dispositivos de una determinada red escuchen si el canal o los recursos de una red están disponibles para realizar una transmisión, para así evitar colisiones en el envío de datos.[81]

Los principales puntos débiles de la tecnología ethernet son la falta de movilidad y complejidad de la instalación, por ello el uso en IoT es limitado para aquellas aplicaciones que requieran un alto ancho de banda o la seguridad que provee el cableado físico.[82]

3.1.8 IEEE 802.15.4(Low Rate WPAN)

Es un estándar que define las reglas para la capa física y los controles de acceso al medio, entre dispositivos que se comunican por medio de redes inalámbricas pequeñas en concreto WPAN(Wireless Personal Área Network), está diseñado para proveer servicios con baja transmisión de datos y con bajos consumos de energía, funciona con direccionamiento IEEE de 16 bits y de 64 bits, opera en rangos de los 10 a 20 m que pueden ser de 20 Kb/s en la banda de 865 MHz, 40 Kb/s en la banda ISM en Estados Unidos y 250 Kb/s en la banda de 2.4 GHz que es específica para la industria científica y médica. Dependiendo estrictamente del servicio que se desea suministrar se pueden implementar las topologías de red sencillas tipo estrella y entre pares. [83]

3.1.9 4G (Cuarta Generación)

Es una tecnología de comunicación inalámbrica diseñada para la telefonía móvil, y es la sucesora de 2G y 3G. Una diferencia notable a las anteriores generaciones, es que 4G se basa en el protocolo IP para operar, y descartar la conmutación de circuitos e implementar solo la conmutación de paquetes. Una

de las ventajas de usar el protocolo IP en redes móviles es que permite pagar por lo que consume el usuario, y además ofrece una mejor velocidad de transmisión y acceso sin que la red se sature.[84]

4G ofrece una velocidad de transmisión entre 100 Mbit/s para usuarios que están en constante movimiento, y 1 Gbits/s para aquellos que tiene una ubicación fija, además mantiene una calidad de servicio (QoS) punto a punto de alta seguridad, permitiendo ofrecer cualquier tipo de servicio, al menor costo posible[85]. Dentro de las tecnologías consideradas 4G se encuentran LTE Advanced (Long Term Evolution) y WiMAX.[86]

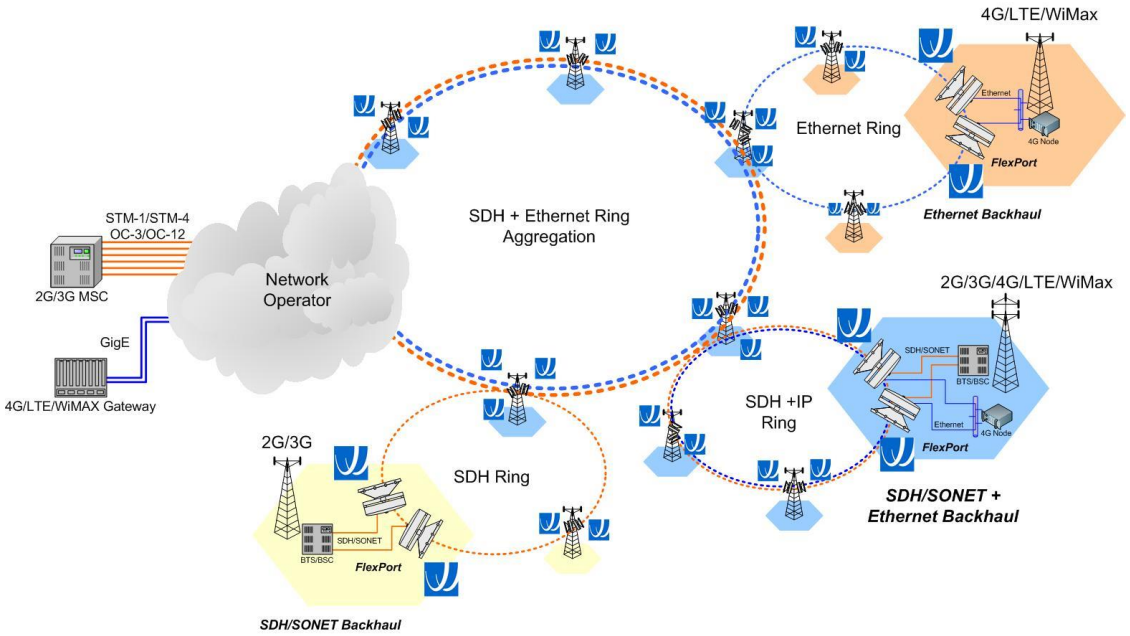


Ilustración 22 Diagrama de una red 4G.

Tomado de Rajowan S, Who needs 4G, ¿whatever that is?. [86]

3.1.10 5G (Quinta Generación)

La red inalámbrica de 5ta generación tiene como objetivo abordar no sólo la telefonía móvil, sino también se espera que sea de uso masivo en el Internet de las Cosas, y se especula que saldrá al mercado para el año 2020. Se caracteriza por utilizar una latencia de 1 milisegundo, además de tener una velocidad de descarga de datos hasta de 20 Gbps y 10 Gbps de subida, ofrece una cobertura del 100%, reduce el 90% en el consumo de energía, lo que

significa que la batería de un dispositivo IoT de baja potencia puede tener una vida útil de hasta 10 años. [87] [88]

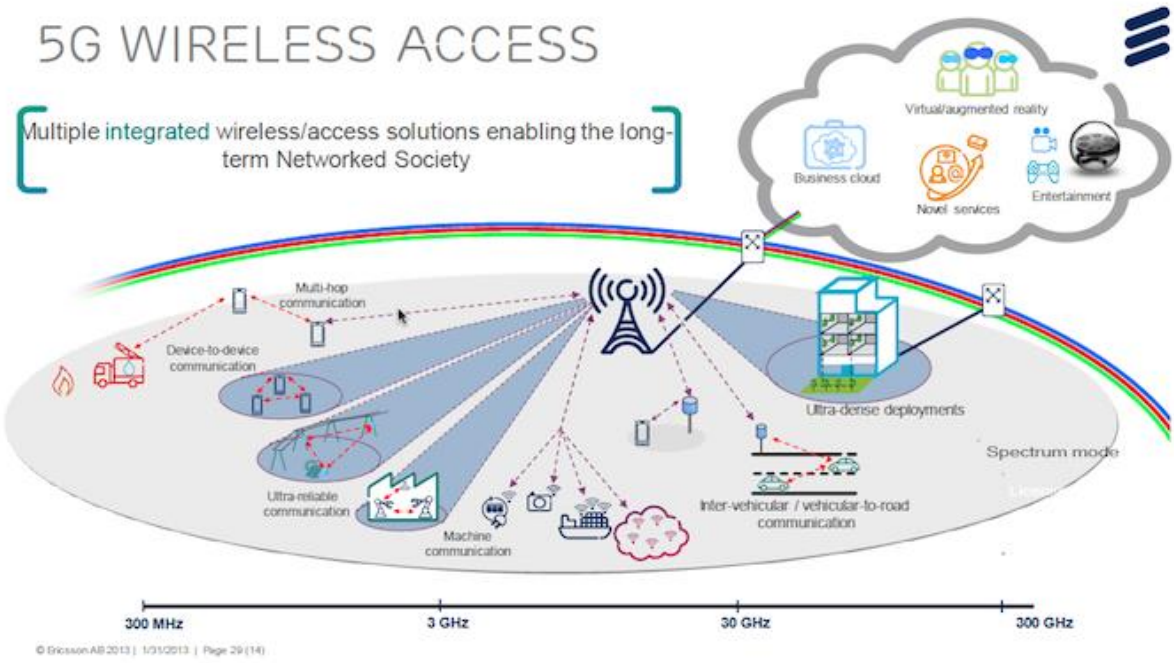


Ilustración 23 Diagrama de red 5G. Tomado de Mobile Europe, "Ericsson CTO: 5G is about integrated wireless technologies, not just speeds". [89]

3.2 CAPA DE INTERNET

3.2.1 IP (Internet Protocol)

Es un protocolo no orientado a conexión, el diseño de IP se creó presuponiendo que el envío de paquetes de datos no sería confiable, únicamente proporciona seguridad a la cabecera y no a los datos contenidos. [90]

Este protocolo provee recursos indispensables para el intercambio de paquetes desde el origen al destino, donde estos son identificados por direcciones de longitud fija, no ofrece ningún proceso de garantía de extremo a extremo (end-to-end), debido a ello no cuenta con ningún control de flujo, ni respaldo de secuenciación. [53]

Las principales características de IP son:

- Fragmenta los paquetes si es necesario.
- El direccionamiento es por medio de direcciones lógicas IP de 32 bits (IPv4) o 128 bits (IPv6).
- Si un Datagrama no es entregado, este estará en la red por un tiempo finito.
- El tamaño límite de un paquete es de 65635 bytes.

Direcciones IP

Todo dispositivo conectado a internet, posee una dirección IP, que es un número único e irrepetible que se le asigna a cada interfaz de red de un dispositivo, el uso de estas direcciones permite a los equipos ser identificados de manera jerárquica y lógica.[53]

Actualmente existen dos versiones o formatos de direcciones IPv4 y IPv6.

IPv4 (Internet Protocol Version 4): fue la primera versión implementada por ARPANET, en 1983. Estas direcciones son representadas por medio de un número binario de 32 bits, estos bits son separados en 4 grupos de 8 bits que son representados en forma decimal. IPv4 permite un espacio hasta de $4.294.967.29\ (2^{32})$ direcciones públicas posibles y es la versión más usada en la actualidad. [91]

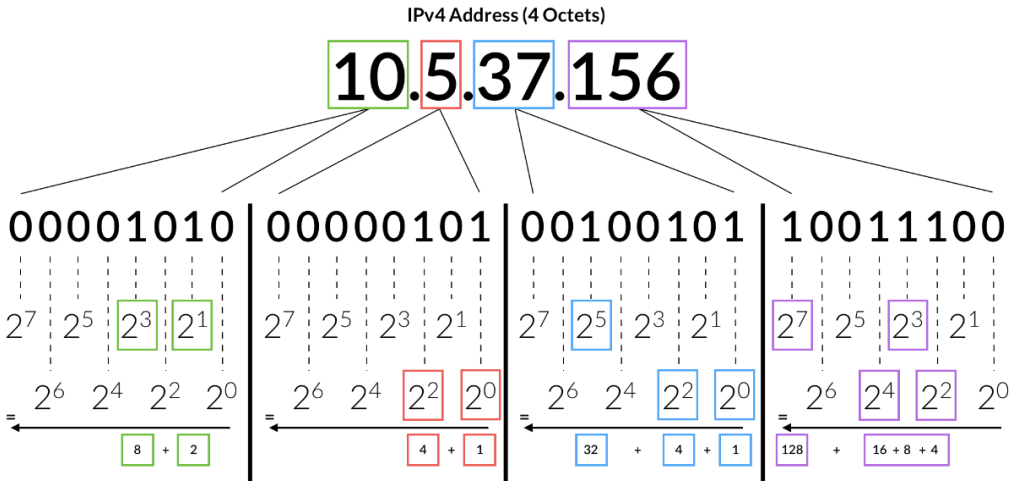


Ilustración 24 Detalle de una dirección IPv4, expresada en notación decimal. Tomado de PRITAM, "Diferencias clave entre IPv4 e IPv6". [92]

IPv6 (Internet Protocol Version 6): es una etiqueta numérica hexadecimal dedicada a identificar de manera lógica y jerárquica un dispositivo que use el protocolo IP (Internet Protocol). Actualmente es el sucesor de IPv4 la arquitectura de este este protocolo es de 128 bits, y está compuesta por 8 segmentos de 2 bytes cada uno que corresponde a unos 3.4x1038 hosts direccionables, esta nueva versión está diseñada para sustituir al estándar IPv4, debido que está cuenta con un límite de direcciones impidiendo el crecimiento de la red. [91]

Las características más destacables de IPv6 se reducen en: ofrecer mayor espacio de direccionamiento, autoconfiguración, movilidad y seguridad, que permite encriptación y autentificación del protocolo, cabe destacar otras como el mejoramiento en la calidad y clase de servicio. [91]

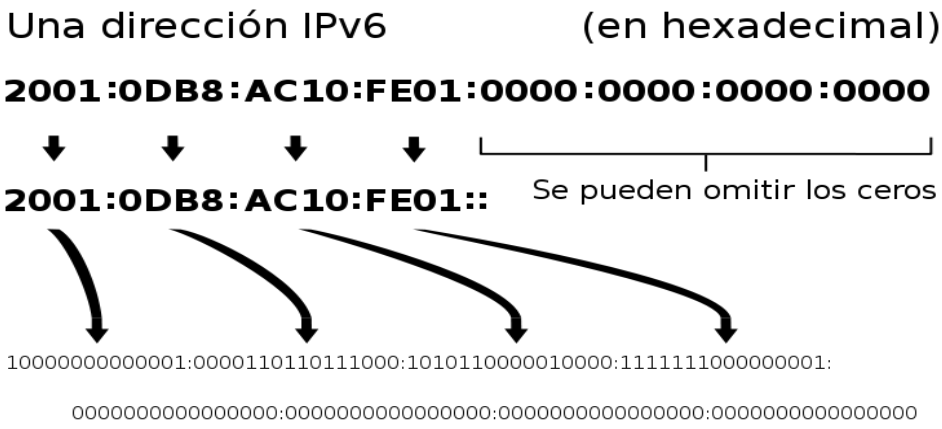


Ilustración 25 IPV6 expresada en hexadecimal y binario. Tomado de PRITAM, "Diferencias clave entre IPv4 e IPv6". [92]

3.2.2 6LOWPAN (IPv6 over Low power Wireless Personal Area Networks)

Es una tecnología o capa de adaptación estándar abierta definida en RFC 6282 por el IETF (Internet Engineering Task Force), fue desarrollado en el 2007 para adecuar el formato de la cabecera de IPv6 sobre redes de sensores

inalámbricos de bajo consumo, que están basadas en el estándar IEEE 802.15.4, opera comprimiendo la cabecera IPv6 y UDP para reducir la sobrecarga durante la transmisión de datos, así mismo utiliza la fragmentación para cumplir con el MTU de IPv6 que se traduce como la unidad máxima de transferencia, es decir, el tamaño límite de bytes por unidad datos que se pueden enviar por medio de un protocolo de comunicación. [93]

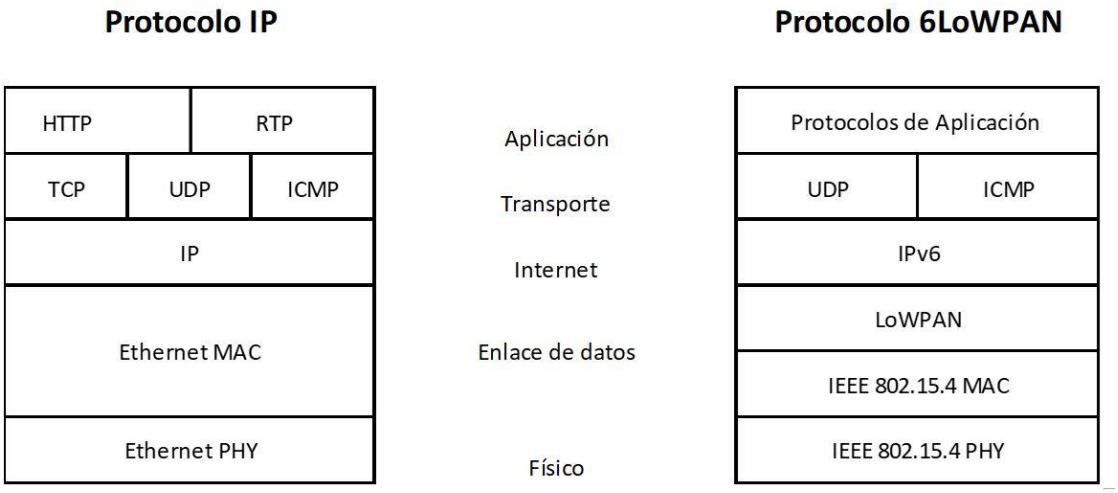


Ilustración 26 Pilas TCP/IP y 6LoWPAN[93]

Utiliza un *Edge Router* (router frontera) como puente para la comunicación entre redes 6Lowpan y otras redes, funciona de manera independiente de los protocolos de aplicación usados en la red 6LoWPAN, de esta forma no se satura con procesamientos y solo se encarga de cumplir 3 acciones [93]:

1) El intercambio de datos entre dispositivos 6LoWPAN e Internet (u otra red IPv6).
2) Intercambio de datos locales entre dispositivos dentro del 6LoWPAN.
3) La generación y el mantenimiento de la subred de radio (la red 6LoWPAN).

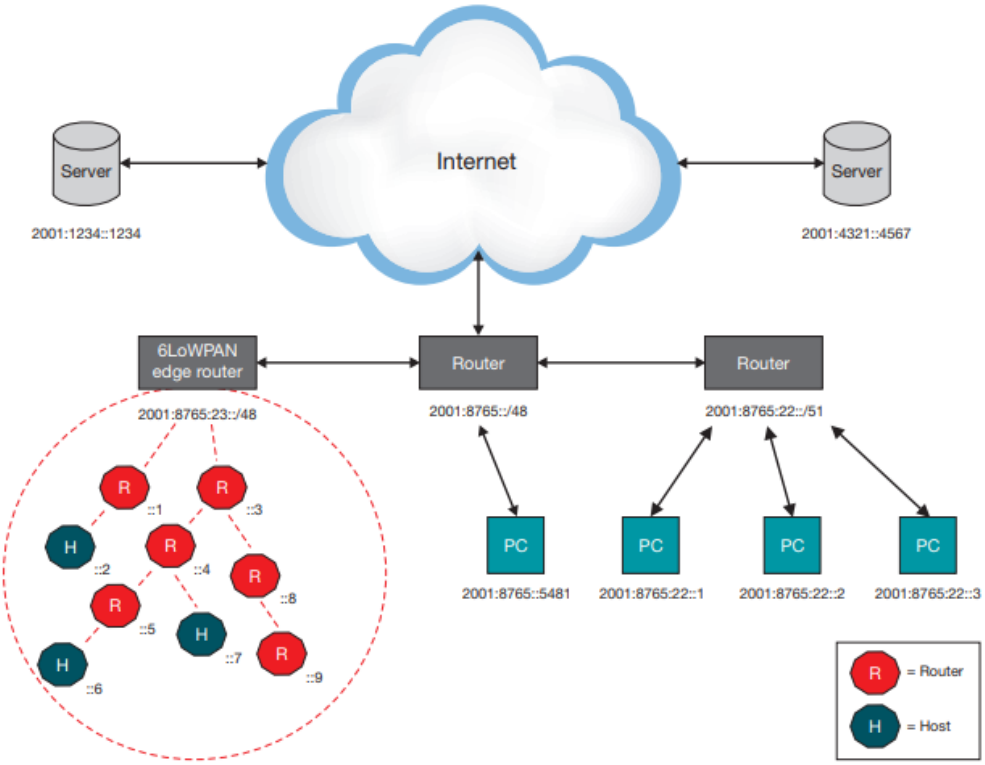


Ilustración 27 Ejemplo de una red IPv6 con una red de malla 6LoWPAN. Tomado de J. Olsson, "6LoWPAN demystified, [93]

3.2.3 Capa de Transporte

La pila de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol):

La pila de protocolos TCP/IP tiene como función el transporte de datos y la rutas que los mismos deben tomar, cabe aclarar que no se trata de un solo protocolo, al contrario, es un conjunto de protocolos que corresponden a las diferentes capas del modelo OSI. La arquitectura de TCP/IP consta de 4 capas en las que se agrupan los protocolos. [94]

CAPA	PROTOCOLOS
Aplicación	HTTP, NFSM DNS, Telnet, FTP, SNMP
Transporte	TCP, UDP
Internet	IPv4, IPv6, ARP, ICMP
Enlace	Ethernet, Token Ring, FDDI

Tabla 5 Modelo de comunicación TCP/IP y sus protocolos en cada capa[94]

3.2.3.1 Protocolos presentes en la capa de Transporte:

TCP (Transmission Control Protocol)

Es uno de los protocolos fundamentales en la red, debido a que brinda apoyo a muchos protocolos que operan en la capa de aplicación, es orientado a conexión ya que el cliente y el servidor deben notificarse y aceptar la conexión entre sí, para comenzar a transmitir la información al cliente que debe recibirlos.[95]

Este protocolo cuenta con ciertas características: permite que la transferencia de datos se transmita en orden, realiza un control de flujo y monitoreo de los mismos para evitar una congestión en la red, no sólo autoriza la multiplexación de los datos, sino que también se puedan enviar segmentos de longitud variada para ser entregados al protocolo IP. [95]

UDP (User Datagram Protocol):

Es un protocolo no orientado a conexión, es decir permite la entrega de datagramas a través de la red sin necesidad de establecer una conexión entre cliente/servidor, debido a que el datagrama proporciona la suficiente información del direccionamiento en su cabecera. Este protocolo es muy simple debido a que no realiza detección de errores, control de flujo y otras características que ofrecen los servicios orientados a conexión. [95]

3.3 PROTOCOLOS IOT IMPLEMENTADOS EN LA CAPA DE APLICACIÓN

3.3.1 HTTP (Hypertext Transfer Protocol)

Es un protocolo de comunicaciones de servicio de internet que maneja el paradigma cliente-servidor y opera en la capa de aplicación de la pila TCP/IP, se encarga del intercambio de información entre los clientes Web (navegadores) y los servidores HTTP, mediante operaciones de solicitud y respuesta.[96]

3.3.2 CoAP (Constrained Application Protocol)

Fue creado para sustituir el protocolo HTTP ya que este era muy pesado para las aplicaciones IoT, posee sentido de interpretación del lenguaje, utiliza la arquitectura RESTful de HTTP, es decir, que por medio de una Interfaz posee un conjunto fijo de operaciones como son GET, POST, PUT y DELETE para relacionarse con los recursos.[97]

Este protocolo es de tipo mensajería ligera para comunicaciones remotas con dispositivos de recursos limitados, funciona intercambiando datos a través de un sistema de paquetes minimizado, además brinda un bajo consumo de energía, puesto que es ideal para dispositivos móviles simples como sensores que se puedan comunicar por nodos inalámbricos o una red de baja potencia con pérdidas, de forma que pueda compartir información interactiva vía internet. [98]

Entre las características del protocolo CoAP cabe mencionar que implementa UDP, y ciertas singularidades de TCP que se van presentando en la transmisión de mensajería, diferenciando si se debe o no comprobar la conexión entre los dispositivos. [99]

A continuación, se nombran otras características del protocolo CoAP:

- Mediante el registro de la cantidad de suscripciones a los contenidos publicados, se llevan a cabo suscripciones por demanda.
- Las peticiones y respuestas se reciben de manera asincrónica, es decir, que los mensajes están separados por cierto periodo de tiempo.
- El diseño del protocolo CoAp permite una traducción fácil a HTTP.
- No se sobrecargan las cabeceras, de esa manera se reduce la complejidad al procesar el mensaje.

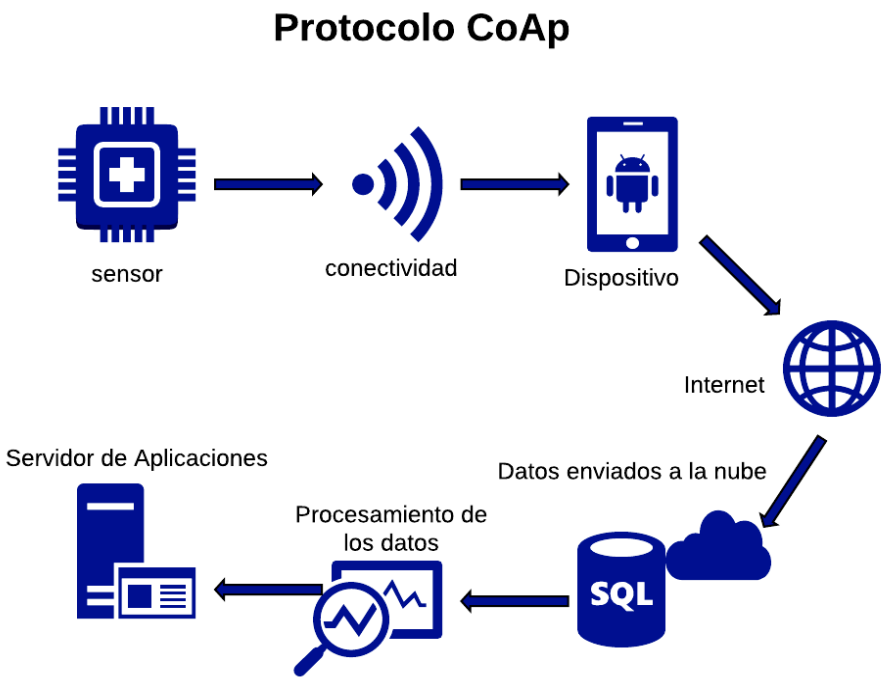


Ilustración 28 Funcionamiento del protocolo CoAp [52]

3.3.3 Protocolo XMPP (Extensible Messaging and Presence Protocol)

Es un protocolo de mensajería instantánea, que incluye una alta gama de aplicaciones para chat, multichat, llamadas de voz, videollamadas y transferencia de archivos entre clientes, está basado en el estándar internacional XML que opera como un meta-lenguaje que delimita lenguajes de

marcado, en consecuencia XMPP se puede adaptar a alguna funcionalidad en especial, además que posee control de acceso, cifrado de datos, autenticación y privacidad.[100]

XMPP anteriormente conocido como el protocolo Jabber, se caracteriza por no necesitar de un servidor central, fue desarrollado por la comunidad de código abierto, al ser libre se encuentra documentado y puede ser usado en diferentes proyectos sin necesidad de aprobación.[100]

El protocolo XMPP permite a los clientes comunicarse entre sí a través de mensajes instantáneos mediante internet, sin importar el sistema operativo que maneje cada uno, esta particularidad lo postula como un protocolo idóneo para aplicar en sistemas IoT, ya que implementa un modelo para la conexión entre redes que manejan otros protocolos de mensajería instantánea; actualmente está presente en aplicaciones como Whatsapp y Facebook Messenger.[100]

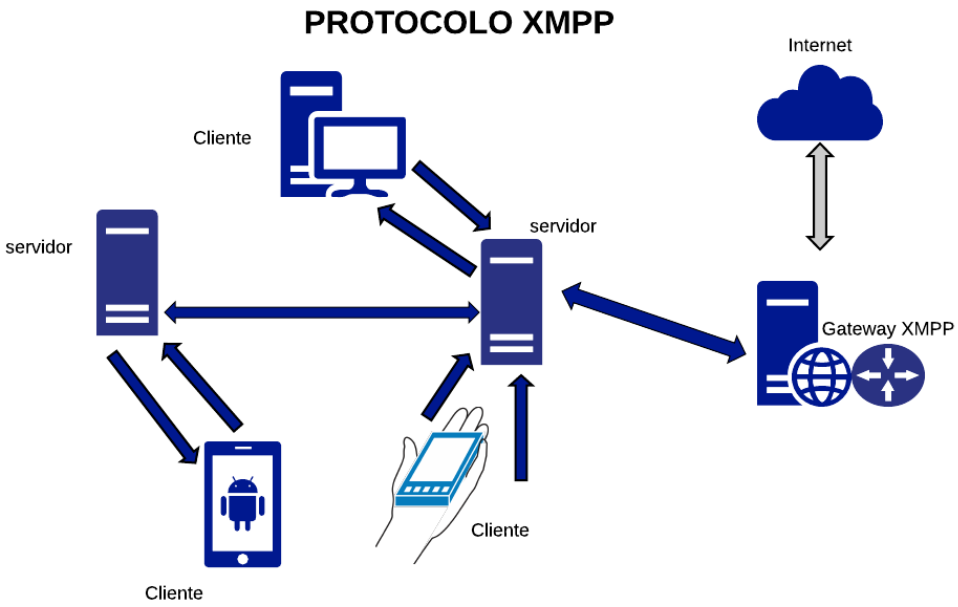


Ilustración 29 Arquitectura XMPP [52]

XMPP orientado a IoT

Los proyectos uXMPP y XMPP Client fueron los primeros en ser orientados a IoT, proporcionaban implementaciones rudimentarias pero ligeras, estos proyectos demostraron que XMPP se podía ejecutar en dispositivos con recursos limitados, asegurando interoperabilidad.[101]

Con XMPP como protocolo subyacente en proyectos de comunicación para IoT, se tiene como objetivo principal simplificar la interconexión máquina a máquina (M2M) y apoyar la comunicación humano a máquina (H2M).[101]

XMPP es un protocolo que se encuentra estandarizado para flujos de datos en tiempo real, por lo tanto, se puede implementar sin tener que apoyarse de un middleware o gateways complejos para la traducción del protocolo en el caso de aplicaciones livianas, esto le brinda una ventaja para ser considerado como un protocolo de comunicación ideal para servicios IoT, además, la XMPP Standards Foundation ofrece un mantenimiento continuo para la familia de protocolos XMPP, lo que permite a los desarrolladores y proveedores de servicios IoT beneficiarse de los aspectos de sostenibilidad y capacidad de expansión a través de extensiones de protocolo (XEP).[101][102]

Por otro lado, para acceder a los nodos sensores de la red, se deben aplicar múltiples técnicas, motivo por el cual resulta ser tedioso ya que se pueden presentar problemas y las traducciones no resultan ser 100 % acertadas.[102]

Fortalezas	Debilidades
Sencillo de implementar.	Alto uso de CPU
Conexiones federadas entre usuarios de diferentes servidores.	Alto consumo de ancho de banda
Ampliamente respaldado por un gran número de compañías y proyectos de código abierto.	Poca resistencia a fallas

Extensible y flexible para aplicaciones múltiples.	Sin apoyo explícito para la calidad del servicio
Define una extensión de protocolo para descubrir información	Tipo de datos simple

Tabla 6 Debilidades y fortalezas del protocolo XMPP para servicios IoT. [103]

3.3.4 Protocolo MQTT (Message Queue Telemetry Transport)

Es un protocolo de tipo mensajería basado en agentes para la comunicación máquina a máquina (M2M), es especial para proveer servicios IoT, fácil de implementar, abierto y ligero, maneja un comportamiento de publicación-suscripción está basado en TCP/IP, por lo tanto, imita el concepto de cliente-servidor, la comunicación puede darse de uno a uno, de uno a muchos y de muchos a muchos, funciona con unos topics (temas) que el cliente (publicador) envía como mensaje al bróker (servidor) y los nodos (otros clientes) que se interesen en el tema deben suscribirse a él, para que este les reenvié el mensaje.[104]

Los anteriores conceptos esclarecen que el protocolo MQTT se compone de tres elementos para su funcionamiento, el publicador, un bróker y suscriptores, donde el bróker opera como intermediario, el suscriptor se registra a un topic y espera que el bróker le informe, así mismo el publicador transmite el tema a los suscriptores por medio del bróker y este se encarga de verificar los permisos correspondientes entre ellos.[104]

MQTT se caracteriza por ser ideal en servicios con recursos limitados, es decir, aquellos que requieren pocos recursos de memoria y procesamiento, además, economiza energía y posee tiempos de respuestas más ágiles, en consecuencia, es ideal para redes inalámbricas, incluso se ajusta a consumos de anchos de banda bajos, algo ideal para aplicaciones IoT en las que se envían cantidades pequeñas de información, implementa mensajes tipo “broadcast” para suscripción y publicación de datos. El protocolo MQTT cumple

estándares de calidad de servicio (QoS) ya que garantiza la optimización del flujo de datos, reduciendo así el tráfico en la red. [104]

MQTT posee tres niveles de calidad del servicio para la entrega de mensajes [105]:

- Nivel 0 (Como máximo una vez): El mensaje del remitente solo será enviado una vez y no hay garantía de ser recibido por el receptor, es decir, el bróker no informa al remitente si el mensaje fue entregado o no. Este nivel, puede ser usado en aplicaciones donde la pérdida de mensajes no sea crítica, ya que los mismos datos no varían mucho y además serán enviados nuevamente en cortos periodos de tiempo como el caso de los sensores. [105]
- Nivel 1 (Al menos una entrega/entrega confirmada): Se confirma la llegada del mensaje, pero se puede presentar duplicidad del mensaje, es decir el cliente enviará varias veces el mensaje hasta que el bróker le confirme que lo ha enviado a la red. [105]
- Nivel 2 (Exactamente una vez/entrega garantizada): la entrega del mensaje al remitente está asegurada exactamente una vez, este nivel es usado en aplicaciones donde la duplicidad y la pérdida de mensajes es crítica de manera que este nivel es más lento, ya que presenta más congestión en el tránsito de datos, porque maneja un doble flujo de comandos para confirmar que el mensaje solo llegue una vez al receptor, ejemplo de ello serían los sistemas de pago. [105]

Existen una especificación del protocolo MQTT, denominada MQTT-SN v1.2.

MQTT-SN V1.2 (para redes de sensores):

Está diseñado específicamente para redes de sensores restringidas, que no dependen de la arquitectura del protocolo TCP/IP para ejecutarse, MQTT-SN puede operar sobre cualquier capa de transporte, por ejemplo, en Zigbee.[106]

Esta especificación puntualiza un mapeo UDP de MQTT e integra un soporte bróker, generalmente esta arquitectura requiere una conexión con el intermediario antes de lograr el envío y recepción de los mensajes, por otro lado, permite construir un sistema de red entre dispositivos restringidos con un intermediario central que se encuentra conectado a muchos clientes, la entrega de mensajes está controlada mediante un bus de mensajes. [106]

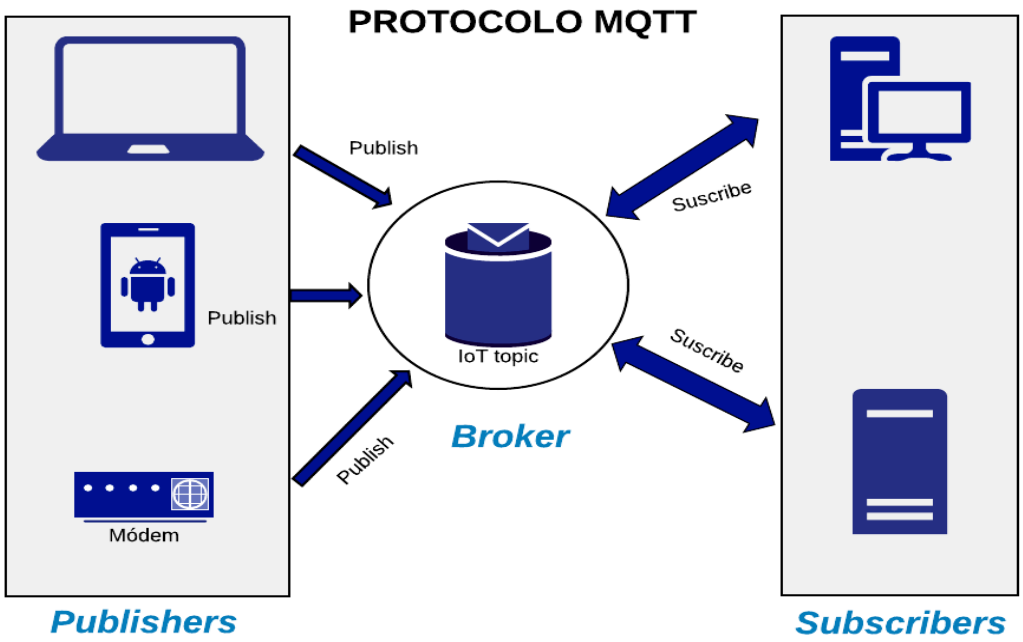


Ilustración 30 Arquitectura del protocolo MQTT[52]

3.3.5 Protocolo AMQP (Advanced Message Queuing Protocol)

Es un protocolo de mensajería estándar que proporciona tecnología middleware, lo que se traduce como lógica de intercambio de información entre aplicaciones, funciona en tiempo real y sigue el modelo de publicación-suscripción para la comunicación entre clientes, fue desarrollado en colaboración de Cisco Systems, IONA Technologies, Novell y Redhat.[107]

AMQP define las reglas de comunicaciones de red y los servicios que se pueden suministrar, para ello se utilizan Exchange (intercambiadores) que obedecen reglas y condiciones especiales, que son suministradas por la

entidad Binding para enrutar adecuadamente los mensajes, estos son alojados en queues (colas) vinculadas, luego son enviados a sus respectivos consumidores (suscriptores), estos pueden visualizar el mensaje o eliminarlo dependiendo de los permisos que posean. [108]

AMQP se caracteriza por implementar reglas de enrutamiento dinámico, es decir, un productor (cliente) puede establecer la ruta que tomará el mensaje, además la entrega del mismo está garantizada. Este protocolo es ideal para aplicaciones que manejan transacciones comerciales y que utilicen servicios basados en la nube o que sean orientados a IoT.[108]

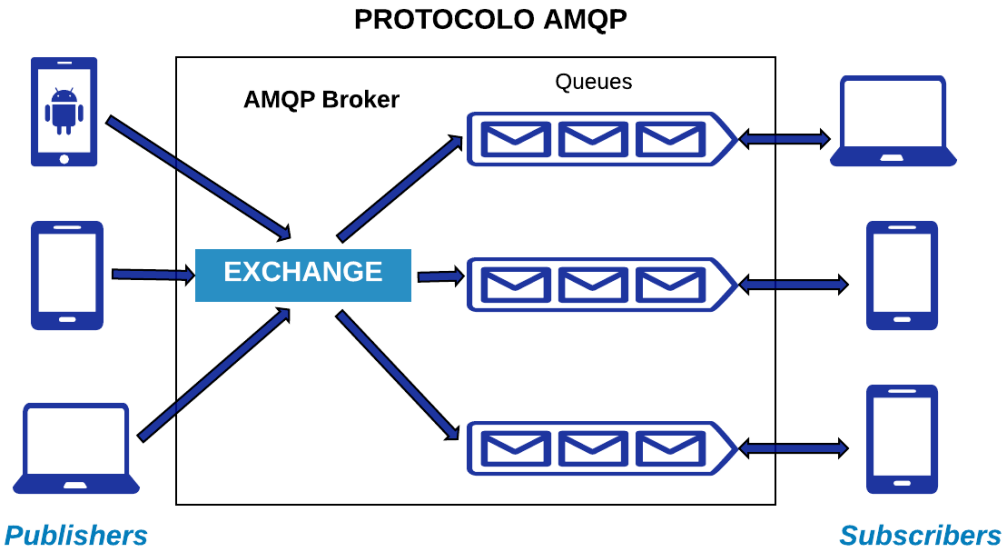


Ilustración 31 Arquitectura del protocolo AMQP. [52]

3.3.6 Protocolo VSCP (Very Simple Control Protocol)

Es un protocolo gratuito, abierto para uso comercial y/o otros servicios, está diseñado para la comunicación M2M, y para otras aplicaciones de control remoto y medición como sensores, proporciona la conexión a dispositivos simples y de bajo costo ligado con máquinas de gama alta. La principal ventaja de este protocolo es que cada dispositivo funcione de manera independiente, para formar parte de un sistema de red distribuida con otros dispositivos, cabe

señalar que VSCP facilita a los nodos recién instalados descubrirse e identificarse y configurarse de modo uniforme, además cuenta con un mecanismo de asignación automática de un ID único para cada nodo nuevo e informa a los hosts y a los otros nodos que está disponible para ser utilizado. [109]

VSCP es un sistema basado en eventos, una vez que ocurre un evento, este se difunde a todos los nodos que se encuentran conectados en la red, cada nodo recibirá y determinará si este evento debe ser manejado o no. Los eventos están estructurados en clases, por ejemplo, controles, alarmas, mediciones, información, entre otros. [109]

Inicialmente VSCP se utilizó para redes CAN, esta red es muy confiable y de bajo costo en la actualidad, y permite la construcción de nodos que puedan desempeñarse de manera segura, eficiente y fiable en su uso cotidiano; sin embargo, VSCP puede ser usado en otros entornos diferentes a redes CAN. [109]

Existen dos niveles del protocolo VSCP [109]:

- **Nivel 1:** Es práctico para enlaces de ancho de banda limitados, por ejemplo, para la transmisión de mensajes en entornos distribuidos basados en la topología bus, y para microcontroladores con recursos restringidos. [109]
- **Nivel 2:** está diseñado para las capas de transporte de mayor nivel, como TCP/IP, que son capaces de manejar una gran cantidad de información, están destinados para los nodos que usen mayor banda ancha. Este nivel usa un GUID (identificador único global) completo para cada paquete. [109]

3.3.7 Protocolo STOMP (Simple/Streaming Text Oriented Messaging Protocol)

Es un protocolo simple orientado a texto, opera de forma similar a los marcos HTTP, un marco contiene un comando, encabezados opcionales y un cuerpo opcional, funciona con cadenas de texto como JSON o XML, es de código abierto, fácil de implementar y concede interoperabilidad, ya que permite a los usuarios comunicarse con todos los intermediarios Stomp bróker disponibles, sin importar el lenguaje de programación en que están escritos, y además funciona sobre TCP. [110][111]

Los clientes Stomp establecen los destinos que tomaran los mensajes, para ello envian un marco (SEND) al servidor, este será el encargado de dar un nombre al destino, que pueden ser direcciones en el caso de un destino especificado o colas cuando el mensaje sea un marco de tipo suscripción (SUBSCRIBE), los clientes recibirán un marco de tipo mensaje del servidor (MESSAGE) y cuando se quieran retirar deberán enviar un mensaje de desconexión, de esta forma el servidor elimina las sesiones y recursos de dicho cliente de forma síncrona. [112]

No hay muchas limitaciones en la arquitectura de los servidores y las funciones, respecto al manejo de la semántica y la asignación del nombre del destino.

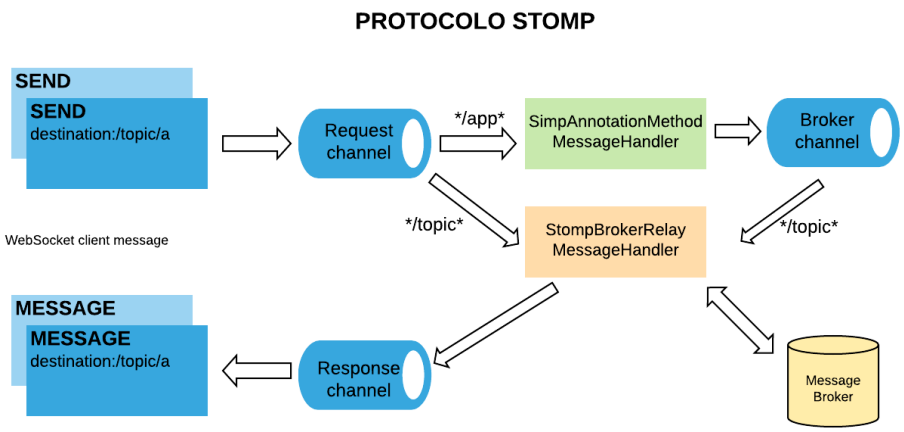


Ilustración 32 Arquitectura del protocolo STOMP [52]

3.3.8 Protocolo OpenWire

Es un protocolo binario que proporciona acceso de forma nativa a ActiveMQ, este es un servidor de mensajería de código abierto (Open Source) e implementa el estándar JMS (Java Message Service), y además permite que la comunicación entre dispositivos sea débilmente acoplada, asegurando que el mensaje sea entregado una sola vez, y que establezca una comunicación asíncrona, es decir, que el proveedor entregue los mensajes al destinatario conforme vayan llegando. [113]

OpenWire fue esquematizado con el objetivo de otorgar un completo control sobre el bróker, y así mismo ser un protocolo completamente funcional, compatible con JMS, rápido, altamente eficiente y que utilice los recursos de la red de forma optimizada. [113]

OpenWire es un protocolo complejo, que transforma objetos a arreglos de bytes y viceversa. Cada arreglo de bytes se le asigna el nombre de “command”, y cada uno de ellos sirve para realizar una función específica en ActiveMQ, por ejemplo, establecer sesiones, creación de colas, manejo de recursos, entre otros. [113]

3.3.9 Protocol DDS (Data Distribution Service)

Es un protocolo para sistemas en tiempo real, usa una lógica de intercambio de información entre aplicaciones, utilizando middleware, opera el modelo publicar/suscribir para el envío, recepción de datos, registro de eventos y comandos entre los nodos en la transmisión M2M. DDS es un estándar API para la conectividad centralizada de los datos de la organización OMG (Object Management Group). [114]

La arquitectura de este protocolo fue diseñada para ser escalable, de baja latencia, confiable y de alto rendimiento, permitiendo así que la transmisión de

datos sea en tiempo real entre los suscriptores y publicadores, su diseño es especial para cubrir necesidades en sistemas IoT. [115]

Este estándar proporciona las siguientes características [114]:

- **Escalabilidad y efectividad del rendimiento:** es una arquitectura completamente descentralizada, permitiendo que los nodos DDS se comuniquen punto a punto a través de UDP/multicast, logrando latencias bajas de 30 µseg (microsegundos).
- **Portabilidad:** se implementó para que admita una gran variedad de lenguajes de programación, como: C/C++, Java, JavaScript, entre otros; y es independiente del sistema operativo y hardware.
- **Seguridad:** contiene sistemas de autentificación, encriptación de la información, y además lleva registros de control de acceso, de esta manera proporciona seguridad de los datos de extremo a extremo.
- **QoS:** maneja políticas de calidad de servicio para el enrutamiento, filtrado de contenido y uso de recursos.

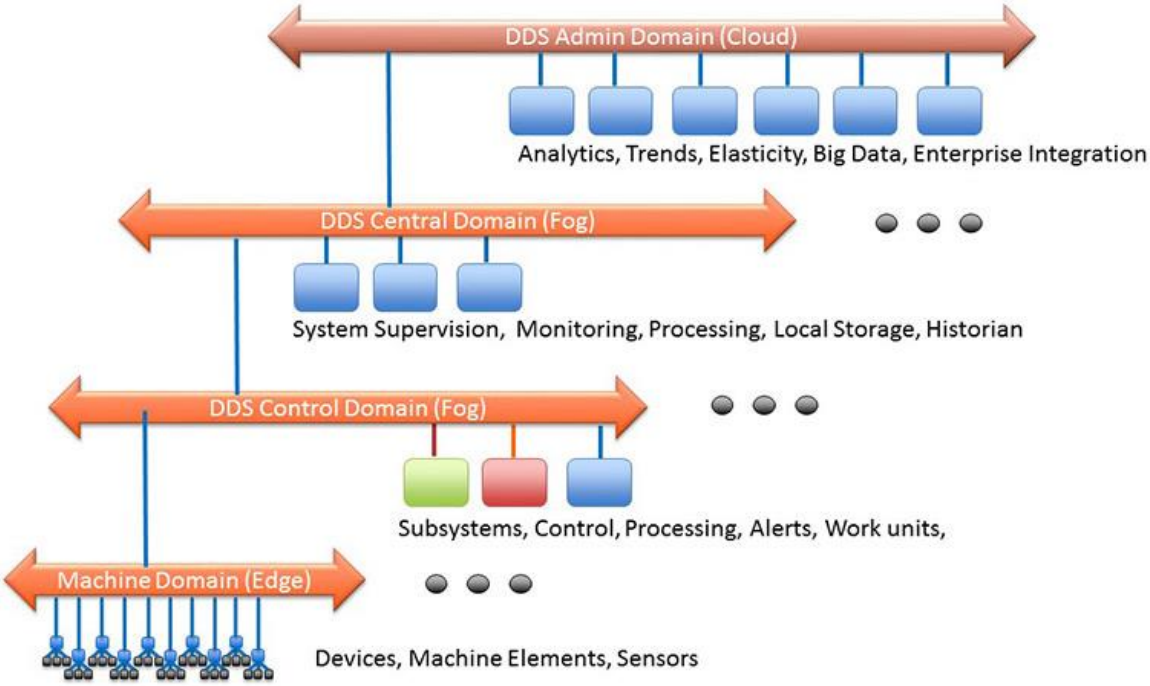


Ilustración 33 Arquitectura del protocolo DDS. Tomado de Object Manegement Group (OMG), "DDS The Proven Data Connetivity Standard for the IoT" [114]

	HTTP	CoAP	XMPP	MQTT	AMQP	VSCP	STOMP	OpenWire	DDS
Transporte	TCP/UDP	UDP/IP	TCP/IP	TCP/IP	TCP/IP	TCP/UDP/IP	TCP/IP	TCP/IP	UDP/IP TCP/IP
Seguridad	TSL	DTLS	MTLS	TLS	TLS	SSL/TLS	SSL/TLS	SSL/TLS	TLS, DTLS, DDS security
Petición-respuesta	SI	SI	SI	NO	NO	Basado en eventos	SI	SI	NO
Publicación - suscripción	NO	SI	SI	SI	SI	Basado en eventos	SI	SI	SI

Tabla 7 comparación de los protocolos que operan en la capa de aplicación.

3.4 PROTOCOLOS PRESENTES EN LA CAPA PRECEPCIÓN, INTERNET Y APLICACIÓN

3.4.1 Z-Wave

El protocolo Z-Wave, es una tecnología de comunicación inalámbrica interoperable, basada en RF (Radiofrecuencia) diseñada concretamente para aplicaciones de monitoreo, control y lectura del estado en ambientes residenciales o comerciales[116], y es considerada como el estándar internacional para la interconexión de sistemas domóticos. Fue desarrollada por la compañía danesa Zensys, como una alternativa más simple y económica comparada con Zigbee.[117]

Una red Z-Wave, puede contener hasta 232 nodos y consta de dos conjuntos de nodos, los dispositivos controladores y esclavos; estos nodos pueden ser configurados para retransmitir el mensaje escuchado, con la finalidad de garantizar la conectividad en el entorno, con los diferentes sistemas dirigidos en el hogar.[118]

Se basa en una topología de red en malla completa, esto implica que no necesita un nodo coordinador, dicho de otra manera, cada dispositivo Z-Wave

instalado en la red se convierte en un repetidor de señal y puede saltar hasta 4 veces en los nodos de tipo escucha. Opera con una banda de frecuencia sin licencia en el rango de 800-900 MHz, y cuenta con alcance de cobertura de 100 metros para el contacto punto a punto, funciona con tan baja potencia que algunos sensores podrían durar por lo menos 10 años [117]. Como está diseñado específicamente para aplicaciones de control y monitoreo, admite velocidades de datos hasta de 100 kbps. [117]

Las señales de Z-Wave pueden viajar fácilmente en a través de las paredes, techos, e igualmente pueden esquivar los obstáculos de manera inteligente para conseguir una cobertura excelente, robusta y completa para el hogar. [118]

Ilustración 34 Aplicación de Z-Wave en la domótica. Tomada de Z-Wave ALLIANCE, "About Z-Wave Technology." [116]

3.4.2 Zigbee

Fue creada por la Zigbee Alliance como una tecnología de comunicación inalámbrica, está basada en el protocolo estándar IEEE802.15.4, de corto alcance en rangos de 10 a 15 m, trabaja en las bandas libres de 2.4 Ghz disponible en todo el mundo, admite una velocidad de transferencia de datos de 250 kbit/s en 16 canales diferentes, 858 MHz para Europa y 915 Mhz para Estados Unidos y Australia, mediante una técnica DSSS que traduce el espectro ensanchado, por secuencia directa (*direct sequence spread spectrum*) se puede lograr un rango de alcance de 150 m [119], su principal objetivo era dar soluciones de bajo consumo energético a diseños de domótica y automatización, funciona con tres tipos dispositivos de red [120]:

Coordinador (ZigBee Coordinator, ZC): existe uno por cada red de nodos y se encarga de establecer la ruta y de controlar la comunicación en la red, por este motivo necesita de un mayor procesamiento de memoria. [120]
Encaminador (ZigBee Router, ZR): Interconecta dispositivos separados en la red, además ofrece un nivel de aplicación para la ejecución de código de usuario.[120]
dispositivo final (ZigBee End Device, ZED): puede establecer comunicación con el nodo padre (encaminador y el coordinador) pero no está autorizado a transmitir. [120]

La comunicación puede ser topología en estrella (star), la topología entre pares (pair), árbol de grupos (cluster tree) y topología malla (mesh). [121]

El protocolo zigbee es fácil de adquirir en el mercado, puesto que tiene más de 30 proveedores de productos y servicios de hardware y software diseñados para satisfacer todas las necesidades en toda la industria IoT.[119]

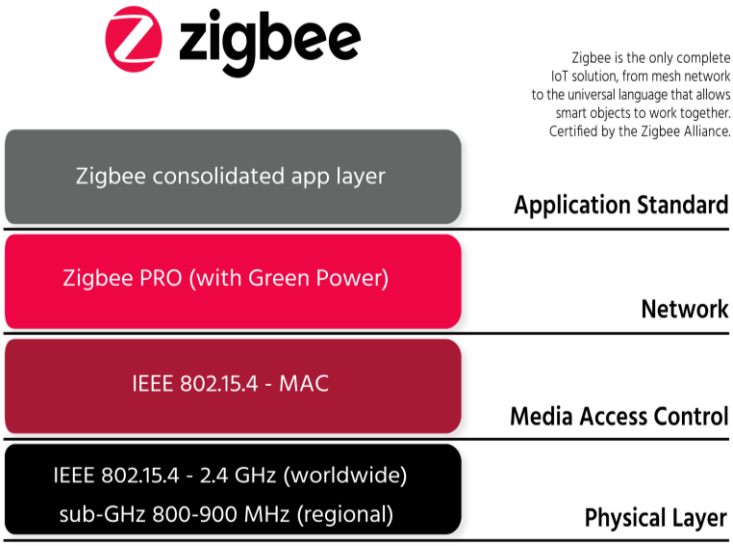


Ilustración 35 Modelo Zigbee. Tomado de Zigbee Press Releases, "The Zigbee Alliance Introduces First Multi-Band IoT Mesh Network Technology for Massive IoT Deployments" [121]

Ilustración 36 Aplicaciones Zigbee.
Tomado de J. Moreno, "ZIGBEE" WIKISPACES [122]

3.4.3 THREAD

Es un protocolo especialmente diseñado para soluciones IoT en el hogar, su topología de red es una robusta malla autorreparable y puede comunicarse con

más 250 nodos, es decir, la red se puede extender a más 250 electrodomésticos en el hogar, su amplio soporte para nodos con sueño permite años de operación, incluso con una sola batería AA el consumo de energía es bastante bajo, además es altamente interoperable con tecnologías IPv6 con 6LoWPAN como base, dicho de otra manera, es compatible y escalable con dichas tecnologías, por otra parte necesita solo una mejora de software para los productos basados en el estándar 802.15.4. [123]

Los dispositivos poseen un código de instalación, así aseguran que solo ellos se puedan conectar a la red y obtener permisos a los recursos asignados a cada uno. [123]

La tasa de transferencia de datos entre nodos es pequeña, de manera que conserva el ancho de banda y la potencia, además el protocolo de enrutamiento simplificado reduce la sobrecarga y la latencia de la red. [123]

Es amigable con el usuario pues este puede monitorear su hogar desde su propio smartphone o Tablet. [123]

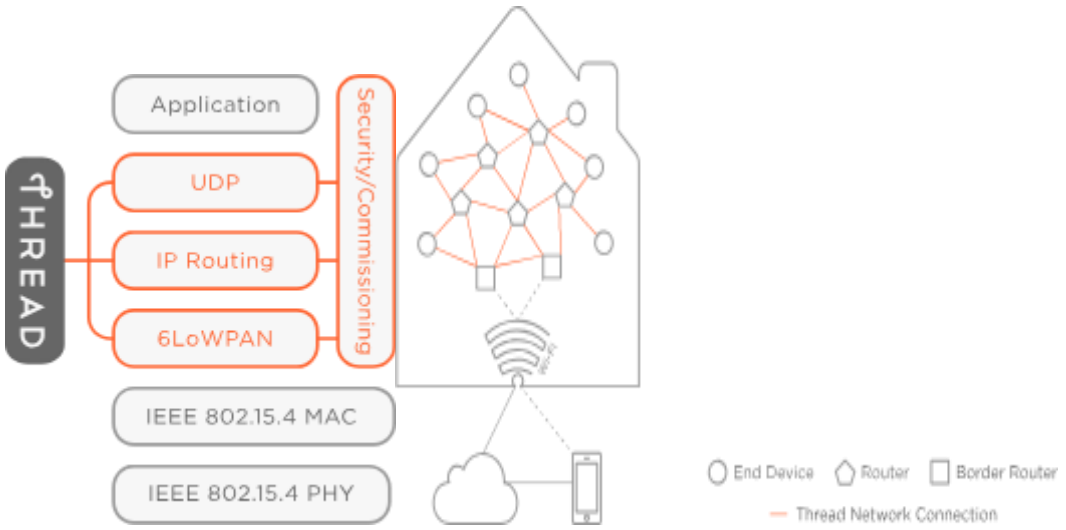


Ilustración 37 Arquitectura Thread. Tomado de THREAD, "POWERFUL TECHNOLOGY DESIGNED FOR THE HOME." [123]**.**

4. APLICACIONES IoT

El crecimiento exponencial del desarrollo tecnológico en los diferentes ámbitos de la sociedad actual, ha transformado la forma de comunicarse y de vivir, existe una gran variedad de aplicaciones, servicios y dispositivos inteligentes disponibles en el mercado.

En este capítulo se expone una panorámica de las aplicaciones más usadas a nivel global.

4.1 SMART CITY (Ciudad Inteligente)

Es una tendencia de nivel global, que se caracteriza por la implementación masiva de tecnologías de la información, en pro de la creación de servicios de interconexión, digitalización social o mejorar los sistemas ya existentes que hacen parte de una ciudad. Tiene como objetivo mejorar la calidad de vida de los ciudadanos, de ahí que una Smart City es un vasto ecosistema que compromete las TIC y una diversidad de redes de servicios IoT, gira en torno a optimizar la gestión de procesos de seguridad pública, el hogar, la educación, la salud, la industria, la agricultura, transporte, gobierno entre otros. [25]

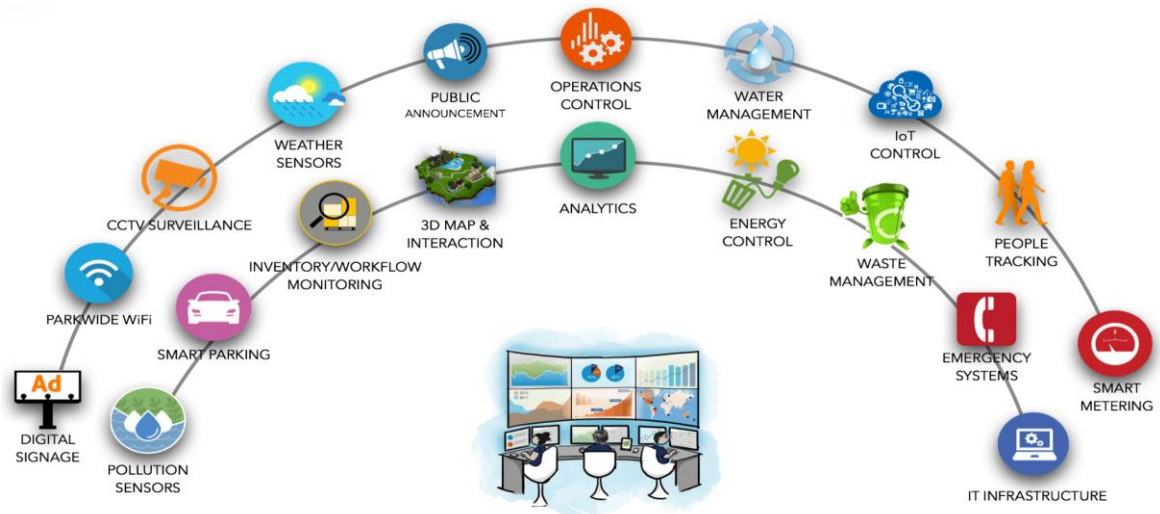


Ilustración 38 Servicios que contiene una ciudad inteligente. Tomado de VTara Energy Group." "IOT Smart Cities [124]

Como ejemplos de ciudades inteligentes están*: Santiago de Chile, con prácticas del fomento del transporte eléctrico o contadores inteligentes, Buzios (Brasil) con el uso de tecnologías de alumbrado público LED, Bogotá (Colombia) con la implantación pionera del sistema de transporte público masivo; el 'Bus Rapid Transit' o Montevideo (Uruguay) que se ha convertido en el mayor exportador de software libre de LATAM. En el ranking internacional, Tokio va a la cabeza en proyectos Smart city, le siguen Londres, Nueva York, Zurich y París.* [125]

4.2 SMART HOME (Casa Inteligente)

Este concepto es también conocido como domótica, se trata de un conjunto de tecnologías encargadas del control y automatización inteligente de una casa, su objetivo es mejorar la calidad de vida de los usuarios proporcionando seguridad y comodidad dentro de un ambiente inteligente. [126]

Un sistema domótico funciona con elementos de entrada de información como sensores, el sistema inteligente se encarga de procesar dicha información y enviar órdenes a unos actuadores o salidas, en cuanto a la red de control del sistema domótico, esta debe integrarse y coexistir con la red de energía eléctrica, y la red de internet de manera transparente para el usuario.[126]

Para considerar que un sistema es domótico, debe poseer las siguientes cualidades:

Ahorro energético: con los datos obtenidos por los dispositivos de control de consumo, se procede a optimizar el gasto energético de los electrodomésticos, para ello se modifican hábitos que a futuro se visualiza como un ahorro monetario al usuario. [126]

Actualmente se implementan en mayor medida sistemas como:

- Termostatos inteligentes.
- Estaciones climatológicas.
- Enchufes inteligentes.
- Smart-lighting.
- Sensores de movimiento de luz.

Accesibilidad: existen sistemas domóticos que se adaptan a cada necesidad, monitorizando diversos elementos electrónicos del hogar, de una forma sencilla, cómoda y transparente para el usuario. [126]

Un smart home es también ideal para personas mayores o que poseen alguna discapacidad, ya que su hogar se convierte en un espacio sin barreras, de ahí que puede realizar un máximo de tareas cotidianas sin depender de otra persona. [126]

Seguridad: por medio de vigilancia automática se puede detectar, corregir y alertar sobre fallas e intrusos en el hogar del usuario. [126]
en el mercado se pueden encontrar sistemas de:

- Alarmas.
- Sensores y detectores de movimiento.
- Cámaras de vigilancia.
- Vigila bebés.

Comunicaciones: establece comunicaciones en tiempo real bidireccionalmente entre el usuario y los electrodomésticos, es decir, que se cuenta con una supervisión remota a través del teléfono móvil, la información que llega al usuario puede ser tipo voz, datos y multimedia. [126]

Ilustración 39 Funcionalidades y dispositivos integrados de una smart home. Tomado de M. S. Obaidat and P. Nicopolitidis, Smart Cities and Homes: Key Enabling Technologies. [127]

El mercado de hogares inteligentes crece exponencialmente, actualmente un 0.5% de los hogares americanos posee hasta 6 electrodomésticos inteligentes y se prevé que para el 2025 al menos el 10 % de la población mundial tendrá un hogar inteligente. *El mercado global de hogares inteligentes tuvo un valor de $ 14.7 mil millones en 2017, y la región de las Américas representa el 48 % de los ingresos mundiales.* [126]

Actualmente los dispositivos más vendidos a nivel mundial son:

Válvulas de radiador: En zonas que poseen temporada invernal, y el uso de radiadores es común para la calefacción, se han diseñado válvulas de radiador inteligente, cuyo objetivo es reducir el coste energético hasta un 37 %, para ello el sistema diseña un plan de acción para cada habitación del hogar y regula la temperatura de cada sitio en horas específicas, además el usuario puede controlarlo de manera de remota desde un teléfono móvil o tablet. [128]

Ilustración 40 Válvulas Inteligentes para un radiador de Netatmo son compatibles con Apple Home Kit y Google Home. Tomado de CASADOMO. [128]

Sensores de calidad del aire: Debido al crecimiento de la contaminación ambiental a nivel mundial, cada vez son más que familias que adquieren purificadores de aire para mantener al mínimo componentes contaminantes presentes en el ambiente de su hogar, gracias a servicios IoT los usuarios conocen la temperatura, la humedad y en qué momento el nivel de contaminación por monóxido de carbono, amoníaco, metano, humo de cigarrillo o contaminantes similares sube, pues los sensores envían mensajes de alerta al teléfono móvil o tablet en tiempo real sobre la calidad del aire, de ahí que el sistema automatiza el filtro acelerando su funcionamiento cuando no hay una alta concentración, de lo contrario el filtro se desacelera para eliminar la mayor cantidad de agentes contaminantes, con dicha información se puede programar en horarios específicos, así optimiza el consumo energético y brinda confort al usuario final. [129]

Ilustración 41 Sensor de calidad del aire. Tomado de ABC SOLUCIONES[129]

Altavoces inteligentes: funcionan como asistentes de voz en el hogar, es decir, la voz se convierte en el control de los electrodomésticos interconectados, esto mejora la experiencia del usuario pues si tuviera 5 dispositivos inteligentes también tendría 5 aplicaciones para usar, el asistente de voz reduce la necesidad de utilizar el teléfono móvil. [130]

Ilustración 42 Altavoz inteligente fabricado por Amazon. Tomado de Amazon [131]

Gráfica 1 Muestra el porcentaje de los usos que le dan las personas a los altavoces inteligentes, se encuestaron alrededor de 800 personas. [130]

4.3 SMART FARMING (Agricultura Inteligente)

El incremento de la población mundial y la modificación de normativas alimentarias, ha aumentado la demanda de alimentos, debido a ello aparecen múltiples inconvenientes para cumplir con los niveles de producción proyectados, dicha problemática no se puede resolver con los métodos tradicionales. Actualmente se implementan soluciones tecnológicas que optimizan al máximo la tierra cultivable y la utilización de insumos. [132]

Ilustración 43 Aplicación de IoT en la Agricultura. Tomado de IoT SIMPLE, "Agricultura Inteligente" [133]

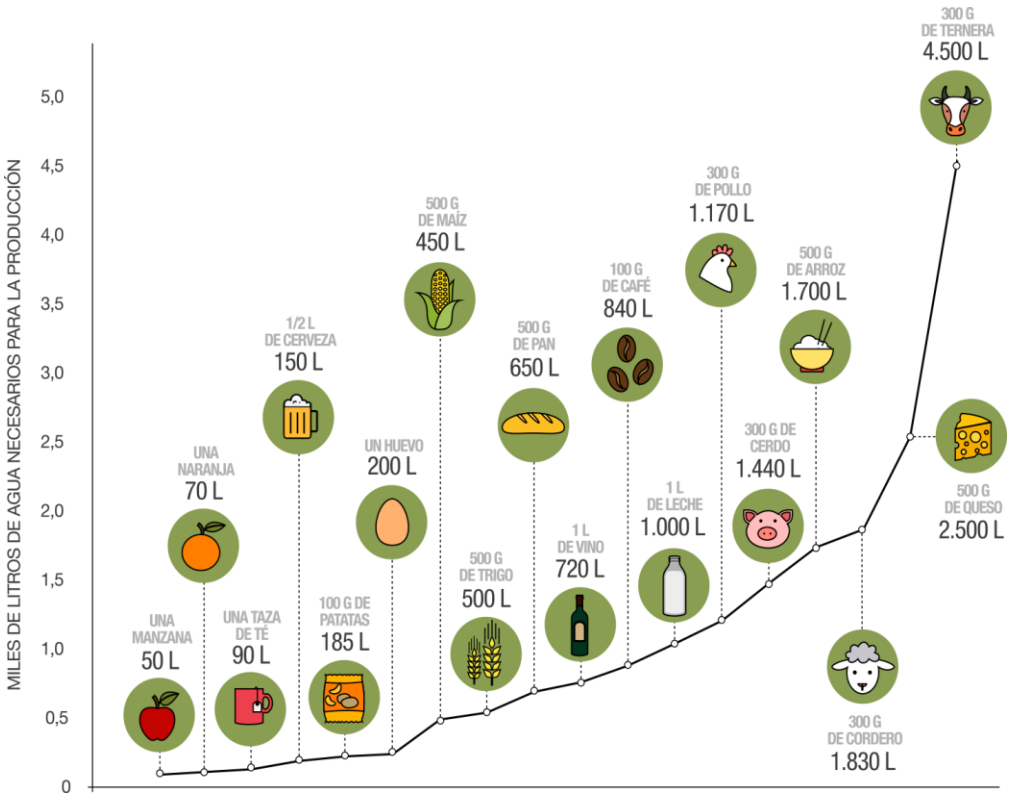
Para lograr una mayor eficiencia y dar solución a las necesidades que se presentan en este sector, se requiere utilizar nuevas herramientas tecnológicas y también recurrir a IoT. La gestión de cultivos basada en la agricultura inteligente comprende los siguientes aspectos. [133]

4.3.1 Aspectos importantes de la agricultura inteligente [134]:

- Agricultura de precisión y conservación.
- Monitorización de la cosecha.
- Información meteorológica.
- Disminución del uso de pesticidas y herbicidas.
- Integración de Sistemas de Información Geográfica.
- Software de gestión (para la toma de decisiones y controlar automáticamente uno o varios sistemas como riego, protección de heladas, fertilización, entre otras).
- Trazabilidad.

El uso de sensores y dispositivos inteligentes, más la integración de aplicaciones, permite adquirir una información detallada del cultivo, el suelo y las variaciones climáticas (presión atmosférica, temperatura, humedad del aire, velocidad y dirección del viento, cantidad de lluvia caída, etc.) en tiempo real, que ayudan a optimizar la producción y la calidad de los productos, realizando mediciones en línea del tamaño del tallo, fruta o cultivo a tratar, así mismo la cantidad de agua requerida para el riego, el valor estimado de la radiación fotosintéticamente, etc. Por otra parte, también ayuda a reducir costos de producción, por ejemplo, en el monitoreo en línea de la temperatura y la humedad del suelo, permitiendo detectar si el suelo es propicio para la proliferación de hongos y plagas en los cultivos. Toda la información recolectada es almacenada para elaborar informes estadísticos, trazabilidad, para hacer acciones correctivas o preventivas, por ejemplo, tomar las medidas necesarias en la dosificación de fertilizantes y fungicidas de manera eficaz y precisa. [135]

El sector agrícola debe enfrentarse a grandes desafíos como los cambios climáticos, la disminución de tierra dedicada al cultivo, menos mano de obra, y los graves problemas de escasez de agua (consume más del 70% del suministro de agua dulce en el mundo). [133]



Gráfica 2 Representativa sobre la cantidad de agua usada en la agricultura. Tomado de Feriberia, "Weblet Importer" [133]

El panorama de la agricultura frente al cambio climático es un desafío que se intensifica debido a los impactos negativos que afectan a los cultivos, a la ganadería y la pesca por igual. Para enfrentar este desafío se requiere inversiones considerables, en adaptación al cambio climático para lograr el aumento de producción requerida, procurando producir efectos de manera simultánea, que ayuden a aumentar la capacidad de adaptación de los cultivos reduciendo las sequías, plagas, enfermedades y entre otras perturbaciones que afectan a este sector. [136]

4.3.2 Servicios y aplicaciones tecnológicas usadas en la agricultura inteligente:

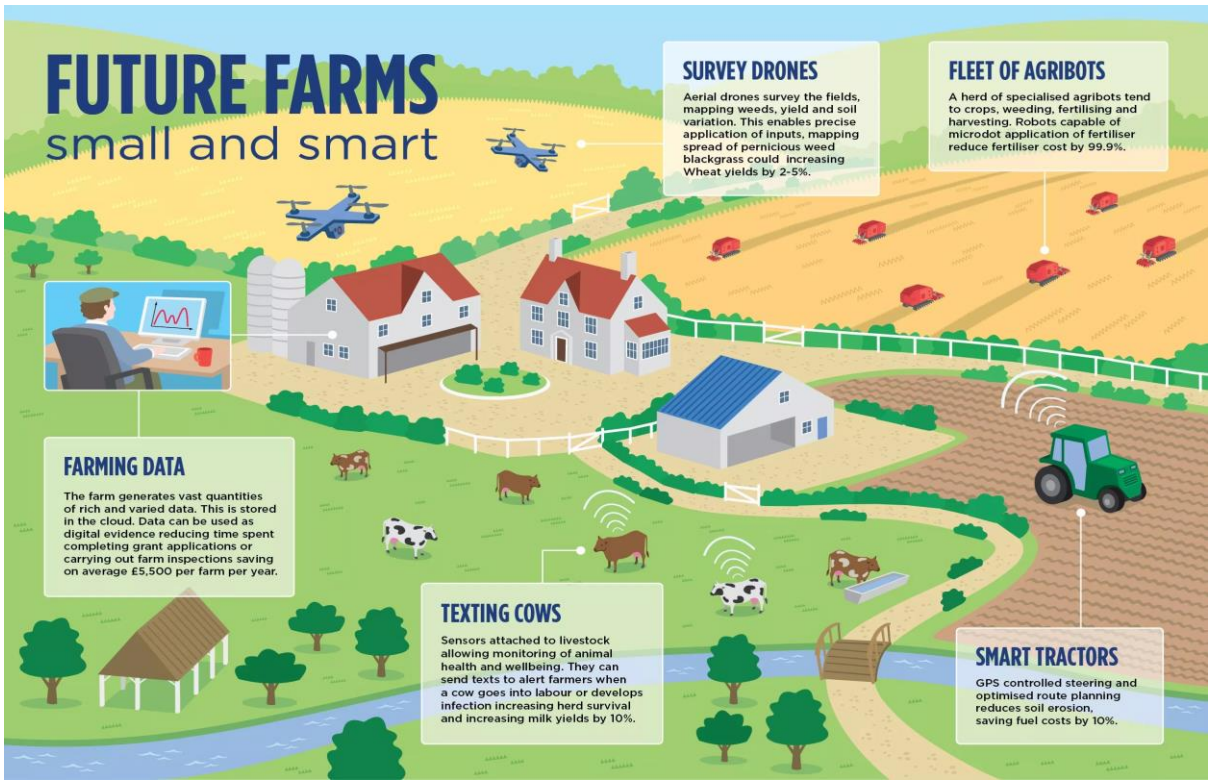


Ilustración 44 Aplicaciones implementadas en Smart farming. Tomado de S. Wolfert, L. Ge, C. Verdouw, and M. J. Bogaardt, "Big Data in Smart Farming – A review" [134]

Monitoreo de ganado: son etiquetas o collares instalados en los semovientes, que permiten hacer un seguimiento en tiempo real de la actividad de los bovinos de manera automática, alertando comportamientos e interacciones inusuales del ganado, y además orienta al agricultor como corregir estos problemas. [137][138]

Los sensores envían alertas de información importante como [138]:

- Problemas de salud (un ejemplo, mastitis).
- Rumiación anormal, patrones de alimentación y zonas de pastoreo.
- Deterioro de la calidad del hábitat.
- Detección de celos.
- Identificación precisa del momento indicado para el ordeño.

- Estado de parto.

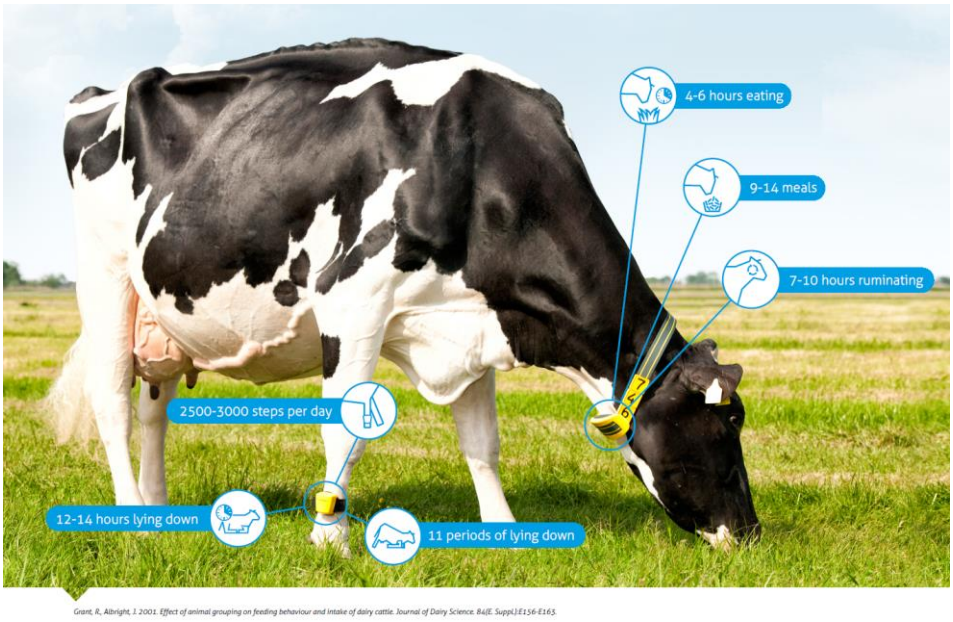


Ilustración 45 Monitoreo y control del ganado. Tomado de NEDAP, "Control de la salud láctea" [137]

Piscicultura: se implementan sensores de monitoreo en una granja de peces, permitiendo a los piscicultores monitorear de manera remota la calidad y condiciones del agua en tiempo real, ya que con cualquier irregularidad se puede ver amenazada la población de peces. IoT optimiza los aspectos de la piscicultura promoviendo la sostenibilidad de las mismas, garantizando que los peces se críen sanos y comestibles. El sistema de monitoreo puede proporcionar la siguiente información [139]:

- Temperatura del agua.
- Los niveles de pH, oxígeno disuelto, la clorofila, amoníaco, entre otros elementos.
- La turbidez.
- Sistemas de alerta (como el entorno de crecimiento deseado o el tamaño de la cosecha).
- Detecta objetos o intrusos desconocidos que tiene contacto con el agua (un ejemplo un insecto invasor).

Ilustración 46 Estanque de peces. Tomado de "Informe de Vigilancia Tecnológica Blue Growth". [140]

Agricultura de precisión: es una técnica de cultivo y gestión agrícola, que hace uso de Tecnologías de la Información (TI), para lograr un óptimo rendimiento y control de cada terreno, estos datos son recolectados por sensores y drones que cuentan con un soporte Back-End, que ayudan a la de toma decisiones en tiempo real en el procesamiento de lotes y hacerlos interoperar como un único sistema integrado. Además, la agricultura de precisión realiza un análisis del suelo, de cultivos y cosechas, para favorecer un óptimo desarrollo de la producción. [141]

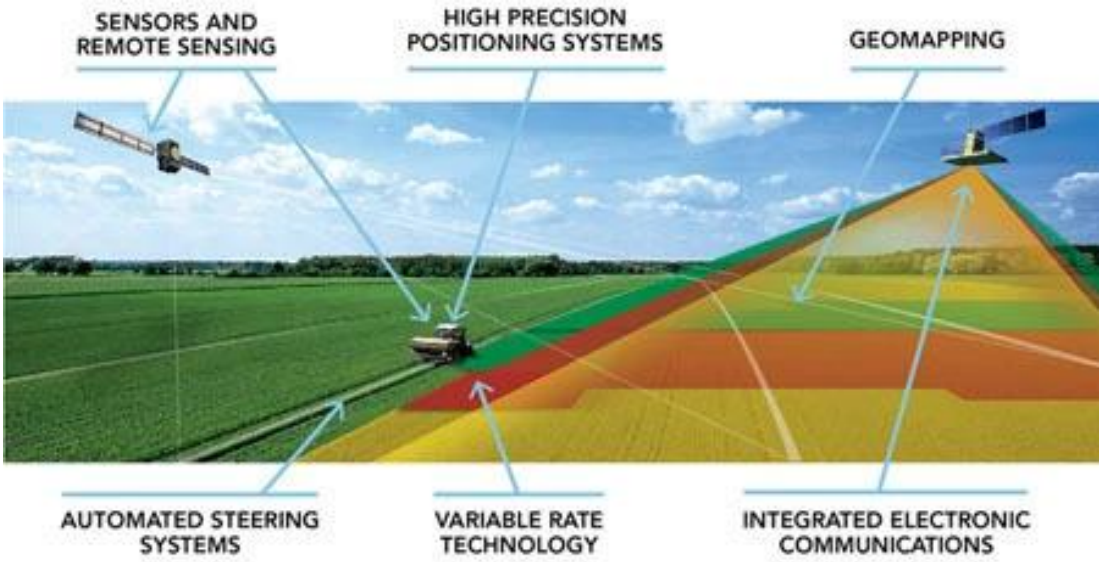


Ilustración 47 Agricultura de precisión. Tomado de PRECISIONAG, "Precision Agriculture and Precision Farming". [142]

Los principales beneficios de la agricultura inteligente son [143]:

- Maximización del rendimiento de cada parcela.
- Minimización y uso óptimo de pesticidas y fertilizantes.
- Reducción del uso de energía, agua y residuos.
- Mejorar la trazabilidad alimentaria.
- Sistema de medición y riego.
- Estaciones meteorológicas.

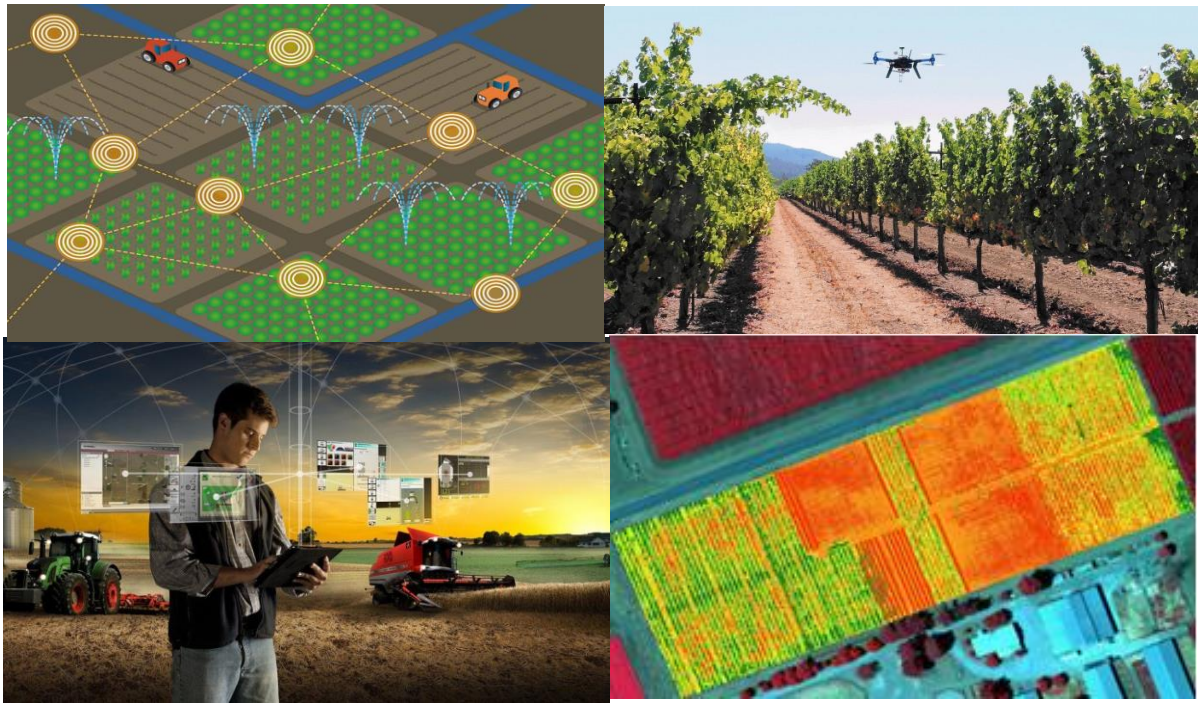


Ilustración 48 Tecnologías implementadas para la agricultura de precisión. Tomado de Joint Research Centre (JRC) of the European Commission, "Precision Agriculture: an Opportunity for Eu Farmers [141]

Invernaderos inteligentes: Este sistema mejora las prácticas agrícolas actuales con la ayuda de microcontroladores, sensores y aplicaciones de IoT, que habitualmente funciona de forma asíncrona, con otras soluciones tecnológicas implementadas en la agricultura. Los sensores capturan datos sobre el crecimiento de la planta, el riego, uso de pesticidas, la iluminación, la temperatura, humedad, entre otros factores. Esta información es enviada a un servidor back-end para un posterior análisis, y además permite a los

agricultores configurar los ajustes del sistema que emitan alertas e informes del rendimiento del invernadero [144].

Los invernaderos inteligentes ofrecen beneficios como:

- Protección contra enfermedades, plagas.
- Eficiencia y ahorro energético con el uso de paneles solares.
- Temporada de cultivos más largas.
- Control y monitoreo del ambiente y de los cultivos.

- Control de riego, climatización, iluminación.

Ilustración 49 Invernaderos inteligentes. Tomado de R. K. Kodali, V. Jain, and S. Karagwal, "IoT based smart greenhouse," [144]

4.4 SMART INDUSTRY (Industria Inteligente)

La evolución tecnológica ha impulsado el desarrollo industrial, dando paso al internet industrial de las cosas (IIoT), se caracteriza en implementar la comunicación máquina a máquina (M2M), utilizar sensores inteligentes especializados a la optimización de diversos sistemas de manufactura, en la automatización de procesos y la implementación de robots. Lo anterior proporciona a la industria un alto nivel de control, ya que dichas tecnologías permiten la recolección de datos, que tras ser analizados influyen en las decisiones más relevantes en cuanto a procesos de producción, calidad y distribución. El internet industrial de las cosas no sólo se reduce a la

manufactura, sino que amplía sus horizontes en sanidad, la energía, la industria aeroespacial entre otras. [145]

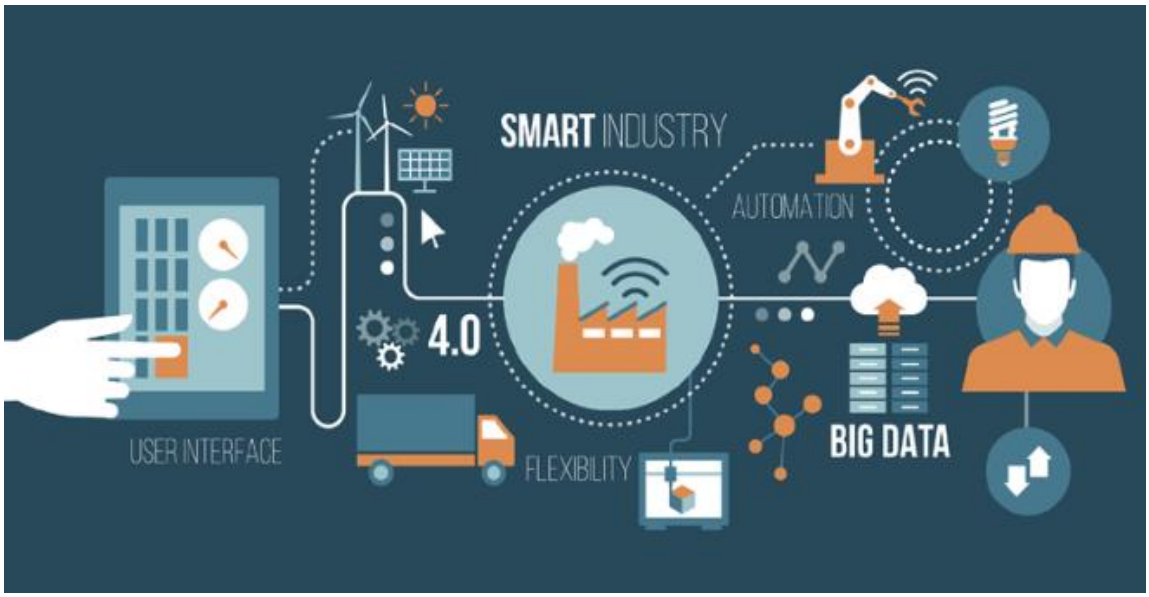


Ilustración 50 Industria inteligente.

Tomado de Agust9sytem "Industrial Automation [145]

4.4.1 Beneficios de implementar IIoT

Minimizar el error humano: Los seres humanos pueden cometer errores de cálculo, sentirse agobiados o fatigados, estos factores pueden provocar caos en el sistema industrial, desde retrasos en una línea de producción hasta la pérdida total de la misma, por ello los sistemas automatizados son ideales para minimizar errores en tiempo real.

Tomar mejores decisiones: en un sistema industrial se cuenta con una gran variedad de datos que se generan a gran velocidad y representan un volumen de información bastante grande. Actualmente con las tecnologías tipo Big Data encargadas de recolectar, almacenar, procesar, analizar y posteriormente obtener un patrón de comportamiento, la toma de decisiones es mucho más eficiente y confiable, ya que las predicciones fueron creadas por algoritmos matemáticos.

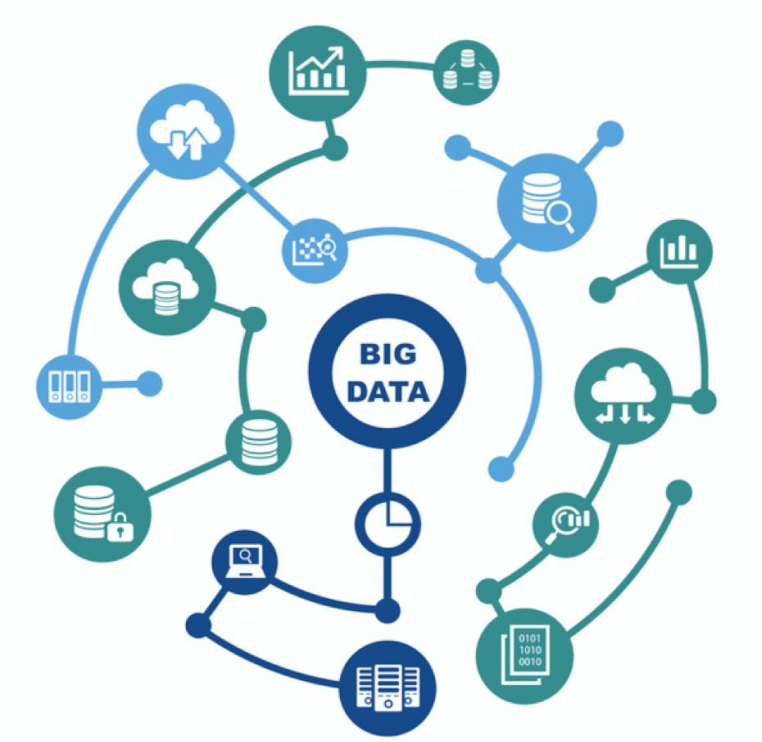


Ilustración 51 Big data aplicado en IIoT.
Tomada de DELLEMC, "Big-Data-Concept" [146]

Fácil adopción: hay una gran variedad de tecnologías y dispositivos disponibles y funcionales en el mercado IIoT, que cuentan con la aprobación de las diversas organizaciones de estandarización existentes.

Reducción de costos: Uno de los principales objetivos de IIoT es optimizar el uso de los recursos presentes en la industria, no sólo en sus plantas de producción, sino también se busca mejorar el rendimiento del transporte y suministro del servicio o producto.

Simulación: gracias a las múltiples plataformas de simulación existentes, se pueden diseñar entornos virtuales controlados, donde se logra observar eventos sometidos a distintas pruebas en tiempo real respecto al comportamiento de los procesos, la maquinaria, ensamble, distribución y el talento humano, todo esto para saber la viabilidad, los costos y tiempos de ejecución que se pueden presentar durante las diferentes etapas industriales.

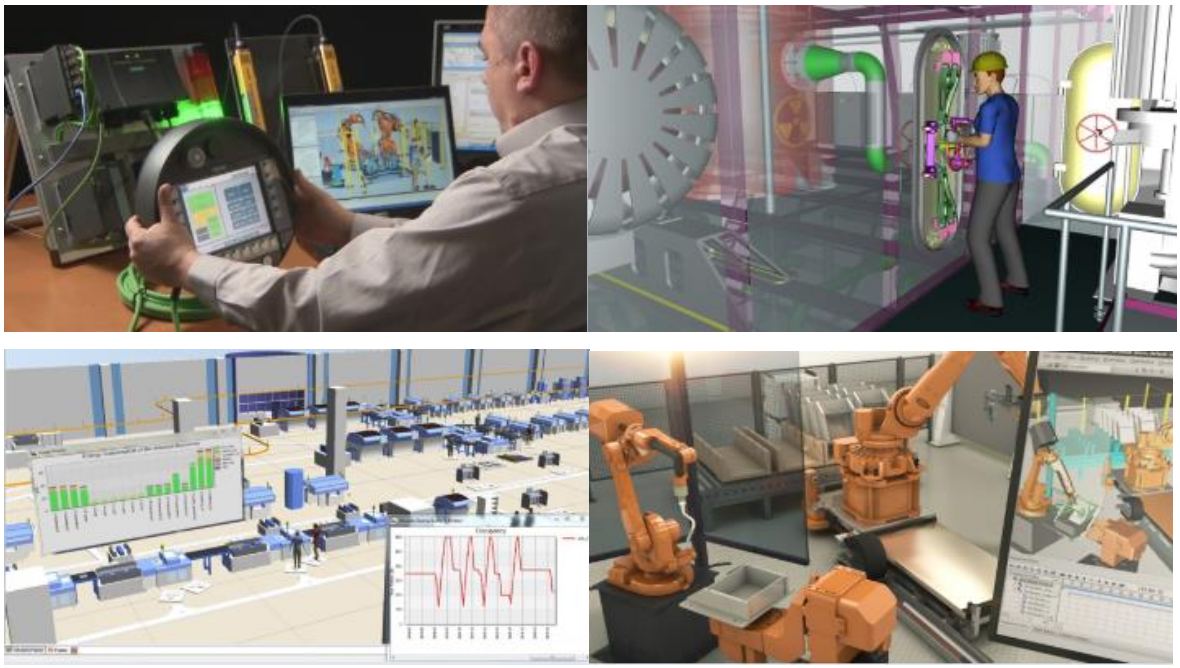


Ilustración 52 Simulación en una planta. Tomado de Tecnomatix [147]

El MIT technology Review ha publicado listas de las 50 compañías más inteligentes desde el año 2010, el análisis se hizo con base en su manera de combinar tecnologías innovadoras con un modelo de negocio efectivo.

A continuación, se nombran las primeras 10 compañías más inteligentes según el MIT en 2017. [148]

Nvidia Sede central Santa Clara, California Máquinas inteligentes para la industria Estado público Años en la lista 2015, 2016, 2017 Valoración $ 90.9 mil millones	1° Puesto
SpaceX Sede central Hawthorne, California Transporte en la industria Estado Privado Años en la lista 2011, 2012, 2013, 2014, 2015, 2016, 2017 Valoración $ 12 mil millones	2° Puesto
Amazon	3° Puesto

Sede central Seattle, Washington Conectividad de la industria Estado público Años en la lista 2013, 2014, 2015, 2016, 2017 Valoración $ 479.3 mil millones	amazon
23andMe Sede Mountain View, California Industria Biomedicina Estado Privado Años en la lista 2016, 2017 Valoración $ 1,1 mil millones	4° Puesto 23andMe
Alphabet Sede Mountain View, California Conectividad de la industria Estado público Años en la lista 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017 Valoración $ 673.9 mil millones	5° Puesto Alphabet
iFlytek Sede Hefei, China Máquinas inteligentes de la industria Estado público Años en la lista 2017 Valoración $ 6.8 mil millones	6° Puesto 科大讯飞 iFLYTEK
Kite Pharma Sede central Santa Mónica, California Industria Biomedicina Estado público Años en la lista 2017 Valoración $ 5,7 mil millones	7° Puesto Kite Pharma FOCUSED ON THE CURE
Tencent Sede Shenzhen, China Conectividad de la industria Estado público Años en la lista 2013, 2014, 2015, 2016, 2017 Valoración $ 350 mil millones	8° Puesto Tencent 腾讯

Regeneron Sede central Tarrytown, Nueva York Industria Biomedicina Estado público Años en la lista 2017 Valoración $ 55.5 mil millones	9° Puesto REGENERON SCIENCE TO MEDICINE®
Spark Therapeutics Sede central Filadelfia, Pennsylvania Industria Biomedicina Estado público Años en la lista 2016, 2017 Valoración $ 1.9 mil millones	10° Puesto Spark™ THERAPEUTICS

Tabla 8 Ranking de empresas Inteligentes[148]

4.5 SMART HEALTH (Salud Inteligente)

El impacto de las nuevas tecnologías en muchas tareas de nuestra vida cotidiana, ha impulsado a que el sistema de salud actual también acuda a utilizar los beneficios que ofrecen la tecnología de la información y comunicación (TIC), para optimizar la calidad de los servicios médicos[149].

Smart Health ofrece servicios y dispositivos especialmente diseñados para entornos y condiciones de la salud de cada paciente, permitiendo la monitorización del ritmo cardiaco, temperatura, entre otros datos fisiológicos en tiempo real, con la ayuda de sensores, etiquetas, parches, bandas inteligentes, y demás dispositivos que permitan un seguimiento y control continuo para aquellos pacientes con alguna discapacidad, enfermedades crónicas, o aquellos que requieran atención inmediata. Estos datos se transmiten a un dispositivo móvil y son enviados a la nube a una base de datos que maneja el proveedor del servicio médico, esta información recolectada, permite observar si el tratamiento está o no funcionando, en caso de algún incidente o variante que pueda afectar la salud del paciente se envía alertas a los centros de salud para tomar las medidas necesarias.

[149] Adicionalmente smart health está siendo utilizado por atletas para mejorar su condición física, y crear buenos hábitos de salud[150].

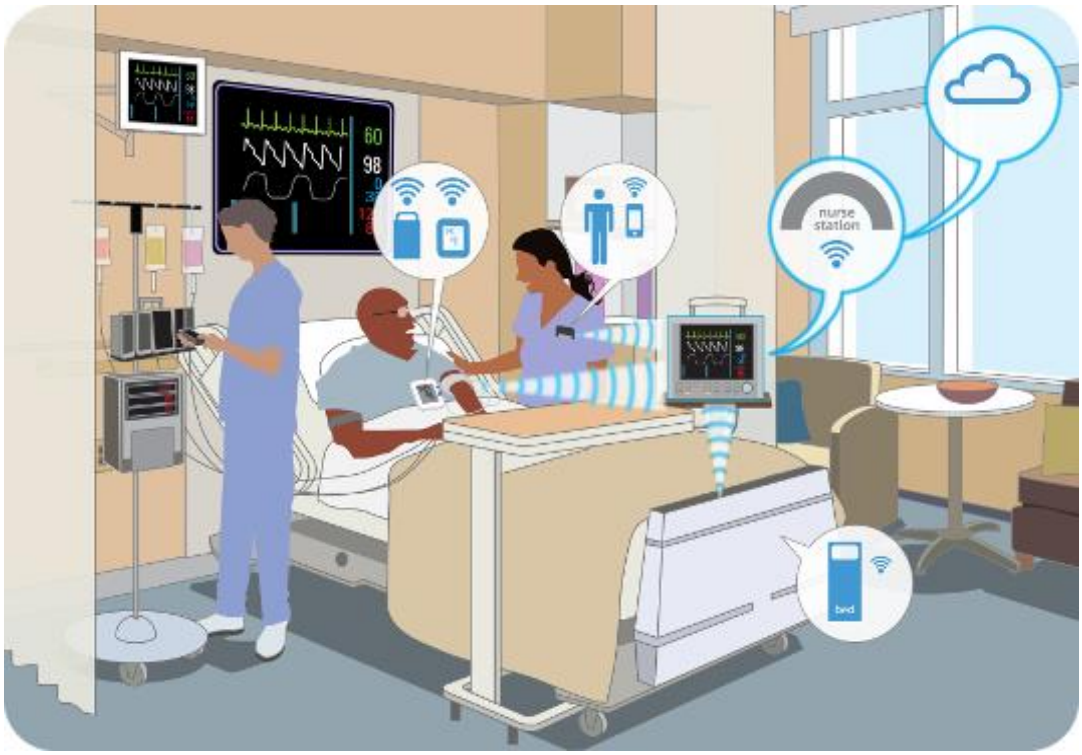


Ilustración 53 Uso de tecnologías IoT en hospitales. Tomado de Ipentechdiary [151]

La implementación de IoT en la salud tiene un impacto positivo en [149]:

- La construcción de un sistema de salud optimizado.
- Disminución de gastos del servicio.
- Toma de decisiones sobre tratamientos médicos que mejoran la calidad de atención al paciente.
- La predicción más acertada de los requerimientos que tiene cada paciente.
- Desarrollo de servicios más eficientes.

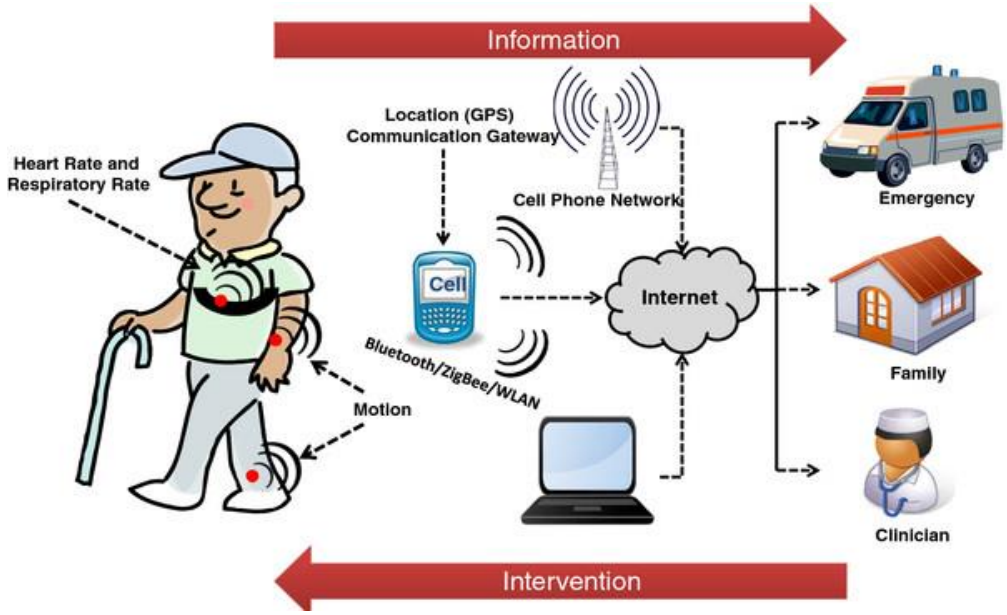


Ilustración 54 Sensores conectados a un paciente para monitoreo de salud remoto. Tomado de de Ipentechdiary [152]

4.5.1 Aplicaciones y Dispositivos IoT que están cambiando las industrias y hábitos de los consumidores

Cápsulas inteligentes: son dispositivos miniatura encapsulados en una píldora o pastilla de apariencia tradicional que recolectan y transmiten información, estas pueden ser ingeridas sin ninguna complicación y ayudan a vigilar las reacciones a los tratamientos médicos en el cuerpo del paciente, rastreando los niveles de medicamento en la sangre y así precisar la dosis adecuada para cada caso. [153]

Una de las empresas que está desarrollando este tipo de cápsulas "inteligentes" es Proteus Digital Health, estas píldoras contienen un microchip del tamaño de un grano de arena que generan una señal cuando entra en contacto con los jugos digestivos, está señal se transmite a un parche adhesivo que se coloca en el torso del paciente, la información recolectada es compartida con el usuario y con el médico mediante un aplicativo web o móvil, permitiendo un control completo sobre la toma del medicamento y respuestas fisiológica del paciente[154].

Otro píldora es Abilify MyCite son tabletas de aripiprazol con un sensor marcador de eventos, este medicamento es un antipsicótico utilizado para pacientes con desórdenes bipolares y esquizofrenia, trastornos depresivos, al igual que la píldora de Proteus Digital Health, está envía señales a un smartphone por medio de un parche que debe utilizar el paciente, así el médico tratante puede saber si el paciente está consumiendo o no el medicamento y en que horarios, además esa información recolectada puede ser complementada con otros datos, por ejemplo, signos vitales, cómo se siente la persona en determinados momentos del día, actividad física, entre otros datos [155].

Algunos factores, como una mala conexión o recepción, o no tener su teléfono inteligente, pueden afectar la consistencia y confiabilidad de los datos que se detectan, recopilan y transmiten. [154]

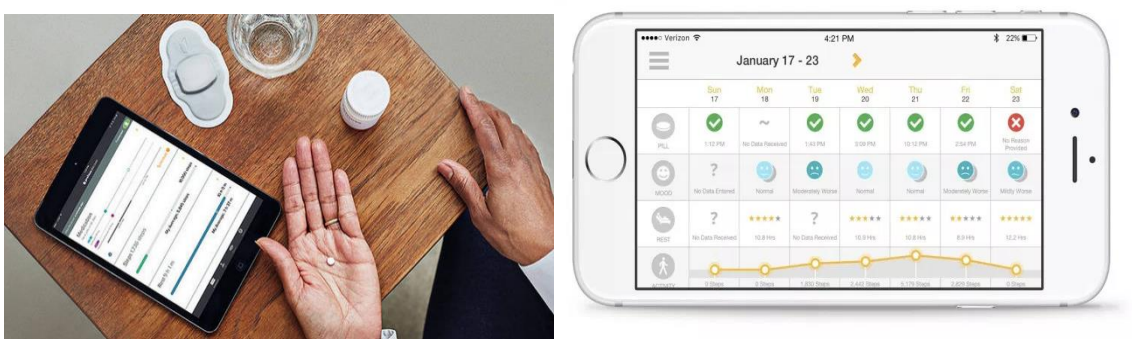


Ilustración 55 Cápsulas Inteligentes.
Tomado de CBINSIGHTS, "Proteus Digital Health [156]

También existe en el mercado PillCam, es una endoscopia capsular que emplea una cámara miniatura alojada dentro de una cápsula desechable y de fácil ingesta. Pillcam va transmitiendo y capturado imágenes a medida que avanza por el sistema digestivo y son enviadas a una serie de sensores, que se han colocado previamente en el abdomen del paciente, en el que también hay una grabadora que recolecta la información transmitida, el objetivo de esta cápsula de video es visualizar la mucosa del colon y detectar la presencia de pólipos (tejidos anormales)[157].

Ilustración 56 Cápsula Pillcam. Tomado de PILLCAM, What Is It? [157]

Hearebles o Smart Headphones (auriculares inteligentes): Estos dispositivos portátiles son considerados como asistentes de salud para el oído, aparte de reproducir música, cuentan con un sistema de monitorización de parámetros biométricos, que miden la temperatura, ritmo cardiaco, la saturación de oxígeno, al igual realizan un seguimiento de la actividad física [158].

Características y beneficios de la tecnología Hearable [158]:

- Signos vitales más precisos: se espera que esta tecnología sea capaz de medir instantáneamente la frecuencia cardiaca, temperatura corporal, presión arterial, oximetría del pulso, señales de electroencefalograma, ECG (electrocardiograma), y más. [158]
- Seguimiento de actividad física. [158]
- Identificación personal biométrica, esta tecnología es desarrollada por la NEC (compañía multinacional japonesa, que proporciona soluciones TI a empresas y al gobierno) utiliza ondas de sonido para identificar acústicamente al usuario, distinguiendo el del tamaño y forma del oído[159].
- Además, los Hearables ayuda a evitar problemas relacionados con los oídos (sordera parcial o completa) simplemente obstruyendo o amplificando los sonidos [156].

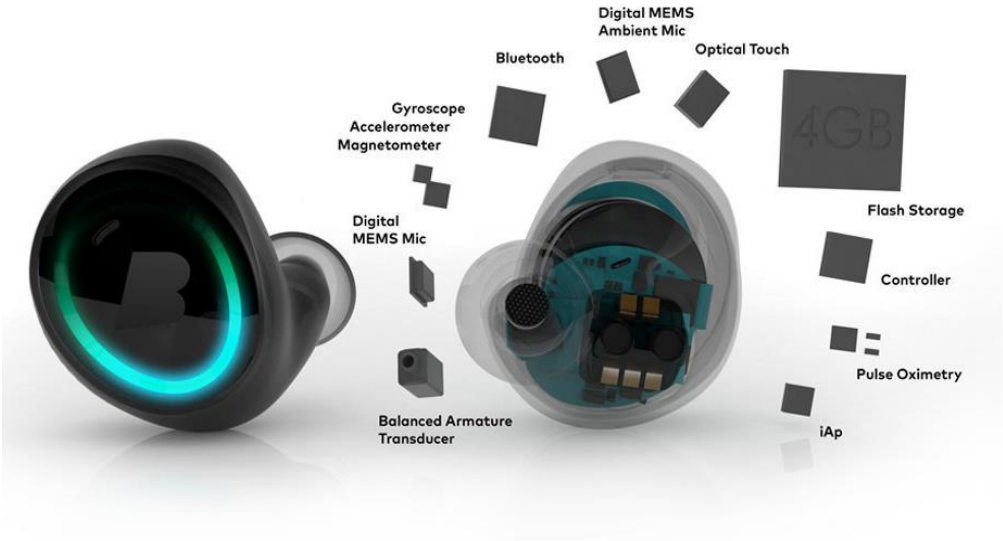


Ilustración 57 Hearables de la empresa Bragi. Tomado de bragi, "Custom Earphones - The Dash Pro - Bragi." [160]

Moodables: Estos dispositivos pueden leer las ondas cerebrales y transmitir corrientes de baja intensidad al cerebro, que proporcionan relajación al usuario. El uso de este dispositivo puede ser beneficioso para un cerebro sano o estresado. Aunque esta idea a un se encuentra en desarrollo[151].

Ilustración 58 Moodables. Tomado de everydayhearing, "The Complete Guide to Hearable Technology in 2018 - Everyday Hearing," [151]

4.5.2 Casos de uso de smart health

Aplicación de monitoreo remoto para pacientes de la tercera edad: Better alerts tiene como objetivo ayudar a las personas mayores a vivir de manera independiente, permitiendo a profesionales de la salud y familiares controlar a distancia a los ancianos que viven solos. Softweb Solutions implementó una aplicación multiplataforma que se comunica con un reloj inteligente, que permite al paciente y a sus cuidadores administrar alertas de toma de medicamentos, además administra sus contactos de emergencia en caso de un incidente[161].

Sistema de monitoreo de frecuencia cardiaca fetal: esta aplicación intuitiva permite a los médicos monitorear y controlar de manera remota los embarazos de alto riesgo, supervisando la frecuencia cardiaca del feto y en caso de presentarse alguna anomalía, emite alertas instantáneas al médico tratante[162].

4.6 SMART ENVIRONMENT (Entorno Inteligente)

La expansión urbana hacia nuevos territorios, ha generado un impacto en el medio ambiente, pues significa nuevos consumos de recursos naturales, agua y energía, además de generar desechos y emisiones de gases, por este motivo, un entorno inteligente se convierte en un apoyo para los desafíos de sostenibilidad que se pueden ver desde dos enfoques, el primero es de prevención y consumo de energía ; *involucrando energía renovable, redes tecnológicas, control de la contaminación y gestión, edificios verdes, gestión urbana verde, eficiencia, reutilización, etc.* [163]. La segunda enfocada a la red urbana y la gestión de recursos; residuos, alumbrado público, gestión de residuos, sistemas de drenaje, monitorear los recursos hídricos, reducir la contaminación y mejorar la calidad del agua[163].

Ilustración 59 Servicios que contiene Smart environment. Tomado de Universidad de Alicante, "Smart Environment." [164]***.***

- **Energía (Smart Grid)**: un ambiente inteligente busca optimizar los diversos recursos presentes en el desarrollo urbano, para garantizar la sostenibilidad del mismo, para ello se implementa una combinación de redes eléctricas y tecnologías de vanguardia que va desde sensores, big data y métodos de control que satisfacen la comunicación bidireccional entre la red eléctrica y el usuario o industria, de esta forma monitorea el consumo y la eficiencia energética, entre los deberes de una red eléctrica inteligente está presente facilitar la incorporación de las energías renovables, la seguridad del suministro, tener pérdidas bajas y altos niveles de calidad [163].

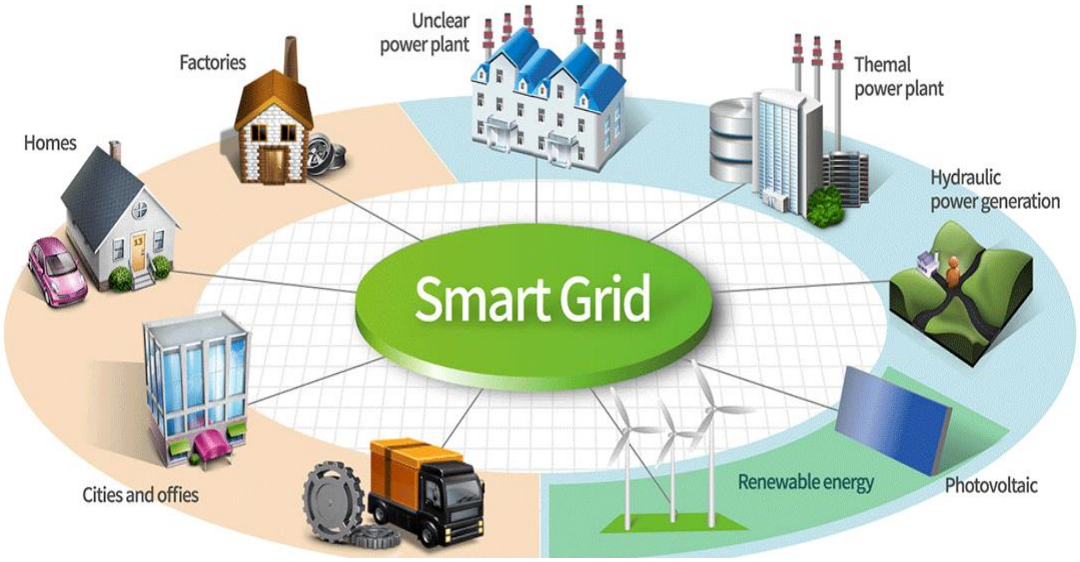


Ilustración 60 Implementación de Smart Grid. Tomado de Universidad de Alicante, "Smart Environment." [164]

- **Agua (Smart Water):** gracias al apogeo del internet de las cosas, servicios en la nube y tecnologías de la información enfocados a la industria, se cuenta con sistemas de redes inteligentes de regulación y automatización en el servicio del agua, estas se encargan del control de suministro, gestión y diagnóstico de calidad, en cada una de las fases que maneja una planta de agua, en su mayoría se implementan sensores de nivel, temperatura, contaminación y abastecimiento, dichos dispositivos y sistemas recopilan volúmenes de datos que tras ser analizados pueden ser de tipo diagnóstico, predicción o emergencia, con dicha información y herramientas de simulación, se modelan escenarios como la hidrodinámica del agua y la calidad del agua en cuencas hidrológicas complejas. [164]

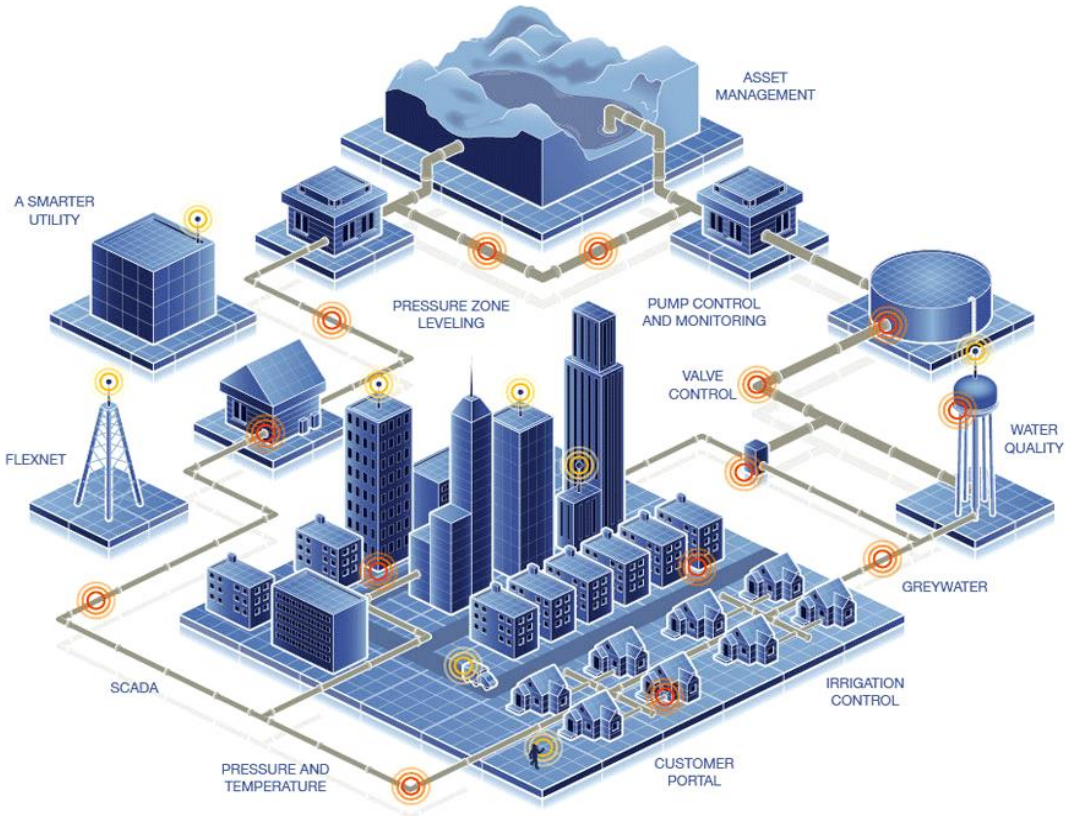


Ilustración 61 Implementación de smart water en una ciudad. Tomado de Jaladhi, "Jaladhi Automations Pvt. Limitado." [165]

- **Residuos (Smart Waste):** para que las ciudades sean más ecológicas, se hace necesario implementar soluciones innovadoras en la gestión de procesos de recolección de los residuos, permitiendo a los ciudadanos y a las empresas gestionar los residuos de manera rentable y responsable con el medio ambiente para mejorar el bienestar de las personas. A través del uso de una tecnología única en la gestión inteligente, algunas empresas de recolección están redefiniendo la manera en la cual se gestionan los residuos. Esta solución combina sensores inteligentes ultrasónicos que monitorean en tiempo real cualquier tipo de desperdicio (desechos mezclados, papel, plásticos, vidrio, ropa, residuos biológicos, metal, etc.), además los sensores pueden ser equipados con una alarma contra incendios y un sensor que indica que el contenedor no está en su lugar, por otro lado, informa a los ciudadanos por medio de una aplicación, cual contenedor vacío es el más cercado. Al proporcionar

esta información en tiempo real se promueve la reducción de residuos, el aumento en el porcentaje de reciclado y la eficiencia en el servicio[166].

Además de la monitorización y control de llenado en tiempo real de los contenedores, smart waste ofrece las siguientes funciones y beneficios[167]:

- Planificación inteligente de la recolección de la basura.
- Uso de vehículos híbridos o eléctricos que reduzcan las emisiones.
- Mejora de la eficiencia del negocio (reducción del costo operacional de la recolección de basura).
- Mejora de la calidad de vida de los ciudadanos (reducción de las emisiones de gases, contaminación acústica y del desgaste de las carreteras).
- Detección de anomalías y problemas de seguridad.

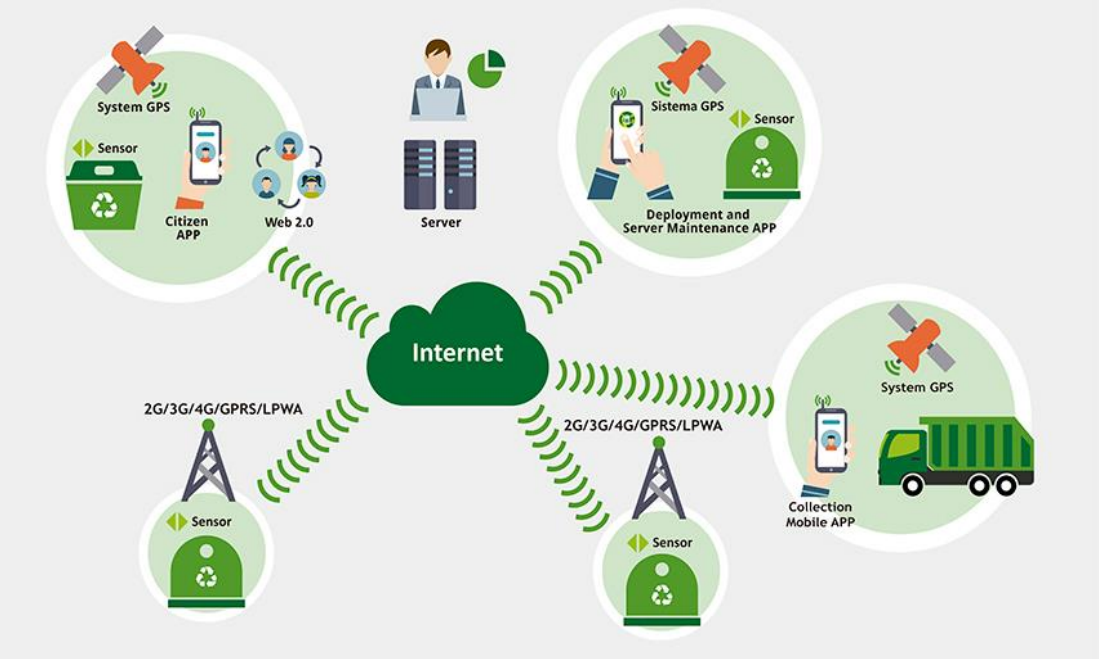


Ilustración 62 Smart Waste. Tomado de Quamtra, "Smart Waste Management Solution Based on Real-Time Data | Quamtra." [168]

- **Medio Ambiente (Smart Green):** gracias a la revolución digital y el uso masivo de tecnologías, la demanda en el consumo energético aumenta exponencialmente a nivel mundial, siendo este uno de los mayores contribuyentes en las emisiones de CO2 (Dióxido de Carbono), por ello se busca brindar soluciones energéticas, sostenibles y rentables con la ayuda de energías renovables, además mejorar el uso eficiente de la energía. Smart green tiene como objetivo la integración de edificios eco-sostenibles que están diseñados para cumplir ciertos objetivos, como la protección de la salud de sus ocupantes, mejorar la productividad de los empleados, usar los recursos de manera eficiente y reducir el impacto global en el medio ambiente; de igual forma se pretende integrar el uso de vehículos inteligentes, entre otras soluciones tecnológicas innovadoras que ayuden a proteger el medio ambiente. [169]

4.7 SMART TRANSPORT AND MOBILITY (Transporte y Movilidad Inteligente)

En la actualidad el tráfico urbano se ha convertido en uno de los problemas más influyentes en la calidad de vida de los ciudadanos, por este motivo se implementó el sistema de transporte inteligente que está enfocado en automatizar la manera en la que se proporciona información sobre el tráfico en tiempo real a los conductores, y tiene como objetivo mejorar la seguridad, la eficiencia en el transporte, ahorrar energía, minimizar el impacto ambiental, y además facilitar la labor de control, gestión y seguimiento por parte de las entidades responsables. [170], [171]zz

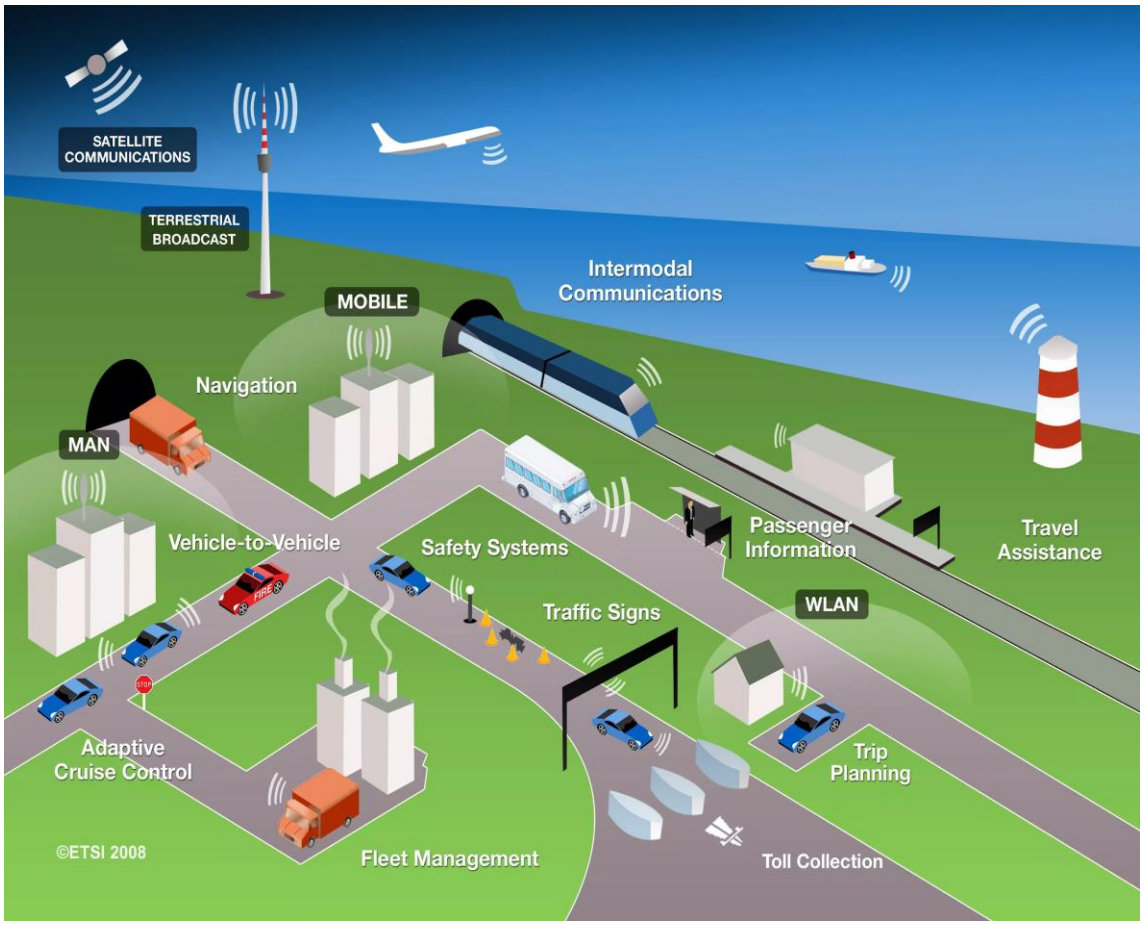


Ilustración 63 Sistema de transporte Inteligente. Tomado de Sandacom, "ITS – Intelligent Transportation Systems – Part 1, Introduction | Innovational Musings". [172]

La tecnología que se utiliza para los Sistemas Inteligentes de Transporte (SIT) es muy amplia, sus dispositivos inteligentes van desde cámaras multiespectrales, sensores como infrarrojos, sensores magnéticos, CMOS (sensor de píxeles activos), etc., que contribuyen a optimizar el transporte y la movilidad en el ámbito urbano, interurbano, autopistas o autovías. [173]

Smart mobility tiene diversas consideraciones que se deben proyectar para una movilidad inteligente y sostenible, la cual debe garantizar la accesibilidad a los sistemas de transporte, reducir los problemas ambientales y la gestión de parqueaderos que se ajusten a las necesidades económicas, sociales y de la ciudad. Además, Smart Mobility prioriza el uso de medios de transporte limpios y no motorizados en determinadas zonas, para reducir las emisiones de gases de Co2. [174]

4.7.1 Aplicaciones y estrategias para Smart Mobility y Sistemas de Transporte Inteligente

Seguridad: se han diseñado sistemas de detección y control del entorno de la infraestructura vial y los vehículos, con la finalidad de reducir anomalías e incidencias en la vía, notificando al conductor y a los sistemas de vigilancia la proximidad y detección de posibles obstáculos (por ejemplo presencia de peatones, ciclistas, animales en la vía), condiciones de colisión, vehículos detenidos o en sentido contrario, entre otros, con la ayuda de sensores incorporados en los automóviles y en la infraestructura vial. [173]

Fiscalización electrónica: es un sistema de inspección de vigilancia y control del tránsito, mediante el uso de equipos electrónicos controlados desde el centro de gestión de movilidad, por ello se han implementado las siguientes soluciones [175]:

- **Detección electrónica de infracciones:** con el uso de sistemas tecnológicos, se recopilan videos, fotografías y datos en tiempo real; que facilitan determinar si un vehículo ha cometido una infracción, de acuerdo con las normas de tránsito establecidas.
- **Conteo y clasificación de vehículos**: esta solución es una aplicación útil en la toma de decisiones para la planeación de tráfico y programación de semáforos.
- **Análisis de origen/destino**: a través de un aforo electrónico vehicular, los sistemas de fiscalización permiten establecer el origen y el destino de los vehículos, facilitando la planeación de servicios de transporte y tránsito.
- **Vehículos robados/embargados/con limitaciones:** facilitan a las autoridades el control e identificación de vehículos con alguna novedad legal.

Centros de gestión de tráfico: se han posicionado como los cerebros en la movilidad, a través de esta entidad se logra una eficiente y óptima atención

respecto a los incidentes que se presentan en las vías, para así mejorar la seguridad y calidad de vida a los ciudadanos. Entre los servicios se gestionan están los siguientes [175]:

- Asistencia de accidentes.
- Sala de situación.
- Monitoreo sistemas de foto detección.
- Monitoreo CCTV (circuito cerrado de televisión).
- Control de patrullas.
- Integración con policía, bomberos y ambulancia.
- Paneles de mensaje variable.
- Semaforización.
- Estadísticas de tráfico.

Información al viajero: ofrece información sobre la programación y tiempos de viaje en los servicios de transporte público, y también muestra a los conductores las mejores rutas y actualizaciones de las condiciones de tráfico, como estados de la vía, incidentes, etc. [172].

Información de transporte público/paradas de autobús y estacionamiento: divulgar información en tiempo real acerca de los horarios, rutas y vacantes de los autobuses, por medio de dispositivos móviles y paneles de visualización en las paradas [176].

Comunicaciones "Vehicle to Vehicle (V2V)" y "Vehicle to Infrastructure (V2I)": para mejorar la seguridad, tiene como objetivo mejorar la convivencia entre los coches y en el entorno por el cual se movilizan[173].

Ilustración 64 Sistemas y redes de monitoreo y vigilancia en el sistema de transporte. Tomado de SITT CIA, "Sistemas Inteligentes de Transporte [177]

Los casos de éxito de Sistemas Inteligentes de Transporte (ITS) han logrado los siguientes resultados [175]:

- Reducción de accidentes.
- Reducción en tiempos de respuesta.
- Reducción en tiempos de viajes.
- Reducción de contaminación ambiental.
- Reducción costos operativos de las vías.
- Incrementar la movilidad del tráfico

4.8 SMART GOVERNANCE (Gobernanza inteligente)

La gobernanza se define según la real academia española como: *el arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía* [178].

A raíz de la adopción masiva del internet, redes sociales, la conectividad 4G, la facilidad para obtener dispositivos y servicios inteligentes, por parte de la

población general, las entidades de gobierno han implementado sistemas de participación ciudadana, es decir, que existe una comunicación entre las personas y los funcionarios públicos a través de plataformas interactivas, donde las tecnologías de comunicación (TIC) juegan un papel protagónico en el desarrollo de servicios para la gestión en territorios digitales, la respuesta y prevención de desastres naturales, la resolución de conflictos, la eficiencia de recursos y estados de opinión online por parte de la ciudadanía, además las TIC protegen la identidad y privacidad de datos de los involucrados, esto crea una sensación de confianza y transparencia. Las plataformas o aplicativos canalizan con más eficacia las demandas, dicho de otra manera, puede filtrarlas por nivel de relevancia, esto ahorra tiempos de trámite, respuesta y costos, de ahí que la sociedad es cada vez más participativa en las decisiones de gobierno.

Dentro del smart governance se encuentran las plataformas educativas basadas en servicios alojados en la nube, los sistemas de mapeo y de información geográfica, también está presente el tema de desechos tecnológicos, su debida recolección y posterior eliminación o reutilización para mermar daños al medio ambiente y la salud humana, además de ello facilita el acceso a datos abiertos del gobierno, de esta manera convierte al ciudadano no sólo en receptor de servicios sino también en un colaborador activo [178].

Componentes de un gobierno inteligente

- Partes interesadas.
- Estructuras y organizaciones.
- Procesos.
    - Intercambio de información
    - Compromiso.
    - Toma de decisiones.
    - Implementación.
- Roles y responsabilidades.

- Datos y tecnologías.
- Legislación y políticas.
- Arreglos de intercambio de información.

Definiciones de Gobierno Inteligente [179]**:**

"Un Gobierno Inteligente no es aquel que solamente incorpora tecnología, si no aquel que pone al ciudadano en el centro de la gestión, que aplica la tecnología para desarrollar procesos para servir a los ciudadanos, que las utiliza para escuchar sus opiniones y demandas, para crear espacios abiertos dinámicos y permeables" [180].

"Nuestro rol como Estado es administrar la incertidumbre; no hay que temerle al cambio, sino hacer que los avances tecnológicos estén al servicio de la gente. Cambiarles la vida a los ciudadanos" [181].

"El desafío de las ciudades para convertirse en "inteligentes" no pasa por cuestiones de dimensión, plazo o desarrollo de herramientas propias. Pasa por aprender a dialogar y generar interfaces válidas y dinámicas entre lo público y lo privado y un equilibrio entre la política y la tecnología" [182].

5. IMPLEMENTACIÓN DE IoT en LATINOAMÉRICA

Según la consultora Machina Research, Latinoamérica tendrá una tasa de crecimiento del 26,95% anualmente en adopción de ecosistemas IoT y Evans Corporation informa que un 60% de los nuevos proyectos de desarrollo tecnológico en Latinoamérica están orientados a servicios IoT y un 22% ya se están ejecutando[183].

En septiembre de 2017, São Paulo organizó la segunda feria comercial latinoamericana enfocada en el Internet de las Cosas, para educar al público sobre la importancia de IoT para el desarrollo en América Latina. Brasil se encuentra entre unos pocos países, junto con Argentina, Chile y México, que están comenzando a adoptar el IoT de manera más amplia[183].

Aun cuando Latinoamérica desea crecer en el ámbito IoT, posee bastantes barreras a superar. El centro de estudios de Telecomunicaciones de América Latina conocido por sus siglas como Cet. ha identificado y punteado a los países latinoamericanos según el grado de adopción IoT que poseen, se basan en la infraestructura de regulación TIC, la adopción tecnológica en empresas, la situación política y económica, la adecuación del marco regulatorio, la capacidad para innovar y las habilidades del personal profesional de cada país[184].

Puesto 1

Chile destaca en el ranking como líder para la adopción del IoT en la región de América Latina. Presenta buena puntuación en la mayoría de indicadores, estando en la mayoría de casos por encima de la media en LAC[184].

Puesto 2

Costa Rica obtiene la segunda mejor puntuación de entre los países de interés para este estudio, solo superado por Chile[184].

Puesto 3

Brasil destaca por su alta puntuación en capacidad para innovar, situándole a la altura de referentes mundiales como pueden ser Nueva Zelanda y Noruega. Por este motivo, la capacidad para innovar debería ser vista como palanca para propulsar el resto de aspectos en los que el país debe mejorar[184].

Puesto 4

México, obtiene una puntuación en el índice ligeramente superior la media de la región. La principal fortaleza se observa en el uso que hace la población de las tecnologías. Por otro lado, y como principal punto de mejora destaca la baja puntuación en la barrera regulatoria[184].

Puesto 5

Argentina se sitúa en la media de la región, destacando sobre todo en el indicador regulatorio. Este hecho puede ser visto como principal oportunidad para el país, que puede ser visto como líder regional en materia regulatoria[184].

Puesto 6

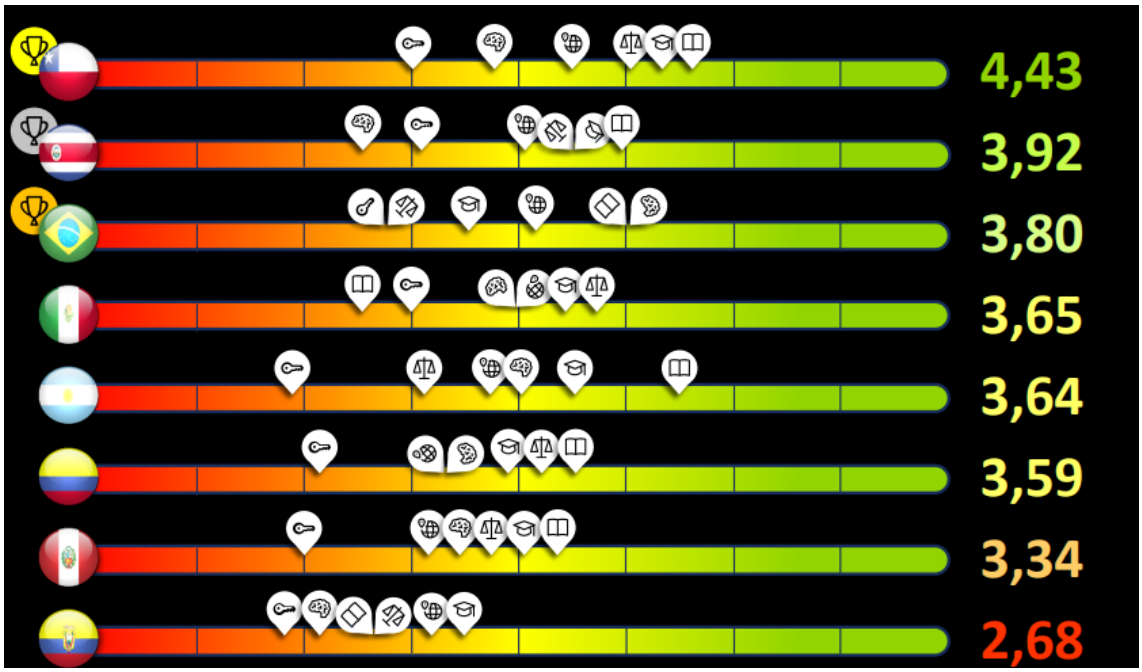
Colombia se encuentra, también muy en sintonía con la media en la región LAC. Destaca su puntuación estabilidad política y regulatoria, siendo los principales puntos de mejora el despliegue de una mejor infraestructura, que actúe como base de cualquier sistema IoT y la capacidad y la actitud frente a la innovación[184].

Puesto 7

Perú debe fijar objetivos para la mejora en las barreras de capacidad innovadora e infraestructura TIC, puesto que no se está viendo aprovechado el potencial del que dispone el país en ambas[184].

Puesto 8

Ecuador es el país con peor puntuación de aquellos contemplados como generadores del 90% del PIB de la región. Aparece a la cola del ranking en el índice de adopción del IoT. Su posición es poco favorable en la mayoría de barreras, siendo sus principales retos la regulación y la adopción de nuevas tecnologías en empresas[184].



Gráfica 3 Grado de adopción del IoT y puntuación en el índice de los países de interés. Tomado de "IoT para el sector empresarial en América Latina" [184]

5.1 Diagnóstico tecnológico de América Latina vs los países pertenecientes a la Organización para la Cooperación y el Desarrollo Económicos (OCDE)

Indicador	OCDE	América Latina
Banda ancha velocidad promedio	16,7 Mbps	6,4 Mbps
Capacidad para innovar (porcentaje de gasto bruto en investigación y desarrollo en relación al PIB)	2%	1%
Desarrolladores de software (porcentaje de población)	1%	0,1%
Eficiencia de organismos regulatorios (puntuación)	4	2,7
Facilidades para pago de impuestos (puntuación)	80	48,7
Facilidades proceso de resolución de insolvencias	83	53,5
Habilidades (graduados en carreras superiores técnicas como porcentaje del total de graduados)	16%	12,6%
Investigadores por millón de habitantes	4143	529
Legislación relativa a TIC (puntuación)	5	3,7
Protección de propiedad intelectual (puntuación)	6	4
Servidores de Internet seguros por cada millón de habitantes	1253	52,2
Usuarios de Internet (porcentaje de población)	79%	57,8%

Tabla 9 Diagnóstico tecnológico de América Latina vs los países OCDE [184]

5.2 CASOS DE USO

5.2.1 Smart Farming (Agricultura Inteligente)

La implementación de la agricultura inteligente, se ha convertido en una tendencia importante en este sector, debido a ello las empresas agroalimentarias están aumentando las inversiones para integrar soluciones IoT en algunos de sus procesos, para así mejorar la calidad de las cosechas, aumentar la producción, reducir costos y así facilitar algunas tareas cotidianas de los agricultores. [185]

5.2.1.1 Mejorando la producción de cultivos de banano y la sostenibilidad agrícola en Colombia utilizando redes de sensores

Una de las implementaciones de IoT en Colombia es Red Tecnoparque, este programa innovador pertenece al SENA Regional de Risaralda, que tiene como objetivo agilizar el desarrollo de proyectos de I+D+I (Investigación, desarrollo e innovación), de ahí que esta organización ha implementado tecnología IoT de Libelium (Empresa multinacional tecnológica española), el proyecto se basa en una red de sensores inalámbricos para monitorear los cultivos de plátano en el área de Lembo, en la región de Santa Rosa de Cabal (Risaralda). [186]

El cultivo de plátano, representa el 9,69% del valor de la producción agrícola y su producción anual se estima alrededor de 3 millones de toneladas en un área de 380,000 hectáreas. Colombia es uno de los mayores exportadores a nivel global, por ello se pretende mejorar y aumentar la productividad de este cultivo. [186]

Los cultivos de plátano son monitoreados y supervisados de manera remota sobre las variaciones ambientales y agronómicas, como la humedad y temperatura del suelo, diámetro de la fruta y el tronco, radiación solar, entre otros parámetros. Estos datos son enviados a la nube a través de redes 3G y

GPRS, para ser visualizada desde cualquier dispositivo móvil o computadora. [187]

La monitorización del cultivo permite conocer la proyección de la cosecha, ayuda a prevenir las enfermedades, optimiza el uso del agua y reduce el consumo de fertilizantes. [187]

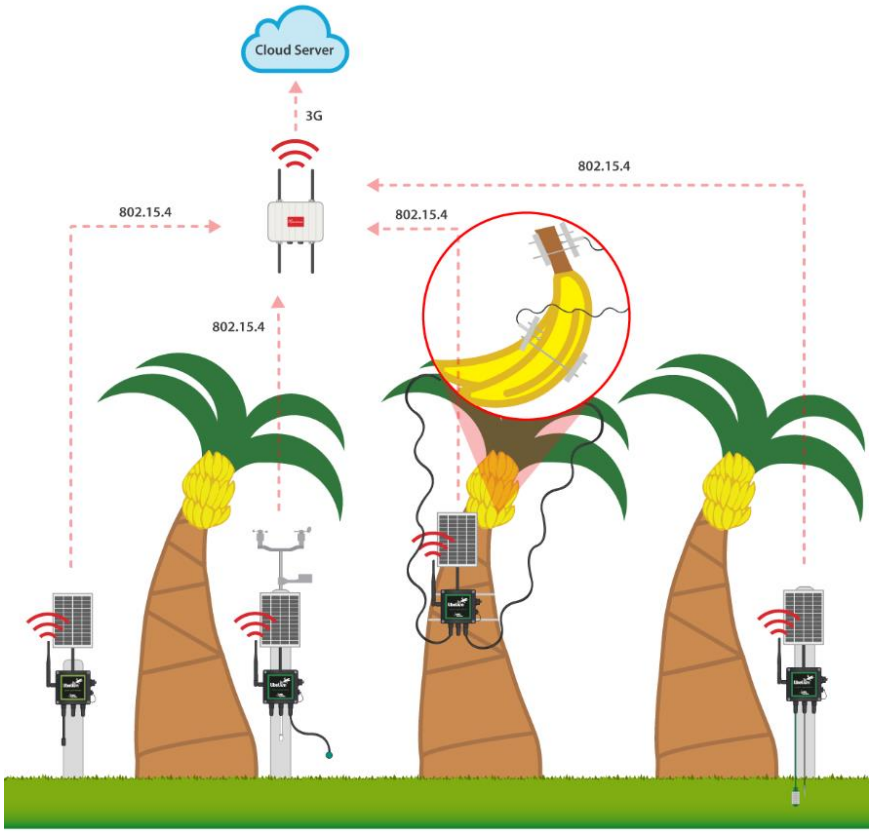


Ilustración 65 Diagrama de funcionamiento de cultivos de plátano. Tomado de Libelium, "Improving banana crops production and agricultural sustainability in Colombia using sensor networks" [187]

5.2.1.2 Monitorización del ganado en Colombia para aumentar la fertilidad.

Claro (Grupo América Móvil) y Celotor en Colombia, han implementado una aplicación IoT para el sector agroindustrial para la monitorización del ganado, permitiendo a los ganaderos detectar el celo de las vacas y así facilitar el proceso reproductivo por inseminación artificial, duplicando las probabilidades

de fecundación; los chips son inyectados en la cola de la vaca. Cada chip es programado con la identificación (nombre y/o número) de cada vaca. [184][188]

Ilustración 66 Se instalan arnés flexible las vacas machorras y toros celadores. Tomado de Celotor, "Instalación y Uso - Celotor - Detector de Celo Bovino." [188]

5.2.1.3 Brasil desarrolla plataforma IoT para riego inteligente del agua

Investigadores brasileños están desarrollando métodos para riego inteligente del agua en el regiones del Sureste y Noroeste de Brasil, el proyecto consiste en una plataforma de gestión inteligente del agua, tiene como objetivo proporcionar al agricultor un mapa diario de recomendación dinámica de riego localizado, teniendo en cuenta un conjunto de información recopilada en tiempo real del clima, el suelo, condiciones del cultivo, al igual que los niveles y la calidad de los sistemas de suministro y la distribución del agua en el área. [189]

Teniendo en cuenta la creciente escasez de agua, se pretende optimizar el recurso natural y resolver la alta demanda de producción[189]. Esta plataforma inteligente de riego, se ha utilizado inicialmente en la producción de soja y vinicultura (Elaboración y crianza del vino). [184]

5.2.1.4 Chile despliega una experiencia pública de IoT en agricultura.

Con la colaboración de la Subsecretaría de Telecomunicaciones (Subtel), el Instituto Nacional de Investigaciones Agropecuarias (INIA) y Telefónica I+D (Investigación y Desarrollo), se realizó el proyecto “Piloto de Agricultura de Precisión”, con la iniciativa de buscar nuevas propuestas y soluciones para el manejo del riego, y a su vez suministrar de tecnología a los medianos y pequeños agricultores. Con la finalidad de optimizar el uso del agua se implementan sensores que recolectan datos de la humedad del suelo, luego son analizados y se estable la cantidad de agua adecuada para cada área, con ello se busca aumentar la producción. [190]

5.2.2 SMART ENVIRONMENT

5.2.2.1 Monitoreo del clima y las condiciones del agua para controlar el cambio climático en el Parque Nacional de Manú en Perú

El parque Nacional del Manú, es un espacio natural protegido y considerado una de las reservas más impresionantes del mundo, es el hábitat de gran biodiversidad de animales y plantas. Esta reserva natural está siendo amenazada por el cambio climático, por ello un grupo de investigadores de RFID Radical Solutions han liderado un proyecto con el objetivo de monitorear el comportamiento de la naturaleza en tiempo real, con el uso de sensores Libelium para recopilar información del suelo, el agua, y el aire, está información recolectada es enviada a la nube con el uso de los protocolos LoRa y 3G. Los sensores instalados en el área, supervisarán el estado de la fauna y flora. [191]

5.2.3 SMART HEALTH

Las soluciones IoT en la salud, ayudarán a reducir costos y optimizar los servicios ofrecidos por este sector, al igual busca mejorar la calidad de vida en pacientes crónicos proporcionando tratamientos más acertados. [184]

El sistema de salud inteligente puede aprovechar los beneficios ofrecidos por IoT, para tener una información detallada sobre la ubicación de los activos en los centros de salud, y a su vez maximizar su uso. Al igual que implementar soluciones IoT para la atención médica en zonas rurales, que cuentan con escasos recurso en los centros de atención que evitan proporcionarles una mejor calidad de vida. [184]

5.2.3.1 Monitorización de Bolsas de Sangre- Veracruz (México)

En Veracruz (México), utilizan tecnología RFID y sensores de temperatura para el rastreo de bolsas de sangre. Con la finalidad de mejorar el control de este recurso, las bolsas de sangre son almacenadas en racks (Gabinetes) que están localizados en refrigeradores a una temperatura cercana a los 4ºc, cada bolsa tiene una etiqueta RFID y una antena transmisora UHF, los datos monitoreados son guardados en estas etiquetas y pueden ser supervisados desde cualquier dispositivo móvil que cuente con acceso al software de la compañía. [184]

5.2.3.2 EMITI, WEARABLE PARA LA MONITORIZACIÓN DE PACIENTES DE TELCEL (Empresa de telefonía mexicana)

Esta operadora móvil ha impulsado en el mercado un wearable Emiti, que es un reloj inteligente capaz de medir por medio de sensores toda actividad física de la persona que lo tenga puesto, como informar a los familiares o cuidadores en caso de un incidente, enviar la ubicación exacta del paciente, monitorear el ritmo cardíaco, oximetría, entre otras variables fisiológicas. Los datos recopilados pueden ser vistos en tiempo real a través de la página web desde cualquier dispositivo inteligente. [184]

5.2.3.3 Soluciones portátiles para ecografías para América Latina y el Caribe

En la región de América Latina, existe un alto porcentaje de zonas rurales, por ello la implementación de soluciones IoT son muy importantes para estas áreas, en donde la atención médica dispone de menos recursos. [184]

Entre los países más afectados en la región de América Latina se encuentran Guatemala, Honduras, República Dominicana, Guyana, Haití, Jamaica, Surinam, Bolivia y Ecuador, que superan la mortalidad maternal de 100 por cada 100.000 nacidos. El proyecto de ecografías portátiles fue desarrollado y premiado por GSMA en 2011 se empezó en diversas zonas de Guatemala. [184]

5.2.4 Ciudades Latinoamericanas consideradas Smart City. [192]

1. **Santiago de Chile.** [193]
    - Los precios de los peajes están automatizados dependiendo el flujo del tráfico.
    - Tiene el gobierno menos corrupto de la región (Gobierno Inteligente y transparente).
    - Movilidad sostenible y de acceso igualitario.
    - Eficiencia energética (hace uso de energía solar y paneles solares).
    - Tiene el metro con más uso en la región.
    - Catalogada como la mejor ciudad para hacer negocios.

2. **México DF.** [192]
    - Pioneros en la construcción de edificios inteligentes y sostenibles.
    - Algunos edificios usan tecnología que absorben la contaminación.
    - La ciudad cuenta con más de 4.000 bicicletas públicas (Iniciativa para crear un smart green).

3. **Bogotá.** [192]
    - Tiene el mejor sistema de rutas para bicicletas, con una amplia conexión al sistema de transporte masivo.
    - El sistema de transmilenio transporta a 1,65 millones de personas al día.
    - Se espera que antes de la próxima década tenga un sistema de metro eléctrico subterráneo.
4. **Buenos Aires.** [192]
    - Combinó la renovación urbana con el desarrollo grupal a través de la inversión en sectores marginados.
    - Creó el Ministerio de la Modernización e implementó una amplia red pública de Wifi.
    - Gobierno Inteligente.
    - Se generó más de 150.000 empleos con la finalidad de implementar tecnología, diseño, mejorar el servicio de salud, etc.

5. **Rio de Janeiro.** [194]
    - Centro de operaciones con la ayuda de IBM para monitorear en tiempo real el tráfico, crímenes, el clima, vigilancia y emergencias.
    - Integración de equipos de red de tráfico como semáforos, carteles de mensajería variables, sensores, etc.
    - Seguridad ciudadana.
    - Energía eficiente.
    - Ambiente Inteligente.
    - Contratación de personal joven para la contribución de puntos con problemas de acumulación de basuras, por medio de registros de imágenes digitales.
    - Renovación y desarrollo como ciudad inteligente y autosostenible para ser sede olímpica y anfitriona de la copa mundial de fútbol.

6. **Curitiba (Brasil).** [192]

- Considerada como la ciudad más ecológica de Latinoamérica según el ranking de Siemens.
- Utilización de buses como sistema de transporte masivo.

7. **Medellín.** [195]
    - Fue catalogada como la ciudad más innovadora del año en el 2013.
    - Reconocida por el metro como su sistema de transporte masivo.
    - Infraestructuras atractivas como museos.
    - Sistemas de alertas tempranas.
    - Sistema de seguridad Urbana.
    - Centro de control del tránsito.
    - Control de flota de transporte público.
    - Detección electrónica de infractores.
    - Paneles de mensajería variables (muestran información de incidentes de tránsito, mensajes de educación vial, inicio y fin de restricción vehicular).
    - Edificios Inteligentes.
    - Centro de control de semáforos.

8. **Montevideo.** [192]
    - Es catalogada como la ciudad con mejor calidad de vida en Latinoamérica.
    - Es la ciudad con mayor cantidad de exportaciones de exportaciones de software.
    - Es un centro de emprendimiento cultural y tecnológico, además cuenta con programas universitarios que apoyan a este sector.

6. DESAFÍOS PRESENTES EN IoT.

Para acceder a servicios IoT se implementan objetos inteligentes como elementos de localización, sensores biomédicos y elementos cotidianos como relojes y teléfonos inteligentes, que poseen la capacidad de compartir datos procesados o en bruto por medio de una red de internet.

La conexión de muchos objetos a internet opera por medio de nodos inteligentes, estos nodos se encargan de la transmisión de datos superficiales, de acceder y autorizar recursos basados en la nube para recolectar información relevante y con ello la posterior toma de decisiones. [196]

La implementación de diversas aplicaciones ha aumentado exponencialmente la cantidad de objetos inteligentes y servicios IoT a nivel global, debido a ese factor de crecimiento se hace necesario considerar los distintos desafíos durante los ciclos de diseño, desarrollo, pruebas y despliegue del hardware y software, por ello es de vital importancia para los proveedores conocer los principales retos que pueden enfrentar en cuestiones de seguridad como la privacidad, el almacenamiento seguro de los datos y la interoperabilidad, conociendo los desafíos que enfrenta se toman medidas que promueven la eficiencia de sus servicios y su impacto en el mercado IoT.

IoT es visto como un ecosistema donde actúan proveedores y usuarios que comparten datos activamente, este ecosistema se compone de objetos, redes,

plataformas y aplicaciones, que necesitan distintos grados de análisis de protección por cada capa y así asegurar la integridad, procesamiento y análisis de los datos que se comparten bidireccionalmente entre los actores del sistema. [1]

Cabe recordar que la capa de percepción debe ser segura contra ataques externos, la capa de red necesita asegurar la agregación y modificación de datos
y por último la capa de aplicación se encarga de autorizar recursos a distintas entidades que hacen parte del sistema IoT. [197]

Otro escenario a considerar es la correcta administración por parte del talento humano que se encarga del mantenimiento del ecosistema IoT, en cuanto a servicios y dispositivos, pues juega un papel importante ya que deben tener en cuenta la heterogeneidad connatural de los ambientes IoT, y los diversos factores a enfrentar si se quiere lograr escalabilidad. [29]

6.1 Consideraciones de seguridad en IoT. [29]

Consideraciones	Descripción
Superficie de ataque muy grande	Se debe considerar que IoT ha tenido un gran impacto en el mercado, por ello los usuarios usan sus servicios en diferentes aplicaciones, sin conocimiento del procesamiento de los datos, permitiendo que IoT tenga acceso en muchas ocasiones a sus datos confidenciales, y así estar expuesto a diversas amenazas.
Dispositivos con recursos limitados	No se pueden llevar controles de seguridad avanzados de manera efectiva en dispositivos con limitaciones de memoria, alcance y procesamiento.
Ecosistema complejo	IoT debe tomarse como un ecosistema que involucra dispositivos, comunicaciones, interfaces y personas,

	por ello mantener su seguridad y correcto funcionamiento resulta complejo.
Fragmentación de ataques y regulaciones	La adopción segmentada y lenta de las regulaciones y los estándares en pro de medidas de seguridad y buenas prácticas IoT, pueden solucionar un problema y dejar otros.
Despliegue generalizado	Además de las aplicaciones IoT actuales, se deben sumar las migraciones masivas de arquitecturas críticas al ambiente inteligente, de ahí que se implementa IoT en la capa superior de infraestructuras heredadas.
Integración de seguridad	Es una misión muy desafiante, ya que existen distintos puntos de vista y condiciones que pueden ser contradictorias en todas las partes interesadas.
Bajo costo	El bajo costo que generalmente se asocia con los dispositivos que integran sistemas IoT, puede afectar la seguridad de hardware y software, ya que los fabricantes pueden inclinarse a limitar las características de seguridad para garantizar un bajo costo y, por lo tanto, la seguridad del producto podría ser fácilmente burlada.
Falta de experiencia	Como es un sistema muy reciente, los conocimientos y la experiencia en su desarrollo no son los adecuados haciendo que sea vulnerable a ataques cibernéticos.
Actualizaciones de seguridad	La aplicación de actualizaciones de seguridad en los servicios IoT es desafiante, ya que las interfaces disponibles para los usuarios, no permite a los mecanismos habituales asegurar que se actualicen de manera automática.
Programación insegura	Debido al crecimiento exponencial de ecosistemas IoT, los proveedores de

	servicios se centran más en la funcionalidad y la usabilidad que en la seguridad, no sólo por la competencia en el mercado sino también por motivos de tiempo y presupuesto en la etapa de diseño y desarrollo.
Obligaciones poco claras	La carencia de obligaciones, generan en muchas ocasiones colisiones y ambigüedades de inseguridad.

Tabla 10 consideraciones de seguridad IoT. [29]

6.2 Principales desafíos de seguridad en el desarrollo de software de ambientes IoT

6.2.1 Autenticación

Los sistemas que manejan una comunicación entre dispositivos IoT, requieren de un proceso de autenticación entre nodos de origen y destino de transferencia de datos, es decir, los pares de enrutamiento, para ello es necesaria la creación de claves criptográficas seguras y la administración de las mismas, sin llegar a sobrecargar el flujo de datos entre los nodos. [198]

Para garantizar la autenticación se recurre a algoritmos de encriptación, distribución de claves políticas, mecanismos de detección de intrusos y las políticas de enrutamiento, para ello es necesario conocer las restricciones de hardware y software de los dispositivos inteligentes que establecerán una comunicación. [198]

6.2.2 Control de acceso

Consiste en la administración de los derechos de acceso que se otorgan a las entidades que hacen parte del sistema, con ello pueden acceder a los diferentes recursos autorizados, bajo la supervisión de mecanismos de control. [199]

Cada nodo de IoT debe soportar los mecanismos de control necesarios para la identificación de objetos que se conectan al mismo nodo, se considera como un desafío en redes heterogéneas, gestionar múltiples autorizaciones por medio de mecanismos de control de acceso que se adapten a cada nodo de la red a la que se encuentran conectados. [199]

6.2.3 Privacidad

En las redes IoT los nodos reúnen información privada sin darse cuenta. Actualmente los mecanismos suministran privacidad centrada en el usuario, orientada al contenido o dirigida al contexto, no obstante, los sistemas IoT recolectan todo tipo de información, desde datos privados de los usuarios hasta datos de hardware y software, por ello necesitan modelos de privacidad idóneos para los objetos. Actualmente existen normativas de privacidad que exigen informar a los usuarios hasta qué punto sus datos privados son gestionados y administrados. [200]

6.2.4 Interoperabilidad

Es un término implementado por la industria de la tecnología de la información (TI) para definir una forma ideal en que los diferentes sistemas de información, tecnologías y dispositivos electrónicos que pertenecen a distintas plataformas se relacionan entre sí, es decir, que puedan comunicarse e intercambiar datos sin restricción alguna, aunque sus protocolos y codificaciones sean distintos.[201]

El hardware y software son dos perspectivas muy importantes para que la interoperabilidad sea un hecho sin importar si es o no compatible con otros ecosistemas IoT, debido a ello se debe tener en cuenta las siguientes capas [202]:

- **La capa dispositivo**, permite la integración de múltiples dispositivos y además se encarga de analizar los flujos de datos que llegan desde diferentes servicios de ecosistemas IoT, por ello es importante considerar esta capa para la interoperabilidad en IoT.[203]
- **La capa de red,** se encarga del enrutamiento, la comunicación y la información de los dispositivos, por ello se debe asegurar la interoperabilidad de protocolos de comunicación entre los mismos.[203]
- **Capa middleware**, posibilita a los servicios IoT interactuar con otras aplicaciones, funciona como una capa de traducción para permitir la administración de los datos almacenados y la comunicación, por ello juega un papel muy importante en la interoperabilidad en IoT, algunos ejemplos de aplicación de middleware son en bases de datos, servidor de aplicaciones, en web, servicios de mensajería, entre otras.[202]
- La **capa de servicio de aplicación**, los servicios IoT manejan diversas plataformas e interfaces para diversos usuarios, el objetivo de interoperabilidad en esta capa es dejar atrás el método de los silos de datos, y reutilizar los mismos en diferentes servicios para un mismo usuario.[202]
- La **capa semántica y de datos**, es la encargada de la traducción e integración de lenguajes de los datos e información.[203]

Gestionar una interoperabilidad transparente en ecosistemas IoT, cuya principal característica es que se componen de miles de millones de dispositivos y protocolos que evolucionan día a día, es un desafío sumamente complejo, actualmente se puede mitigar dicha problemática haciendo uso de estandarizaciones.

A continuación, algunas organizaciones encargadas de definir estándares de comunicación y procesos tecnológicos.[204]

Organizaciones	Ejemplos de estándares importantes en el panorama de interoperabilidad

ISO (International Organization forStandardization)	ISO 10303 (STEP), formalización de datos de producto, ISO 2700x, etc.
IEC (International Electrotechenical Commissoion)	TC 65, para la medida, control y automatización de procesos industriales (integración entre datos de productos y procesos de producción)
IETF - Internet Engineering Task Force RFCs	IP, TCP, UDP, TLS (y otros protocolos de comunicación)
W3C – World Wide Web Consortium	HTMLx, XML, JSON (y otros lenguajes de representación e intercambio de información)

Tabla 11 Organizaciones y estándares de comunicaciones en el panorama de Interoperabilidad.[204]

La seguridad IoT está compuesta por un conjunto de consideraciones que se verán expuestas en la Ilustración 67.

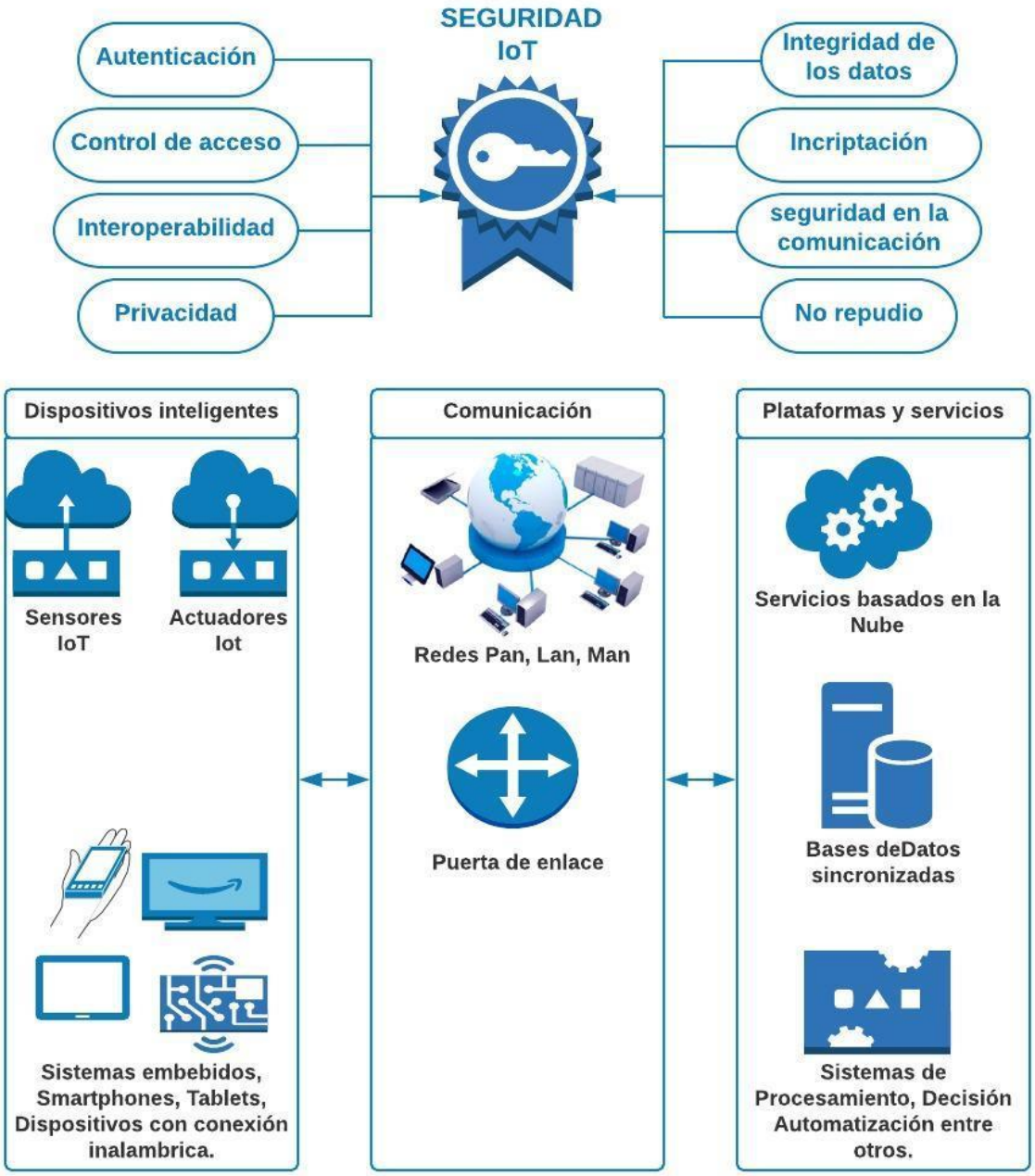


Ilustración 67 Consideraciones de seguridad. [29]

6.3 INCIDENTES DE SEGURIDAD IoT

6.3.1 Puerto Rican Electric Power Authority (PREPA) (Medidores inteligentes puertorriqueños pirateados en 2009)

La autoridad de energía eléctrica de puerto rico, solicitó al FBI que investigara incidentes de robos de energía generalizados, se creía que estaba relacionado con el despliegue de su medidor de energía inteligente. Según el FBI el ataque requirió acceso físico a los medidores inteligentes, y se cree que los antiguos empleados del fabricante del medidor los estaban alterando para reducir las facturas de energía a cambio de dinero en efectivo, para ello piratearon los medidores inteligentes utilizando un dispositivo convertidor óptico, conectado a una computadora portátil, después de hacer esa conexión, la configuración para registrar el consumo de energía se modificó utilizando un software que se podía descargar de Internet. [205][29]

Ilustración 68 Medidores eléctricos hackeados. Tomado de Ireland Elizabeth, "Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread | Metering.com" [205]

6.3.2 Foscam IP baby-cam (Hackeada en 2013)

Investigadores de ciberseguridad descubrieron una vulnerabilidad en las cámaras inalámbricas Foscam, en una presentación titulada "Mirar o ser

observado: volteando su cámara de vigilancia en su contra". Más tarde, el 10 de agosto del mismo año, un atacante se aprovechó de un exploit señalado por los investigadores para agregar su propio nombre de usuario - "Root" - y contraseña para el dispositivo, de esa manera inició sesión y obtuvo el control de una de esas cámaras en Houston, Texas, que se usaba como monitor para bebés. El atacante pudo ver, oír y hablar a través de la cámara, otro caso similar en 2016, una familia de Minnesota, denunció que su monitor de bebés tomaba fotos de su hijo para después publicarlas en Internet.[29]

La vulnerabilidad es que estos dispositivos cuentan con claves de conexión comunes en todos los terminales, con lo que son prácticamente reconocibles y accesibles.[29][206]

Ilustración 69 Monitor para bebés. Tomado de Kashmir Hill, "'Baby Monitor Hack' podría suceder a otros 40,000 usuarios de Foscam" [206]

6.3.3 TARGET (Robo De Datos en 2013)

Entre el 27 de noviembre y el 16 de diciembre del 2013, la cadena de minoristas TARGET fue víctima del robo de información personal de sus consumidores. En época navideña, les robaron unos 70 millones de datos personales de sus clientes, como sus nombres, direcciones, números de

teléfonos y direcciones de email y a otros 40 millones se les robó información de sus tarjetas de crédito y débito. La intrusión en los sistemas de Target se remonta a la red credenciales robadas a un proveedor externo de IoT HVAC (Heating, Ventilating and Air Conditioning) un sistema de climatización inteligente. Se cree que Target permitió a ese proveedor de HVAC el acceso remoto a su red con el fin de informar las fluctuaciones de temperatura. Los piratas informáticos aprovecharon esa situación e instalaron un malware que escaneaba la información de la tarjeta de crédito del cliente cuando el cajero de la tienda efectuaba el cobro, el código malicioso enviaba los datos a un servidor.[207]

Ilustración 70 Sucursal de Target. Tomado de TARGET [207]

6.3.4 VTech (robo de datos 2015)

La compañía china de juguetes inteligentes conectados a internet fue víctima del ataque de un grupo de piratas informáticos, quienes robaron millones de cuentas de clientes y perfiles de niños de todo el mundo, entre ellos, España, EE.UU., Francia, Canadá y Alemania.[208]

Accedieron a los datos almacenados de los clientes en la base de datos de la 'Learning Lodge', que permite a los clientes la descarga de aplicaciones, juegos, libros electrónicos y otros contenidos educativos.[208]

La información personal robada no estaba encriptada, e incluía nombres, direcciones de correo electrónico, contraseñas, preguntas y respuestas secretas para la recuperación de contraseñas, direcciones IP, direcciones postales, historial de descargas, registros de chat y nombres, fotos, géneros y fechas de nacimiento de los niños. [29][208]

Ilustración 71 Productos de VTech. Tomado de VTech.[208]

6.3.5 OVH hosting provider (Ataque DDos 2016)

OVH es un proveedor de alojamiento web y telecomunicaciones francés, que fue atacado por un DDoS, (Distributed Denial of Service), que significa “ataque distribuido denegación de servicio”, dicho de otra manera ataca al servidor desde muchos ordenadores para que deje de funcionar, este DDos es procedente de Mirai botnet, un malware que se enfoca en infectar dispositivos

de baja potencia conectados a internet como routers domésticos, cámaras de vigilancia y de circuito cerrado de televisión, Mirai infectó más de un millón de dispositivos IoT por medio del puerto Telnet. Utilizaron los dispositivos IoT para generar tráfico de red falso alcanzando un punto máximo de 1Tbps en el ataque a OVH, un día después realiza un DDoS al sitio web "Krebs on Security" que superó los 620 Gbps de tráfico, por lo que es también uno de los mayores registros en la historia en términos de volumen. [29]

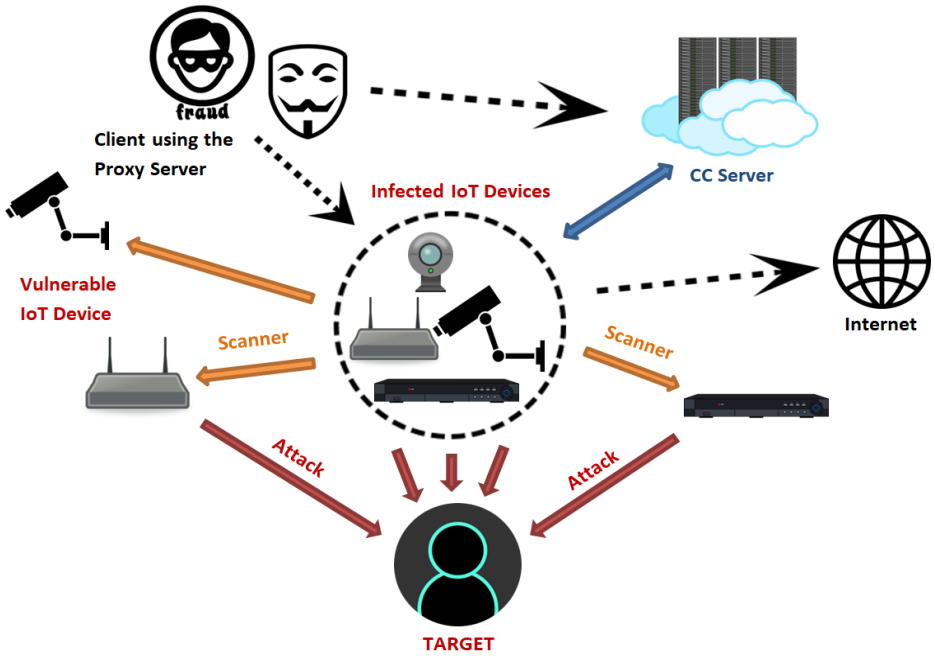


Ilustración 72 Bot basado en Mirai convierte dispositivos IoT en servidores proxy. Tomado de FORTINET, "OMG: Bot basado en Mirai convierte dispositivos IoT en servidores proxy". [209]

6.3.6 Cloudpets (Robo de datos 2017)

La compañía de juguetes de cloudpets vende juguetes que se pueden conectar a internet a través de Android y iOS, con el fin de poder intercambiar mensajes de voz entre amigos gracias al micrófono incluido en el juguete, los niños pueden enviar mensajes a sus padres y viceversa, facilitando la comunicación cuando los padres no pueden estar cerca. [29]

CloudPets utilizaba una base de datos MongoDB y un servidor cloud Amazon, sin configuraciones de autenticación, de ahí que cualquier persona podía entrar y descargar las grabaciones y datos personales de los usuarios, un pirata informático aprovechó dicha vulnerabilidad para secuestrar dicha información y pedir rescate para no hacerla pública 2 millones de grabaciones correspondientes a más 800.000 cuentas diferentes.[29]

Ilustración 73 Juguete CouldPets. Tomado de CouldPets. [210]

6.4 AMENAZAS EN AMBIENTES IOT SEGÚN LA AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA)

6.4.1 Actividad vil / abuso

Amenazas	Descripción	Escenarios afectados
Malware	Softwares maliciosos que permanecen ocultos, y tiene como objetivo infiltrarse sin la autorización del usuario para dañar, corromper o robar información. Su impacto es alto.	• Dispositivos y sensores IoT • Plataformas y Backend

Exploit Kits	Es un software que se encarga de explorar un sistema y señalar las vulnerabilidades o agujeros de seguridad, en ambientes IoT no son fáciles de detectar y su impacto varía de alto a crucial, dependiendo de los activos afectados.	● Dispositivos IoT ● Arquitecturas basadas en IoT
Ataques dirigidos	Su objetivo principal es recopilar información y permanecer ocultos, su detección suele ser muy difícil y con frecuencia son descubiertos después de que han extraído una gran cantidad de datos.	● Plataforma y Backend ● Información ● Arquitecturas basadas en IoT
DDoS	Ataque distribuido de denegación de servicio, es decir, que múltiples sistemas infectados atacan a un solo objetivo para sobrecargarlo y que colapse.	● Dispositivos y sensores IoT ● Plataformas y Backend ● Arquitecturas basadas en IoT
Ataques de privacidad	Es una de las amenazas más comunes y afecta tanto a la privacidad del usuario, como a la exposición de elementos de red, para personal no autorizado.	● Dispositivos y sensores IoT ● Plataformas y Backend ● Información
Modificación de la información	En este caso, el objetivo no es dañar los dispositivos, sino manipular la información para causar caos u obtener ganancias monetarias.	● Dispositivos IoT ● Plataformas y Backend ● Arquitecturas basadas en IoT ● Información

Tabla 12 Actividad vil / abuso. [29]

6.4.2 Interceptación / secuestro

Amenazas	Descripción	Escenarios afectados
Man in the middle	En este ataque de espionaje, el atacante puede observar, interceptar mensajes y modificar a su voluntad, procurando que ninguna de las víctimas se entere que la comunicación ha sido quebrantada.	● Comunicación ● Dispositivos IoT ● Información
Secuestro del protocolo de comunicación IoT	La atacante toma control absoluto sobre la comunicación existente entre dos dispositivos de la red, con ello puede forzar la desconexión o denegación de servicio, además de visualizar datos sensibles.	● Comunicación ● Dispositivos IoT ● Información ● Toma de decisiones
Intercepción de comunicación	Es un software espía, que se encarga de la intercepción no autorizada de una comunicación privada, como llamadas telefónicas, mensajes instantáneos, etc.	● Comunicación ● Dispositivos IoT ● Información
Reconocimiento de red	El atacante obtiene información interna sobre la red: dispositivos conectados, protocolo utilizado, puertos abiertos, servicios en uso, etc.	● Comunicación ● Dispositivos IoT ● Información ● infraestructura.
Secuestro de sesión	Obtención o robo de cookies, el atacante actúa como un host legítimo para tener acceso no autorizado a los datos o servicios de un sistema.	● Comunicación ● Dispositivos IoT ● Información
Reproducción de mensajes	El atacante envía o retrasa repetidas veces un mensaje, con el fin de manipular o bloquear el dispositivo de destino.	● Dispositivos IoT ● Información ● Toma de decisiones

Tabla 13 Interceptación / secuestro.[29]

6.4.3 Interrupciones

Amenazas	Descripción	Escenarios afectados
Caída de la red	Falla o interrupción del servicio de internet. Dependiendo de la fracción afectada y del tiempo requerido de restauración, la importancia de esta amenaza varía de alta a crítica	• Infraestructura • Comunicaciones
Fallas de los dispositivos	Mal funcionamiento a nivel de hardware en los dispositivos IoT.	• Dispositivos IoT
Falla del sistema	Falla a nivel del software que afecta a los servicios IoT y aplicaciones.	• Dispositivos y sensores IoT • Plataforma y Backend
Pérdida de servicios de soporte	Los servicios de soporte no están disponibles sin conexión, se crea un caos en el funcionamiento del sistema de información.	• Todos los activos

Tabla 14 Interrupciones.[29]

6.4.4 Daños / Pérdidas de TI (Tecnología de la información)

Amenaza	Descripción	Escenarios afectados
Datos / fuga de información sensible	Difundir datos privados, de manera intencional a entidades no autorizadas. La importancia de esta amenaza varía dependiendo del tipo de información filtrada.	• Dispositivos y sensores IoT • Plataforma y Backend

Tabla 15 Daños / Pérdidas de TI (Tecnología de la información).[29]

6.4.5 Fallas / Mal funcionamiento

Amenazas	Descripción	Escenarios
Vulnerabilidades de software	Los dispositivos IoT más comunes a menudo son vulnerables debido a contraseñas débiles/predeterminadas,	• Dispositivos y sensores IoT • Plataforma y Backend • Arquitectura

	errores de software y errores de configuración, lo que plantea un riesgo para la red.	basada en IoT ● Aplicaciones y servicios
Fallas de terceros	Errores en un componente activo de la red causados por la configuración errónea de otro componente con conexión directa con él.	● Dispositivos y sensores IoT ● Plataforma y Backend ● Arquitectura basada en IoT ● Aplicaciones y servicios

Tabla 16 Fallas/Mal funcionamiento. [29]

6.5 Otras Amenazas

Desastre natural: estos acontecimientos implican inundaciones, fuertes vientos, nevadas, deslizamientos de tierra, entre otros desastres naturales y ambientales, que podrían dañar físicamente los dispositivos causando su interoperabilidad. Pueden afectar a los dispositivos y sensores IoT, al igual que su arquitectura, plataformas y Back-end.[29]

Ataques físicos: hace referencia a actos de sabotaje como el vandalismo, terrorismo, robo y manipulación de información, que afecten de manera permanente los dispositivos, plataformas, arquitecturas y servicios IoT.[29]

CONCLUSIONES

Desde los inicios de Internet se marcó un precedente en la sociedad y la forma de interrelacionarse, consolidando una nueva estructura de trabajo y vida, pues también se logró conectar a internet objetos y dispositivos inteligentes, de ahí surgió el concepto de Internet de las Cosas (IoT), y gracias a la miniaturización de dispositivos electrónicos y de bajo costo, el mercado IoT creció exponencialmente no sólo como servicios a grandes industrias sino también llegando a la población general con múltiples aplicaciones orientadas a diversos sectores como el gobierno, la educación, la salud, el transporte, la agricultura y la industria en general.

Se debe tener en cuenta que actualmente existen modelos y una amplia variedad de protocolos de comunicación dedicados a las diferentes capas de arquitectura IoT (capa de percepción, de internet y aplicación), no obstante, al ser un ecosistema ciberfísico se ve expuesto a desafíos de interoperabilidad y seguridad como la privacidad de los datos, el control de acceso y la autenticación, además se identificaron los diversos puntos de riesgo dentro de un ecosistema IoT teniendo en cuenta los componentes y actores que interactúan entre sí.

Cada protocolo está sujeto a requisitos y restricciones específicas que se deben conocer a la hora de desarrollar algún servicio IoT, pues cabe recordar que los protocolos y las tecnologías están orientados a una o varias capas de la arquitectura IoT, por ejemplo, en rangos de alcance, si el escenario fuera en agricultura inteligente se implementarían los protocolos Sigfox, LoRa o cualquier otra tecnología de largo alcance y bajo consumo energético (LPWA), un segundo escenario puede ser en la domótica o salud inteligente, donde se podría utilizar el protocolo Zigbee, Bluetooth o Wifi, que resultan ser de bajo costo y de fácil instalación, por otro lado si fuera el pago de peajes se podría usar las tecnologías RFID o NFC por su identificación por radiofrecuencia y de corto alcance, motivo por el cual poseen un alto grado de seguridad.

Cada vez son más los mercados que despliegan servicios IoT, la competencia en cuanto a desarrollo de aplicaciones, dispositivos y servicios inteligentes es muy amplia, sin embargo aún se presentan serios incidentes de seguridad e interoperabilidad, en las diferentes fases de diseño, desarrollo, escalabilidad del servicio y actualizaciones, ya que muchas empresas se enfocan en ser los primeros en ofrecer un servicio IoT y omiten algunas consideraciones de seguridad primordiales, de ahí que se convierten en blanco fácil para ciberataques y problemas legales.

Actualmente existen organismos encargados de la estandarización de dispositivos electrónicos y telecomunicaciones, estas regulaciones se deben tener en cuenta a la hora de desarrollar un servicio IoT, pues con ello se logra brindar interoperabilidad, es decir, que los dispositivos y protocolos hablen el mismo idioma, de esta manera se mantiene la calidad del servicio.

REFERENCIAS

[1] L. C. Karen Rose, Scott Eldridge, *The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World*, no. October. Internet of Society, 2015.

[2] Gartnet, “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016.” [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. [Accessed: 12-Aug-2018].

[3] B. M. Leiner *et al.*, “Brief History of the Internet 1997.”

[4] Postcapes, “Internet of Things Infographic | What Is The "Internet of Things"?” [Online]. Available: https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/. [Accessed: 11-Aug-2018].

[5] Postscapes, “2018 IoT Products | Overview of the Most Popular Smart Home Devices.” [Online]. Available: https://www.postscapes.com/internet-of-things-award/winners/. [Accessed: 11-Aug-2018].

[6] Silicon, “Los sensores inteligentes y autónomos marcarán un antes y un después en el IoT | Silicon.” [Online]. Available: https://www.silicon.es/los-sensores-inteligentes-autonomos-marcaran-despues-iot-2351992?inf_by=5b48fe02671db8f2638b4e1c. [Accessed: 11-Aug-2018].

[7] The Valley, “Sensores. Los dispositivos que alimentan IoT - The Valley Digital Business School.” [Online]. Available: https://thevalley.es/blog/sensores-los-dispositivos-alimentan-iot/. [Accessed: 11-Aug-2018].

[8] TUATARA TECH, “Sensores (Sensors) vs Actuadores (Actuators) | Tuatara Tech.” [Online]. Available: http://www.tuataratech.com/2015/06/sensores-sensors-vs-actuadores-actuators_8.html. [Accessed: 11-Aug-2018].

[9] eveliux, “Concepto de red y tipos de redes.” [Online]. Available: http://www.eveliux.com/mx/Concepto-de-red-y-tipos-de-redes.html. [Accessed: 11-Aug-2018].

[10] arrow, “Conectividad inalámbrica para la Internet de las cosas: no existe la talla única | Arrow.com.” [Online]. Available: https://www.arrow.com/es-mx/research-and-events/articles/wireless-connectivity-for-the-internet-of-things-one-size-does-not-fit-all. [Accessed: 11-Aug-2018].

[11] Zigbee Alliance, “Zigbee Light Link | Zigbee Alliance.” [Online]. Available: https://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbee-light-link/. [Accessed: 11-Aug-2018].

[12] Gobierno TI, “TIPOS DE REDES INFORMATICAS – REDES POR ALCANCE – PARTE 1 | Gobierno TI.” [Online]. Available: https://gobiernoti.wordpress.com/2013/09/05/internet-la-red-de-redes-—-redes-por-alcance/. [Accessed: 11-Aug-2018].

[13] DCME, “Classification of Networks (LAN,MAN,WAN) - Diploma Computer Engineering(DCME).” [Online]. Available: https://sites.google.com/site/cprorgrams/sem-4/ch--nw/introduction-to-networks-and-topologies/classification-of-networks-lanmanwan. [Accessed: 11-Aug-2018].

[14] M. B. Yassein, S. Aljawarneh, and E. Masa’deh, “A new elastic trickle timer algorithm for Internet of Things,” *J. Netw. Comput. Appl.*, vol. 89, pp. 38–47, 2017.

[15] R. Buyya and A. V. Dastjerdi, *Internet of Things: Principles and Paradigms*. 2016.

[16] K. Hafner and M. Lyon, *Where Wizards Stay Up Late: The Origins of the Internet*. 1996.

[17] J. Salazar and S. Silvestre, *Internet de las cosas*. 2016.

[18] IBM, “Protocolos TCP/IP,” *IBM*, 2018. [Online]. Available: https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.networkcomm/tcpip_protocols.htm. [Accessed: 25-Mar-2018].

[19] B. Cedón, “La historia del Internet de las Cosas (IoT),” 2018. [Online]. Available: http://www.bcendon.com/el-origen-del-iot/. [Accessed: 24-Mar-2018].

[20] Postscapes, “History of IoT,” *Background Information and Timeline of the*

Trending, 2018. [Online]. Available: https://www.postscapes.com/internet-of-things-history/.

[21] D. Evans, “Internet de las cosas Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo,” Cisco Internet Business Solutions Group (IBSG), 2011.

[22] K. Asthon, “That ‘Internet of Things’ Thing In the real world, things matter more than ideas.,” *RFID J.*, 2009.

[23] J. Doe, “Historia del IOT - Revolucion IOT,” *Revolicioniot*, 2018. [Online]. Available: http://revolucioniot.com/historia-del-iot/.

[24] J. de A. de I. (IAB) H. Tschofenig, “Consideraciones arquitectónicas en Smart Object Networking,” 2015.

[25] a Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014.

[26] R. Davies, “The Internet of Things The Internet of Things,” no. May, p. 6, 2015.

[27] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[28] R. H. Weber, “Internet of Things - New security and privacy challenges,” *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[29] M. Ross, A. J. Jara, and A. Cosenza, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, no. November. 2017.

[30] BICS, “Soluciones integrales de conectividad IoT global que ofrecen un modelo de pago por tamaño (pay-as-you-grow) basado en API.” [Online]. Available: https://bics.com/es/services/conectividad-iot-global/. [Accessed: 01-Sep-2018].

[31] S. Kulkarni, “Communication Models in Internet of Things : A Survey,” vol. 3, no. 11, pp. 87–91, 2017.

[32] D. M. H. Tschofenig ARM Ltd, J. Arkko, D. Thaler, “Architectural Considerations in Smart Object Networking,” in *Internet Architecture Board (IAB)*, 2015.

[33] U. N. Kar and D. K. Sanyal, “An overview of device-to-device communication in cellular networks,” *ICT Express*, 2018.

[34] A. Asadi, Q. Wang, and V. Mancuso, “A survey on device-to-device communication in cellular networks,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.

[35] Google Cloud, “Overview of Internet of Things.” [Online]. Available: https://cloud.google.com/solutions/iot-overview. [Accessed: 12-Jun-2018].

[36] M. Nazir, “Cloud Computing: Overview & Current Research Challenges,” *IOSR J. Comput. Eng.*, vol. 8, no. 1, pp. 14–17, 2012.

[37] S. Kumar and R. H. Goudar, “Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey,” *Int. J. Futur. Comput. Commun.*, vol. 1, no. 4, pp. 356–360, 2012.

[38] A. Youssef, “Exploring Cloud Computing Services and Applications,” *J. Emerg. Trends Comput. …*, vol. 3, no. 6, pp. 838–847, 2012.

[39] Microsoft Azure IoT, “Plataformas de servicio.” [Online]. Available: https://azure.microsoft.com/es-es/overview/what-is-paas/. [Accessed: 13-Jun-2018].

[40] Microsoft Azure, “Basics of Azure IoT.” [Online]. Available: https://docs.microsoft.com/es-es/azure/iot-fundamentals/. [Accessed: 14-Jun-2018].

[41] Microsoft Azure, “IoT Hub documentation.” [Online]. Available: https://docs.microsoft.com/es-es/azure/iot-hub/. [Accessed: 13-Jun-2018].

[42] Microsoft Azure, “Device-to-cloud communications guidance.” [Online]. Available: https://docs.microsoft.com/es-es/azure/iot-hub/iot-hub-devguide-d2c-guidance. [Accessed: 13-Jun-2018].

[43] A. Glória, F. Cercas, and N. Souto, “Design and implementation of an IoT gateway to create smart environments,” *Procedia Comput. Sci.*, vol. 109, pp. 568–575, 2017.

[44] Y. H. Lee and S. Nair, “A Smart Gateway Framework for IOT Services,” *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pp. 107–114, 2017.

[45] Microsoft Azure, “What is Azure IoT Edge - preview.” [Online]. Available: https://docs.microsoft.com/en-us/azure/iot-edge/how-iot-edge-works. [Accessed: 14-Jun-2018].

[46] Microsoft Azure, “Azure IoT.” [Online]. Available: https://azure.microsoft.com/en-us/overview/iot/. [Accessed: 14-Jun-2018].

[47] OwnCloud, “ownCloud 9.0 Enables Full Federation,” *OwnCloud*. .

[48] CODECADEMY, “Back-End Web Architecture | Codecademy.” [Online]. Available: https://www.codecademy.com/articles/back-end-architecture. [Accessed: 01-Aug-2018].

[49] Equipo Altran, “El front-end y el back-end de las Smart Cities,” 2017. [Online]. Available: http://equipo.altran.es/el-front-end-y-el-back-end-de-las-smart-cities/. [Accessed: 15-Jun-2018].

[50] Iei, “Fitness Solution.” [Online]. Available: http://ieismartcity.com/fitness-solution/. [Accessed: 15-Jun-2018].

[51] William Stallings *et al.*, “Communication networks: Topology and links.,” *Creative Commons*, vol. s, no. 9. p. 99, 2013.

[52] A. NAYYAR, “Internet of Things: The protocols landscape,” *OpenSource*, 2017. [Online]. Available: https://opensourceforu.com/2017/07/internet-things-protocols-landscape/. [Accessed: 22-Apr-2018].

[53] K. Curran, “Internet protocols,” *Underst. Internet A Glimpse into Build. Blocks, Appl. Secur. Hidden Secrets Web*, pp. 7–16, 2009.

[54] Postscapes, “IoT Standards and Protocols,” *Postscapes*. [Online]. Available: https://www.postscapes.com/internet-of-things-protocols/. [Accessed: 24-Apr-2018].

[55] T. Edition, *Wireless Networking in the Developing World*. 2013.

[56] F. Ramón, G. Pedraja, V. Quílez, S. De Alcatel, and T. De Red, “IEEE 802.11(Wi-Fi) El estándar de facto para WLAN,” pp. 28–33, 2011.

[57] S. Song and B. Issac, “Analysis of Wifi and Wimax and Wireless Network Coexistence,” *Int. J. Comput. Networks Commun.*, vol. 6, no. 6, pp. 63–77, 2014.

[58] Jatin Parekh, “WiFi’s evolving role in IoT, WiFi is often the obvious choice for IoT, but limitations have lead to the addition of two new specifications,

802.11ah and 802.11ax," *Network World*, 2017. [Online]. Available: https://www.networkworld.com/article/3196191/lan-wan/wifi-s-evolving-role-in-iot.html. [Accessed: 02-Apr-2018].

[59] K. Fitchard, "Are you ready for the next chapter of Wi-Fi? Meet 802.11ax," *GIGAOM*, 2015. [Online]. Available: https://gigaom.com/2014/06/12/next-phase-of-wifi-80211ax/. [Accessed: 02-Apr-2018].

[60] SEMTECH, "What is LoRa®?" [Online]. Available: https://www.semtech.com/technology/lora/what-is-lora. [Accessed: 28-Mar-2018].

[61] J. Kos, "On the Limits of Empahty," *Jstor, Art J.*, vol. 88, no. 1, pp. 139–157, 2006.

[62] LoRa Alliance, "What is the LoRaWAN™ Specification?" [Online]. Available: https://lora-alliance.org/about-lorawan. [Accessed: 28-Mar-2018].

[63] inteliLIGHT®, "LoRaWAN based street lighting solutions become a reality with the new inteliLIGHT® LoRa™ controllers being presented and demonstrated for the first time by Flashnet during the LoRa™ Alliance meeting in Paris.," *inteliLIGHT®*. [Online]. Available: https://intelilight.eu/worlds-first-lora-street-lighting-control-solution-released-flashnet/. [Accessed: 16-Apr-2018].

[64] Sigfox, "Sigfox Technology Overview." [Online]. Available: https://www.sigfox.com/en. [Accessed: 05-Apr-2018].

[65] P. McDermott-Wells, "What is Bluetooth?," *Potentials, IEEE*, vol. 23, no. 5, pp. 33–35, 2005.

[66] D. Garin, M. Hazard, and A. J. González, "Bluetooth," 2013.

[67] Bluetooth, "SIG INTRODUCES BLUETOOTH LOW ENERGY WIRELESS TECHNOLOGY, THE NEXT GENERATION OF BLUETOOTH WIRELESS TECHNOLOGY," *Bluetooth Special Interest Group (SIG*, Bellevue, WA, USA, p. 1, 2009.

[68] R. Kennelly, *IEEE standards for physical and data communications.*, vol. 30, no. 2. 2003.

[69] EMF Explained 2.0, "BLUETOOTH & HEALTH - L2." [Online]. Available:

http://www.emfexplained.info/eng/?page=25530. [Accessed: 28-Apr-2018].

[70] T. YUDEN, “Bluetooth® low energy modules with an embedded antenna smaller than current small-type modules are developed.” [Online]. Available: https://www.yuden.co.jp/or/solutions/ble/. [Accessed: 20-Apr-2018].

[71] B. Borowicz, “The Internet of Things and Bluetooth,” *Gridconnect*, 2016.

[72] J. de C. y Leon, “Radiofrequency identification technology and its main applications,” *Obs. Reg. la Soc. la Inf.*, pp. 30–56, 2007.

[73] L. Jerry and C. Barbara, “Shrouds of Time: The History of RFID,” *AIM Publ.*, p. 11, 2001.

[74] J. I. Portillo García, A. B. Bermejo Nieto, and A. M. Bernardos Barbolla, *Technological surveillance report: radiofrequency identification technology (RFID)*. 2008.

[75] National Institute of Communication Technologies, “Guide on security and privacy of RFID technology,” *Mayo 2010*, p. 49, 2010.

[76] N. R. Gonzalez and D. R. Merlano, “Radio frequency identification rfid,” 2007.

[77] GS1 Spain, “EPC / RFID.” [Online]. Available: https://www.gs1es.org/epc-rfid-identificador-unico/. [Accessed: 20-Apr-2018].

[78] “FACULTAD DE CIENCIAS PURAS Y NATURALES TUTOR METODOLÓGICO : M . SC . ALDO VALDEZ ALVARADO,” 2014.

[79] NFCForum, “Simplifying IoT : Connecting , Commissioning , and Controlling with Near Field Communication (NFC) NFC Makes the Smart Home a Reality,” *NFC Forum White Pap.*, no. June, 2016.

[80] NFC forum, “Why The Internet Of Things needs NFC.” [Online]. Available: https://nfc-forum.org/nfc-and-the-internet-of-things/iot-infographic/. [Accessed: 06-Apr-2018].

[81] I. 802. . W. Group, “IEEE 802.3 ETHERNET WORKING GROUP,” 2018. [Online]. Available: http://grouper.ieee.org/groups/802/3/. [Accessed: 10-Apr-2018].

[82] B. Valle and J. David, “IoT : TECNOLOGÍAS , y desarrollo,” *Repos. UOC*,

p. 273, 2014.

[83] IEEE 802.15, “IEEE 802.15 WPAN™ Task Group 4 (TG4).” [Online]. Available: http://www.ieee802.org/15/pub/TG4.html. [Accessed: 11-Apr-2018].

[84] R. K. Singh and R. Singh, “4G LTE Cellular Technology: Network Architecture and Mobile Standards,” *Int. J. Emerg. Res. Manag. &Technology*, vol. 9359, no. 12, pp. 1–6, 2016.

[85] A. Kumar, A. Aswal, and L. Singh, “4G Wireless Technology : A Brief Review,” no. 2, pp. 35–43, 2013.

[86] R. S, “Who needs 4G, whatever that is?,” 2012. [Online]. Available: http://www.e-news.press/who-needs-4g-whatever-that-is/. [Accessed: 21-Apr-2018].

[87] A. Gohil, H. Modi, and S. K. Patel, “5G technology of mobile communication: A survey,” *2013 Int. Conf. Intell. Syst. Signal Process. ISSP 2013*, pp. 288–292, 2013.

[88] D. Brake and | June, “5G and Next Generation Wireless: Implications for Policy and Competition,” *5G Next Gener. Wirel. Implic. Policy Compet.*, no. June, pp. 1–22, 2016.

[89] Mobile Europe, “Ericsson CTO: 5G is about integrated wireless technologies, not just speeds,” *Mobile Europe*, 2013. [Online]. Available: https://www.mobileeurope.co.uk/news-analysis/ericsson-cto-5g-is-about-integrated-wireless-technologies-not-just-speeds. [Accessed: 21-Apr-2018].

[90] Cisco Systems Inc., “Dual Stack IPv4 / IPv6 Devices,” p. 625513, 2010.

[91] Cisco *et al.*, “Location-based services,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2, no. 3, pp. 1–10, 2013.

[92] PRITAM, “Diferencias clave entre IPv4 e IPv6,” 2018. [Online]. Available: https://pagedesignweb.com/key-differences-between-ipv4-and-ipv6/. [Accessed: 21-Apr-2018].

[93] J. Olsson, “6LoWPAN demystified,” *Texas Instruments*, p. 13, 2014.

[94] D. T. Britt and C. Matthews, “Front cover TCP / IP Tutorial and,” *Contract*,

vol. 1, no. December 2006, p. 1004, 2006.

[95] W. Goralski, “Protocols and Layers,” *Illus. Netw.*, pp. 3–46, 2009.

[96] R. Fielding *et al.*, “Hypertext Transfer Protocol -- HTTP/1.1,” pp. 1–176, 1999.

[97] CoAp technology, “CoAP RFC 7252 Constrained Application Protocol.” [Online]. Available: http://coap.technology/. [Accessed: 15-Apr-2018].

[98] Seebo, “IoT Connectivity for Industry 4.0 Explained Navigating IoT Protocols.” [Online]. Available: https://www.seebo.com/iot-connectivity/. [Accessed: 22-Mar-2018].

[99] Arrow, “Protocols for the Internet of Things.” [Online]. Available: https://www.arrow.com/es-mx/research-and-events/articles/protocols-for-the-internet-of-things. [Accessed: 22-Mar-2018].

[100] XMPP Community, “XMPP Community.” [Online]. Available: https://xmpp.org. [Accessed: 24-Mar-2018].

[101] M. Kirsche and R. Klauck, “Unify to bridge gaps: Bringing XMPP into the Internet of Things,” *2012 IEEE Int. Conf. Pervasive Comput. Commun. Work. PERCOM Work. 2012*, no. March 2012, pp. 455–458, 2012.

[102] A. Talaminos-Barroso, M. A. Estudillo-Valderrama, L. M. Roa, J. Reina-Tosina, and F. Ortega-Ruiz, “A Machine-to-Machine protocol benchmark for eHealth applications - Use case: Respiratory rehabilitation,” *Comput. Methods Programs Biomed.*, vol. 129, pp. 1–11, 2016.

[103] A. Talaminos-Barroso, M. A. Estudillo-Valderrama, L. M. Roa, J. Reina-Tosina, and F. Ortega-Ruiz, “A Machine-to-Machine protocol benchmark for eHealth applications - Use case: Respiratory rehabilitation,” *Comput. Methods Programs Biomed.*, vol. 129, pp. 1–11, 2016.

[104] MQTT Community, “MQTT Community.” [Online]. Available: http://mqtt.org/. [Accessed: 27-Mar-2018].

[105] Ermesh, “Ermesh – Ingeniería y diseño de Internet of Things-.” [Online]. Available: http://www.ermesh.com/protocolo-mqtt-niveles-qos/. [Accessed: 27-Mar-2018].

[106] S. Roth, “IoT for tiny devices: Let’s talk MQTT-SN,” *Software Engineering*, 2014. [Online]. Available: https://www.zuehlke.com/blog/en/iot-for-tiny-

devices-lets-talk-mqtt-sn/. [Accessed: 28-Mar-2018].

[107] A. Communnity, “AMQP Committe,” 2014. [Online]. Available: https://www.amqp.org/. [Accessed: 28-Mar-2018].

[108] B. Carstoiu and D. Carstoiu, “a New Grid Caching System Based on Amqp Protocol,” no. 1, pp. 473–477, 2008.

[109] VSCP Community, “Very Simple Control Protocol.” [Online]. Available: http://www.vscp.org/. [Accessed: 29-Mar-2018].

[110] C. C. A. V3.0, “STOMP Protocol Specification.” [Online]. Available: https://stomp.github.io/stomp-specification-1.2.html. [Accessed: 29-Mar-2018].

[111] Community Documentation, “jboss.org.” [Online]. Available: https://docs.jboss.org/hornetq/2.2.5.Final/user-manual/en/html/interoperability.html. [Accessed: 30-Mar-2018].

[112] D. Bekerman and D. Breslaw, “Cómo Mirai usa el protocolo STOMP para lanzar ataques DDoS.” [Online]. Available: https://www.incapsula.com/blog/mirai-stomp-protocol-ddos.html. [Accessed: 29-Mar-2018].

[113] Activemq.apache, “OpenWire Protocol Manual.” [Online]. Available: http://activemq.apache.org/apollo/documentation/openwire-manual.html#OpenWire_protocol_details. [Accessed: 30-Mar-2018].

[114] Object Manegement Group (OMG), “DDS The Proven Data Connetivity Standard for the IoT.” [Online]. Available: http://portals.omg.org/dds/. [Accessed: 31-Mar-2018].

[115] A. Corsaro and D. Ph, “The DDS Tutorial,” *Read. Writ.*

[116] Z-Wave ALLIANCE, “About Z-Wave Technology.” [Online]. Available: https://z-wavealliance.org/about_z-wave_technology. [Accessed: 26-Apr-2018].

[117] P. Lamkin, “Z-Wave explained: What is Z-Wave and why is it important for your smart home?,” *The Ambient*, 2018. [Online]. Available: https://www.the-ambient.com/guides/zwave-z-wave-smart-home-guide-281. [Accessed: 27-Apr-2018].

[118] S. S. Z-WAVE, “Smart home products with Z-Wave inside work together,

use just one app to connect and control your smart home from anywhere." [Online]. Available: http://www.z-wave.com/learn. [Accessed: 27-Apr-2018].

[119] J. M. Moreno and D. Ruiz Fernandez, "Informe Técnico: Protocolo ZigBee (IEEE 802.15.4)," p. 36, 2007.

[120] J. Maestre, *Domótica para ingenieros*, 2015th ed. 2015.

[121] Zigbee Press Releases, "The Zigbee Alliance Introduces First Multi-Band IoT Mesh Network Technology for Massive IoT Deployments," *Zigbee Alliance*, 2017. [Online]. Available: http://www.zigbee.org/zigbee-introduces-multi-band-iot-mesh-network/. [Accessed: 23-Apr-2018].

[122] M. G. M. and J. Moreno, "ZIGBEE," *WIKISPACES*, 2012. [Online]. Available: https://sx-de-tx.wikispaces.com/ZIGBEE. [Accessed: 23-Apr-2018].

[123] THREAD, "POWERFUL TECHNOLOGY DESIGNED FOR THE HOME." [Online]. Available: https://www.threadgroup.org/What-is-Thread. [Accessed: 29-Apr-2018].

[124] vtaraenergygroup., "IOT Smart Cities – VTara Energy Group." [Online]. Available: http://vtaraenergygroup.com/index.php/portfolio/iot-smart-cities/. [Accessed: 22-Jul-2018].

[125] J. C. Alcalde, "Smart Citie," *economipedia*, 2018. [Online]. Available: http://economipedia.com/definiciones/ciudad-inteligente-smart-city.html. [Accessed: 30-Aug-2018].

[126] Tech Reviews, "Hometech? What is it? Smarthome Ideas for better Living," 2018. [Online]. Available: http://smarthome-hometech.com/smarthome-simplified/. [Accessed: 22-Jul-2018].

[127] M. S. Obaidat and P. Nicopolitidis, *Smart Cities and Homes: Key Enabling Technologies*. 2016.

[128] CASADOMO, "Válvulas inteligentes para radiadores que permiten controlar y gestionar el consumo energético • CASADOMO," 2017. [Online]. Available: https://www.casadomo.com/2017/09/12/valvulas-inteligentes-radiadores-permiten-controlar-gestionar-consumo-energetico. [Accessed: 22-Jul-2018].

[129] Ensmartech, “Los 3 mejores purificadores de aire inteligentes Reseñas • Ensmartech,” 2017. [Online]. Available: https://ensmartech.com/reviews/best-smart-air-purifier-review. [Accessed: 22-Jul-2018].

[130] ABC SOLUCIONES, “Para qué sirven los altavoces inteligentes que tan de moda están ahora,” 2018. [Online]. Available: https://www.abc.es/tecnologia/informatica/soluciones/abci-para-sirven-altavoces-inteligentes-moda-estan-ahora-201801170211_noticia.html. [Accessed: 22-Jul-2018].

[131] wwwhat’s new, “Amazon estaría trabajando en un altavoz inteligente de grandes dimensiones,” 2017. [Online]. Available: https://wwwhatsnew.com/2016/11/29/amazon-estaria-trabajando-en-un-altavoz-inteligente-de-grandes-dimensiones/. [Accessed: 22-Jul-2018].

[132] F and Ertiberia, “Weblet Importer,” *grupo fertiberia*, 2017. [Online]. Available: http://www.fertiberia.com/es/blog/2017/noviembre/agricultura-inteligente-1-contexto-idóneo/. [Accessed: 09-Jul-2018].

[133] Feriberia, “Weblet Importer,” *grupo fertiberia*, 2017. [Online]. Available: http://www.fertiberia.com/es/blog/2017/diciembre/agricultura-inteligente-2-agricultura-de-precision/. [Accessed: 09-Jul-2018].

[134] S. Wolfert, L. Ge, C. Verdouw, and M. J. Bogaardt, “Big Data in Smart Farming – A review,” *Agric. Syst.*, vol. 153, pp. 69–80, 2017.

[135] IoT SIMPLE, “Agricultura Inteligente — IoT Simple.” [Online]. Available: http://www.iotsimple.com/agricultura-inteligente/. [Accessed: 22-Jul-2018].

[136] Banco Mundial, “Agricultura inteligente con respecto al clima.” [Online]. Available: http://www.bancomundial.org/es/topic/climate-smart-agriculture. [Accessed: 22-Jul-2018].

[137] NEDAP, “Control de la salud láctea - Herd Health Management - Nedap.” [Online]. Available: https://www.nedap-livestockmanagement.com/dairy-farming/solutions/nedap-cowcontrol/health-monitoring/. [Accessed: 22-Jul-2018].

[138] Afimilk, “Cow welfare | Afimilk,” *Afimilk vital know-how in every drop*, 2017. [Online]. Available: https://www.afimilk.com/needs-

solutions/cows/cow-welfare. [Accessed: 11-Jul-2018].

[139] N. S. Paulin, N. Anupriya, and S. Prasanthi, “Pisciculture Environment Control Using Automated Monitoring System,” vol. 1, no. 2, pp. 60–65, 2017.

[140] “Informe de Vigilancia Tecnológica Blue Growth: IoT en el sector marino.”

[141] PRECISIONAG, “Precision Agriculture and Precision Farming | PrecisionAg.” [Online]. Available: https://www.precisionag.com/. [Accessed: 22-Jul-2018].

[142] CEMA, “Precision Farming: key technologies & concepts | CEMA - European Agricultural Machinery.” [Online]. Available: http://cema-agri.org/page/precision-farming-key-technologies-concepts. [Accessed: 22-Jul-2018].

[143] Joint Research Centre (JRC) of the European Commission, “Precision Agriculture: an Opportunity for Eu Farmers- Potential Support With the Cap 2014 - 2020,” *Eur. Union*, p. 56, 2014.

[144] R. K. Kodali, V. Jain, and S. Karagwal, “IoT based smart greenhouse,” *2016 IEEE Reg. 10 Humanit. Technol. Conf.*, pp. 1–6, 2016.

[145] August9system, “Agust9sytems|Industrial Automation in malaysia,india,Singapore |Industrial Software in malaysia,india,Singapore |Energy management|IoT|IIoT|Manufacturing Software|Manufacturing Execution Systems Manufacturing Operations Management|SCADA|PLC|DCS|Automation|InstrumentationProductivity| Operations Efficiency|Process Control Manufacturing Optimization/Optimisation.” [Online]. Available: http://www.august9systems.com/index.php. [Accessed: 22-Jul-2018].

[146] DELLEMC, “Big-Data-Concept.png.” [Online]. Available: https://blog.dellemc.com/uploads/2016/02/Big-Data-Concept.png. [Accessed: 22-Jul-2018].

[147] Siemens, “Tecnomatix.” [Online]. Available: https://www.plm.automation.siemens.com/global/en/products/tecnomatix/.

[148] MIT Tecnology review, “50 Smartest Companies 2017.” [Online]. Available:

https://www.technologyreview.com/lists/companies/2017/intro/#spark-therapeutics. [Accessed: 22-Jul-2018].

[149] BeSmart, “Smart Health | BeSmart.” [Online]. Available: http://www.besmart.company/soluciones/smart-health/. [Accessed: 22-Jul-2018].

[150] J. Rudner, C. McDougall, V. Sailam, M. Smith, and A. Sacchetti, “Interrogation of Patient Smartphone Activity Tracker to Assist Arrhythmia Management,” *Ann. Emerg. Med.*, vol. 68, no. 3, pp. 292–294, Sep. 2016.

[151] Heypaylees, “Aplicaciones de Internet of Things en la asistencia sanitaria | HeyPayless.” [Online]. Available: https://www.heypayless.com/5-iot-applications-that-will-change-the-face-of-healthcare/. [Accessed: 22-Jul-2018].

[152] Ipentechdiary, “IoT | opentechdiary,” 2015. [Online]. Available: https://opentechdiary.wordpress.com/tag/iot/. [Accessed: 22-Jul-2018].

[153] cbinsights, “11 Surprising Applications For The IoT In Healthcare, Retail, Agriculture, And More.” [Online]. Available: https://www.cbinsights.com/research/surprising-iot-applications/. [Accessed: 22-Jul-2018].

[154] CBINSIGHTS, “Proteus Digital Health - CB Insights.” [Online]. Available: https://www.cbinsights.com/company/proteus-digital-health. [Accessed: 22-Jul-2018].

[155] abilifymycite., “El sistema ABILIFY MYCITE®.” [Online]. Available: https://www.abilifymycite.com/. [Accessed: 22-Jul-2018].

[156] solutionanalysts, “5 IoT Applications That Will Change the Face of Healthcare - solutionanalysts.” [Online]. Available: https://www.solutionanalysts.com/blog/5-iot-applications-that-will-change-the-face-of-healthcare/. [Accessed: 22-Jul-2018].

[157] PILLCAM, “What Is It? | About PillCam COLON Capsule Endoscopy.” [Online]. Available: http://ous.pillcamcolon.com/es/about/what-is-it. [Accessed: 22-Jul-2018].

[158] everydayhearing, “The Complete Guide to Hearable Technology in 2018 - Everyday Hearing,” 2018. [Online]. Available:

https://www.everydayhearing.com/hearing-technology/articles/hearables/. [Accessed: 22-Jul-2018].

[159] NEC, “NEC biometrics technology uses sound to distinguish individually unique ear shape: Press Releases | NEC,” 2016. [Online]. Available: https://www.nec.com/en/press/201603/global_20160307_01.html. [Accessed: 22-Jul-2018].

[160] bragi, “Custom Earphones - The Dash Pro - Bragi.” [Online]. Available: https://www.bragi.com/thedashpro/customize/. [Accessed: 22-Jul-2018].

[161] softwebsolutions, “Remote Patient Monitoring App on Mobile.” [Online]. Available: https://go.softwebsolutions.com/resources/remote-patient-monitoring-mobile-app.html. [Accessed: 22-Jul-2018].

[162] softwebsolutions, “Cross-platform mobile app for a fetal heart rate monitoring system.” [Online]. Available: https://go.softwebsolutions.com/resources/mobile-app-for-fetal-heart-rate-monitoring-system.html. [Accessed: 22-Jul-2018].

[163] N. B. Aletà, C. M. Alonso, and R. M. A. Ruiz, “Smart Mobility and Smart Environment in the Spanish cities,” *Transp. Res. Procedia*, vol. 24, pp. 163–170, 2017.

[164] Universidad de Alicante, “Smart Environment.”

[165] Jaladhi, “Jaladhi Automations Pvt. Limitado.” [Online]. Available: http://jaladhi.com/solutions/grid_management.php. [Accessed: 22-Jul-2018].

[166] Sigfox, “Smart Waste Management Solution | Sigfox Partner Network.” [Online]. Available: https://partners.sigfox.com/products/smart-waste-management-solution. [Accessed: 22-Jul-2018].

[167] citibrain, “Gestión Inteligente de los Residuos Urbanos | Smart Waste.” [Online]. Available: http://www.citibrain.com/es/solutions/smart-waste-es/. [Accessed: 22-Jul-2018].

[168] Quamtra, “Smart Waste Management Solution Based on Real-Time Data | Quamtra.” [Online]. Available: http://www.quamtra.com/en/technology/. [Accessed: 22-Jul-2018].

[169] DNV GL, “Smart Green Cities - DNV GL.” [Online]. Available:

https://www.dnvgl.com/energy/themes/smart-green-cities.html. [Accessed: 22-Jul-2018].

[170] P. Sayeg and P. Charles, “Sistemas de transporte inteligentes,” *GIZ-SUTP, Div. 44 Medio Ambient. e Infrestructura*, p. 58, 2004.

[171] A. Jesús and G. García, “IoT : Dispositivos , tecnologías de transporte y aplicaciones,” 2017.

[172] Sandacom, “ITS – Intelligent Transportation Systems – Part 1, Introduction | Innovational Musings,” 2010. [Online]. Available: https://sandacom.wordpress.com/2010/01/12/its-intelligent-transportation-systems-part-1-introduction/. [Accessed: 22-Jul-2018].

[173] CIDAUT, “I+D+I Sistemas de Transporte Inteligente.” [Online]. Available: https://www.cidaut.es/es/sistemas-de-transporte-inteligente. [Accessed: 22-Jul-2018].

[174] Universidad Alicante, “Smart Mobility: Movilidad Urbana.”

[175] SITT CIA, “Sistemas Inteligentes de Transporte — SITT.” [Online]. Available: https://www.sittycia.com/its/. [Accessed: 22-Jul-2018].

[176] Office of the government Hong kong, “Smart Mobility.” [Online]. Available: https://www.smartcity.gov.hk/develop_plans/mobility/. [Accessed: 22-Jul-2018].

[177] SecureWeek, “Las redes de transporte inteligentes desempeñan un papel clave en la urbanización - SecureWeek,” 2018. [Online]. Available: https://www.secureweek.com/2018/04/06/las-redes-de-transporte-inteligentes-desempenan-un-papel-clave-en-la-urbanizacion/. [Accessed: 22-Jul-2018].

[178] R. W. S. Ruhlandt, “The governance of smart cities: A systematic literature analysis,” *Cities*, no. October 2017, pp. 1–23, 2018.

[179] smart government Argentina, “Smart Government.” [Online]. Available: http://www.smartgovernment.com.ar/index.php. [Accessed: 22-Jul-2018].

[180] P. Seijo, “Concepto de Gobierno Inteligente,” in *smart government Argentina*, 2018.

[181] A. Freire, “Smart Government Argentina,” in *Smart Government*, 2018.

[182] L. Lanza, “Smart Government Argentina,” in *Smart Government*.

[183] IoT Evolution, “Is Latin America Ready for an IoT Boom?” [Online]. Available: http://www.iotevolutionworld.com/iot/articles/436542-lat-america-ready-an-iot-boom.htm. [Accessed: 11-Aug-2018].
[184] A. Latina, “IoT para el sector empresarial en América Latina.”
[185] L. R. Basso, C. Pascale Medina, E. S. de Obschatko, and J. Preciado Patiño, *Agricultura inteligente: la iniciativa de la Argentina para la sustentabilidad en la producción de alimentos y energía*. 2013.
[186] Enterprise IoT Insights, “Case study: Colombia implements smart farming project via Libelium’s sensor platform.” [Online]. Available: https://enterpriseiotinsights.com/20170220/smart-farm/case-study-smart-farming-tag23-tag99. [Accessed: 11-Aug-2018].
[187] Libelium, “Improving banana crops production and agricultural sustainability in Colombia using sensor networks | Libelium.” [Online]. Available: http://www.libelium.com/improving-banana-crops-production-and-agricultural-sustainability-in-colombia-using-sensor-networks/. [Accessed: 11-Aug-2018].
[188] Celotor, “Instalación y Uso - Celotor - Detector de Celo Bovino.” [Online]. Available: http://www.celotor.com/es/celotor/instalacion-y-uso. [Accessed: 11-Aug-2018].
[189] Media Telecom, “Brasil desarrollará plataforma IoT para riego inteligente del agua - Mediatelecom % %.” [Online]. Available: https://www.mediatelecom.com.mx/2017/08/04/brasil-desarrollara-plataforma-iot-para-riego-inteligente-del-agua/. [Accessed: 11-Aug-2018].
[190] Brecha cero, “Chile despliega experiencia pública privada de IoT en agricultura - Brecha Cero.” [Online]. Available: http://brechacero.com/chile-despliega-experiencia-publica-privada-de-iot-en-agricultura/. [Accessed: 11-Aug-2018].
[191] A. Asín and D. Gascón, “Libelium White paper,” pp. 1–64, 2017.
[192] U. N. C. on S. and T. for Development, “Smart Cities in Latin América,” p. 30, 2016.
[193] SantiagoSmartCity, “Santiago Ciudad Inteligente.” [Online]. Available: http://web.sesantiago.cl/. [Accessed: 11-Aug-2018].

[194] S. Keon, L. Heeseo, R. Kwon, H. Cho, J. Kim, and D. Lee, “International Case Studies of Smart Cities: Rio de Janeiro,” *Inter-American Dev. Bank*, no. June, 2016.

[195] J. G. Bayo, “Estudios de casos internacionales de ciudades inteligentes: Medellin, Colombia,” p. 56, 2016.

[196] S. Albishi, B. Soh, A. Ullah, and F. Algarni, “Challenges and Solutions for Applications and Technologies in the Internet of Things,” *Procedia Comput. Sci.*, vol. 124, pp. 608–614, 2017.

[197] A. Tzounis, N. Katsoulas, T. Bartzanas, and C. Kittas, “Internet of Things in agriculture, recent advances and future challenges,” *Biosyst. Eng.*, vol. 164, pp. 31–48, 2017.

[198] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018.

[199] S. Wachter, “Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR,” *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 436–449, 2018.

[200] A. Scarfò, “The Cyber Security Challenges in the IoT Era,” *Secur. Resil. Intell. Data-Centric Syst. Commun. Networks*, pp. 53–76, 2018.

[201] G. Aloi *et al.*, “A Mobile Multi-Technology Gateway to Enable IoT Interoperability.”

[202] and M. P. Giancarlo Fortino, Maria Ganzha, Carlos Palau, “Interoperability in the Internet of Things IEEECS,” *IEEE COMPUTER SOCIETY*, 2016. [Online]. Available: https://www.computer.org/web/computingnow/archive/interoperability-in-the-internet-of-things-december-2016-introduction. [Accessed: 03-Jul-2018].

[203] and M. P. Giancarlo Fortino, Maria Ganzha, Carlos Palau, “Interoperabilidad para la Internet de las Cosas,” *IEEE COMPUTER SOCIETY*, 2016. [Online]. Available: https://www.computer.org/web/computingnow/archive/interoperability-in-the-internet-of-things-december-2016-introduction-spanish-version.

[Accessed: 02-Jul-2018].

[204] J. G. G. L. P. GONZÁLEZ, “ESTÁNDARES PARA LA INTEROPERABILIDAD,” Madrid, España.

[205] Ireland Elizabeth, “Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread | Metering.com,” *Metring & smart energy*, 2012. [Online]. Available: https://www.metering.com/regional-news/north-america/puerto-rico-smart-meters-believed-to-have-been-hacked-and-such-hacks-likely-to-spread/. [Accessed: 26-Jun-2018].

[206] Kashmir Hill, “‘Baby Monitor Hack’ podría suceder a otros 40,000 usuarios de Foscam,” 2013. [Online]. Available: https://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/#1435a0d158b5. [Accessed: 26-Jun-2018].

[207] KrebsonSecurity, “Target Hackers Broke in Via HVAC Company — Krebs on Security,” 2014. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. [Accessed: 26-Jun-2018].

[208] ABC Tecnología, “Ciberataque a la compañía de juguetes VTech: robados los datos de millones de niños de todo el mundo,” 2015. [Online]. Available: https://www.abc.es/tecnologia/redes/abci-ciberataque-compania-juguetes-vtech-robados-datos-millones-ninos-todo-mundo-201512011210_noticia.html. [Accessed: 26-Jun-2018].

[209] FORTINET, “OMG: Bot basado en Mirai convierte dispositivos IoT en servidores proxy,” 2018. [Online]. Available: https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.html. [Accessed: 26-Jun-2018].

[210] D. Sarabia, “Un oso de peluche expone en Internet dos millones de conversaciones entre padres e hijos,” *Eldiario.es*, 2017. [Online]. Available: https://www.eldiario.es/tecnologia/peluche-Internet-millones-conversaciones-padres_0_617338646.html. [Accessed: 28-Jun-2018].