< ANDALUCÍA CONECTADA >

ESTADO DEL ARTE Y TENDENCIAS

INTERNET DE LAS COSAS E INTERNET DE TODO

MAYO 2021

Andalucía se mueve con Europa

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

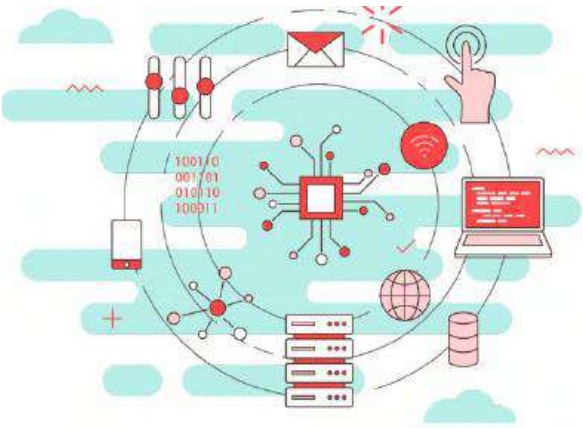
Junta de Andalucía

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 FUNDAMENTOS DEL IoT e IoE



“IoT supone un mundo en el que miles de millones de objetos pueden percibir, comunicar y compartir información, todos ellos interconectados a través de redes públicas o privadas usando el Protocolo de Internet (IP). **La definición común de Internet de las cosas la especifica como una red de objetos físicos.** Pero Internet no es sólo una red de ordenadores, sino que se ha convertido en una red de dispositivos de todo tipo y tamaño, vehículos, teléfonos inteligentes, electrodomésticos, juguetes, cámaras, instrumentos médicos y sistemas industriales, animales, personas, edificios, etc.” (1)

Un ejemplo sencillo de aplicación de IoT puede ser un sistema de control de temperatura, que monitoriza continuamente la temperatura de una ubicación. En función de los datos medidos, la aplicación de control, que se ejecuta en la nube, puede decidir intervenir activando una respuesta, como se observa en la siguiente figura. En este ejemplo se pueden ver los componentes principales de una solución IoT: sensores, actuadores, datos que se envían a la aplicación que está en la nube y la aplicación que toma decisiones.

Figura 1: Un ejemplo de aplicación de IoT (2)

Debido al desarrollo de las tecnologías inteligentes capaces de comunicar e intercambiar importantes volúmenes de información y a los avances en las tecnologías de conexión,

nuestro entorno se está transformando en un "Internet de todo" (Internet of Everything, IoE). IoE proporciona vínculos no sólo entre las cosas, sino también entre datos, personas y procesos (3):

> "No sólo los dispositivos mecánicos y electrónicos pueden ser conectados juntos en un entorno de IoT, también se pueden incluir organismos vivos como plantas, animales de granja y, obviamente, personas. Por ejemplo, un interesante proyecto en Essex (Reino Unido), The Cow Tracking Project[1], ha conectado vacas a Internet a través de etiquetas de posicionamiento vía radio, para monitorizarlas en tiempo real. Los dispositivos informáticos y de salud digitales vestibles ("wearables"), como las pulseras cuantificadoras, son ejemplos de cómo las personas se están conectando en el panorama del Internet de las Cosas. Pero no sólo hay que tener en cuenta a las cosas, datos, personas, etc. cuando se habla del IoE. También son muy importantes los procesos. El proceso juega un papel importante en la forma en que cada una de estas entidades - personas, datos y cosas - trabaja con otras para generar valor en el mundo conectado del IoE. Con los procesos correctos, las conexiones se vuelven relevantes y añaden valor porque la información correcta es entregada a la persona adecuada en el momento adecuado y de la manera apropiada." (3)

> ***La Internet de las cosas es un cambio de paradigma en el ámbito de las Tecnologías de la Información. Si bien IoT ofrece oportunidades muy interesantes, sigue siendo un reto gestionar las cosas que permiten la integración sin fisuras del mundo físico en el mundo de la información y los datos.***

La siguiente tabla resume algunos de los términos que se utilizan en este documento:

Concepto	Descripción
Dispositivo	Un dispositivo, objeto, nodo o "cosa" es un sistema que capta señales de su entorno, envía datos a la nube donde se ejecuta el procesamiento de los mismos y, en ocasiones, actúa sobre su entorno en función de las ordenes que recibe.
Sensor	Sistema capaz de captar distintos parámetros del entorno que le rodea.
Actuador	Sistema capaz de realizar acciones sobre su entorno cuando recibe una orden por parte de la aplicación IoT.
Gateway	Dispositivo de comunicaciones que recoge los datos de los nodos IoT y los reenvía a los servidores en la nube a través de Internet.

1 https://www.essex.ac.uk/research-projects/cow-tracking

Arquitectura IoT	Marco de referencia que se utiliza para representar los componentes que forman parte de IoT y las relaciones que existen entre ellos.
Plataforma	Conjunto de tecnologías, sistemas y servicios que proporcionan un marco de trabajo establecido que permite el desarrollo de aplicaciones completas IoT.
Cloud Computing	Servicios que se ejecutan en servidores ajenos al usuario del servicio, ubicados generalmente en Internet, que son propiedad del proveedor del servicio.
Edge Computing	Variación del Cloud Computing en la que parte de los datos pueden ser almacenados y procesados en dispositivos frontera cercanos a los nodos IoT, antes de enviarlos a la nube.
Fog Computing	Variación del Cloud Computing en la que parte del almacenamiento y del procesamiento de los datos se realiza en los dispositivos, antes de enviarlos a la nube.
Protocolo	Estándares de comunicación que permiten el intercambio de datos entre sistemas.
Router	Dispositivo que interconecta redes entre sí.
QoS	Quality of Service o Calidad de Servicio, conjunto de parámetros técnicos que debe garantizar un servicio.
LAN	Redes de área local, conjunto de tecnologías que permiten la implementación de redes corporativas.
WAN	Wide Area Netork, red de área extensa. Tecnologías de redes que dependen de proveedores y que se utilizan para conectar redes corporativas remotas.
WSN	Wireless Sensor Network, Red de Sensores Inalámbricos. Son redes de nodos IoT que pueden establecer comunicaciones entre ellos de manera dinámica.
Web Service	Tecnologías de comunicación entre sistemas, que se apoyan el protocolo HTTP y se basan, generalmente, en el envío de datos entre un sistema que actúa como cliente y otro sistema que actúa como servidor.
Broker	Elemento central en sistemas de publicación/subscripción que recibe y reenvía mensajes.
M2M	Tecnologías que permiten la comunicación de datos entre sistemas o máquinas: “machine to machine”.
Criptografía	Tecnologías de seguridad utilizadas para lograr la confidencialidad, integridad y autenticidad de las comunicaciones.
Cortafuegos	Sistema de seguridad que protege una red corporativa o doméstica filtrando el tráfico entre redes y permitiendo o denegando conexiones en función de las reglas definidas en su configuración.
IDPS	Sistema de seguridad que previene y detecta intrusiones en redes corporativas, generando alertas si es necesario.
Endpoint	Sistema final en una aplicación, generalmente hace referencia a un sistema como un ordenador de escritorio, portátil, servidor, Tablet, etc. conectado a una red corporativa.

Biometría	Conjunto de tecnologías que utilizan características físicas de las personas en sistemas de autenticación.
VPN	Virutal Private Network, Red Privada Virtual. Tecnología utilizada para lograr conexiones remotas seguras a través de Internet.
Vulnerabilidad	Deficiencia de programación de una aplicación o sistema desde el punto de vista de la seguridad que permite que pueda ser atacado, explotando dicha vulnerabilidad.
Blockchain	Tecnología descentralizada basada en protocolos criptográficos que permite un registro inmutable e histórico de información y la interacción entre partes que no tienen por qué establecer relaciones previas de confianza entre ellas.
Onion Routing	Alternativa al enrutado tradicional de datos que se realiza en Internet para lograr, a través de tecnologías criptográficas, el anonimato y la privacidad de los datos.
Programación segura	Tecnologías que permiten desarrollar aplicaciones robustas desde el punto de vista de la seguridad de las mismas. Entornos de desarrollo que contemplan la seguridad dentro del proceso de programación de las aplicaciones.
Ingeniería social	Conjunto de técnicas utilizadas para conseguir información sensible sobre personas o empresas, a través de la manipulación o el engaño a usuarios legítimos.
Big Data	Conjunto de tecnologías que se utilizan para el tratamiento y procesamiento de grandes cantidades de datos, con el objetivo de obtener conocimiento a partir de los datos.
Inteligencia artificial	Conjunto de algoritmos que, ejecutados en sistemas, intentan imitar las capacidades cognitivas de los humanos.
Gemelo Digital	Replica digital virtual de un producto o de un proceso, que simula su comportamiento y permite mejorar su rendimiento o analizar su respuesta ante determinadas circunstancias.
Smart City	Las ciudades inteligentes son ciudades que, gracias a tecnologías como el IoT y otras, garantizan un desarrollo sostenible, una mayor eficiencia en el uso de los recursos disponibles o aumentar la calidad de vida de los ciudadanos, entre otros objetivos.
Smart Factory	Fabrica Inteligente, concepto de planta de producción que recopila datos de máquinas y del entorno, los procesa y obtiene resultados que permiten optimizar procesos productivos, mejorar el mantenimiento preventivo, etc.
Smart Grid	Red de distribución de electricidad inteligente, son redes de distribución de energía en las que la aplicación de tecnologías de información como el IoT permiten una gestión y un uso más racional y eficiente de la energía.
Wearables	Dispositivos vestibles que captan datos de las personas que los portan.

Tabla 1: Terminología usada en el documento. (Fuente: elaboración propia).

1.1 MODELO DE CAPAS Y DE DESPLIEGUE IoT

Del mismo modo que en otras tecnológicas se realiza una abstracción para presentar un modelo de capas funcionales, en IoT también se pueden diferenciar capas en las que se agrupan diferentes actividades. Sin embargo, en la actualidad, no existe un modelo arquitectónico estandarizado de capas ya que entre los diferentes proveedores existen diferencias en la definición del número de capas, las funciones que incorporan e incluso en la denominación de éstas. A pesar de las múltiples diferencias, se puede extraer un común denominador de las capas principales como el siguiente modelo de referencia que se ilustra a continuación (4):

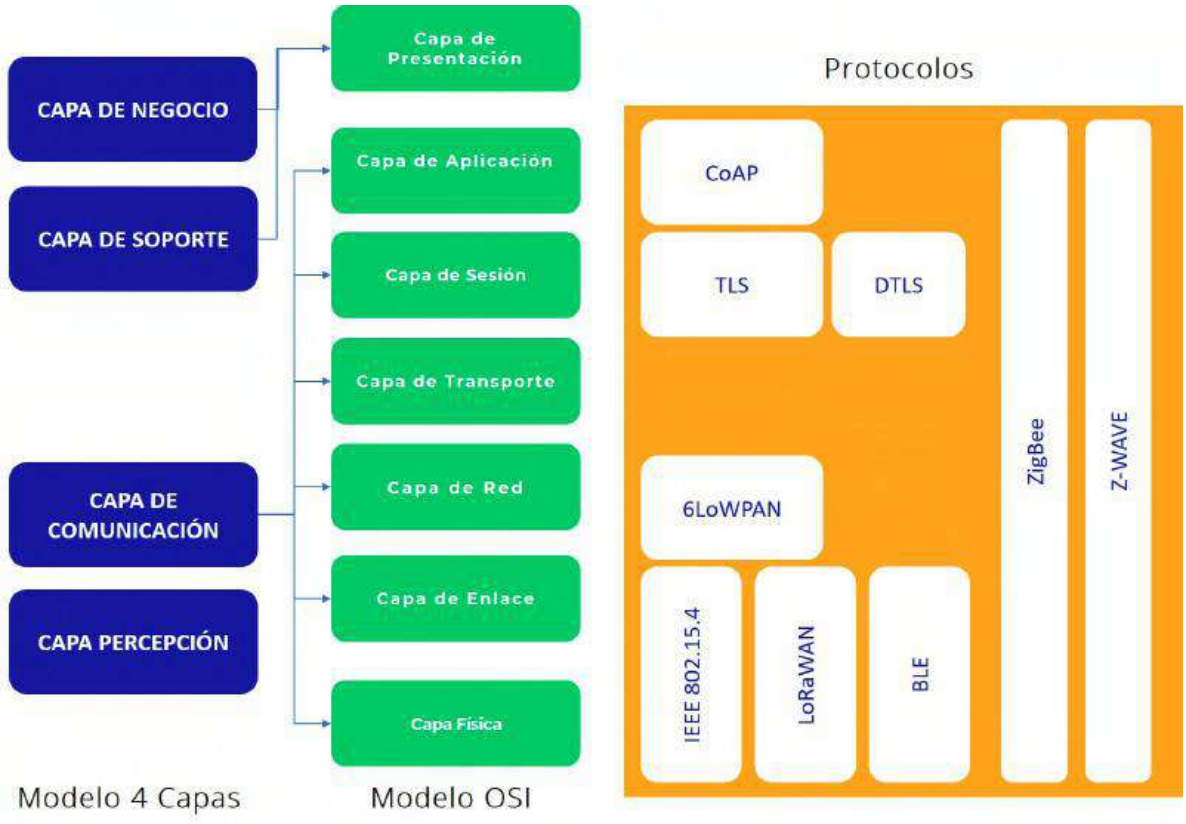


Figura 2: Modelo de capas IoT y protocolos utilizados en las distintas capas.

(Fuente: Elaboración propia basado en (4))

La ilustración contempla un paralelismo con las capas de comunicación del modelo OSI (en color verde) y a su vez con algunos de los protocolos de comunicación más significativos en IoT representados cada uno a la altura de los niveles del modelo OSI que alcanzan.

A continuación, se describe cada una de las capas del **Modelo de Cuatro Capas** representado y las funciones principales que conllevan:

- **Capa de percepción**: representa los sensores físicos de una solución IoT. El objetivo es recoger información de varios dispositivos y procesarla. Esta capa implementa alguna de las siguientes funcionalidades de:

- Las funciones inherentes a los sensores, medir y capturar información del mundo físico y transformarlo al mundo digital.
- Las funciones propias de los actuadores, los cuales transformarán órdenes procesadas desde el ámbito digital al físico.
- Funciones Edge que implica capacidades de procesamiento de cierta capacidad.
- Funciones Fog que implica capacidades de procesamiento y almacenamiento de elevado rendimiento e incluso distribuido.
- Abstracción de las entidades de activos que debe ser representada en las capas superiores. A través de una representación de una entidad virtual, se proporciona una abstracción de identificación de los sensores y actuadores, controladores y contiene una descripción de las relaciones entre ellos. Representa un contexto en el que se pueden entender los datos del sensor, se activa la actuación y se lleva a cabo la interacción con otras entidades que sean representadas.

> **Capa de comunicación**: se ocupa de la transferencia de datos de un objeto hacia la capa de soporte. Esta capa debe implementar las funcionalidades de:

- Abstracción de la conectividad, para encapsular los detalles de las tecnologías de comunicación subyacentes, utilizando una o más API comunes para exponer un conjunto de servicios de conectividad.
- Funciones de comunicaciones que permiten la independencia de la tecnología de acceso para lo que deberá disponer de conectores específicos con los principales protocolos utilizados en el mundo IoT.
- Funciones de Ciberseguridad. Se emplean los mecanismos de comunicación y gestión segura.

Esta capa puede representar funciones de *middleware* por lo que se encargaría también de recoger la información de los dispositivos y también enviar información a aquellos que dispongan de actuadores, por lo que implicaría funciones de:

- Ingesta y recopilación de datos, así como la modelización de los mismos y de su persistencia.
- Abstracción de estados, condiciones y comportamientos de los dispositivos.
- Gobernanza de datos para la seguridad de la información.
- Almacenamiento de datos y analíticas avanzadas.

> **Capa de soporte**: su objetivo principal es la gestión de servicios desde un primer nivel. Esta capa permite a los programadores de soluciones IoT abstraerse de la plataforma de hardware. Las funciones que conllevan son:

- Gestión de dispositivos que implica las facultad de almacenar las características necesarias que definen las capacidades del dispositivo, aprovisionamiento y despliegue, la administración y control de los activos y la competencia de monitoreo y diagnóstico.
- Gestión de accesos de forma segura en función de los roles definidos.
- Monitorización de eventos (logs) del sistema.

> **Capa de negocio**: se utiliza para proporcionar los servicios que están siendo solicitados por el cliente. Esta capa contiene funciones de gestión de aplicaciones y servicios específicos que interactúan con los servicios expuestos en la capa anterior. Sobre esta capa recae, por lo tanto, la creación de distintas verticales de negocio.
Esta capa de la arquitectura debe implementar las funcionalidades de:

- Operaciones de extremo a extremo empresarial, que integra el modelo IoT con las funciones tradicionales específicas de los sistemas industriales, incluidos los que respaldan procesos y actividades empresariales: ERP, CRM, PLM/ALM, MES, gestión de activos, gestión del ciclo de vida del servicio, facturación y pago, planificación del trabajo y sistemas de planificación.

- Capacidad de diseño, desarrollo y personalización mediante APIs, programación estándar e interfaces para generar aplicaciones y funcionalidades específicas, proporcionando la personalización de las interfaces y alcanzando el desarrollo, conectividad y apoyo en las distintas capas de la arquitectura de la plataforma.

Este modelo supone una aproximación o una referencia inicial a las arquitecturas IoT, arquitecturas que se verán con más detalles en el apartado de “Plataformas IoT e IoE”, dentro del capítulo dedicado a “Elementos Técnicos”. No obstante, como se ha explicado al inicio, no hay un criterio o estándar que defina cómo debe ser la arquitectura de una solución IoT. Diferentes investigadores han propuesto variaciones o arquitecturas similares en las que puede variar el número de capas y sus funciones.

Opciones de Despliegue:

Otra forma de observar una arquitectura IoT es en relación a las opciones para su despliegue. Por un lado, la forma más común y que se presenta en la mayoría de las arquitecturas IoT que se verán en el apartado de "Plataformas IoT e IoE", es el mostrado en la siguiente figura, donde se aprecia una arquitectura que identifica dos tipos de sistemas: por un lado, sistemas ubicados en la Plataforma, normalmente alojados en la "Nube" (*on-Cloud o Cloud Computing*), lejos de los dispositivos IoT, y, por otro lado, sistemas ubicados en el Borde "*Edge*" (*on-Premise o Edge Computing*), que incluye los dispositivos de sensorización, control, procesamiento e incluso, dependiendo de la capacidad de almacenamiento y procesado, los denominados sistemas en la "Niebla" (Fog o Fog Computing).

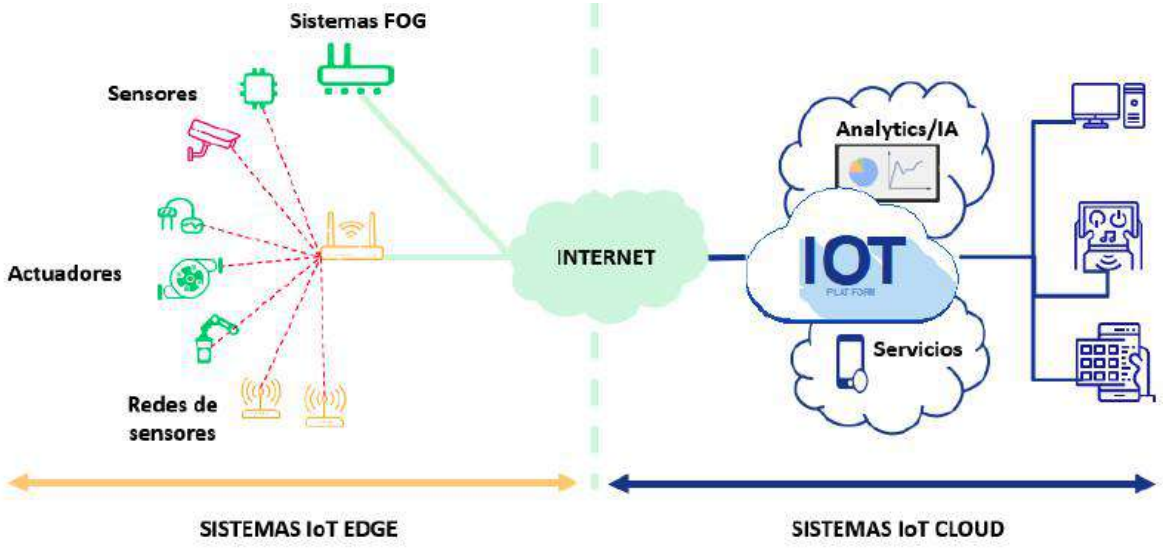


Figura 3: Diferenciación Sistemas IoT Edge y Cloud. (Fuente: Elaboración propia)

Por lo tanto, lo más usual es tener plataformas IoT cuya parte de software de Plataforma se encuentra desplegada en la Nube, ofreciendo sus servicios y utilidades de gestión y analítica en formato SaaS o PaaS. Pero esta opción no siempre es viable por requerimientos de seguridad, comunicaciones, o por otras necesidades de los clientes, por lo que otra forma de despliegue de la parte de Plataforma IoT en estos casos es on-premise en servidores o CPDs ubicados en la propia instalación.

Un estudio de 39 plataformas de IoT (5) concluyó en una arquitectura genérica y con características comunes para las plataformas de IoT. En la figura se muestra esa arquitectura de IoT en su forma más completa, y se presentan dos posibilidades. Los diversos módulos y servicios de IoT pueden desplegarse en modo local (on-premise), o en lo que se denomina la nube, dependiendo de las restricciones que imponga cada caso de uso.

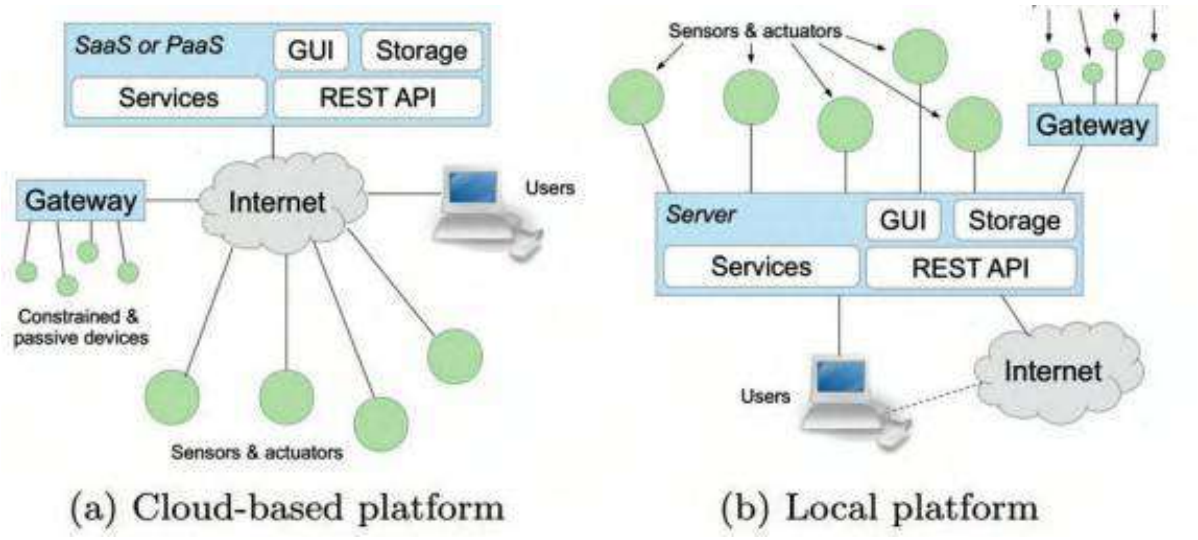


Figura 4: Arquitectura generalizada de IoT (5).

Los módulos genéricos de estas plataformas son los siguientes (5):

- Actuadores o nodos sensores, es decir, "cosas" que actúan en función de los datos/ comandos recibidos, o que generan información y luego la envían.
- Gateways o Pasarelas que "ocultan" dispositivos restringidos que podrían estar comunicándose a través de redes no basadas en IP ("legacy") y/o incapaces de implementar la interfaz necesaria para conectarse con la plataforma por sí mismos.
- Una interfaz de plataforma que recibe los datos de los dispositivos y que interacciona como intermediario entre esos datos y otros módulos (gateway y distribuidor de datos).
- Almacenamiento de datos, a menudo distribuido, al que pueden acceder otros módulos de la plataforma.
- Varios módulos de servicio que acceden a datos históricos o a datos entrantes en streaming y generar conocimiento y tienen diferentes capacidades de procesamiento (es decir, "aplicaciones de Big Data").
- Interfaces gráficas para que los usuarios puedan gestionar el sistema y validar los resultados de la producción (es decir, "Business Insights").

Los nodos y gateways, se encuentran desplegados siempre en el lado Edge, donde se encuentran los sensores y actuadores que, por ejemplo, se pueden encontrar localizados en plantas de producción, edificios inteligentes, etc. Aquí, se aprovecha la información de las comunicaciones, cuyos retardos son mínimos y operan en tiempo real entre los sistemas dados. En esta parte, se recoge principalmente la telemetría de los procesos, para luego agregarla y pre-procesarla bien de forma local, si la plataforma IoT está on-premise, o, de forma remota, si la plataforma está en la nube. Los dispositivos o nodos suelen estar apoyado por un gateway que proporciona la unificación y conectividad hacia la Plataforma en cualquier formato de despliegue. En el modo Cloud, el gateway actúa como límite de una red WAN, aislando a la red local (de ahí el nombre de edge). Este formato común

de arquitectura permite localizar los controles y las operaciones (es decir, la analítica y la computación local o de borde). Su principal beneficio, es que, de esta manera, estamos rompiendo la complejidad de los sistemas de IoT, permitiendo escalar tanto en el número de activos gestionados como en la red (6).

La red de acceso permite que los flujos de datos y el control se establezcan entre las capas de Borde y Plataforma. Esta red puede tratarse de una red privada o una red corporativa a través de la Internet pública o una red 2G/3G/4G/5G.

La capa de Plataforma recibe la información de telemetría del lado Edge. Asimismo, se encarga de ejecutar los comandos de control procedentes del lado Plataforma, y algunos de estos comandos pueden ser reenviados al lado Edge (de nube a dispositivo). Integra y analiza el flujo de información proveniente del Nivel Edge y otros sistemas. Proporciona funciones de gestión de dispositivos y activos (por ejemplo, actualizaciones del firmware para gateways). También ofrece servicios no específicos del dominio, como la consulta y el análisis de datos. Los bloques funcionales de la Plataforma de la nube son los mismos que en cualquier plataforma genérica de IoT (6).

En el lado de la Plataforma IoT, también se recibe los flujos de datos procesados que vienen de los dispositivos Edge hacia los diferentes servicios de la Plataforma. También puede enviar comandos de control a los Niveles de Borde y a la Plataforma. Este nivel es el principal beneficiario del sistema de IoT. Las aplicaciones empresariales se ubican en este nivel (ERP, CRM, etc.)

Como se verá en los siguientes apartados la mayoría de las plataformas presentan una arquitectura similar diferenciando claramente los sistemas fog/edge de los sistemas disponibles en la nube (cloud).

1.2 SEGURIDAD Y PRIVACIDAD

> ***La seguridad es un desafío crítico para el desarrollo de IoT, ya que constituye una versión ampliada del modelo convencional de Internet no segura y combina múltiples tecnologías.***

La seguridad de las soluciones IoT es una de las mayores preocupaciones de los desarrolladores y de los usuarios. Las aplicaciones IoT tienen que hacer frente a los ataques tradicionales ya conocidos y, además, es necesario que aseguren en todo momento las transmisiones de datos desde los dispositivos a otros dispositivos o a la nube. IoT debe tener en cuenta los siguientes retos a la hora de desarrollar soluciones seguras (4):

> Interoperabilidad de los distintos elementos que componen una solución.
> Dispositivos con recursos limitados.
> Resistencia a los ataques físicos y los desastres naturales.
> Control autónomo de los dispositivos IoT.
> Grandes volúmenes de información.
> Protección de la privacidad en los dispositivos.
> Escalabilidad de las soluciones IoT.

Para responder a estos retos se están desarrollando herramientas de búsqueda y seguridad. Existen diferentes motores de búsqueda basados en la web para la exploración genérica de vulnerabilidades de todo tipo de dispositivos como Zmap[2] o Censys[3], y otras herramientas en línea como Thingful[4] que se utilizan para recopilar datos de dispositivos IoT conectados, pero Shodan es actualmente el más extendido para el estudio de la ciberseguridad en IoT debido a la facilidad de uso de sus interfaces web y APIs.

"Shodan[5] es un motor de búsqueda para explorar Internet y así encontrar dispositivos conectados. Su principal uso es proporcionar una herramienta a los investigadores y desarrolladores de ciberseguridad para detectar dispositivos vulnerables conectados a Internet sin necesidad de escanearlos directamente" (7).

Debido a sus características, Shodan puede utilizarse para realizar auditorías de ciberseguridad en sistemas y dispositivos de IoT utilizados en aplicaciones que requieren estar conectados a Internet. "La herramienta permite detectar las vulnerabilidades de los dispositivos de IoT que están relacionadas con dos problemas comunes de ciberseguridad en IoT: la aplicación de mecanismos de seguridad débiles y la falta de una configuración de seguridad adecuada" (7).

Shodan es, básicamente, un motor de búsqueda que analiza qué servicios ofrecen las direcciones IP públicas de Internet. Es decir, Shodan intenta descubrir si detrás de una dirección IP hay un servidor Web, un servidor de aplicaciones, un router, una cámara web, un dispositivo de control industrial, etc.

Además de eso, también intenta descubrir si estos dispositivos y servicios que descubre ofrecen algún tipo de vulnerabilidad que haga que puedan ser puestos en compromiso.

2 https://zmap.io/
3 https://censys.io/
4 https://www.thingful.net/
5 https://www.shodan.io/

> ***En los últimos años, varios investigadores han utilizado Shodan para evaluar la seguridad de diferentes dispositivos de IoT. Por ejemplo, se ha utilizado Shodan para detectar dispositivos como routers, cortafuegos o cámaras web que utilizaban credenciales predeterminadas o contraseñas simples.***

Shodan se ha utilizado en coordinación con otras herramientas como Masscan[6] y Nmap[7] para detectar en routers DSL ciertas vulnerables, así como en impresoras y dispositivos de IoT afectados por el virus Heartbleed[8]. También se ha utilizado Shodan para detectar cámaras web y cámaras inteligentes conectadas: los investigadores encontraron miles de ellas mal configuradas o sin controles de seguridad.

Shodan almacena en sus bases de datos resultados repartidos por todo el mundo. Se pueden ver sus direcciones IP públicas, ubicación geográfica, principales servicios, etc.

Además de esto, en algunos casos es posible incluso acceder a la imagen de la cámara en cuestión, bien porque no se han establecido mecanismos de autenticación o bien porque son los de fábrica.

1.2.1 Amenazas de seguridad en IoT

> "Internet de las Cosas, como cualquier red de comunicaciones, está expuesta a diversos tipos de vulnerabilidades y amenazas de seguridad. Además, los objetos de IoT tienen la capacidad de interactuar con su entorno de manera automática y autónoma, sin ningún control de factores externos y, por esta razón, pueden causar diversos problemas de seguridad y privacidad. Por último, las múltiples interconexiones, ya sea entre los usuarios y los objetos o entre los objetos, generan enormes cantidades de datos que son difíciles de gestionar." (4)

Para analizar las amenazas a las que se enfrentan los sistemas IoT, se ha utilizado el modelo de cuatro capas que se ha introducido en el apartado anterior, "Modelo de capas IoT" (4), mediante el cual se observan diferentes niveles de las potenciales amenazas a tener en cuenta:

- Capa de percepción.
- Capa de comunicación.
- Capa de soporte.
- Capa de negocio.
- Múltiples capas

6 https://github.com/robertdavidgraham/masscan
7 https://nmap.org/
8 https://heartbleed.com

Amenazas a la seguridad en la capa de percepción

A continuación, se enumeran las principales amenazas que predominan en la capa de percepción (4):

> **Desastres naturales y amenazas ambientales.**
> **Amenazas físicas de origen humano:** escuchas, vandalismo, manipulación de dispositivos, etc. En este conjunto se incorporan los ataques de tipo Canal Lateral, que se fundamenta en la obtención de la información mediante el análisis sofisticado de la implementación física del dispositivo detectando los consumos de energía, fugas electromagnéticas, medidas de tiempo o sincronización o el sonido del procesador en la ejecución de algoritmos o funciones de encriptación.

Amenazas a la seguridad en la capa de comunicación

Existen varios tipos de ataques que se pueden dar a este nivel. Como ejemplo, en los ataques de sumidero el propósito de los nodos maliciosos es dirigir el tráfico de la red a un nodo específico (4). El nodo S representa el gateway de la red, el dispositivo encargado de enviar los datos recogidos por el resto de nodos hacia Internet, por ejemplo. El resto de nodos representan nodos de una red de sensores inalámbricos que pueden usar distintas tecnologías de interconexión: Zigbee, por ejemplo. El nodo E representa un nodo malicioso que, o bien ha sido añadido por el atacante, o bien ha sido puesto en compromiso por el atacante, que es capaz de "engañar" al resto de nodos para que les envíe los datos que recogen:

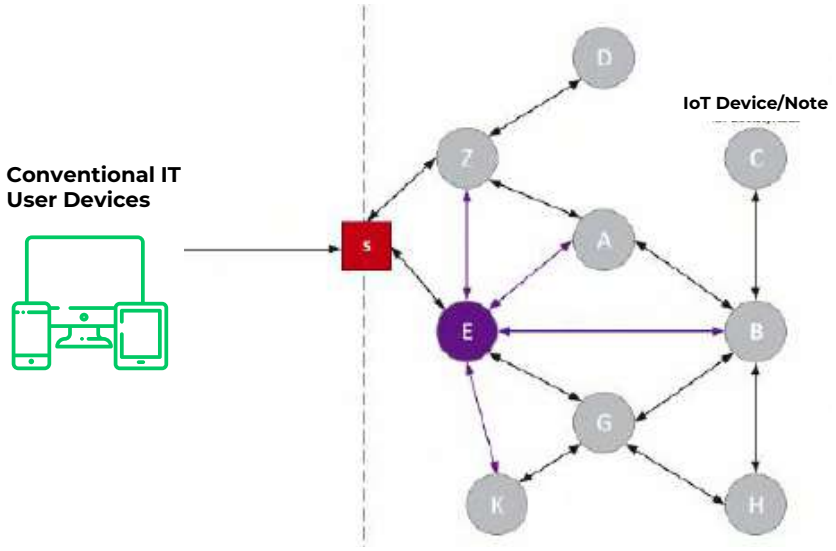


Figura 5: Ataque de sumidero (4).

Otro tipo de ataque muy conocido es el ataque de hombre en el medio (MiTM, *Man in The Middle*): el atacante puede observar los mensajes de comunicación que se intercambian entre dos sistemas o nodos IoT.

Amenazas a la seguridad en la capa de soporte

Las tecnologías clave de la capa de soporte son la computación en la nube, fog computing y edge computing. Su utilización plantea una serie de problemas de seguridad, como el acceso no autorizado a los recursos de las aplicaciones o servicios de software inseguros, que se deben a la dependencia de los proveedores de este tipo de tecnologías (4).

Amenazas de seguridad en la capa de negocio

Las amenazas de esta capa intentan aprovechar las debilidades de los usuarios en cuanto al uso seguro de las aplicaciones. Incluyen las técnicas de ingeniería social y también el aprovechamiento de las lagunas de programación de las aplicaciones (4).

Amenazas de seguridad de múltiples capas

También existen ataques que pueden realizarse en múltiples capas, como, por ejemplo, los ataques de denegación de servicio[9], las botnets[10], o las amenazas persistentes avanzadas (APTs)[11] (4).

1.2.2 Contramedidas de defensa

A continuación, se contemplan posibles soluciones de seguridad para las amenazas mencionadas.

Contramedidas en la capa de percepción

El Proyecto OWASP IoT[12] ha señalado que la seguridad física inadecuada sigue estando entre las 10 principales vulnerabilidades de IoT (8).

> "Cuestiones técnicas como el diseño de la infraestructura, el diseño y la colocación de sensores, los procedimientos de mitigación, la capacitación personal y los mecanismos de recuperación pueden gestionar eficientemente los desastres naturales y las amenazas ambientales.
>
> Por otra parte, para hacer frente a las amenazas físicas causadas por el hombre, el primer paso es asegurar que sólo los usuarios y objetos legítimos puedan acceder a los dispositivos físicos y a su información. Por lo tanto, se necesitan sistemas de autenticación de usuarios y mecanismos de control de acceso físico. Los mecanismos de autenticación de usuarios, como los sistemas basados en contraseñas, los sistemas

9 https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos
10 https://www.kaspersky.es/resource-center/threats/botnet-attacks
11 https://www.kaspersky.es/blog/que-es-una-apt/966/
12 https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

basados en tokens (por ejemplo, las tarjetas electrónicas y las tarjetas inteligentes) y los sistemas biométricos pueden determinar si un usuario o un objeto puede acceder a los recursos físicos y a sus datos." (4)

Contramedidas en la capa de comunicación

Los protocolos de comunicación usados en IoT ya incorporan en su mayoría mecanismos de seguridad que garantizan la confidencialidad, integridad y autenticidad de las comunicaciones (9). Pero también presentan limitaciones y posibles vulnerabilidades. La siguiente tabla presenta las capacidades de seguridad y las vulnerabilidades de los principales protocolos (4).

Protocolo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Protección frente a ataques de repetición	Vulnerabilidades o limitaciones
IEEE 802.15.4	Sí	Sí	No	Sí	Sí	No protege los mensajes ACK. No implementa todos los modelos de claves. Control de acceso ineficiente.
ZigBee	Sí	Sí	No	Sí	Sí	Vulnerable frente a ataques de repetición. Vulnerable frente a ataques de interferencia. Control de acceso ineficiente. Problemas en la gestión de claves.
Z-Wave	Sí	Sí	No	Sí	Sí	Vulnerabilidades en aplicaciones específicas. Vulnerable frente a ataques de interferencia.
BLE	Sí	Sí	No	Sí	No	Vulnerable frente a ataques de repetición. Vulnerable frente a ataques de interferencia. Problemas en la gestión de claves.
LoRaWAN	Sí	No	No	No	No	Vulnerable frente a ataques de repetición. Vulnerable frente a ataques de interferencia. Problemas en la gestión de claves.
6LoWPAN	No	No	No	No	No	No proporciona medidas de seguridad.
RPL	Sí	Sí	No	No	Sí	Vulnerable frente a ataques de red.
TLS	Sí	Sí	No	Sí	Sí	Pesado para aplicaciones IoT.
DTLS	Sí	Sí	No	Sí	Sí	Varias limitaciones para aplicaciones IoT.
CoAP	Vía DTLS	Vía DTLS	No	Vía DTLS	Vía DTLS	Depende de DTLS.

Tabla 2: Seguridad de los protocolos de comunicaciones IoT (4).

Es necesario seleccionar en cada caso los protocolos de comunicación que puedan cumplir con los requisitos de seguridad que se establezcan en las aplicaciones IoT.

Además del uso de protocolos de comunicación seguros, entre las contramedidas más utilizadas y con mayor efectividad en la capa de comunicación se encuentran los sistemas cortafuegos y los sistemas de detección y prevención de intrusiones.

- **Sistemas Cortafuegos:** Un sistema cortafuegos es un sistema de protección, constituido por un hardware, un software, o por ambos componentes, que controla las actividades

de la red continuamente haciendo uso de un conjunto de reglas predefinidas. Estos sistemas tienen la función de analizar el tráfico de la red desde distintos niveles, desde los paquetes de red de bajo nivel hasta los paquetes de protocolos de aplicación (10).

Un cortafuegos, en un entorno de IoT, puede instalarse en un nodo intermedio central y si la capacidad del dispositivo IoT lo permite también en éste, de tal forma que se encargará de la comunicación entre los dispositivos de IoT y los sistemas IT convencionales.

- **Sistemas de Detección y Prevención de Intrusiones:** Los sistemas de detección y prevención de intrusiones IDPS comprenden un conjunto de mecanismos de protección que tienen por objeto detectar, registrar y prevenir posibles amenazas en tiempo real. Como en el caso de los sistemas de cortafuegos, un IDPS puede instalarse en los nodos de IoT o en un nodo intermedio (4).

Contramedidas en la capa de soporte

En esta capa son necesarios sistemas de autenticación a distancia y mecanismos de control de acceso. También es crítico garantizar la seguridad de las comunicaciones a este nivel mediante el uso de protocolos de seguridad como el protocolo TLS para el cifrado (4).

Otras tecnologías interesantes a este nivel son las redes privadas virtuales (VPNs)[13] para los accesos remotos a dispositivos o redes, tecnologías como Blockchain[14] para lograr la confianza entre participantes o el Onion Routing[15] para garantizar el anonimato y la privacidad de los datos.

Además, las técnicas de programación segura, los cortafuegos y los sistemas IDPS son contramedidas importantes, ya que pueden evitar la pérdida o la fuga de datos.

Contramedidas en la capa de negocio

Los mecanismos de seguridad en la capa de negocio tienen que asegurar la protección de las aplicaciones y del sistema operativo de los dispositivos de IoT y de las interfaces de usuario.

> "Las principales amenazas a la seguridad de las aplicaciones de software se deben a la programación insegura. Las posibles soluciones para este problema pueden ser la utilización de un lenguaje de programación de alto nivel, que gestiona automáticamente los problemas de memoria. También, como en la capa de soporte, la seguridad del sistema operativo debe ser mejorada por varias herramientas y procesos de seguridad, como el control de acceso y los sistemas IDPS (11). Por último, los procesos de gestión y formación son muy críticos a este nivel, ya que pueden proteger a los usuarios de las técnicas de ingeniería social." (4)

13 https://www.osi.es/es/actualidad/blog/2016/11/08/te-explicamos-que-es-una-vpn-y-para-que-se-usa
14 https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/
15 https://www.xataka.com/basics/red-tor-que-como-funciona-como-se-usa

Además, en esta capa de negocio también es necesario tener en cuenta la normativa concerniente a la protección de datos de los usuarios. Los diferentes usuarios de soluciones IoT deben atenerse al Reglamento General de Protección de Datos de la UE (GDPR). Los usuarios de productos y servicios de IoT deben poder ejercer sus derechos de información, acceso, borrado, rectificación, portabilidad de los datos, restricción del procesamiento, objeción al procesamiento y su derecho a no ser evaluados sobre la base de un procesamiento automatizado.

1.2.3 Privacidad desde el diseño

Además de las contramedidas de defensa expuestas, es muy importante la adopción de metodologías seguras de desarrollo de los distintos componentes que participan en una solución de IoT: dispositivos, sensores, actuadores, protocolos de comunicación, gateways, plataformas, etc. Además, se ha de tener en cuenta no sólo la seguridad de los sistemas en sí mismos, sino también la garantía de privacidad de los datos que puedan recoger y enviar. En este sentido, es muy recomendable la adopción del concepto de "privacidad desde el diseño" o Privacy by Design (PbD) (12), un modelo integral de privacidad definido por Ann Cavoukian, delegada de protección de datos de Ontario, en la década de los 90.

En el artículo referenciado, se defiende que la privacidad debe ser abordada desde la perspectiva del diseño. La privacidad debe incorporarse a los sistemas y tecnologías de datos conectados en red por defecto. El Reglamento (UE) 2016/679, General de Protección de Datos, en su artículo 25 y bajo el epígrafe 'Protección de datos desde el diseño y por defecto', incorpora a la normativa de protección de datos la práctica de considerar los requisitos de privacidad desde las primeras etapas del diseño de productos y servicios. Por lo tanto, le confiere la categoría de requisito legal. (13) La privacidad debe estar integrada en cada estándar, protocolo y proceso. Los principios definidos en PbD son los siguientes (12):

- **Proactivo, no Reactivo; Preventivo no Correctivo:** El enfoque busca medidas proactivas más que reactivas.
- **Privacidad como configuración por defecto:** La privacidad desde el diseño pretende ofrecer el máximo grado de privacidad asegurando que los datos personales estén automáticamente protegidos en cualquier sistema informático o práctica empresarial.
- **Privacidad embebida en el diseño:** Está integrada en el diseño y la arquitectura de los sistemas informáticos y las aplicaciones empresariales y no como un complemento.
- **Funcionalidad total:** Privacidad desde el diseño trata de dar cabida a todos los intereses y objetivos legítimos.
- **Seguridad extremo a extremo – Protección de todo el ciclo de vida:** La privacidad desde el diseño se extiende de forma segura a lo largo de todo el ciclo de vida de los datos involucrados.
- **Visibilidad y transparencia:** Privacidad desde el diseño trata de asegurar a todas las partes interesadas.
- **Respeto por la privacidad del usuario:** La privacidad desde el diseño requiere que los

operadores y diseñadores mantengan, por encima de todo, los intereses del individuo en primer lugar.

1.2.4 Criptografía ligera

Tal y como se ha sugerido en las secciones anteriores, uno de los principales desafíos a los cuales se ha enfrentado el boom de IoT en la última década es que hoy en día aún no se disponen de estándares claros y aceptados globalmente. Por lo tanto, los fabricantes de dispositivos de IoT no tienen manuales de referencia para diseñar sus productos y que cumplan unos mínimos requisitos de seguridad y privacidad.

En este contexto, es todavía más flagrante la falta de estándares en el área de Criptografía, la ciencia sobre la que se sustentan todas las capacidades que se exigen a un sistema seguro en el ámbito de la ciberseguridad (por ejemplo: autenticación, confidencialidad e integridad).

No obstante, la culpa no es solo de un fabricante de IoT en concreto por ejemplo no incorporar en su dispositivo los algoritmos de cifrado adecuados, por ejemplo. Lo cierto es que la mayoría de los algoritmos estandarizados hoy en día fueron diseñados en los años 80 y 90, cuando aún no existía IoT. Por aquel entonces ni se imaginaba el impacto que podría llegar a tener el IoT en el futuro. En consecuencia, es normal que los algoritmos criptográficos de cifrado que están presentes en billones de dispositivos, como AES (14), no fueran diseñados para ser óptimamente usados en dispositivos con recursos limitados (i.e., memoria, batería o procesamiento). En resumen, estos algoritmos no forman parte de lo que llamamos *Criptografía ligera*: algoritmos diseñados con las necesidades de dispositivos de recursos limitados en mente, y que tienen en cuenta que dichos dispositivos pueden ser fácilmente acechados por un atacante para llevar a cabo ataques de canal lateral (i.e., *Side-channel attacks*).

Aunque en los últimos años ha habido algún intento de estandarización, como por ejemplo de ISO (15) (serie de ocho documentos que contienen estándares de criptografía ligera), la verdad es que la comunidad criptográfica ha permanecido a la espera de NIST, el National Institute of Standards and Technology de Estados Unidos de América, ya que es la organización que más influencia tiene en el mundo de los estándares criptográficos.

NIST publicó un documento con un estado del arte de la criptografía ligera en 2017, declarando sus intenciones de llevar a cabo un proceso de estandarización (16). La cronología de los eventos que han ocurrido desde entonces se puede observar en la siguiente figura:

Figura 6: Cronología del proceso de estandarización de NIST para criptografía ligera (16).

En 2018 NIST publicó la convocatoria oficial de la competición que querían llevar a cabo. Para empezar en el ámbito de la criptografía ligera, NIST prefirió centrarse solo en algoritmos de cifrado autenticado con datos asociados (*Authenticated Encryption with Associated Data – AEAD*) así como en funciones resumen (*Hash functions*). Los parámetros que se definieron y que regirían en la competición a la hora de escoger los nuevos estándares son los siguientes:

> Rendimiento del algoritmo en Software (*Throughput*)
> Consumo de memoria en Software
> Tamaño del código binario en Software
> Protección contra ataques de canal lateral en Software
> Rendimiento del algoritmo en Hardware (*Throughput*)
> Recursos necesarios en Hardware (*Área*)
> Protección contra ataques de canal lateral en Hardware

Como se puede ver, los parámetros son diferentes a cualquier otra competición criptográfica que se haya llevado a cabo anteriormente, y por lo tanto NIST motivó a la comunidad criptográfica a innovar en este sentido, y proporcionar candidatos que fueran realmente diseñados para un entorno IoT. Con *Software*, NIST se refiere a implementaciones que se puedan ejecutar en microprocesadores de, como mínimo, 32 bits, aunque la mayoría de las propuestas acabaron siendo compatibles con procesadores de 8 bits. Con *Hardware*, NIST se refiere tanto a plataformas de FPGAs como de ASIC.

En febrero de 2019, fecha límite para enviar propuestas a NIST, la competición de criptografía ligera empezó oficialmente con 56 candidatos. En agosto de 2019 NIST seleccionó 32 propuestas, que pasaron a segunda ronda. Actualmente, la competición sigue en segunda ronda y la comunidad científica está dedicando sus esfuerzos a investigar qué candidatos son los más prometedores. En principio se espera que la competición termine a finales de 2021 o mediados de 2022, y los primeros estándares de criptografía ligera de NIST tendrían que estar definidos para 2023.

1.3 INTEROPERABILIDAD

> ***Los sistemas informáticos, en muchas ocasiones, están distribuidos y tienen una naturaleza dinámica. La interoperabilidad se define como la capacidad de dos o más sistemas o componentes para intercambiar datos y utilizar información.***

Los sistemas informáticos, en muchas ocasiones, están distribuidos y tienen una naturaleza dinámica. Además, esos sistemas se basan en tecnologías heterogéneas y utilizan diferentes representaciones de la información. Estos factores obstaculizan el intercambio y el procesamiento de datos entre los diferentes agentes (dispositivos, máquinas, controladores, sensores...). Por lo tanto, para lograr la plena interoperabilidad, la información intercambiada no sólo debe tener una base sintáctica común, sino también una estructura y una semántica comunes (17).

De acuerdo con la ISO/IEC 2382:2015 "Information technology — Vocabulary"[16], la interoperabilidad es: "La capacidad de comunicar, ejecutar un programa o transferir datos entre varias unidades funcionales de manera que se requiera que el usuario tenga un conocimiento escaso o nulo de las características únicas de esas unidades". Ésta es una de las definiciones más clásicas de interoperabilidad, pero existen otras.

La interoperabilidad se puede definir como un proceso para garantizar la accesibilidad y disponibilidad continuas de la información, y la capacidad de un sistema para utilizar la información de otros sistemas (18). La interoperabilidad se refiere a un problema de representación de datos, establecimiento de redes e intercambio de información de plataformas. También sostienen que la cuestión de la integración es un problema de interoperabilidad. Para lograr integrar los niveles superiores de una empresa con la planta de producción (integración vertical) o diferentes empresas entre sí (integración horizontal) se necesitan estrategias óptimas de interoperabilidad. Además, la interoperabilidad es una propiedad necesaria para transferir datos desde plataformas y dispositivos heterogéneos, de modo que se necesite poca o ninguna participación humana (19).

1.3.1 Tipos de Interoperabilidad

La interoperabilidad se puede clasificar teniendo en cuenta distintas perspectivas. La clasificación más genérica describe cuatro tipos o niveles de interoperabilidad (20):

- **Interoperabilidad técnica**: permite las comunicaciones entre máquinas mediante protocolos de comunicación y la infraestructura de hardware/software necesario para

16 https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en

que esos protocolos funcionen.

- **Interoperabilidad sintáctica**: proporciona una sintaxis y una codificación comunes a los datos intercambiados, mediante lenguajes de representación de datos como el eXtensible Markup Language (XML) o el HyperText Markup Language (HTML).
- **Interoperabilidad semántica**: garantiza que haya un significado y una comprensión comunes de los datos intercambiados. Concretamente, la interoperabilidad semántica garantiza que los sistemas informáticos puedan intercambiar datos de manera inequívoca, compartiendo el significado de los mismos. También es una base para permitir una lógica computable eficaz de la máquina (por ejemplo, algoritmos de aprendizaje de la máquina), al tiempo que impulsa la inferencia, la extracción de conocimientos y el descubrimiento de conocimientos. Asimismo, la interoperabilidad semántica facilita la federación de datos y servicios entre los sistemas de información, lo cual es particularmente útil en los escenarios que implican sistemas ciberfísicos interconectados.
- **Interoperabilidad organizativa**: Permite el intercambio de datos entre organizaciones que dependen de infraestructuras diferentes y sistemas de información heterogéneos. Este nivel de interoperabilidad requiere una interoperabilidad técnica, sintáctica y semántica satisfactoria.

En la siguiente tabla se mapean estos niveles de interoperabilidad satisfactorias con las capacidades de comunicación o aplicación que presenta un dispositivo o sistema (21):

Característica	Descripción	Nivel de Interoperabilidad
Capacidades de Comunicación de un dispositivo		
Protocolos de Comunicación	Esta característica consiste en todos los protocolos de las capas 1 a 7 del modelo de referencia OSI, es decir, desde el acceso al medio físico hasta el protocolo de la capa de aplicación.	Técnica
Interfaz de Comunicación	Esta característica consiste en la definición del servicio de comunicación de la capa de aplicación, incluidos los servicios y los parámetros de servicio. Pueden ser necesarios mecanismos de mapeo adicionales. El rendimiento dinámico del sistema de comunicación forma parte de esta característica.	
Acceso a datos	Esta característica consiste en la definición de la operación del objeto o los atributos del parámetro de acceso del bloque de entrada de datos, salida de datos y parámetros	Sintáctica
Capacidades de Aplicación de un dispositivo		
Tipos de datos	El tipo de datos de entrada o salida de datos o los parámetros utilizados definen esta característica.	Sintáctica
Semántica de datos	Esta característica consiste en los rasgos característicos (atributos de los parámetros) de los datos de la aplicación, que pueden ser el nombre de los datos, las descripciones de los datos, la gama de datos, el valor de sustitución de los datos, el valor por defecto, la persistencia de los datos, contexto, etc.	Semántica

Característica	Descripción	Nivel de Interoperabilidad
Funcionalidad de la aplicación	Esta característica consiste en especificar las dependencias y reglas de consistencia dentro de los Elementos Funcionales. Esto se hace en la parte de descripción de datos o en una sección separada de comportamiento.	Organizacional Funcional
Funcionamiento dinámico	Esta característica consiste en limitaciones de tiempo que influyen en los datos o en el comportamiento general del dispositivo. Por ejemplo, la tasa de actualización de un valor de proceso puede influir en los algoritmos de bloque.	

Tabla 3: Características de dispositivos a nivel de interoperabilidad. (21)

Hoy en día la interoperabilidad técnica está casi resuelta por la amplia difusión de las tecnologías de Internet. La combinación de los paradigmas emergentes como la IoT, las nuevas tecnologías, la computación en la nube, el concepto máquina a máquina (M2M), la computación orientada a servicios (SOC), la arquitectura orientada a servicios (SOA), unido a una amplia difusión de la tecnología de la información (IT), están impulsando poderosas y, sobre todo, nuevas oportunidades de negocio para las empresas al facilitar la integración de dispositivos, sistemas, aplicaciones y componentes (22). Sin embargo, si por un lado estas tecnologías y enfoques están resolviendo la interoperabilidad técnica, por otro lado, no son capaces por sí solas de manejar la gran heterogeneidad de los modernos procesos y/o dispositivos complejos. El problema de la interoperabilidad está lejos de ser resuelto y la difusión y proliferación de nuevas tecnologías y dispositivos es cada vez más compleja.

Es necesario normalizar y homogeneizar la forma en que se representan y estructuran los datos para hacer frente al problema de la integración de los datos de los sistemas de múltiples proveedores en aras de la generación de conocimientos y la distribución de información a todos los nodos de adopción de decisiones necesarios.

1.3.2 Paradigmas de interacción

Hay varios problemas de diseño que condicionan la forma en que los sistemas y dispositivos se comunican en una arquitectura IoT. La forma en que un sistema se integra en las arquitecturas de red, el flujo de información entre los sistemas finales, la frecuencia de los mensajes, la sincronicidad, la seguridad, la capacidad de los dispositivos y sus funciones en las redes de comunicación son algunas de las limitaciones que deben considerarse para la clasificación de los protocolos. Existe un conjunto básico de paradigmas por los que funcionan la mayoría de los protocolos de aplicación de Internet. Entre ellos figuran los siguientes (17):

- **"Paradigma de extremo a extremo:** El modelo de conexión a Internet se basa en la utilización de la capa de transporte subyacente para proporcionar un servicio transparente de flujo de datos entre los procesos de aplicación, o los denominados puntos finales de aplicación. Al considerar la capa de aplicación, esto puede denominarse un paradigma de extremo a extremo en el que sólo los puntos finales participan en los intercambios de protocolos de aplicación.

- **Sesiones de streaming en tiempo real:** Muchas aplicaciones tratan con flujos de datos en tiempo real, como pueden ser los datos recopilados por sensores. El protocolo de Internet funciona básicamente con un enfoque de mejor esfuerzo (Best Effort), sin garantías de calidad de servicio (QoS). Sin embargo, los protocolos de Internet ya ofrecen un buen marco para trabajar con flujos en tiempo real. El protocolo de transporte en tiempo real (RTP) [RFC3550] encapsula los flujos con la información apropiada de tiempo y secuencia, mientras que el protocolo de control RTP complementario (RTCP) se utiliza para controlar el flujo.
- **Paradigma publicador y subscriptor:** es un paradigma de mensajería asíncrona en el que los editores envían datos sin saber quién es el receptor, y los receptores se suscriben a los datos en función del tema o el contenido de los mismos. Se puede implementar utilizando intermediarios centralizados que emparejan a los editores y los suscriptores. Esta disociación de los puntos finales de la aplicación permite la escalabilidad y la flexibilidad. En el caso de IoT, este paradigma desempeña un papel importante, ya que la mayoría de las aplicaciones se centran en los datos, es decir, no es tan importante quién envía los datos, sino más bien cuáles son los datos.
- **Paradigma del servicio web:** Los servicios web son definidos por el W3C como un sistema de software diseñado para soportar comunicaciones interoperables de máquina a máquina a través de una red. Los servicios web en su conjunto suelen funcionar entre clientes y servidores a través de HTTP. Principalmente hay dos formas diferentes de servicios web: servicios web basados en servicios (SOAP) y servicios web basados en recursos (REST). Este paradigma se utiliza ampliamente en los sistemas de máquina a máquina (M2M)".

1.3.3 Formatos de comunicación

Las formas de intercambiar datos entre los sistemas son múltiples. Este proceso se denomina Intercambio Electrónico de Datos (IDE) y depende de los protocolos utilizados y de los formatos diseñados para esos protocolos. Los datos pueden comunicarse entre sistemas en muchos formatos diferentes. Según la fuente de los datos, el protocolo utilizado o el tipo de dispositivo, estos formatos de intercambio de datos pueden ser diferentes. A continuación, se enumeran algunos de esos formatos (17).

- **Comma separated values (CSV)[17]**
- **JSON (JavaScript Object Notation)[18]**
- **XML: Extensible Markup Language (XML)[19]**
- **Data Stream o Flujo de datos[20]**

17 https://tools.ietf.org/html/rfc4180
18 https://www.json.org/json-es.html
19 https://www.w3.org/standards/xml/core
20 https://www.confluent.io/learn/data-streaming/

1.3.4 Protocolos de comunicación

En cuanto a los protocolos de comunicaciones, en la sección "4.1 Modelos de comunicación" se presentan los protocolos estandarizados más comúnmente utilizados en el ámbito de las soluciones IoT.

1.3.5 Servicios Web

Los servicios web son un marco para la creación de aplicaciones distribuidas. Los servicios web en su conjunto pueden funcionar entre clientes y servidores a través de HTTP. Por tanto, también se han convertido en una opción interesante a la hora de comunicar y hacer interoperables dispositivos y aplicaciones en un entorno IoT.

Hay dos formas diferentes de servicios web: Simple Object Access Protocol (SOAP) and REpresentational State Transfer (REST), que se describen a continuación (17).

SOAP

Originalmente desarrollado por Microsoft, SOAP se ha convertido en una recomendación del W3C. El formato de mensajes que utiliza se basa en XML y en protocolos de capa de aplicación (HTTP, HTTPS, FTP, etc), estos se utilizan para la negociación y la transmisión de los mensajes. SOAP permite que los procesos que se ejecutan en un cliente desde sistemas operativos heterogéneos (como Linux o Windows) puedan acceder de un servidor mediante llamadas a servicios web y recibir respuestas independientemente del lenguaje y las plataformas. En la siguiente figura se presenta la arquitectura utilizada en el protocolo SOAP.

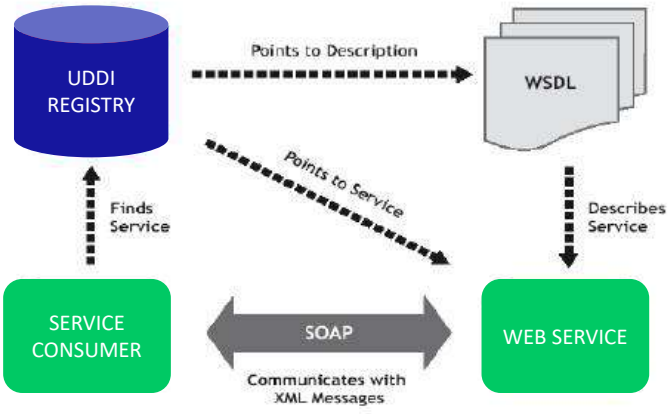


Figura 7: Arquitectura SOAP (17).

REST

Representational State Transfer (REST) o RESTful utiliza el protocolo HTTP para hacer llamadas entre máquinas. Las aplicaciones RESTful utilizan peticiones HTTP para crear y/o actualizar recursos, leer datos o realizar consultas y eliminar datos. REST es una alternativa ligera a las RPC (Remote Procedure Calls) y a los Servicios Web. REST permite la independencia

entre diferentes plataformas (Unix, Windows, Mac, ...), así como independizar el lenguaje de programación (C++ puede hablar con Java, etc.), está basado en estándares (ya que se ejecuta sobre HTTP) y puede ser fácilmente utilizado en presencia de cortafuegos.

REST no tiene ninguna característica de seguridad como la encriptación, la garantía de calidad de servicio o la gestión de sesiones, etc. pero se puede habilitar HTTPS para ser utilizado por REST.

1.3.6 Tecnologías de publicación-suscripción y mensajería

La suscripción a publicaciones es fundamental para Internet de las cosas. La mayoría de los sistemas y plataformas de IoT han adoptado este paradigma de comunicación para intercambiar información en forma de mensajes. Hay una serie de tecnologías que utilizan este paradigma. Los protocolos de mensajería más relevantes de publicación-suscripción son (17):

- **Message Queuing Telemetry Transport (MQTT)[21]:** es un protocolo de mensajería "ligero" basado en la suscripción a publicaciones para su uso en la parte superior del protocolo TCP/IP.
- **Extensible Messaging and Presence Protocol (XMPP)[22]:** es un protocolo de comunicaciones para middleware orientado a la mensajería basado en el XML.
- **Advanced Message Queuing Protocol (AMQP)[23]:** es un estándar abierto para el intercambio de mensajes entre aplicaciones u organizaciones.

1.3.7 Interoperabilidad Semántica

A pesar de las directrices marcadas por los modelos o arquitecturas de referencia, todavía hay desafíos que deben abordarse para lograr una visión integral de la interoperabilidad en el ámbito del IoT (23):

1. Interoperabilidad: las nuevas tecnologías para representar e intercambiar datos deben coexistir con los sistemas heredados que representan e intercambian datos en diferentes formatos, es decir, XML, texto plano, etc. Así pues, los nuevos formatos de datos deben coexistir con los antiguos.
2. Identificación global única: se debe permitir la intercomunicación entre un gran número de componentes a través de Internet. Por lo tanto, debe existir un mecanismo de enlace entre los distintos componentes de una solución IoT.
3. Disponibilidad de datos: los componentes deben intercambiar y realizar análisis complejos en tiempo real sobre datos generados por diferentes sensores. Por lo tanto, se necesitan mecanismos estándar para la representación e intercambio de datos.

21 https://mqtt.org/
22 https://xmpp.org/
23 https://www.amqp.org/

4. Normalización: IoT abarca muchas normas para cubrir diferentes aspectos de los procesos de aplicación. Estas normas cambian dinámicamente a medida que surgen nuevos componentes o tecnologías. Así pues, los estándares crecen en tamaño y número, lo que dificulta la interoperabilidad entre ellos.
5. Integración: los datos y componentes deben ser añadidos, eliminados o reemplazados sin afectar a la gestión del proceso de aplicación.
6. Multilingüismo: dado que los componentes de IoT interactuarán en todo el mundo, deben intercambiar entre ellos y los humanos los datos en su propio idioma.

La Web Semántica proporciona las tecnologías necesarias para afrontar los retos mencionados (23):

1. Interoperabilidad: los vocabularios de la Web Semántica permiten establecer relaciones y vincular datos de dominios heterogéneos, representados en diferentes formatos. Por lo tanto, al aplicar las tecnologías de la Web Semántica para representar los datos, tanto los nuevos dispositivos como los sistemas heredados podrían intercambiar datos y tener una comprensión común de estos datos.
2. Identificación global única: de acuerdo con los principios de la Web Semántica y los datos vinculados, se utilizan identificadores universales de recursos (Universal Resource Identifier, URI) de HTTP para identificar cualquier tipo de componente. Aplicando este mecanismo, los componentes de IoT serían identificados unívocamente y podría auto-ubicarse y comunicarse entre sí.
3. Disponibilidad de datos: la Web Semántica abarca mecanismos de representación e intercambio de datos. Por consiguiente, los datos pueden intercambiarse, procesarse y analizarse independientemente del sistema que los genere o del formato en que se almacenen.
4. Normalización: los vocabularios de la web semántica pueden utilizarse para representar en el mismo formato y vincular datos de diferentes normas, vinculando así los datos de diferentes dominios.
5. Integración: la web semántica permite añadir nuevos vocabularios y nuevos datos estableciendo relaciones con datos anteriores de manera escalable.
6. Multilingüismo: la Web Semántica permite definir vocabularios en diferentes idiomas de manera sencilla.

2 ELEMENTOS TÉCNICOS

En esta sección se abordarán los componentes fundamentales de una solución IoT: desde los protocolos de comunicaciones que se utilizan en distintos ámbitos, los sensores y actuadores que interactúan con el mundo físico y las plataformas IoT que ofrecen los proveedores para facilitar el desarrollo de estas soluciones.

2.1 MODELOS DE COMUNICACIÓN

> ***El modelo de comunicación entre dispositivos representa dos o más dispositivos que se conectan y comunican directamente entre sí, y no a través de un servidor de aplicaciones intermediario.***

2.1.1 Comunicaciones dispositivo-dispositivo

En este tipo de comunicación los dispositivos IoT se comunican entre sí sin la intervención de un tercero (24). Los protocolos y redes de comunicaciones han ido evolucionando hacia el sector de IoT para cumplir con las especificidades de este tipo de redes:

- Baja velocidad de transmisión de datos
- Baja frecuencia de transmisión
- Movilidad y servicios de localización
- Conexiones bidireccionales seguras
- Bajo consumo de energía
- Largo alcance de comunicación

Estos requisitos han dado lugar al desarrollo de las llamadas "Low Data Rate Wireless Personal Networks (LR-WPN)", en la siguiente figura se refiere a las redes de corto alcance "Short Range", que ya disponen del grupo de trabajo 802.15 WG[24] en el organismo estandarizador IEEE.

> "Las tecnologías de radio de corto alcance ampliamente utilizadas (por ejemplo, ZigBee, Bluetooth) no están adaptadas a los escenarios que requieren una transmisión de largo alcance. Las soluciones basadas en las comunicaciones de telefonía móvil (por ejemplo, 2G, 3G y 4G) pueden proporcionar una mayor cobertura, pero consumen una energía excesiva en el dispositivo. Por lo tanto, los requisitos de las aplicaciones de IoT han impulsado la aparición de nuevas tecnologías de comunicación inalámbrica: las redes de área amplia de baja potencia. Proporcionan una comunicación de largo alcance de hasta 10 a 40 km en zonas rurales y de 1 a 5 km en las zonas urbanas." (25)

En la siguiente figura se observa una comparativa de estas tecnologías en función del alcance y la velocidad de transmisión:

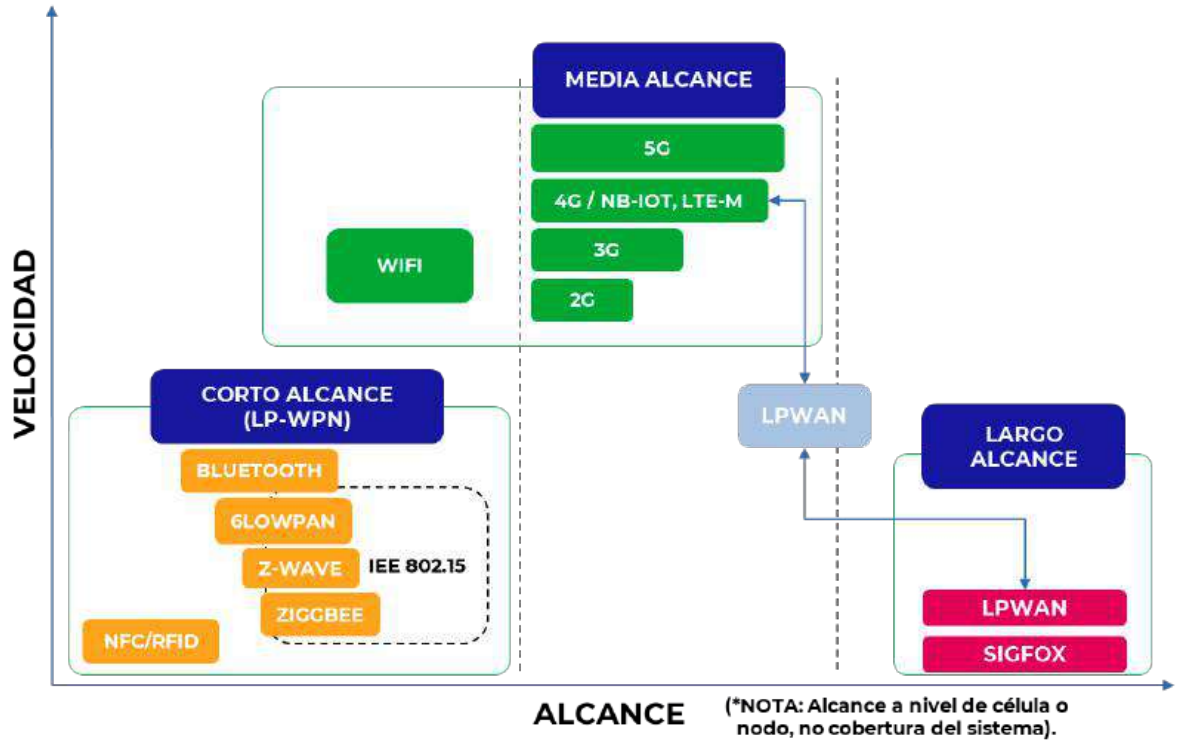


Figura 8: Relación de velocidad frente a alcance de tecnologías de comunicación.

(Fuente: Elaboración propia)

24 https://www.ieee802.org/15/

IEEE 802.15.4[25]

Es un protocolo de comunicaciones inalámbrico diseñado para dispositivos con un consumo bajo de energía y con necesidades también bajas de velocidad de transmisión. Es el caso de las redes de sensores inalámbricos, que son utilizadas en multitud de aplicaciones IoT. Ofrece una tasa de transferencia máxima de 250 Kbps y un alcance de decenas de metros entre dispositivos. Opera en 3 bandas libres de la banda ISM: 868 MHz, 915 MHz y 2.4 GHz.

Muchos de los protocolos de comunicaciones inalámbricos de bajo consumo utilizan IEEE 802.15.4 en sus niveles más bajos: ZigBee, WirelessHART, etc.

Este estándar permite que los nodos adyacentes se interconecten entre sí y construyan topologías de manera dinámica, permitiendo la transmisión de datos entre nodos que no disponen de conectividad directa a través de los nodos intermedios. Cuando es necesaria una conexión hacia el exterior, bien sea hacia Internet o hacia una red corporativa, es obligada la presencia de un nodo concentrador o *hub*, que habitualmente se denomina gateway, y tiene, normalmente, funcionalidades de *router*:

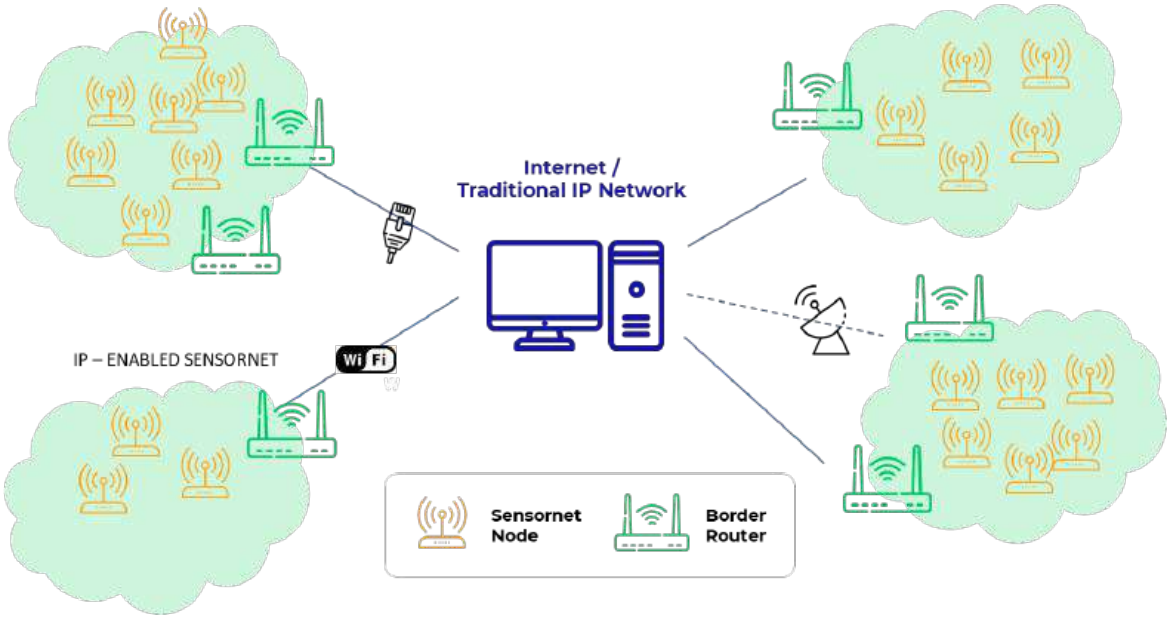


Figura 9: Red de sensores inalámbricos conectada a Internet (26).

Una de las características del protocolo IEEE 802.15.4 y, por tanto, de ZigBee y del resto de protocolos que incorporan IEEE 802.15.4, es la posibilidad de formar distintas topologías de red en malla, en función de las necesidades y al área geográfica a cubrir por los nodos de la red. En la siguiente figura se observan algunas de estas topologías en una red ZigBee:

25 https://standards.ieee.org/standard/802_15_4-2020.html

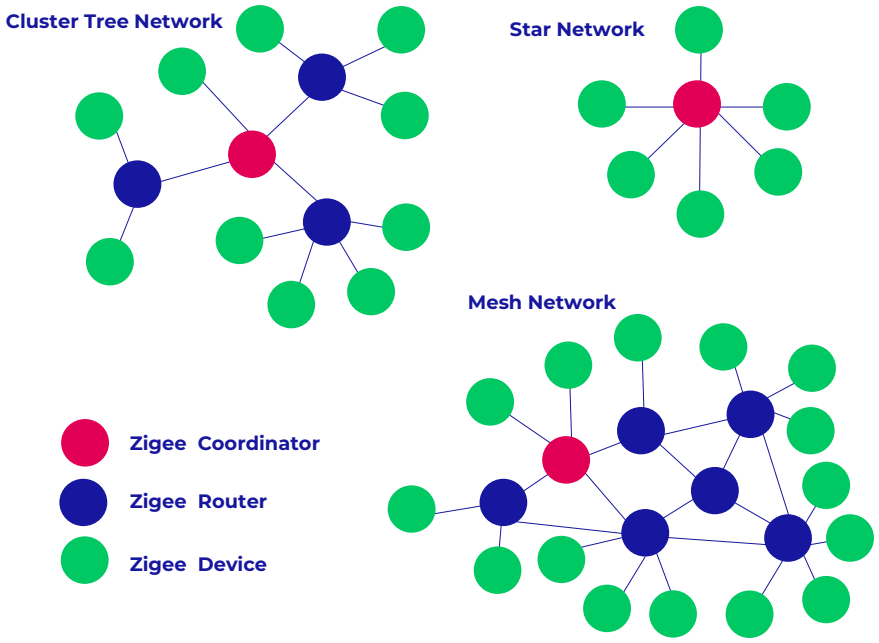


Figura 10: Topologías en ZigBee (27).

Zigbee[26]

Es un protocolo muy utilizado en las llamadas redes de sensores inalámbricos (WSN, Wireless Sensor Networks), debido al reducido coste económico de su fabricación y a la creciente demanda de este tipo de tecnologías. Esta tecnología inalámbrica nació dentro del consorcio ZigBee Alliance.

En principio, el ámbito en el que esta tecnología cobra más fuerza es en domótica. La razón de ello son diversas características que lo diferencian de otras tecnologías:

> Bajo consumo
> Topología de red en malla
> Fácil integración (se pueden fabricar nodos con muy poca electrónica)
> Alcance reducido, entre 10 y 20 metros
> Velocidades de transferencia de datos muy bajas y alcanzar velocidad máxima de 250 kbit/s.
> Opera generalmente en la banda de 2.4 Ghz, que es parte de la banda ISM (Industrial, Scientific and Medical), así como en la 868 MHz (Europa) y en la 915 MHz (E.E.U.U., Japón).

ZigBee define la interconexión entre los distintos nodos de la red, pero en el caso de que sea necesaria una conexión hacia Internet para comunicar datos hacia servidores externos, por ejemplo, es necesaria la presencia de un nodo concentrador, *hub* o gateway, que se conectará por un lado con la red ZigBee y, por otro lado, dispondrá de una conexión a Internet o hacia una red local con otro tipo de tecnologías comunes como fibra, ADSL, ethernet, etc., como se puede observar en la siguiente figura:

26 https://zigbeealliance.org/

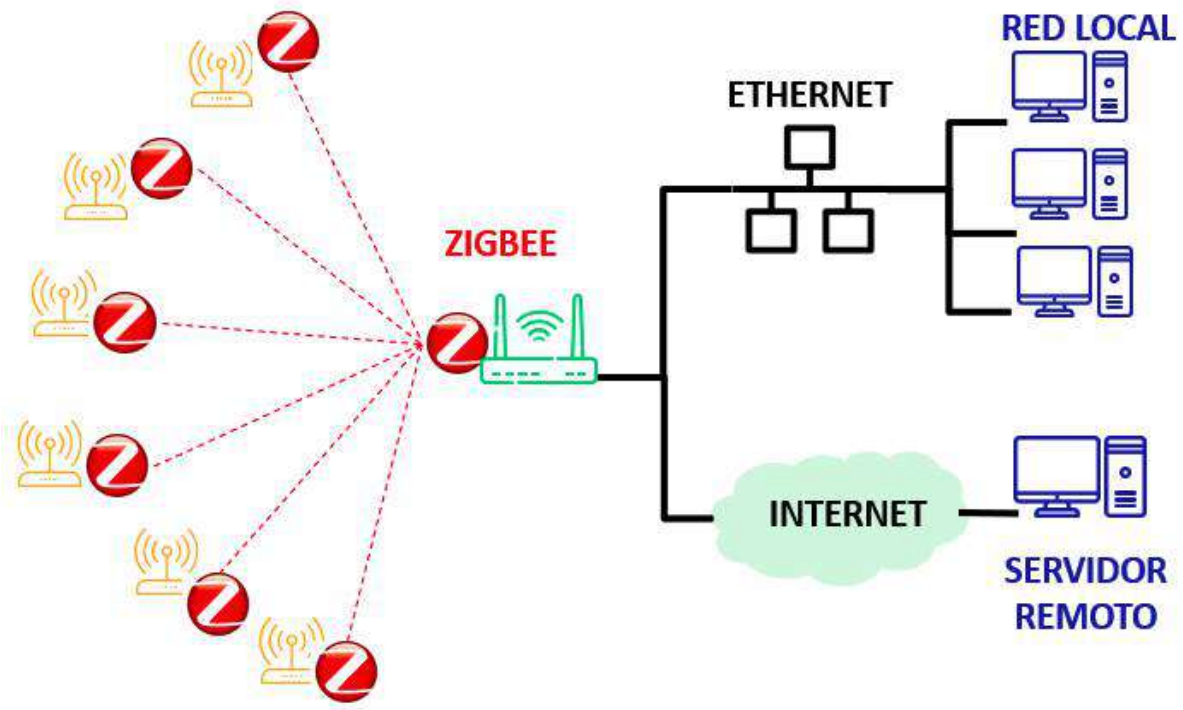


Figura 11: Conexión de una red ZigBee hacia otras redes. (Fuente: Elaboración propia)

Por último, ZigBee incorpora medidas de seguridad para asegurar el intercambio de datos entre nodos. Por ejemplo, es posible cifrar los datos con el protocolo AES.

Z-Wave

El protocolo Z-Wave comparte muchas de las características de ZigBee pero intenta mejorar algunas de las debilidades de éste. Es un protocolo promovido por la Z-Wave Alliance[27] y, de esta iniciativa, se ha desarrollado como un protocolo cerrado, en contraposición a ZigBee. Esto provoca que la interoperabilidad de los productos certificados por la Z-Wave Alliance esté garantizada, independientemente del fabricante, pero, por el contrario, no tenga capacidad de ser modificado o adaptado por desarrolladores como en el caso de los protocolos abiertos.

2.1.2 Comunicaciones dispositivo-nodo de enlace

En este tipo de comunicación los nodos IoT usan un gateway para enviar datos a la nube. Existe un nodo que actúa como intermediario entre el dispositivo y el servicio en la nube y proporciona seguridad y otras funcionalidades como la traducción de datos o protocolos (24). Este nodo intermediario puede ser un Smartphone o un concentrador domótico, por ejemplo.

27 https://z-wavealliance.org/

Bluetooth (BLE) Bluetooth de baja energía[28]

Bluetooth, en su versión BLE, es una tecnología de conectividad inalámbrica de baja potencia utilizada de forma generalizada en muchos tipos de dispositivos. Se ha usado extensamente en despliegues de IoT durante mucho tiempo, sobre todo en modo de baja energía Bluetooth y todos los componentes opcionales están bajo licencia GPL y son esencialmente de código abierto.

Ethernet[29]

El estándar de red cableada Ethernet IEEE 802.3, y otros estándares de la familia 802, proporcionan una opción de bajo costo, muy conocida y probada. Es el estándar de red cableada por excelencia. Además, Ethernet tiene la capacidad de adaptarse a necesidades específicas y así surgen estándares como Ethernet Industrial o Power over Ethetnet (PoE).

A medida que las aplicaciones IoT requieren un mayor ancho de banda, Ethernet puede proporcionar el rendimiento necesario. Además, Ethernet también puede ser una alternativa debido a su capacidad de alimentar a los dispositivos a través del cable de red usando el estándar PoE.

WiFi, WiFi6[30] [31]

El estándar inalámbrico Wi-Fi puede utilizarse para conectar prácticamente cualquier elemento a Internet. También se puede usar para conectar nodos IoT, desde electrodomésticos hasta señales de tráfico, aunque su principal inconveniente para este tipo de soluciones es su alto consumo de energía (28). La mayoría de los sensores y dispositivos IoT operan con baterías. Con Wi-Fi 6 (el nuevo estándar IEEE 802.11ax), esto deja de ser una preocupación.

> ***Wi-Fi 6 es una de las principales alternativas en el futuro para la conectividad IoT.***

28 https://www.bluetooth.com/specifications/
29 https://www.ieee802.org/3/index.html
30 https://www.ieee802.org/11/
31 https://standards.ieee.org/project/802_11ax.html

Al operar a 5 GHz, Wi-Fi 6 evita la altamente congestionada banda de frecuencia de 2,4 GHz. Fue diseñado desde el principio para mejorar el rendimiento de los datos, aumentar la robustez y reducir el consumo de energía sin obstaculizar el rendimiento.

2.1.3 Comunicaciones dispositivo-nube

En este tipo de comunicación los nodos IoT tienen la capacidad de enviar datos directamente hacia la nube, sin la intervención de un gateway (24).

Se tienen las tecnologías **LoRa**[32] y **Sigfox**[33], como estándares de LPWAN, las cuales son tecnologías nativas de comunicación para IoT. Normalmente dependen de una infraestructura de un operador. En el caso LoRa, por el contrario, dos posibilidades, se tiene la opción de desplegar una infraestructura o red propia, en cuyo caso, para conectar con la nube, sí requerirá de un gateway; y también tiene la posibilidad de utilizar redes de operadoras. Actualmente en LoRa hay varios operadores que ya tienen redes disponibles comercialmente con una constante evolución de cobertura en sus planes de extensión. Sigfox, por el contrario, es una red únicamente privada de servicios de comunicación IoT desplegada y gestionada por un operador francés con su propia tecnología que aspira a ser un operador global.

NB-IoT[34] **(CAT-B)** y **LTE-M (Cat M1 o Cat M)** se comprenden también dentro del estándar LPWAN, en caso refiriéndose a evoluciones del **LTE/4G** adaptadas a IoT, caracterizadas por ser de más bajo consumo y con posibilidad de su implementación mediante dispositivos de bajo coste. NB-IoT y LTE-M funcionan mediante comunicación tipo celular, por lo que utilizan las redes de operadoras de telefonía móvil. LTE-M dispone de mayor velocidad de datos, mejor movilidad y permite transmitir voz a través de la red, y en contraste NB-IoT utiliza menor ancho de banda y su coste es menor.

El estándar LPWAN, a diferencia del estándar IEEE 802.15.4 o Zigbee, que ya se han comentado en esta sección, se han diseñado pensando en despliegues masivos de dispositivos IoT. Sobre todo, se han optimizado para lograr un consumo de energía bajo en los nodos IoT (29).

32 https://lora-alliance.org/
33 https://www.sigfox.com/
34 https://www.3gpp.org/news-events/1785-nb_iot_complete

Tecnología 5G[35]

"La tecnología 5G cambiará radicalmente el ámbito de las redes de comunicaciones. No pasará mucho tiempo antes de que la sociedad mundial tenga que adaptarse a la nueva forma de vida tecnológica. Esta nueva norma tecnológica promete mucho más que un simple desarrollo de las tecnologías de comunicación móvil existentes. En casi todos los ámbitos de la vida se producirán amplios cambios en la digitalización, la sociedad y la economía. Hasta ahora, el objetivo principal ha sido ampliar las condiciones de infraestructura de las redes convencionales en general, a fin de garantizar la disponibilidad de la red para todos los dispositivos móviles. En los próximos años, además de la continuación en el establecimiento de redes en el marco de IoT 5G, la atención se centrará en satisfacer las crecientes necesidades de la sociedad en red de manera aún más óptima que antes (30)."

La aplicación de la tecnología 5G en IoT permite tiempos de respuesta más cortos y transmitir datos en tiempo real ya que puede alcanzar hasta 20 gigabits por segundo. Con estas capacidades de comunicación, uno de los sectores que más se beneficiará en la aplicación de la Internet de las cosas será la Industria 4.0 con la tecnología 5G (30).

IPv6[36]

Independientemente del protocolo de comunicaciones que utilicen los nodos IoT para comunicarse entre sí, para poder enviar y recibir datos hacia y desde Internet es necesario que los propios dispositivos, el concentrador o hub de la red, dispongan del protocolo IP. En la actualidad, Internet y las redes corporativas están migrando desde la versión 4 del protocolo IP (IPv4) a la versión 6, IPv6, que incorpora una serie de mejoras fundamentales para la extensión de soluciones IoT a través de Internet:

> Aumento del número de direcciones.
> Mejor rendimiento.
> Utilización en redes de sensores inalámbricos.
> Mayor seguridad al implementar cifrado e Ipsec, habilitando autenticación y encriptado.
> Autoconfiguración para descubrir de forma autónoma la dirección que se asigna.

Por tanto, es cada vez más importante que se utilice IPv6 en las soluciones IoT, siempre que sea posible, para evitar problemas de escalabilidad o interoperabilidad en el futuro. De hecho, IoT puede ser un factor crítico a la hora de traccionar el cambio progresivo de Internet (y de las redes corporativas) hacia una red que opere enteramente sobre IPv6.

35 https://www.etsi.org/technologies/5g
36 https://tools.ietf.org/html/rfc2460

2.1.4 Modelo de intercambio de datos a través del back-end

> "El modelo de intercambio de datos a través del back-end se refiere a una arquitectura de comunicación que permite exportar y analizar datos de objetos inteligentes de un servicio en la nube en combinación con datos de otras fuentes." (24)

Una arquitectura de intercambio de back-end permite que los datos recogidos de dispositivos de IoT se agreguen y analicen y propone un enfoque de servicios de nube asociados para lograr la interoperabilidad de los datos de dispositivos inteligentes alojados en la nube (24).

A continuación, se numeran algunos de los protocolos usados actualmente para este tipo de comunicación de back-end, entre entidades (por ejemplo: plataformas) que necesitan compartir datos (31):

- AMQP[37]
- CoAP[38]
- HTTP (REST/JSON)[39]
- MQTT[40]
- XMPP[41]

2.1.5 Redes definidas por Software

Las redes definidas por software (SDN) constituyen un nuevo paradigma de gestión de red donde el control no reside ya en la configuración distribuida de los diferentes dispositivos que componen la red (conmutadores, enrutadores...) si no en un controlador central. Es decir, es el controlador el que dicta las reglas de cómo procesar cada paquete o flujo de red entrante a un dispositivo en concreto y no el dispositivo en sí. Así, se divide de forma efectiva la red en dos planos: el plano de transmisión de información (también llamado el plano de datos) y el plano de control. Es un concepto estrechamente relacionado con la virtualización de redes y es una tecnología cada vez más utilizada en los centros de datos.

Esto sucede porque gracias a la gestión central de la red, es posible su reconfiguración dinámica de forma sencilla en un único punto. Esto dota a las redes definidas por software de una flexibilidad que no disponen las redes convencionales.

Como ya se ha visto en redes IT convencionales, este paradigma tiene un gran potencial para el IoT. Las principales ventajas de esta tecnología para IoT pueden resumirse de la siguiente forma (32) (33):

- Utilización efectiva de los recursos de red: El control central de la red definida por software permite reconfigurar los recursos (p.ej. ancho de banda) asignados a cada

37 https://www.amqp.org/
38 https://tools.ietf.org/html/rfc7252
39 https://www.w3.org/TR/2004/NOTE-ws-arch-20040211/#relwwwrest
40 https://mqtt.org/
41 https://xmpp.org/

dispositivo, de forma que se hace un uso óptimo de la red, minimizando el coste de despliegue de redes IoT.

> Seguridad dinámica: La reconfiguración dinámica abre la puerta a minimizar el impacto de ataques a gran escala, como Mirai[42], limitando la conectividad de los dispositivos afectados.

> Resiliencia. De forma similar al caso de la seguridad, fallos en la red pueden ser rápidamente subsanados, redirigiendo el tráfico de distinta forma y minimizando los puntos únicos de fallo y aumentando considerablemente la resiliencia y robustez de la red, manteniendo la conectividad de los dispositivos.

Si bien sus ventajas son considerables, las redes definidas por software aún no son ampliamente utilizadas en entornos IoT. Sin embargo, conforme la complejidad de las redes IoT vaya aumentando, la adopción de SDN será algo natural para poder gestionar la conectividad de millones de dispositivos.

2.2 Sensores

> ***"Un sensor es un dispositivo (típicamente electrónico) que detecta eventos o cambios en su entorno físico (por ejemplo: temperatura, sonido, calor, presión, flujo, magnetismo, movimiento y parámetros químicos y bioquímicos) y proporciona una salida correspondiente" (34).***

Los sensores convierten magnitudes físicas a señales eléctricas que pueden ser recogidas, procesadas y transmitidas por microcontroladores u otros dispositivos digitales.

Dado que el elemento sensor (por ejemplo, un termopar o un piezoeléctrico), por sí solo suele producir una salida analógica, a menudo requiere o incorpora un convertidor analógico-digital, ya que tienden un puente entre las magnitudes físicas y el mundo digital (redes de comunicación e internet).

42 https://en.wikipedia.org/wiki/Mirai_(malware)

Los sensores pueden ser muy sencillos, con una función básica de recogida y transmisión de datos, o inteligentes. Estos últimos proporcionan unas mayores capacidades para procesar o filtrar los datos, de tal manera que sólo utilizarán la pasarela de IoT cuando se cumplen unas condiciones muy específicas. En este último caso, un dispositivo IoT sensorizado requiere como mínimo de tres elementos (34):

- Sensor(es)
- Microcontroladores y elementos asociados (memorias, periférico, etc.)
- Pasarela de IoT para la conectividad de envío de datos filtrados a otros sistemas

La siguiente figura muestra los componentes de un sensor inteligente, los cuales se han marcado en azul:

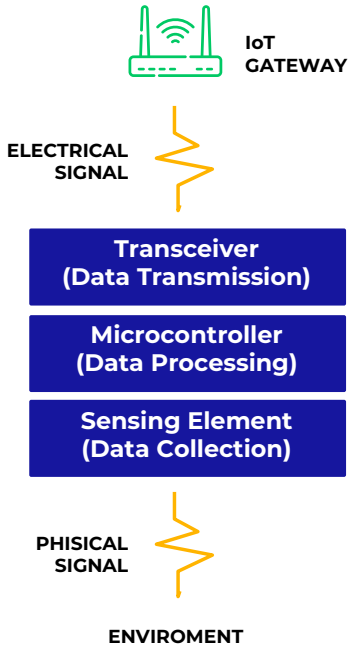


Figura 12: Componentes de un sensor inteligente (34).

2.2.1 Tecnologías de sensorización

A continuación, se enumeran las tecnologías de sensorización más comunes, clasificadas en función de los tipos de magnitud física y las tecnologías empleadas (34):

- **Sensores de temperatura**: Las tecnologías más comunes empleadas en la sensorización de temperatura son las siguientes:
  - **Sensores de termopar:** Se compone de dos metales diferentes, unidos en un extremo. En los extremos no unidos del termopar se genera una tensión proporcional a la temperatura del punto de unión, que es donde se mide la temperatura. Existen varios tipos, en función del rango de temperaturas y la sensibilidad deseadas de forma muy económica.

- **Sensores de detección de temperatura resistivo** (*Resistance Temperature Detector*, RTD): Los RTD son dispositivos de detección de temperatura cuya resistencia cambia con la temperatura. Su coste es superior y su rango de temperatura puede ser similar, en algunos casos, a los termopares.
- **Termistores:** Similar a los RTD, el termistor es un dispositivo sensor de temperatura cuya resistencia cambia con la temperatura. La principal diferencia consiste en la tecnología con la que se fabrican (cerámicas y polímeros), lo que hace que la variación de resistencia sea mucho mayor, menos predecible y menos estándar, en comparación con los RTD. El rango de temperatura que cubren es claramente inferior, aunque su coste es más económico.
- **Sensores semiconductores (circuitos integrados):** Se basan en el incremento de la conductividad de los semiconductores en función de la temperatura.

> **Sensores de presión**: Los sensores de presión se usan para medir la presión de gases o líquidos. También pueden emplearse para detectar y localizar la fuerza ejercida sobre una superficie o para medir parámetros biomédicos en dispositivos *wearables*.

Figura 13: Ejemplos de sensores de presión. Fuentes: Force Sensing y Fitbit (34).

Las tecnologías principales en las que se basan son las siguientes (35):

- **Sensores basados en galgas de presión piezo-resistivas**: Son las más comunes y simples de utilizar, proporcionando una lectura proporcional a la presión con una circuitería de adaptación simple. Pueden proporcionar medidas de hasta 150 MegaPascales. Su principal desventaja es que el sensor tiene que ser alimentado y que su salida depende de la temperatura.
- **Sensores de presión capacitivos**: Son especialmente idóneos para aplicaciones de presión reducida y entornos difíciles. Consumen poca energía, por lo que pueden alimentarse externamente, por baterías de larga duración o incluso por medios inalámbricos. Proporcionan una respuesta muy rápida.
- **Sensores de presión piezo-eléctricos**: Su principal ventaja es su robustez y baja potencia. Se emplean en entorno muy hostiles, desde grandes vibraciones a altas temperaturas, como por ejemplo prensas.

> **Sensores de caudal:** Los sensores de caudal se utilizan para detectar y registrar la tasa de caudal de fluidos en una tubería o un sistema (34).

Figura 14: Un ejemplo de sensor de caudal (34).

Las tecnologías más empleadas son:

- **Anemómetros térmicos**: Relacionan el caudal de un líquido o gas con el calor que se emana de un sensor de temperatura que es atravesado por él.
- **Sensores de presión diferencial**: Son los más comunes en líquidos. Su principio se fundamente en que la presión que cae a lo largo del sensor es proporcional al cuadrado del caudal.
- **Sensores de caudal basados en turbinas**: Se basan en que la velocidad de la turbina será proporcional al caudal, de tal forma que se pueden contar los giros de la turbina (pulsos eléctricos) en el tiempo.

Existen otras tecnologías de sensores de caudal, basadas en ultrasonidos, láser u otras aplicaciones, orientadas a diferentes aplicaciones (36).

> **Sensores de nivel**: Los sensores de nivel se utilizan para medir el nivel de los fluidos de forma continua o en valores puntuales (34).

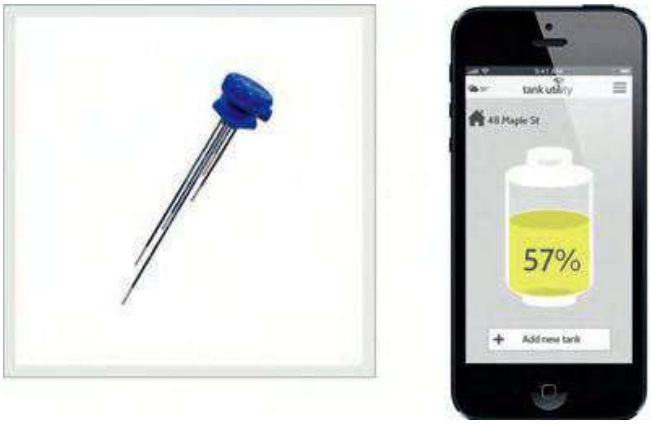


Figura 15: Sensores de nivel con monitorización remota de propano (Wi-Fi)

Fuente: Tank Utility. (20)

- **Sensores de imagen**: Los sensores de imagen son sensores sofisticados usados en cámaras digitales, equipos de imágenes médicas y equipos de visión nocturna (34). Debido a la complejidad de las propias imágenes (matrices de decenas de miles de puntos), su trasmisión, manipulación y procesamiento exigen de capacidades superiores al resto de sensores mencionados. Del mismo modo, corresponden a equipos de mayor coste, tanto del sensor como de todo el sistema embebido asociado.

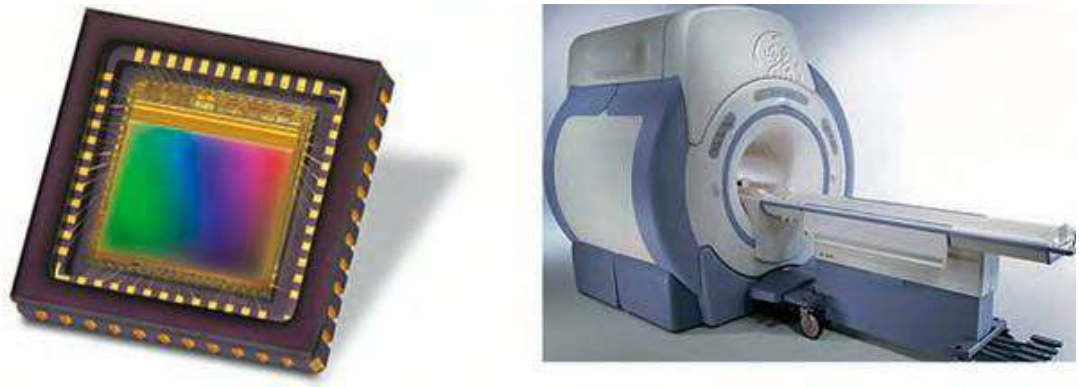


Figura 16: Ejemplos de sensores de imágenes. Fuente: e2v & DGDL (34).

- **Sensores de sonido (micrófonos):** La sensorización de sonido, por medio de uno o varios micrófonos (arrays), puede tener varias aplicaciones prácticas. Por ejemplo, la detección de niveles de ruido, que puede tener efectos perjudiciales tanto para los humanos (por ejemplo, riesgo cardio-vascular) como para los animales (por ejemplo, pérdida de audición). Existen sensores que proporcionan directamente el nivel de ruido, permitiendo al usuario generar alarmas o tomar acciones de control. Los micrófonos pueden tener otras muchas aplicaciones, desde la grabación de sonidos sospechosos, la detección de voz o la monitorización del estado de salud de dispositivos industriales (maquinaria, ascensores, etc.), donde unos patrones de sonido diferentes pueden indicar problemas de mantenimiento (37).

Las principales tecnologías en que se basan los micrófonos empleados en dispositivos IoT son las siguientes:

- **Micrófonos dinámicos**: basados en el movimiento de una bobina (por la presión del sonido) sobre un campo magnético. Proporcionan buena calidad para audio, pero son muy sensibles a vibraciones y otros aspectos ambientales.
- **Micrófonos piezo-eléctricos**: El sonido desplaza un elemento piezo-eléctrico, el cual genera una carga (corriente) proporcional a la fuerza aplicada por el sonido. Se utilizan en entornos hostiles, pero el ruido de medida es superior.
- **Micrófonos capacitivos**: la variación de la distancia entre la superficie de contacto del sonido (diafragma) y otra posterior se traslada en un cambio de capacidad. Sus buenas características hacen que sean las escogidas para aplicaciones de precisión.

Además de los comentados hasta ahora, existen otros tipos de sensores de contaminación

del aire, de proximidad y de desplazamiento, de movimiento basados en infrarrojos, de humedad, de velocidad, acelerometría, magnetómetros, giróscopos, etc. (34)

2.2.2 Interfaces entre sensores y microcontroladores/dispositivos

Generalmente, para que cualquiera de los sensores descritos previamente pueda conectarse con una red (y posteriormente a internet), tiene primero que ser conectado a un microcontrolador, el cual se comunicará posteriormente con un Gateway, con una red local o directamente a Internet, empleando las tecnologías de comunicación descritas en el apartado 4.1. La lectura desde el microcontrolador de los datos del sensor suele darse empleando alguno de los siguientes formatos:

- **Líneas analógicas:** Los sensores más básicos proporcionan medidas que se leen en un microcontrolador como una tensión analógica en una entrada ADC. Muchos de ellos requieren además de circuitos de adaptación, para ajustar la magnitud generada por el sensor (capacidad, corriente, tensión) a la tensión y niveles esperados por la entrada ADC del microcontrolador.
- **RS232:** Muchos sensores emplean comunicaciones serie (línea serie) para comunicar sus lecturas, de forma digital, con un microcontrolador.
- **SPI (Serial Peripheral Interface):** Es un protocolo serie que emplea 4 señales (MOSI, MISO, CLK, CS) para comunicar periféricos (como chips de sensores) con microcontroladores.
- **I2C (Inter IC Communications):** La mayoría de sensores digitales permiten emplear el anteriormente citado SPI o I2C para leer sus valores de salida. En el caso de I2C, se emplea un bus común para datos de transmisión/recepción y un reloj.
- **RFID**: Una forma de acceder a las lecturas de un sensor o identificarlo es RFID, el cual es interesante por dos motivos: es inalámbrico y permite alimentar remotamente el sensor (sensores RFID pasivos). RFID puede permitir desde leer la identificación de un dispositivo (como los tags de las autopistas o centros comerciales) hasta leer valores de sensores sin ninguna batería o alimentación (passive wireless sensors).

RFID consta de dos partes: un nodo o etiqueta y un lector. Generalmente, el primero tiene dos componentes: un microchip que almacena y procesa la información (pudiendo leer de un sensor) y una antena para recibir y transmitir la señal. El nodo responde con la información escrita en su memoria o con capturas realizadas de un sensor en vivo y, a continuación, transmitirá los resultados de la información obtenida al lector, que será un dispositivo necesariamente cercano.

Además de para sensorización, RFID se puede utilizar para identificación de dispositivos y para tracking logístico. Las principales características de RFID son las siguientes:

- Una de las ventajas de la etiqueta RFID es que no necesita estar en línea de visión directa con el lector y puede ser leída a una distancia de hasta 12 metros, aunque esto depende de la frecuencia de comunicación (por ejemplo, en UHF) y otros factores. Las etiquetas alimentadas por baterías (Tags RFID activos) suelen tener un rango de cobertura de 100

metros para su lectura, aunque esto también depende de la tecnología empleada.

> Los datos de las etiquetas RFID pueden ser modificados según las necesidades de la empresa, a diferencia y como ventaja, frente a los datos de los códigos de barras que son muy difíciles de cambiar una vez desplegados.
> Las etiquetas RFID son duraderas. Los códigos de barras, en comparación, se imprimen en un producto a la vista de todos. Pueden ser cambiados o deteriorados con facilidad. Las etiquetas RFID, por el contrario, pueden ser reutilizados en múltiples productos y permanecer ocultas. Asimismo, son capaces de almacenar mucha más información.
> Como elemento relativo a la seguridad, los datos de las etiquetas RFID pueden ser cifrados, de tal manera que se puede evitar que usuarios no autorizados, accedan, cambien o falsifiquen los datos contenidos.
> La tecnología RFID tiene capacidad de leer múltiples etiquetas simultáneamente (hasta ciento de etiquetas).

La siguiente figura muestra los principales componentes de un sistema RFID: una etiqueta RFID programable para almacenar datos, un lector con una antena para leer las etiquetas y un software de aplicación alojado en un ordenador para analizar los datos:

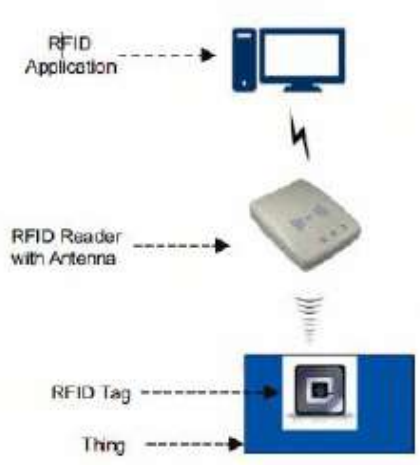


Figura 17: Principales componentes de una solución RFID (34)

2.3 ACTUADORES

> ***"Un actuador es un tipo de mecanismo que se encarga de controlar o actuar en un sistema. Toma una fuente de datos o energía (por ejemplo, la presión del fluido hidráulico, u otras fuentes de energía) y convierte los datos/energía en una magnitud que modifica las propiedades del sistema."*** **(34)**

Tipos de actuadores

- **Actuadores eléctricos**: Son dispositivos que tienen la capacidad de accionar pequeños motores convirtiendo la energía en par mecánico. Este par que se genera se utiliza para accionar válvulas o puertas, por ejemplo, y de este modo controlar ciertos equipos.
- **Actuadores Lineales Mecánicos**: Convierten señales eléctricas generadas por un dispositivo IoT en movimiento lineal. Puede generarse directamente con motores lineales o convirtiendo movimientos angulares a lineales con dispositivos como husillos y cadenas.
- **Actuadores hidráulicos**: Se componen de un cilindro hidráulico que utiliza la energía hidráulica para posibilitar un proceso mecánico.
- **Actuadores neumáticos**: Funcionan de manera similar que los actuadores hidráulicos, pero se utiliza gas comprimido en lugar de líquido.
- **Actuadores piezo-eléctricos:** Son actuadores que provocan desplazamientos (generalmente de pequeña magnitud) a partir de señales eléctricas, sin necesidad de activar motores. Generalmente proporcionan movimientos cortos, pero pueden dar una fuerza relativamente alta y constante. Son totalmente silenciosos, por lo que se emplean en cámaras, móviles, etc. Como tampoco necesitan lubricación o mantenimiento, se utilizan también en entornos de vacío o criogénicos.

2.4 Plataformas IoT e IoE

> ***Las plataformas de IoT son un middleware que integra aplicaciones y hardware a la vez que proporciona un entorno para el análisis de datos.***

Una plataforma de IoT es una arquitectura multicapa, que puede conllevar diferentes tecnologías, y que permite la gestión, el aprovisionamiento directo y la automatización de los dispositivos conectados dentro del campo de actuación de Internet de las Cosas. Los beneficios y ventajas que aporta una plataforma IoT son aplicables a múltiples dominios. Las plataformas que posibilitan IoT ofrecen las capas de arquitectura y las tecnologías necesarias para adquirir, tratar, almacenar, analizar y ofrecer datos recogidos de sensores y dispositivos en general. La lista de plataformas IoT disponibles en el mercado es extensa.

"Las plataformas de IoT también son un middleware que integra aplicaciones y hardware a la vez que proporciona un entorno para el análisis de datos. Estas plataformas transfieren información entre dos capas de IoT: hardware y aplicaciones. Asimismo, transmiten datos desde una gran variedad de hardware a la nube para hacerlos útiles para las aplicaciones, mientras que transfieren comandos de las aplicaciones al hardware" (38). En la siguiente figura se puede observar este concepto de plataforma IoT:

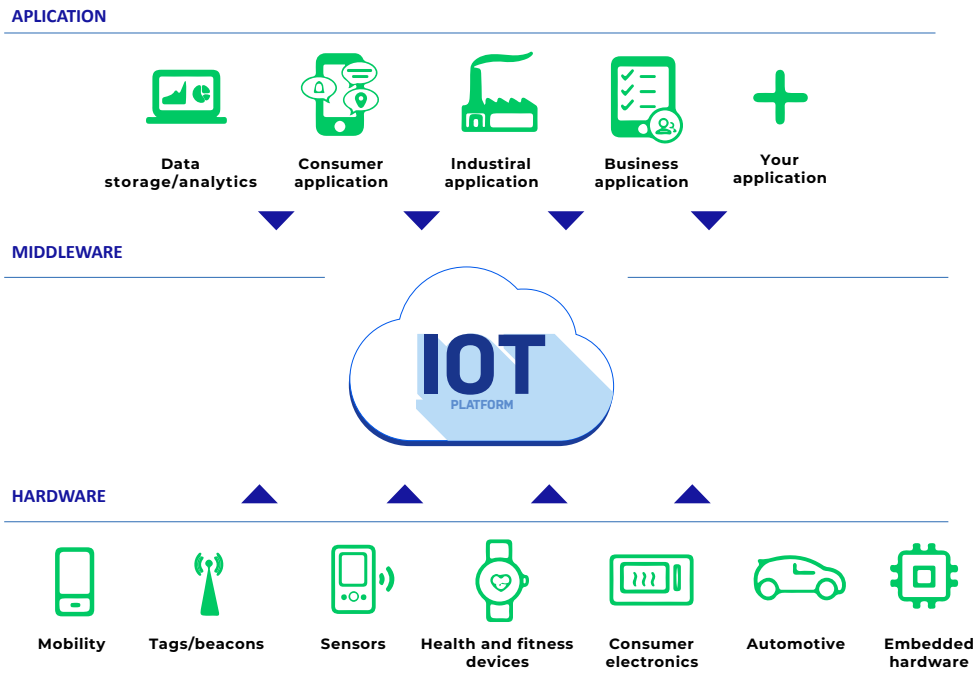


Figura 18: Concepto de plataforma IoT (38).

Las capacidades más importantes que aporta una plataforma IoT son (38):

> Desarrollo de aplicaciones.
> Gestión de datos a escala.
> Analítica de datos.
> Interoperabilidad e integración.
> Gestión de dispositivos.
> Seguridad.

2.4.1 Criterios de selección de Plataformas IOT

A continuación, se describen algunos de los criterios más importantes que los gestores o desarrolladores de soluciones IoT deben tener en cuenta a la hora de elegir una plataforma concreta:

> El tipo de servicio que es necesario que proporcione el proveedor. Es decir, si la plataforma del proveedor proporciona un:
    - Servicio IaaS[43] (Infrastructure as a Service), en el que el desarrollador tiene un mayor control sobre las aplicaciones y los sistemas operativos, mientras que la plataforma proporciona servicios como las comunicaciones o el almacenamiento.
    - Servicio PaaS[44] (Platform as a Service), en el que el desarrollador puede elegir los entornos de desarrollo de las aplicaciones entre los que ofrece el proveedor para crear y distribuir aplicaciones, pero no es elegible la infraestructura subyacente.
    - Servicio SaaS[45] (Software as a Service), en el que el desarrollador tiene un control menor sobre las aplicaciones, ya que está limitado a utilizar los servicios a nivel de aplicación que le ofrece el proveedor, y generalmente programa las aplicaciones a través de las APIs que ofrece el proveedor.
> Otra opción es que el desarrollador aloje parte de la solución en su propia infraestructura, lo que puede darle mayor control sobre la aplicación, y utilice los servicios de una plataforma para completar los servicios que no puede o no le interesa ofrecer por sí mismo (comunicaciones o almacenamiento, por ejemplo). En este caso la integración entre la plataforma del proveedor y los recursos del desarrollador es crítica.
> Frente al proveedor de la plataforma es importante poder garantizar la privacidad de los datos de clientes de la aplicación desarrollada. Es decir, el proveedor debe garantizar al desarrollador que en ningún caso accederá a datos de clientes.
> Un criterio muy importante es que la plataforma permita la escalabilidad de la aplicación, es decir, que la aplicación pueda crecer en número de usuarios, funcionalidad, etc. sin que la plataforma suponga un obstáculo.
> Existen plataformas de código abierto, que permiten al desarrollador mayor control no

43 https://en.wikipedia.org/wiki/Cloud_computing#Infrastructure_as_a_service_.28IaaS.29
44 https://en.wikipedia.org/wiki/Platform_as_a_service
45 https://en.wikipedia.org/wiki/Software_as_a_service

solamente sobre su aplicación, sino también sobre los servicios que ofrece el proveedor, pudiendo evaluar y, en algunos casos, modificar el código de módulos de la plataforma. Además, en este tipo de plataformas, como un cualquier proyecto de código abierto que tenga relativo éxito, existe una comunidad de usuarios que colaboran en la continua evolución de la plataforma. Sin embargo, otras empresas prefieren una plataforma propietaria cerrada que garantiza el soporte del proveedor en todo momento.

- La cuestión de la interoperabilidad es muy importante como criterio. Para ello la plataforma debe ofrecer mecanismos como APIs que permitan la conectividad con distintos tipos de servicios, dispositivos, etc. Además, es interesante que aporten APIs para la propia gestión de la plataforma.
- La capacidad de la plataforma de gestionar los dispositivos desplegados en la solución IoT: la puesta en marcha de los mismos, su inventariado, actualizaciones, posibilidad de darlos de baja, restaurar los valores de fábrica, configuración remota, etc.
- La capacidad de la plataforma de ofrecer herramientas para el tratamiento y el procesamiento de grandes volúmenes de datos o, en su caso, de integrar soluciones de terceros que lo permitan. Es un criterio importante debido al volumen de datos generalmente creciente de las soluciones IoT, ya sea por el incremento de usuarios o por el incremento de sensores y dispositivos desplegados. La elección de una plataforma no adecuada en este sentido puede convertirse en un efecto limitante de las aplicaciones IoT.
- La capacidad de la plataforma de aportar un motor de decisión que ayude al desarrollador en la toma de decisiones que sea necesaria programar en la aplicación en función de los datos captados por los sensores y otras fuentes de datos. Así, el desarrollador no se ve obligado a implementar la lógica de la toma de decisiones en la aplicación, y utiliza los algoritmos que lo ofrece la plataforma.
- La ciberseguridad de las aplicaciones IoT es un punto crítico para su adopción y despliegue. Por tanto, un criterio importante a la hora de elegir una plataforma IoT es la arquitectura de ciberseguridad que ofrece, y los mecanismos de control de ciberseguridad y privacidad que garantiza.
- En muchas aplicaciones IoT, el hecho de que la plataforma proporcione información relativa a la ubicación de los nodos desplegados es importante. Por ejemplo, que la plataforma permita localizar los nodos ubicados en un círculo de 1 Km alrededor de unas coordenadas concretas. Este factor puede depender no solo de la plataforma sino de los dispositivos IoT.
- En cuanto a los protocolos de comunicaciones soportados por la plataforma, considerar aquellas que ofrezcan varias alternativas actualizadas en los protocolos de área extensa (es decir, que no se corra el peligro de que puedan quedar obsoletas en un tiempo) y que se basen en estándares no propietarios.
- En línea con el criterio anterior, es importante tener en cuenta los protocolos de comunicaciones soportados por los nodos, en el caso de que sean aportados por el proveedor, de cara a integrar dispositivos de otros fabricantes en la solución desarrollada.

> El número e importancia de despliegues ya realizados con una plataforma determinada. Que existan casos de uso en la plataforma en los sectores en los que se quiera desarrollar nuevas aplicaciones.
> El hecho de que exista una comunidad importante de desarrolladores que utilice la plataforma y que de soporte es también un criterio a tener en cuenta, cuando se trata de las plataformas basadas en código abierto.

2.4.2 Plataformas IoT

Este apartado presenta una selección de las plataformas IoT más utilizadas. A continuación, se describen algunas de esas plataformas IoT como ejemplos de las funcionalidades que pueden ofrecer y que tienen presencia en Europa.

En la siguiente figura se muestra el cuadrante mágico de Gartner donde se sitúan las principales plataformas industriales del panorama internacional posicionadas por la relación de facilidad de implementación y su posicionamiento en el mercado.

Figura 19: Cuadrante mágico de Gartner de Plataformas Industriales IoT (39).

En la siguiente tabla se listan las plataformas IoT mostradas en el cuadrante mágico anterior en orden alfabético de acuerdo con la empresa desarrolladora.

Empresa - Plataforma	URL
Altizon - Datonis MInt	https://altizon.com
AWS IoT	https://aws.amazon.com/es/iot/
Braincube	https://braincube.com/solutions/iiot-platform/
Davra	https://davra.com/
Eurotech - Everyware Cloud	https://www.eurotech.com/en/products/iot/
Exosite - Murano IoT	https://www.exosite.com/murano-iot-platform
Flutura - Cerebra Platform	https://www.flutura.com/
GE Digital - Predix	https://www.ge.com/digital/iiot-platform
Hitachi Vantara - Lumara	https://www.hitachivantara.com/es-latam/products/iot.html
IBM Watson IoT Platform	https://www.ibm.com/es-es/cloud/watson-iot-platform
Litmus Automation	https://litmus.io
Microsoft - Azure IoT Hub	https://azure.microsoft.com/es-es/services/iot-hub/
Oracle IoT Intelligent Applications	https://www.oracle.com/internet-of-things/
PTC - IIoT Thingworx	https://www.ptc.com/es/products/thingworx
QIO Technologies (Específica de IA)	https://qio.ai/
RootCloud	http://en.rootcloud.com/
Samsung SDS	https://www.samsungsds.com/us/iot/iot.html?referrer=https://www.google.com/
Software AG - Cumulocity IoT	https://www.softwareag.cloud/site/product/cumulocity-iot.html#/

Tabla 4: Listado de Plataformas Industriales IoT según Cuadrante Mágico Gartner

Gartner presenta las plataformas seleccionadas de acuerdo con la presencia y visibilidad en el mundo industrial, sin embargo, hay otras plataformas que se enfocan en otros sectores o son más transversales, y que no se encuentran representadas en el listado anterior.

A continuación, se incluyen otras plataformas también relevantes en el panorama internacional con una madurez de más de cinco años en el mercado. Se pueden encontrar en las referencias (40), (41), (42) y en la referencia de la herramienta de selección de Gartner (43) aplicando los filtros de búsqueda "*Manufacturing*", "*Services*", "*Energy and Utilities*" y "*Transportation*".

Empresa - Plataforma	URL
Alibaba IoT Cloud Solutions	https://www.alibabacloud.com/solutions/IoT
Prodea - Arrayent Connect Platform	http://prodea.com/platform/
Ayla IoT Platform	https://www.aylanetworks.com/
Bosch IoT Suite	https://developer.bosch-iot-suite.com/
Bsquare	https://www.bsquare.com/products-and-services/iot-software-services/
Cisco IoT	https://www.cisco.com/c/en/us/solutions/internet-of-things/
Ericsson IoT Platform	https://www.ericsson.com/en/internet-of-things/platform
Evrythng	https://evrythng.com/
Fiware	https://www.fiware.org/
Google Cloud	https://cloud.google.com/
HPE Universal IoT Platform	https://www.hpe.com/emea_europe/en/solutions/iot-platform.html
IoTivity	https://iotivity.org/
IoTSens	https://www.iotsens.com/es/
Kaa IoT Platform	https://www.kaaproject.org/
Kloudq IIoT	https://kloudq.com/
Siemens - MindSphere	https://siemens.mindsphere.io/
Schneider Electric - Wonderware Industrial IoT	https://www.wonderware.es/internet-de-las-cosas-industrial-iiot/
Octoblu	https://octoblu.github.io/
SAP Leonardo IoT	https://help.sap.com/viewer/product/SAP_Leonardo_IoT/1904b/en-US
ThinSpeak	https://thingspeak.com/
Verizon - ThingSpace	https://thingspace.verizon.com/index.html

Tabla 5: Listado de Plataformas IoT adicionales

Las plataformas de IoT pueden clasificarse según la empresa que presta el servicio:

> Plataformas IoT de proveedores de servicios de comunicación (CSP): Los proveedores de servicios de comunicación (del inglés Communication Service Provider CSP) están formados por grandes proveedores de servicios en la nube como Amazon, Microsoft o IBM. Cada uno de estos CPS proporciona su propia plataforma de IoT: AWS IoT, Microsoft Azure IoT o IBM Watson IoT. Estas plataformas constituyen casi el 80% del mercado, con unos ingresos de 52.000 millones de dólares (a diciembre de 2018). Sin embargo, eso

no significa que no haya otros proveedores aparte de los mencionados anteriormente. Otros proveedores notables son Oracle, Google, Alibaba, etc.

> Plataformas construidas sobre las plataformas CSP: En esta categoría podemos encontrar cientos de plataformas ofrecidas tanto por grandes como por pequeñas empresas. Proveen servicios especializados desarrollados dependiendo del negocio que manejan.

En los listados anteriores se pueden encontrar ejemplos de los dos tipos de plataformas.

A continuación, se describen con más detalle una serie de plataformas que sirven de ejemplo de las capacidades y funcionalidades que aportan este tipo de soportes para el desarrollo de aplicaciones. Se han seleccionado plataformas como AWS IoT, Microsoft Azure IoT e IBM Watson, que son plataformas orientadas al desarrollo de cualquier tipo de aplicación en cualquier sector empresarial, muy conocidas y utilizadas tanto en el panorama nacional como en europeo. Dos de estas plataformas que se describen con más detalle, son de código abierto: Fiware y Thingsboard, ya que ésta es una característica de interés en este tipo de entornos y puede ser una alternativa efectiva para las empresas que estén valorando desarrollar aplicaciones IoT. Por último, se han seleccionado plataformas enfocadas en el sector industrial, en lo que se ha definido como Industrial IoT, y que en este ámbito son las que más presencia y popularidad están demostrando: ThingWorx de PTC, Bosch IoT Suite y Siemens MindSphere.

2.4.2.1 Amazon Web Services IoT

“Amazon Web Services (AWS) IoT es una plataforma en la nube que permite conectar dispositivos a los Servicios de AWS y a otros dispositivos, securizar los datos y las interacciones, procesar y actuar sobre los datos de los dispositivos y, además, permite que las aplicaciones interactúen con los dispositivos incluso cuando están fuera de línea. AWS IoT soporta la comunicación de mensajes entre dispositivos y puede procesar y encaminar esos mensajes a los *endpoints* de AWS y a otros dispositivos de manera fiable y segura.” (44)

La siguiente figura presenta las principales características y servicios de la arquitectura AWS IoT:

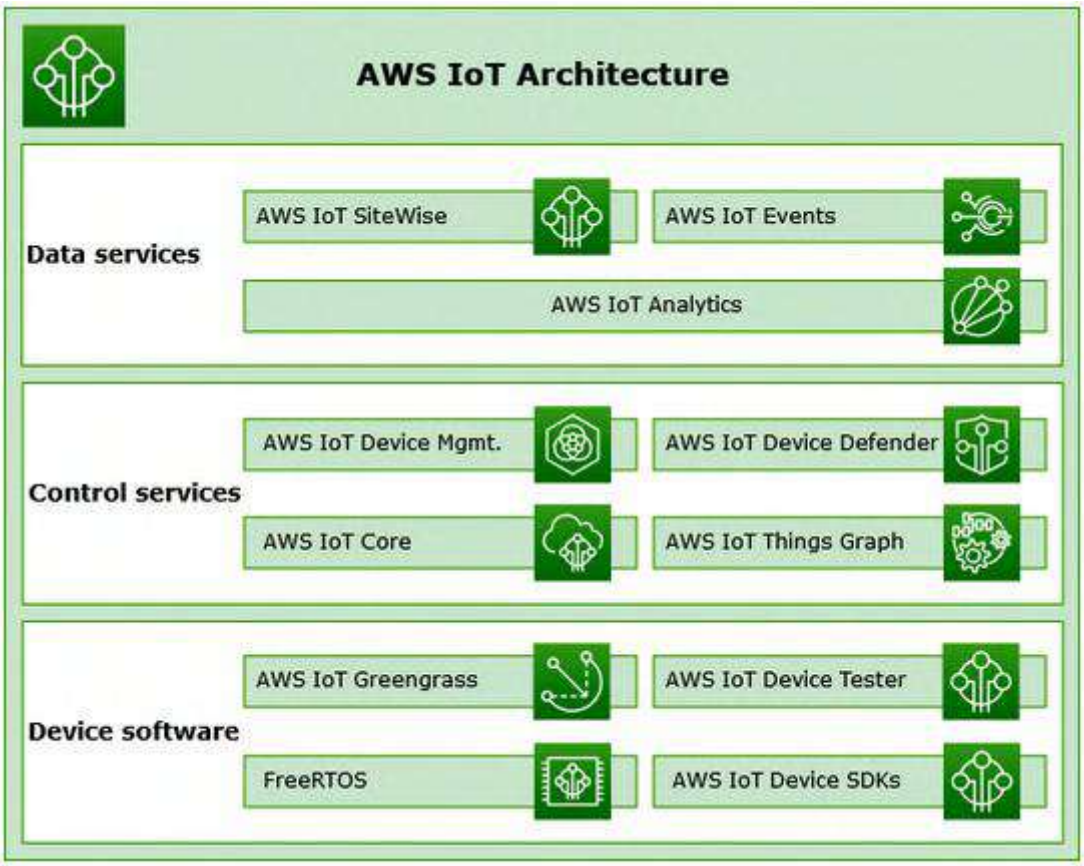


Figura 20: Arquitectura de AWS IoT[46]

Los principales módulos de AWS IoT a destacar son:

- **AWS IoT SiteWise**: transmite mensajes a todos los dispositivos con baja latencia, recopilando, almacenando y monitorizando los mensajes basados en MQTT o APIs ejecutados desde un gateway.
- **AWS IoT Event:** este servicio tiene las funciones de ser un Motor de Reglas, sin tener que gestionar ninguna infraestructura, para construir aplicaciones de IoT que procesan, recogen, analizan y actúan sobre los datos generados por los dispositivos conectados a escala global.
- **AWS IoT Analytics:** permite ejecutar análisis de datos IoT de forma masiva, filtrando, transformando o enriqueciendo los datos de IoT.
- **AWS IoT Core:** es un servicio que habilita la conectividad entre dispositivos y la nube de AWS, así como con otros servicios de manera sencilla.
- **AWS IoT Device Management:** módulo que se encarga de la administración de los dispositivos para su monitorización a través de un túnel seguro, de tal forma que se accede de forma remota al mismo para administrar su software o firmware.
- **AWS IoT Device Defender:** permite una comunicación segura y eficiente entre los dispositivos y AWS IoT. Se auditan continuamente las configuraciones IoT para confirmar

46 https://docs.aws.amazon.com/es_es/iot/latest/developerguide/aws-iot-how-it-works.html

el cumplimiento de las mejores prácticas.

- **AWS IoT Greengrass:** mediante este módulo el desarrollador puede ejecutar funciones propias de servicios de AWS o contener Dockers o incluso incluir funciones de machine learning.
- **AWS IoT Device SDK**: SDK para ayudar a los desarrolladores a conectar dispositivos hardware o aplicaciones móviles.

Con esta arquitectura, AWS IoT ofrece las siguientes funcionalidades principales:

- Conexión y gestión de dispositivos.
- Securización de las conexiones de los dispositivos y de los datos.
- Procesamiento y respuesta en base a los datos de los dispositivos.
- Lectura y escritura del estado del dispositivo en cualquier momento.

2.4.2.2 Microsoft Azure IoT

Microsoft Azure IoT es una plataforma de IoT diseñada para proporcionar servicios de IoT accesibles para todas las organizaciones, sin importar el tipo industria o el tamaño de la empresa. Proporciona 3 servicios principales de IoT:

Azure IoT Hub[47]: Permite la conexión, la supervisión y la gestión de numerosos activos de IoT. Actúa como un "*bróker*", o distribuidor de mensajes alojado en la nube, con el objeto de posibilitar la comunicación entre las aplicaciones de IoT y los dispositivos que gestiona de forma bidireccional. El servicio Azure IoT Hub asegura las comunicaciones:

- Gestiona que el acceso al broker de IoT por los dispositivos se realice de forma segura.
- Se encarga del control de acceso de los dispositivos y de las conexiones a nivel de cada dispositivo.
- Gestionando automáticamente el arranque y registro en el sistema de los dispositivos sin intervención humana.
- Proporcionando múltiples tipos de autenticación para distintos tipos de dispositivo.

Una de las posibilidades de Azure IoT Hub es que se puede integrarse con otros servicios de Azure para crear soluciones completas de extremo a extremo. Algunos ejemplos son:

- Azure Event Grid: permite a las empresas reaccionar rápidamente a los eventos críticos de manera fiable, escalable y segura.
- Azure Logic Apps: automatiza los procesos empresariales.
- Azure Machine Learning: agrega a la solución modelos de aprendizaje automático y de IA.
- Azure Stream Analytics: ejecuta cálculos analíticos en tiempo real en el flujo de datos de los dispositivos.

47 https://docs.microsoft.com/en-us/azure/iot-hub/about-iot-hub

Azure IoT Edge[48]: es un servicio que se soporta sobre el Hub de IoT para desplegar la inteligencia disponible en la nube en los dispositivos de IoT Edge localmente. "Azure IoT Edge mueve el análisis de la nube y la lógica de negocio personalizada a los dispositivos. Al empaquetar la lógica de negocio en contenedores estándar, estos contenedores pueden ser desplegados en dispositivos permitiendo su monitorización desde la nube".

Azure IoT Central[49]: es una aplicación SaaS que facilita la conexión, la monitorización y la administración de los activos de IoT a escala.

2.4.2.3 IBM Watson IoT

La Plataforma Watson de Internet de las Cosas es un servicio alojado en la nube y totalmente administrado. Facilita la obtención de valor de los dispositivos de Internet de las Cosas (IoT). Los dispositivos (sensores, puertas de enlace...) se conectan a la plataforma utilizando recetas de IBM y envían datos de forma segura a la nube utilizando el protocolo MQTT (44). Los dispositivos pueden ser configurados y administrados usando cuadros de mando en línea personalizados. Usando las APIs seguras proporcionadas por las aplicaciones de la plataforma se puede acceder a los datos en vivo y a los históricos rápidamente.

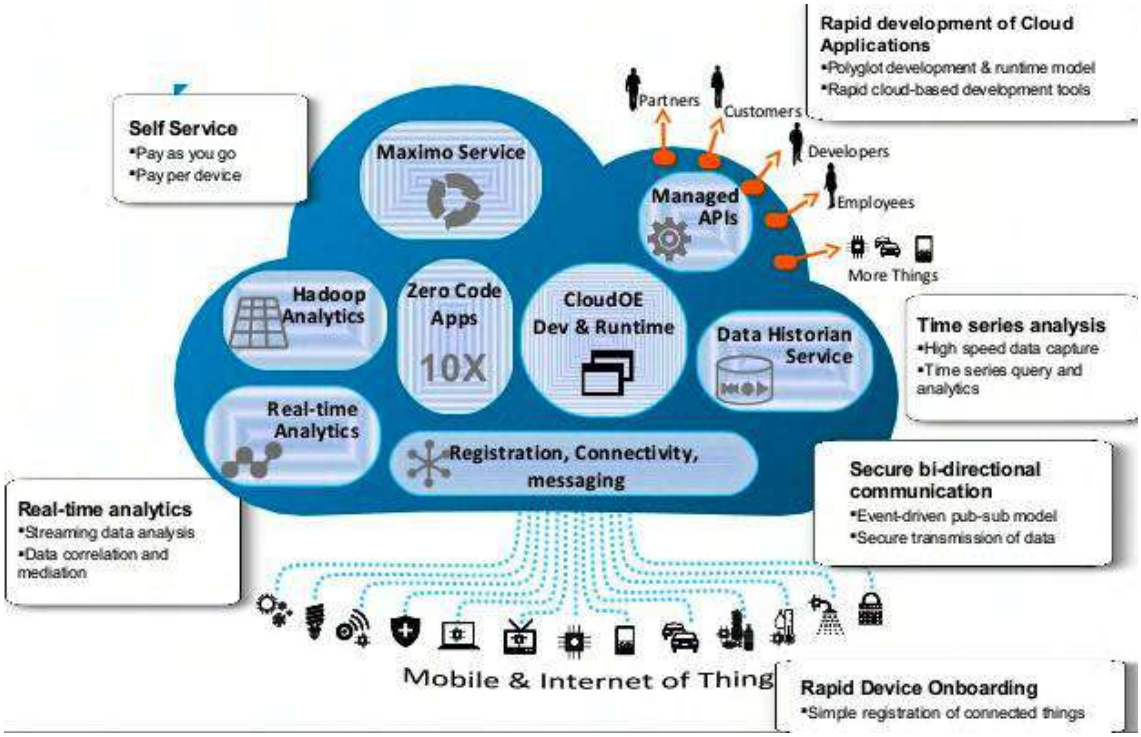


Figura 21: IBM Internet of Things Cloud[50]

48 https://docs.microsoft.com/en-us/azure/iot-hub/about-iot-hub https://docs.microsoft.com/en-us/azure/iot-edge/about-iot-edge
49 https://azure.microsoft.com/en-us/services/iot-central
50 http://www.slideshare.net/ArrowECSMarketing/internet-of-things-and-ibm

La plataforma considera los siguientes conceptos (45):

- **Organizaciones:** IBM Watson IoT identifica cada organización que conecta elementos a la nube. A cada organización se le da una identificación. La identificación de la organización asegura que los datos sólo sean accesibles desde los dispositivos y aplicaciones relacionados con esa organización.
- **Dispositivos:** un dispositivo puede ser cualquier cosa que tenga una conexión a Internet y tenga datos que quiera introducir en la nube. Un dispositivo no puede interactuar directamente con otros dispositivos. Los dispositivos son capaces de aceptar comandos de las aplicaciones. Los dispositivos se identifican de manera única a la plataforma Watson con un token de autenticación que sólo será aceptado por ese dispositivo. Los dispositivos administrados pueden realizar operaciones como las actualizaciones de ubicación, descarga y actualización de firmware, y reinicio y restablecimiento de fábrica.
- **Aplicaciones:** una aplicación es cualquier elemento que tenga una conexión a Internet y quiera interactuar con los datos de los dispositivos y/o controlar el comportamiento de esos dispositivos de alguna manera.
- **Gateways o puertas de enlace:** son una clase especializada de dispositivo. Tienen las capacidades combinadas de una Aplicación y un Dispositivo que les permite servir como puntos de acceso que proporcionan conectividad al servicio a otros dispositivos sin la capacidad de conectarse directamente.
- **Eventos:** son el mecanismo por el cual los dispositivos publican datos a la plataforma Watson IoT.
- **Comandos:** son el mecanismo por el cual las aplicaciones pueden comunicarse con los dispositivos.

Con estos componentes, la plataforma IoT ofrece una serie de funcionalidades que se enumeran a continuación:

- **Registro de dispositivos:** la plataforma permite la gestión del inventario de la organización, configurar la seguridad y almacenar metadatos para millones de dispositivos únicos.
- **Conectividad:** permite conectar de forma segura los dispositivos, las puertas de enlace (gateways) y las aplicaciones directamente a la plataforma Watson a través de MQTT. También permite modelar los datos del dispositivo como eventos y controlar el flujo de eventos hacia las aplicaciones.
- **Soporte de la puerta enlace:** en muchos casos en los que no se puede hacer una conexión directa entre el servicio y un dispositivo, la plataforma permite que los dispositivos de puerta de enlace se conecten y proporcionen una conectividad indirecta para múltiples dispositivos.
- **Administración de dispositivos:** opcionalmente, un usuario puede permitir que la plataforma Watson gestione el ciclo de vida de los dispositivos.
- **Integración de servicios externos de terceros.**
- **Historizadores.**

Los desarrolladores pueden desarrollar sus aplicaciones utilizando varios protocolos y lenguajes como HTTP, MQTT, Python, C, Java o Node.

2.4.2.4 FIWARE

FIWARE es una plataforma de *middleware*, impulsada por la Unión Europea, para el desarrollo y despliegue global de aplicaciones. El objetivo de FIWARE es facilitar la creación y el despliegue de aplicaciones y servicios en Internet en diversas áreas, como las ciudades inteligentes, el transporte sostenible, la logística, la energía renovable y la sostenibilidad ambiental (44).

FIWARE define la arquitectura y las especificaciones para configurar aplicaciones inteligentes, gestionar y asegurar grandes cantidades de datos y compartirlos con el mundo (45). También incluye una implementación de referencia.

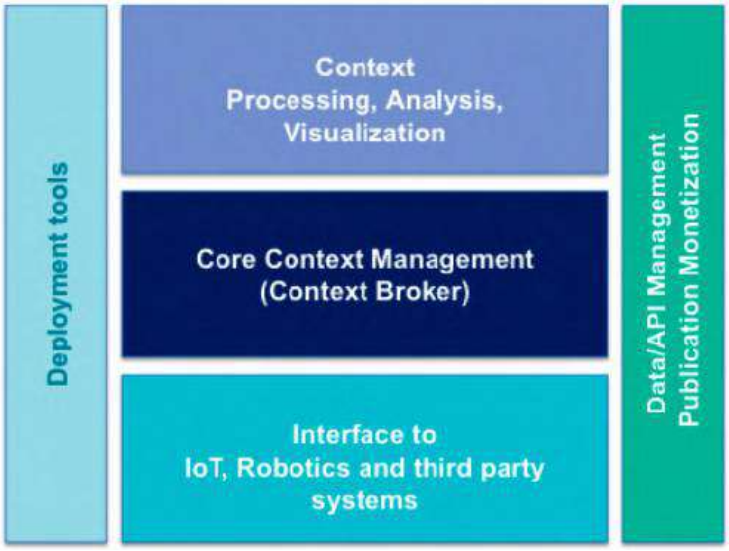


Figura 22: Arquitectura de FIWARE[51]

La arquitectura de FIWARE consiste en un número de elementos que se llaman habilitadores genéricos (generic enablers, GE para abreviar) (46). Estos se ocupan de temas como:

> Gestión de datos
> Habilitación la comunicación de los dispositivos IoT
> Seguridad y autenticación
> Alojamiento en la nube
> Interfaces de usuario

En el núcleo de la solución se encuentra el gestor de contexto que define un conjunto de APIs para almacenar y recuperar datos, suscribirse a los cambios, consultar y asegurar los datos y compartirlos con aplicaciones de terceros.

51 https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE_Architecture

La Junta de Andalucía, a través de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades y Telefónica han puesto en marcha FIWARE ZONE, que es una iniciativa para apoyar y fomentar soluciones inteligentes en distintos sectores de la economía y el desarrollo como SmartCities, Industria 4.0, etc. FIWARE Zone se constituye como el Digital Innovation Hub (DIH) de Andalucía para impulsar la digitalización y transformación de las empresas a través de tecnologías como IoT, Big Data e inteligencia artificial con FIWARE como conector de estas.[52]

2.4.2.5 Thingsboard IoT

ThingsBoard[53] es una plataforma IoT de código abierto que permite un rápido desarrollo, gestión y escalado de proyectos de IoT. Su objetivo es proporcionar una solución bien en la nube o en las instalaciones del usuario (on-premise) que ofrezca infraestructura del lado del servidor para aplicaciones de IoT. Sus características principales son:

> Proveer dispositivos, activos (assets) y clientes, y definir las relaciones entre ellos.
> Recopilar y visualizar datos de los dispositivos y activos.
> Analizar la telemetría entrante y disparar alarmas mediante el procesamiento de eventos.
> Controlar dispositivos mediante llamadas de procedimientos remotos (RPC).
> Construir flujos de trabajo basados en eventos del ciclo de vida del dispositivo, eventos creados por REST API, solicitudes RPC, etc.
> Diseñar paneles de mando dinámicos y presentar la telemetría de los dispositivos o activos.
> Habilitar características específicas del caso de uso utilizando cadenas de reglas personalizadas.
> Enviar los datos del dispositivo a otros sistemas.

ThingsBoard está diseñado para ser:

> Escalable: la plataforma escalable horizontalmente, construida con las principales tecnologías de código abierto.
> Tolerante a fallos: no hay un solo punto de fallo, todos los nodos del clúster son idénticos.
> Robusto y eficiente: un solo nodo servidor puede manejar decenas o incluso cientos de miles de dispositivos, dependiendo del caso de uso. El clúster ThingsBoard puede manejar millones de dispositivos.
> Personalizable: añadir nuevas funcionalidades es fácil con los widgets personalizables y los nodos del motor de reglas.
> Duradero: no se pierden datos.

52 https://fiware.zone/
53 https://thingsboard.io/docs/getting-started-guides/what-is-thingsboard

La arquitectura es la mostrada en la siguiente figura:

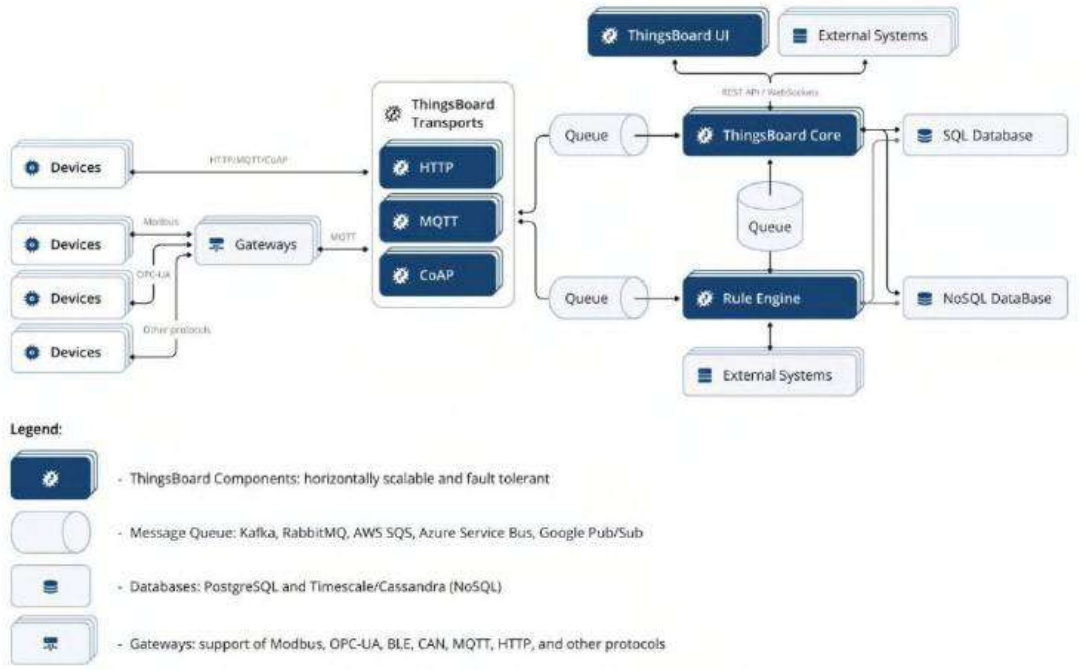


Figura 23: Arquitectura ThingsBoard[54]

Los principales componentes son:

- **ThingsBoard Transports**: ThingsBoard utiliza los protocolos MQTT, HTTP y CoAP basados en APIs. Estos protocolos se encuentran disponibles en las aplicaciones/firmware del dispositivo.
- **ThingsBoard Core**: ThingsBoard Core gestiona la utilización de WebSockets, así como las llamadas a la API de REST.
- **ThingsBoard Rule Engine**: El corazón del sistema de ThingsBoard es el Motor de Reglas y tiene la capacidad de procesar los mensajes entrantes.
- **ThingsBoard Web UI**: ThingsBoard proporciona un componente para alojar contenido del interfaz de la web.

2.4.2.6 ThingWorx

ThingWorx es la plataforma IoT en la nube de PTC. Es una plataforma muy orientada al mundo industrial IoT con capacidad para gestionar el desarrollo de todo el ciclo de vida las aplicaciones IoT industriales. Ha sido una de las primeras plataformas orientadas al sector industrial.

Facilita a las empresas mediante herramientas y tecnologías, desarrollar e implementar rápidamente aplicaciones robustas y ampliando las experiencias del mundo IoT incorporando la realidad aumentada.

54 https://thingsboard.io/docs/reference

Para la facilidad del desarrollador incorpora también herramientas de arrastrar y soltar que permiten implementar las características de la aplicación especificada. Así mismo, cuenta con un conjunto de algoritmos que ayudan en el análisis y la presentación de datos adecuados.

Los componentes principales de la plataforma son:

- **ThingWorx Core:** es un módulo de la plataforma que utiliza la Application Enablement Platform (AEP) como motor de diseño para aplicaciones de IoT en tiempo de ejecución.
- **Servicios de conexión ThingWorx:** proporciona conectividad lista para usar a dispositivos industriales, servidores de conexión, adaptadores de dispositivos en la nube y conectores de marcos de integración. Los servicios de conexión de ThingWorx Foundation, como los agentes de software y los kits de herramientas sirven para establecer la conectividad entre ThingWorx Foundation y activos (dispositivos) a través del método de comunicación y el hardware
- **ThingWorx Edge:** utiliza una tecnología de comunicación segura, independiente, fácil implementar y escalable a nivel de red para habilitar comunicaciones bidireccional entre dispositivos, equipos, sensores,y el servidor ThingWorx.

Mediante el uso del conjunto de aplicaciones software que incluye Thingworx, se habilitan las siguientes características:

- Abstracción de dispositivos IoT y sus componentes y servicios relacionados mediante el concepto de modelos por el cual se modelan tanto los datos como las características de los dispositivos.
- Plataforma multipropósito.
- Capacidad de desarrollos rápidas.
- Agilidad y flexibilidad en cuanto a la implementación mediante opción Cloud, local o híbrida optimizadas para Microsoft Azure.
- Ecosistema expansivo mediante soluciones de software industrial y compatibilidad con una amplia gama de productos y servicios.

2.4.2.7 Bosch IoT Suite

Bosch IoT Suite[55] es la plataforma de software de Bosch basada en código abierto para soluciones de IoT. Proporciona un servicio en la nube de IoT que ofrece diferentes capacidades para conectar, administrar, controlar y actualizar dispositivos con facilidad. En la siguiente imagen se muestra su arquitectura, incluida la distribución de la aplicación.

55 https://www.bosch-iot-suite.com/

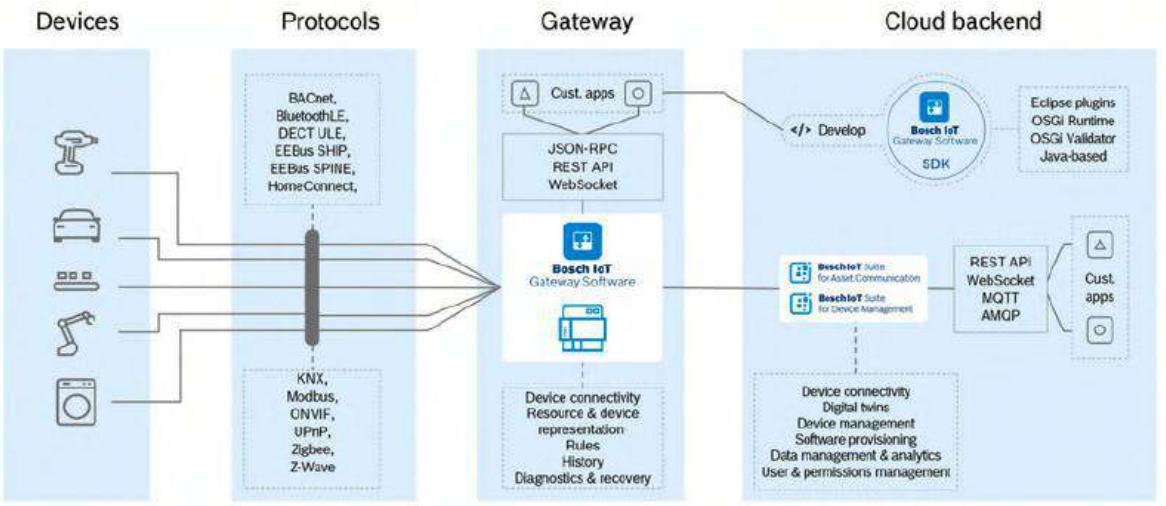


Figura 24: Arquitectura Bosch IoT[56]

El principal componente de la Suite Bosch IoT es el Gateway o pasarela. La pasarela es un componente de software que se puede implementar en más de 40 tipos de dispositivos. Proporciona soporte para la mayoría de los protocolos de conectividad. Permite modelar los datos, dispositivos y servicios en el borde (edge) de una manera uniforme. Estas son las características clave del componente software:

> Protocolos de conectividad con dispositivos.
> Modelado de datos y recursos: modelado uniforme de los dispositivos conectados y sus funciones.
> Abstracción de dispositivos y gemelos digitales locales: Ofrece una interfaz unificada para aplicaciones a dispositivos.
> Motor de reglas: permite la ejecución automática de reglas de negocio predefinidas.
> Almacenamiento de datos locales: Permite almacenar datos en el gateway sin conectividad con la nube.
> Seguridad en el borde (edge).
> Diagnósticos locales inteligentes.
> Gestión y actualización remota: agentes de gestión remota.
> Enfoque modular y framework dinámico: configuración flexible de los módulos y componentes incluidos en las imágenes en tiempo de ejecución, dependiendo de las características requeridas por cada despliegue concreto.
> Independen cia de la plataforma.

56 http://documentation.bosch-si.com/iot/SDK/v10/en/index.htm#95520.htm

2.4.2.8 Siemens MindSphere

MindSphere[57] es la plataforma IoT en la nube de Siemens. Conecta una amplia gama de dispositivos que permiten la aplicación de servicios en ellos permitiendo aprovechar la riqueza de datos generados por la Internet de las Cosas (IoT) con análisis de datos avanzados. Al igual que las otras alternativas ofrece un importante número de aplicaciones. La figura muestra la arquitectura propuesta por MindSphere.

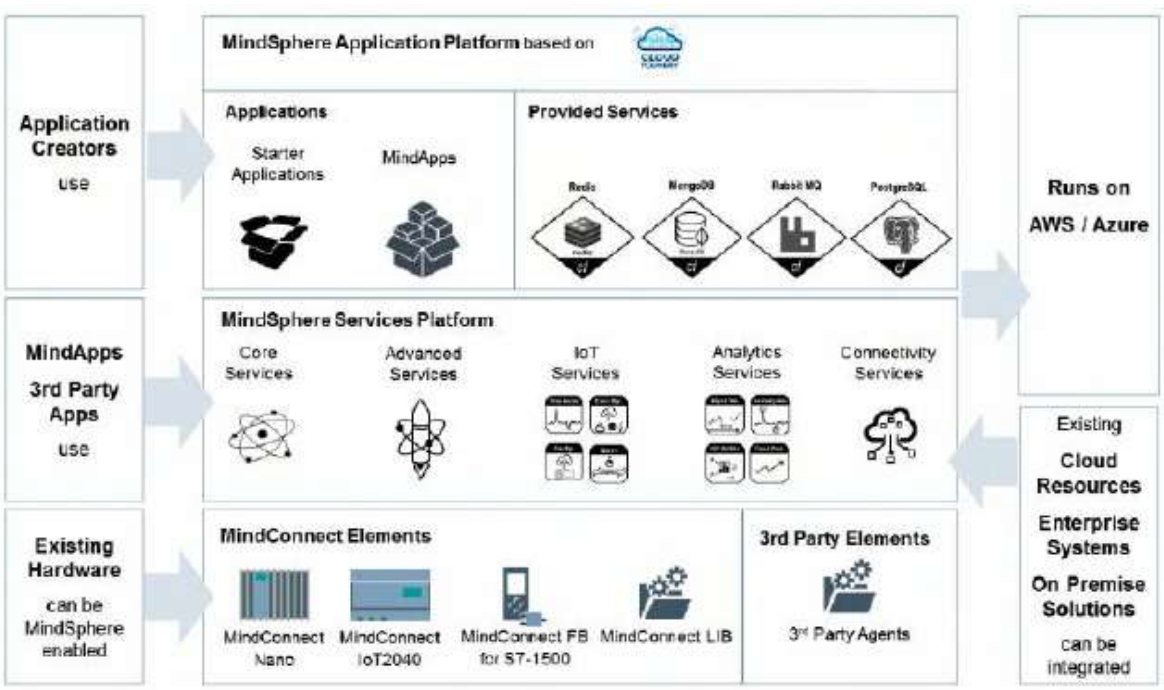


Figura 25: Arquitectura MindSphere[58]

MindConnect proporciona opciones de conectividad segura entre dispositivos, máquinas y plantas, con la nube de MindSphere. Esta conectividad se establece utilizando tanto protocolos característicos de IoT, como MQTT, HTTPS, CoAP, LWM2M, AMQP, XMPP, protocolos de comunicación, LoRaWAN, 6LowPan, así como también soporta una amplia gama de protocolos clásicos del ámbito industrial, como S7, Open Platform Communication Unified Architecture (OPC UA), Modbus y otros.

.

57 https://www.plm.automation.siemens.com/media/global/en/Siemens-MindSphere-Whitepaper-69993_tcm27-29087.pdf
58 https://assets.new.siemens.com/siemens/assets/api/uuid:8f510f778fb6d39f4c1562e9fd5a535d1c2d7a8b/digitalization-day-lab-mindsphere.pdf

3 CASOS DE USO DEL IoT e IoE

> ***Los dispositivos de IoT se utilizan en todo tipo de verticales de la industria y mercados de consumo, y el segmento de consumidores representa alrededor del 60 por ciento de todos los dispositivos conectados a IoT en 2020. Se prevé que esta proporción se mantenga en este nivel durante los próximos diez años.***

"Los dispositivos de IoT se utilizan en todo tipo de verticales de la industria y mercados de consumo, y el segmento de consumidores representa alrededor del 60 por ciento de todos los dispositivos conectados a IoT en 2020. Se prevé que esta proporción se mantenga en este nivel durante los próximos diez años." (47).

El uso de las tecnologías IoT, también, permite una infinita cantidad de aplicaciones empresariales diferentes en cada una de las verticales. En esta sección, en la siguiente tabla, se presentan algunos ejemplos, agrupados por actividades sectoriales, junto con la referencia de un caso real:

FÁBRICAS INTELIGENTES

Caso de uso	Descripción
Gestión de activos corporativos	La gestión de activos impulsada por IoT aumenta la visibilidad en tiempo real de los activos y ayuda a las empresas a optimizar sus recursos. Plataforma de gestión de activos Maximo de IBM: https://www.ibm.com/business-operations/enterprise-asset-management/eam
Mantenimiento predictivo	Utilización de sensores IoT para monitorizar máquinas y detectar posibles fallos de componentes antes de que ocurran. Servicio de mantenimiento predictivo de Iotsens: https://www.iotsens.com/mantenimiento-predictivo/

Automatización y optimización de los procesos industriales	Las empresas pueden llevar un registro en tiempo real de los parámetros de las máquinas dentro de una planta usando redes IP y redes de dispositivos IoT. Lo que habilita a los fabricantes para utilizar estos datos para automatizar los flujos de trabajo y optimizar los sistemas de producción. La automatización y la optimización permite a las empresas industriales optimizar la calidad, reducir los costos y aumentar el volumen de la producción. La monitorización de máquinas industriales y sistema de recopilación de datos de producción de Zyfra: https://www.zyfra.com/product/mdcplus/
Gestión de la energía	Los dispositivos de IoT monitorizando datos en tiempo real pueden ayudar a los fabricantes a gestionar el consumo de energía en diferentes entornos. WebNMS IoT Energy Management: https://www.webnms.com/iot/energy-management.html
SMART CITIES O CIUDADES INTELIGENTES	
Iluminación inteligente	Alumbrado público dotado de sensores IoT. Los sensores recogen datos sobre el estado del tráfico, peatones, etc. Con esos datos, las luces de las calles proporcionan una iluminación óptima. Philips Smart Lighting: https://www.lighting.philips.es/soporte/contacto/tendencias-en-iluminacion/smart-city/iot-iluminacion-inteligente
Smart Parking o Aparcamiento inteligente	Sistemas de ayuda a los problemas de aparcamiento basados en sensores IoT. Sistema de estacionamiento inteligente Mobidev: https://mobidev.biz/blog/iot-based-smart-parking-system
Monitorización del ruido	Sistemas de monitorización del ruido urbano e industrial, con la posibilidad de advertir en tiempo real a las empresas que violan los umbrales de ruido. Sistema de monitorización de ruido Kunak: https://www.kunak.es/productos/monitorizacion-ambiental/monitor-de-ruido/
Gestión de residuos	Gestión inteligente de residuos urbanos basados en contenedores que cuentan con sensores IoT. Ecubelabs CleanCityNetworks: https://www.ecubelabs.com/waste-analytics-platform/
GESTIÓN DEL AGUA	
Conservación del agua	Monitorización del nivel de llenado de depósitos de agua equipados con sensores IoT. Gestión integral de suministro de agua. Plataforma de gestión de agua Wellintel: https://wellntel.com/
Regadío inteligente	Sensores de IoT que determinan las condiciones climáticas y la humedad del suelo para obtener la cantidad apropiada de agua que el suelo necesita. Bosch Yield's Sensing+ solution: https://bosch.io/customers/agriculture/the-yield-iot-in-agriculture-from-oysters-to-apples/

Gestión de fugas	Los sensores de IoT pueden detectar cambios de temperatura, fugas de agua, fugas químicas y nivel de presión en los tanques de agua. Detectores de fugas de la empresa Lioote: https://iioote.com/en/senseiot/
Gestión de la calidad del agua	Detección de las sustancias químicas disueltas en el agua, identificación de parámetros como el total de sólidos disueltos, bacterias, cloro, etc. Libelium Smart Water: https://www.libelium.com/iot-solutions/smart-water/
SALUD DIGITAL	
Detección de caídas	Los sensores IoT pueden detectar caídas y pedir ayuda para que se reduzca el tiempo que los ancianos permanecen en el suelo después de una caída. Servicio de detección de caídas Wallabot: https://walabot.com/walabot-home
Refrigeradores médicos	Los refrigeradores médicos dotados de sensores IoT permiten cumplir todas las normas de seguridad y las regulaciones nacionales del mercado farmacéutico. Sistema de monitorización de temperatura Efento: https://getefento.com/application/temperature-monitoring-for-medicines-and-vaccines-in-health-clinics
Monitorización de pacientes	Los médicos pueden observar los datos de los pacientes y proporcionar diagnósticos tempranos sin necesidad de que los pacientes estén físicamente presentes en los centros de salud o hospitales. Telit Healht Monitoring: https://www.telit.com/industries-solutions/healthcare/health-monitoring
HOGARES INTELIGENTES	
Control remoto de aparatos y electrodomésticos	Los electrodomésticos y aparatos domésticos dotados con IoT permiten a los residentes controlar los dispositivos de forma remota para evitar incidentes y ahorrar energía. Además, teniendo en cuenta las entradas de los sensores, estos dispositivos pueden tomar decisiones autónomas. Plataforma Samsung Smart Things: https://www.samsung.com/us/smart-home
Cerraduras inteligentes	Cerraduras basadas en biometría que pueden alertar a los propietarios sobre las condiciones de seguridad de su hogar. Cerradura basada en el reconocimiento del iris Eyelock: https://www.eyelock.com
Detección de movimiento	Sistemas de monitorización de video con grabación en la nube y detección de movimiento. Sistema de monitorización de video Manything: https://manything.com/

LOGÍSTICA INTELIGENTE	
Seguimiento de flotas	Los sistemas de seguimiento de flotas que incorporan tecnología IoT mejoran la seguridad y proporcionan informes precisos y completos que dan a los administradores de la flota una total transparencia respecto a las actividades de la misma. Plataforma de gestión de flotas de Telefónica Fleet Optimise: https://iot.telefonica.com/es/solutions/optimise/fleet-optimise
Vehículos conectados	Los sensores están mejorando los vehículos junto con la IA y las capacidades analíticas. Estos sensores proporcionan comunicación con el conductor para suministrarle información útil sobre otros vehículos en la carretera y la infraestructura de la misma, a fin de ayudarle a tomar decisiones más seguras o más informadas Prototipo de camión semiautónomo de Mercedes-Benz: https://www.mercedes-benz.com/en/innovation/autonomous/the-long-haul-truck-of-the-future
SMART METERING O MEDICIÓN INTELIGENTE	
Smart Grid o Red Inteligente	Para las empresas de servicios públicos, IoT permite la gestión de datos a distancia y la capacidad de supervisión para gestionar mejor los flujos de energía que entran y salen de sus redes, y dar a los usuarios los conocimientos necesarios para comprender sus inversiones en infraestructura energética. Plataforma de gestión energética Lumin: https://www.luminsmart.com
Contadores Inteligentes	Permiten obtener datos en tiempo real de consumos de energía y agua. Contadores Inteligentes Kamstrup: https://www.kamstrup.com/es-es/soluciones-de-medicion-de-electricidad/contadores-de-electricidad-inteligentes

Tabla 6: Casos de uso de IoT.

4 EVOLUCIÓN DE TECNOLOGÍAS Y TENDENCIAS A FUTURO

Una de las fuentes más relevantes cuando se habla de tendencias tecnológicas a futuro es Gartner[59], una empresa estadounidense que se dedica fundamentalmente a la consultoría y a la investigación. Gartner creó hace unos años una forma gráfica de representar la evolución de tecnologías prometedoras a medio y largo plazo, denominada "*Hype Cycle*". La siguiente ilustración sirve para indicar el ciclo de vida conceptual de una tecnología emergente en cuanto a la madurez, adopción y aplicación de tecnologías específicas a través de cinco fases.

En algunos casos, Gartner publica estudios específicos sobre algunas tecnologías emergentes, como es el caso de IoT. En la siguiente figura se muestra la gráfica relativa a 2020 para IoT.

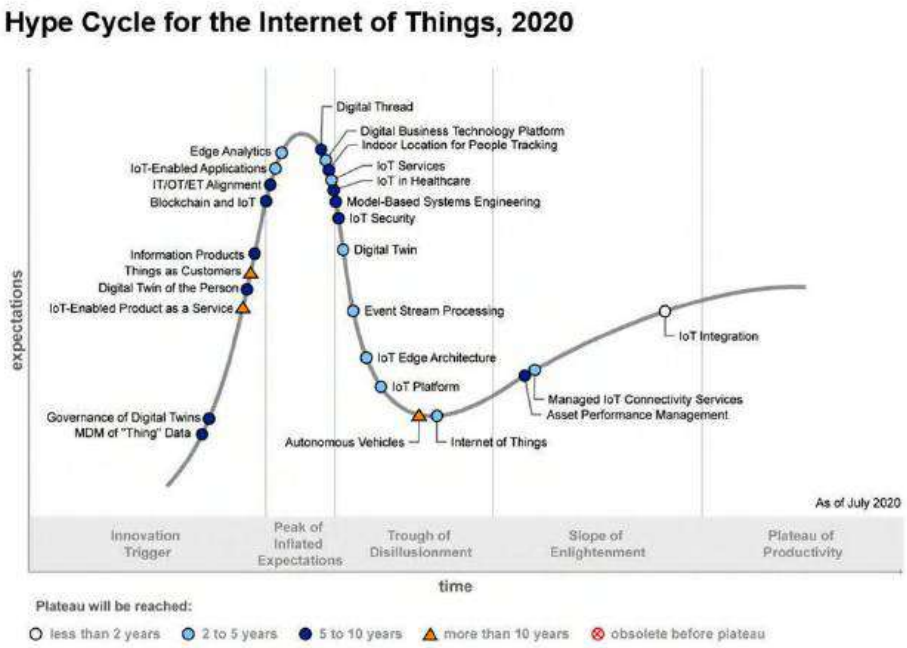


Figura 26: Hype Cycle para IoT, julio 2020.[60]

59 https://www.gartner.com
60 https://www.gartner.com/en/newsroom/press-releases/2020-08-18-gartner-identifies-five-emerging-trends-that-will-drive-technology-innovation-for-the-next-decade

4.1 IoT, Inteligencia artificial y Big Data

> ***Con la enorme cantidad de datos disponibles hoy en día, es importante analizarlos para obtener información significativa. La idea detrás del uso de estas tecnologías es extraer información procesable de estos datos.***

"La aplicación de la Inteligencia Artificial en soluciones IoT permitirá actuar sobre los datos de manera automatizada y en tiempo real, para lograr que los dispositivos sean "inteligentes"." (48)

"Se pronostica que la cantidad de dispositivos de Internet de las cosas (IoT) en todo el mundo casi se triplicará de 8,74 mil millones en 2020 a más de 25,4 mil millones de dispositivos de IoT en 2030. En 2020, la mayor cantidad de dispositivos de IoT se encuentra en China con 3,17 mil millones de dispositivos." (47). "La IA se aplicará a una amplia gama de información de IoT, incluyendo video, imágenes fijas, voz, actividad del tráfico de la red y datos de los sensores" (49). Con el objetivo de aprovechar la enorme cantidad de datos disponibles hoy en día, es necesario analizar estos datos para obtener información significativa de tal forma que se favorezca una mejora en la toma de decisiones (50).

Ante tal ingente cantidad de datos que se está generando y que se prevé que aumente en los próximos años, es necesario dotarse de infraestructuras y herramientas que permitan almacenar y gestionar este volumen de información teniendo en cuenta las siguientes características:

- La velocidad con la que se adquiere las medidas e información procedente de dispositivos y con la que debe procesar para proporcionar conocimiento de valor en tiempo real.
- La variedad o heterogeneidad de los datos, que como se ha mencionado puede proceder de múltiples fuentes, tanto no estructurada como, por ejemplo, imágenes fijas, vídeo, voz, etc. y estructuradas, por ejemplo, datos de sensores ya pre-procesada, series temporales, etc. El modelo relacional tradicional se ha relegado por la persistencia de nuevos tipos de datos, modelos no relacionales que se agrupan como NoSQL.
- Los requisitos de volumen a almacenar pueden alcanzar terabytes.
- La variabilidad en cuanto a que los cambios en la tasa de datos, su formato y la calidad repercuten en las aplicaciones y análisis posteriores.

> La veracidad en relación con la fiabilidad, aplicabilidad, ruido, sesgo, anormalidad y otras propiedades de calidad de los datos.

Todas estas características son propias de la definición de Big Data y, por lo tanto, implican que la evolución tecnológica de IoT va de la mano de la evolución del Big Data.

Asimismo, para ofrecer una analítica avanzada, tanto IoT como Big Data se apoyan en la Inteligencia Artificial para generar soluciones prácticas y que están revolucionando la automatización y la analítica predictiva.

Esta importante aportación del Big Data y la IA al ámbito de IoT destaca como una tendencia presente y a futuro para las funcionalidades que proporcionan a las soluciones.

Un buen ejemplo de IoT, Big Data e IA trabajando juntos se puede encontrar en la industria de la maquinaria/fabricación para desarrollar soluciones de mantenimientos preventivos (51).

4.2 Blockchain en IoT

> ***Blockchain es una base de datos transaccional que se organiza enlazando en forma de cadenas de bloques de transacciones y cifrada para proteger la privacidad y seguridad de éstas. Su información se guarda en un registro que se almacena y se gestiona de forma distribuida, como un libro mayor distribuido, entre diferentes nodos de red de equipos que aseguran su integridad.***

Blockchain es una base de datos transaccional que se organiza enlazando en forma de cadenas de bloques de transacciones y cifrada para proteger la privacidad y seguridad de éstas. Su información se guarda en un registro que se almacena y se gestiona de forma distribuida, como un libro mayor distribuido, entre diferentes nodos de red de equipos que aseguran su integridad.

La seguridad es una preocupación importante en IoT que ha obstaculizado su despliegue a gran escala. Otro problema con las redes de IoT actuales es la escalabilidad (52). La tecnología de cadena de bloques (Blockchain) o de libro mayor distribuido (DLT), tiene el potencial de ayudar a abordar algunos de los desafíos de seguridad de IoT (52):

> "En esencia, un sistema de cadena de bloques consiste en un libro de contabilidad digital distribuido, compartido entre los participantes en el sistema, que reside en Internet: las transacciones o los eventos se validan y registran en el libro de contabilidad y no pueden modificarse ni eliminarse posteriormente. Proporciona un medio para

> que la información sea registrada y compartida por una comunidad de usuarios. Dentro de esta comunidad, los miembros seleccionados mantienen su copia del libro de contabilidad y deben validar colectivamente toda nueva transacción mediante un proceso de consenso antes de que sean aceptadas en el libro de contabilidad." (52)

La tecnología Blockchain puede ayudar a resolver cuestiones de seguridad y escalabilidad en soluciones IoT, cuestiones como la no necesidad de que los participantes confíen entre sí, la imposibilidad de modificar transacciones, la transparencia entre los participantes o la rapidez en el procesamiento de las transacciones realizadas por miles de dispositivos puede ser solucionada mediante esta combinación de IoT y Blockchain.

La evolución tecnológica que combina IoT con Blockchain pone de manifiesto que esta evolución representa también una tendencia, ya que hay empresas que ya construyen sus plataformas basando sus características de seguridad en Blockchain. Estas permiten facilitar el procesamiento y la coordinación de transacciones entre las diferentes partes que interactúan en un sistema de IoT. De este modo, se cubren áreas de seguridad como la autenticación, autorización, cifrado y cumplimiento. Las principales ventajas que proporciona son:

- Escalabilidad: si se elimina la sobrecarga de administración de certificados, gracias a los "libros distribuidos de contabilidad" (distributed ledgers), se reduce el tráfico en la nube y la escalabilidad es más sencilla.
- Seguridad: reforzando la seguridad en cifrados débiles, paquetes maliciosos y ataques de "man-in-the-middle", o impidiendo el acceso a dispositivos no autorizados.
- Privacidad: ofreciendo mecanismos para verificar, facilitar y hacer cumplir los permisos habilitando solo los usuarios con los permisos adecuados.

4.3 IoT y Edge Computing

El Edge Computing es una alternativa a la computación en la nube y desplaza parte del procesamiento de los datos de la nube hacia los dispositivos que se ocupan de capturar datos del entorno.

> "Hasta ahora, los dispositivos de IoT se basan en la nube para almacenar los datos. Con la adopción del Edge Computing, en lugar de enviar todos los datos del dispositivo de IoT a la nube, los datos se transfieren primero a un dispositivo local que se encuentra más cerca del dispositivo de IoT o en el borde de la red. A continuación, después de clasificar y calcular los datos, los dispositivos de almacenamiento local envían una parte de los datos a la nube." (50)

Este enfoque en el dispositivo ayuda a reducir la latencia de las aplicaciones críticas, a disminuir la dependencia de la nube y a manejar mejor el enorme caudal de datos que generan las soluciones IoT (53).

> "Un ejemplo de esta tendencia es la cámara de seguridad interior Nest Cam IQ[61], que utiliza el procesamiento de visión en el dispositivo para observar el movimiento, distinguir a los miembros de la familia y enviar alertas sólo si alguien no es reconocido o no se ajusta a los parámetros predefinidos." (53)

Por tanto, el Edge Computing ofrece varias ventajas en los entornos IoT, como pueden ser la reducción de costos de conectividad, la anonimización de datos antes de enviarlos a la nube y así mejorar la privacidad de los usuarios o la mejora de la latencia en las comunicaciones (53).

Si bien, en los últimos años, existe una tendencia clara de migrar todos los datos, procesamiento y otros servicios a la nube (Cloud Computing), como se puede derivar del éxito que los grandes proveedores como Amazon, Microsoft Azure o Google tienen, es necesario subrayar que no todas las aplicaciones, ni necesidades de todos los clientes, pueden sostenerse con este modelo. Por un lado, existe clientes como en el sector de la defensa y la seguridad, que, por cuestiones de seguridad, confianza e incluso normativas, no pueden relegar su información en entornos no controlados por la organización como podría parecer la nube. Y también existen aplicaciones en las que tampoco tiene sentido enviar toda la información recogida por sensores en un servicio, (por ejemplo, de 24x7x365 días de una cámara de vídeo), con cierto peso en cada cuerpo mínimo de datos, para ser procesada en la nube y posteriormente retornar una respuesta al componente Edge. Esto puede conllevar elevados costes relativos al almacenamiento y a los flujos de información derivados. También, hay que tener en cuenta que existen una multitud de aplicaciones críticas y de tiempo real, como ciertos procesos industriales, que no pueden esperar a las latencias derivadas del flujo de datos hacia la nube y a una respuesta procesada o de control que retorna de ésta hacia el dispositivo Edge. Asimismo, se debe añadir el factor de la potencial pérdida de comunicación con la nube, dependiente de la infraestructura de comunicación o de un operador, de tal forma que pueda afectar al rendimiento o criticidad de los procesos. En definitiva, frente a la aparente tendencia dominante Cloud Computing, se dan casos en los que esta evolución no puede ser una realidad, por lo que Edge Computing representa la otra gran alternativa necesaria.

4.4 Gemelo Digital (Digital Twin)

> "Un gemelo digital es una representación digital de un objeto o sistema físico. La tecnología detrás de los gemelos digitales se ha expandido para incluir sistemas grandes como edificios, fábricas e incluso ciudades." (54)

La aplicación del concepto de gemelo digital al mundo de IoT permite a los diseñadores de soluciones IoT optimizar despliegues, mejorar el rendimiento de las aplicaciones, detectar problemas, etc. (54)

61 https://store.google.com/us/product/nest_cam_iq

Asimismo, en la mayoría de los casos un gemelo digital no es posible sin la tecnología IoT, u otras fuentes de datos, ya que son precisamente los datos proporcionados los que dan vida al modelo digital nutriéndole de información en tiempo real.

El gemelo digital es otra gran tendencia a tener en cuenta en los próximos años, aunque en la actualidad pocas son las empresas que han alcanzado implementaciones reales y completas. Queda un recorrido relativo para que sea una tecnología madura y en plena producción. Hasta el momento, se han realizado pruebas conceptuales, algunas implementaciones de cierto alcance en algunos sectores y demostradores. Para ello algunas grandes empresas están orientado sus componentes tecnológicos para ofrecer una solución integral la cual implica una conjunción de elementos tales como: software de diseño y modelización 3D CAD/CAM que definen geométricamente el producto y permiten su simulación y la validación de los diseños (CAE), herramientas que almacenan la información generada por las herramientas de diseño y simulación para gestionar el ciclo de vida del producto como las de PLM/ALM y, por otro lado, tecnologías como Big Data, IoT, Realidad Aumentada, Realidad Virtual e incluso Inteligencia Artificial. Teniendo en cuenta toda su dimensión, un Gemelo Digital es una tecnología compleja en la que intervienen muchas piezas. Es por ello, por lo que todavía requiere una evolución tecnológica orientada fundamentalmente a la integración de sistemas y tecnologías que ahora mismo están en continuo desarrollo.

4.5 IoT Social, Legal y Ética

> "A medida que IoT madure y se despliegue más ampliamente, una amplia gama de cuestiones sociales, legales y éticas crecerá en importancia. Entre ellas figuran la propiedad de los datos y las deducciones que se hacen de ellos; el sesgo algorítmico; la privacidad; y el cumplimiento de normas como el Reglamento General de Protección de Datos (RGPD)". (49)

Es decir, al tratar en muchas ocasiones con información de carácter personal y sensible, las aplicaciones IoT no sólo tienen que considerarse en su diseño cuestiones técnicas, sino que deben tener en cuenta cuestiones éticas como la posibilidad de identificar al autor de los datos recogidos, la definición de fronteras entre la vida pública y la privada de las personas o los posibles ataques a la vida de las personas usuarias. (55)

También surgen cuestiones sobre la capacidad y la existencia de leyes preparadas para proteger a los usuarios en ese entorno. (55)

> "Se deben aplicar soluciones técnicas eficaces para animar a los usuarios a participar en las redes IoT. Tales soluciones pueden ser técnicas avanzadas de cifrado, firmas electrónicas, legislaciones para limitar el uso de los datos recogidos por terceros, y otras. Las nuevas leyes y normas deberían complementar las diferentes leyes

> existentes para mantener la seguridad y la privacidad completas y cubrir todas las cuestiones legales". (55)

Existe un amplio espacio de desarrollo en el IoT y la relación legal y ética. Si bien la RGPD contempla unas directivas exigentes que contemplan el tratamiento y la propiedad de los datos, la protección de los mismos, el sesgo y otras cuestiones éticas, todavía dicha relación debe adaptarse continuamente a las nuevas implementaciones y nuevos desarrollos asegurando la aplicación normativa y la adaptación de ésta a la nueva realidad y a las evoluciones que se deriven.

4.6 Infonomía y venta de datos

> "La infonomía es la disciplina emergente de la gestión y la contabilidad de la información con el mismo o similar rigor y formalidad que otros activos y pasivos tradicionales (como los activos financieros, físicos e intangibles y el capital humano). La Infonomía postula que la información en sí misma cumple todos los criterios de los activos formales de las empresas y cada vez es más importante que las organizaciones se comporten como si la información fuera un activo real[62]."

Según Gartner (49), la compra y venta de datos captados por soluciones IoT se convertirá en una parte esencial de muchos entornos de IoT. Muchas empresas ya están vendiendo datos recogidos por sus aplicaciones IoT. Las empresas deben ser conscientes de los riesgos y oportunidades que ofrece esta monetización de los datos.

4.7 Gobernanza de IoT

> "A medida que IoT continúa expandiéndose, será cada vez más necesario de un marco de gobernanza que asegure un comportamiento adecuado en la creación, el almacenamiento, el uso y la eliminación de la información relacionada con los proyectos de IoT. La gobernanza abarca desde tareas técnicas sencillas como la auditoría de dispositivos y la actualización de firmware hasta cuestiones más complejas como el control de los dispositivos y el uso de la información que generan. Las empresas deben asumir la función de educar a sus organizaciones en cuestiones de gobernanza y, en algunos casos, invertir en personal y tecnologías para abordar la gobernanza." (49)

62 https://www.gartner.com/en/information-technology/glossary/infonomics

Las soluciones de IoT implican muchas tecnologías diferentes y requieren ciclos de desarrollo complejos, incluidas pruebas importantes y una vigilancia continua (56). La gobernanza de las soluciones de IoT puede considerarse como la aplicación de la gobernanza empresarial, la gobernanza de las Tecnologías de la Información y la gobernanza de la arquitectura empresarial (EA) a la Internet de las cosas, como se muestra en la siguiente figura:

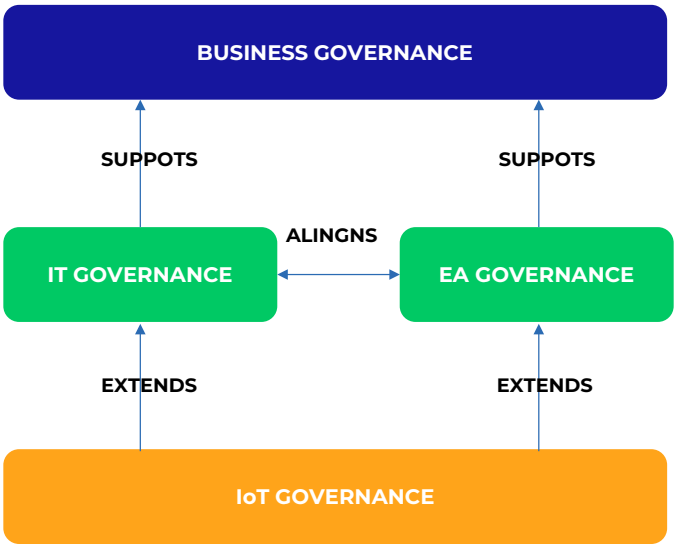


Figura 27: Un modelo de gobernanza IoT (56).

Como se puede observar la gobernanza planteada supone un reto que implica diferentes actores en el entorno empresarial en su sentido más amplio. Este reto supone una tendencia a futuro debido a que no solo no está resuelta, sino que conlleva la integración de estos actores, sus implicaciones tecnológicas y tener en cuenta los aspectos como los enumerados en los apartados de IoT Social, Legal y Ético, de la Infonomía y venta de datos.

4.8 Hardware y sistemas operativos confiables

> "La seguridad es seguramente el área de preocupación técnica más importante para las organizaciones que despliegan sistemas de IoT. A corto plazo, se espera ver el despliegue de combinaciones de dispositivos y aplicaciones que, en conjunto, creen sistemas de IoT más fiables y seguros." (49)

Algunos de los mecanismos de protección que irán incorporando los dispositivos IoT para aumentar su nivel de seguridad son (57):

- "Raíz de confianza (Root of Trust): es un proceso de arranque validado por hardware que asegura que el primer código ejecutable en el dispositivo comienza desde una fuente inmutable.
- Módulos de gestión de claves y plataformas de confianza: las claves criptográficas son fundamentales para garantizar un sistema seguro. Hay estándares de hardware para la

seguridad de claves y un mecanismo particularmente popular es el Trusted Platform Module (TPM)[63].

> Seguridad del almacenamiento: los dispositivos de almacenamiento, como los módulos flash y los discos, deben disponer de tecnología de cifrado y seguridad. Además del cifrado, también es necesario considerar la seguridad de los medios de almacenamiento cuando se desmantelan o se eliminan.
> Seguridad física: En muchos escenarios, un dispositivo de IoT estará ubicado en lugares remotos y desatendidos ´, sin las protecciones de los dispositivos locales".

La tecnología IoT debe ser acompañada en su evolución por la securización de sus sistemas. De hecho, la seguridad es uno de los elementos que más preocupa en la adopción de esta tecnología, por lo que, garantizar este componente será una constante en el desarrollo de IoT y por lo que representa una tendencia clave a futuro.

4.9 Experiencia de usuario en IoT

> "La experiencia de usuario (UX) de IoT cubre una amplia gama de tecnologías y técnicas de diseño. Será impulsada por cuatro factores: nuevos sensores, nuevos algoritmos, nuevas arquitecturas de experiencia y contexto, y experiencias con conciencia social. Dado que cada vez se producen más interacciones con cosas que no tienen pantallas ni teclados, los diseñadores de UX tendrán que utilizar nuevas tecnologías y adoptar nuevas perspectivas si quieren crear una UX superior que fomente su uso y la retención de los usuarios." (49)

Existen actualmente algunas recomendaciones básicas que ayudan a los desarrolladores a pensar en la dirección correcta a la hora de crear buenas aplicaciones de UX para IoT (58): diseño de soluciones orientado al uso de datos, diseño centrado en el usuario y diseño que garantice la seguridad de los datos.

Por otro lado, más allá de aplicar las recomendaciones de UX para aplicaciones propiamente IoT, esta tecnología también genera soluciones que ayudan en sí mismas a crear experiencias de usuario novedosas, como puede ser en el mundo de los vídeo juegos o mediante aportaciones a la realidad aumentada o virtual.

De un modo u otro, en el contexto comercial está claro que tienen mayor éxito los productos y servicios que atienden cuidadosamente las experiencias de usuario. Por lo tanto, toda mejora de UX, su aplicación y la creación de nuevos dispositivos IoT que desarrollen esta dirección, representan una tendencia a futuro que se desarrollará en paralelo con la evolución tecnológica en general.

63 https://www.iso.org/standard/66510.html

4.10 Nuevas tecnologías de redes inalámbricas para IoT

> "La creación de redes de IoT implica equilibrar un conjunto de requisitos que compiten entre sí, como el costo de los puntos finales, el consumo de energía, el ancho de banda, la latencia, etc. Ninguna tecnología de redes optimiza todo esto y las nuevas tecnologías de redes de IoT proporcionarán a las empresas una mayor elección y flexibilidad. En particular, las empresas deberían explorar la tecnología 5G y la próxima generación de satélites de órbita terrestre baja." (49)

El despliegue de nuevas soluciones IoT se verá acompañado de la expansión de redes 5G en todo el mundo. Las redes 5G proporcionan una conectividad más rápida y fiable que las redes móviles anteriores y, junto con el despliegue definitivo del protocolo IPv6, posibilitarán el aumento de dispositivos IoT de todo tipo y de sectores como la ciudad inteligente, los vehículos conectados o la atención sanitaria. Se espera que en un futuro próximo se forme un ecosistema completo de sensores y dispositivos inteligentes totalmente conectados (59).

Las redes inalámbricas y las futuras mejoras que se van implementando representan una evolución tecnológica que no ha parado de desarrollarse y que impacta directamente en el desarrollo de IoT. Se espera que esta tendencia se mantenga constante en los próximos años y continúe incrementándose.

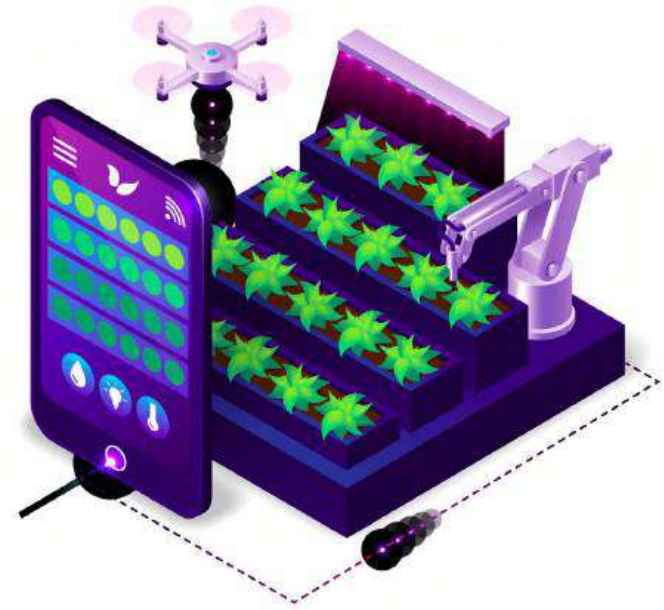
5 PRESENTACIÓN DE LOS PRINCIPALES ACTORES A NIVEL INTERNACIONAL

> ***La IoT es un conjunto heterogéneo de actores económicos, de diferentes sectores, que juntos constituyen este nuevo mercado.***

La IoT agrupa un conjunto heterogéneo de actores económicos, de diferentes sectores, que juntos constituyen este nuevo mercado. Sus principales actores son:

- Diseñadores y fabricantes de objetos conectados,
- Los fabricantes de los componentes electrónicos de estos objetos,
- Operadores y administradores de redes de transmisión de datos,
- Los gestores de las plataformas de recopilación y procesamiento de datos,
- Diseñadores de software de interfaces entre objetos y usuarios,
- Proveedores de servicios que recogen, analizan y utilizan los datos de los usuarios proporcionados por los objetos conectados,
- Los reguladores públicos, que garantizan el cumplimiento de las leyes en lo que respecta al respeto de la vida y los datos privados, así como las normas de seguridad para los objetos conectados.

5.1 PANORAMA DE ORGANIZACIONES Y ESTÁNDARES DE LA INDUSTRIA



> ***Algunas de las organizaciones de la industria centran sus esfuerzos en un determinado ámbito de aplicación de IoT, mientras que otras participan en la definición de tecnologías transversales que se aplican a diversas aplicaciones de IoT.***

El panorama de la industria de IoT está lleno de diferentes organismos y organizaciones de estandarización que tratan varios aspectos de la tecnología. Como suele ser el caso en los inicios de un ciclo tecnológico, algunas de las organizaciones están abordando el mismo problema y, por lo tanto, un subconjunto de las normas que se están proponiendo se superponen y compiten por la adopción de la corriente principal (60). Esto crea confusión en la industria e inevitablemente retrasa el desarrollo de productos, ya que los fabricantes no quieren hacer apuestas sobre estándares que tal vez nunca despeguen en el mercado.

“Algunas de las organizaciones de la industria centran sus esfuerzos en un determinado ámbito de aplicación de IoT, mientras que otras participan en la definición de tecnologías transversales que se aplican a diversas aplicaciones de IoT. Además, no todas las organizaciones están definiendo activamente sus propias normas; más bien, algunas están promoviendo la armonía y la alineación entre otras, que definen y ratifican estándares.

Lo que es común a todas estas normas y estándares es que todas se basan en (o están migrando hacia) una capa de normalización común, la capa de red IP, que garantiza la interoperabilidad de los sistemas y se adapta a una multitud de tecnologías de capa de enlace, además de una gran cantidad de protocolos de aplicación” (60).

Esta sección se centrará en los organismos que operan en las capas físicas, de enlace de datos, de red y de transporte del modelo OSI y también se tocarán un subconjunto de organismos que operan en la capa de aplicación.

IEEE (Institute of Electrical and Electronics Engineers)

"El IEEE es un organismo estandarizador de tecnología consolidado, que, entre otras cosas, ha definido los estándares de Ethernet y las redes de área local inalámbricas (LAN). Dado su legado y experiencia en tecnologías de redes de capa física y de enlace, el IEEE se embarcó en la definición de una serie de estándares de capas físicas y de enlace para IoT" (60). Entre ellos se incluye la familia de protocolos inalámbricos de baja potencia 802.15.4, el estándar de Wi-Fi de largo alcance 802.11ah, así como las normas de Power Line Communications. Estas últimas definen las tecnologías de transporte de datos en red sobre el cableado eléctrico convencional.

"Más allá de los esfuerzos en la estandarización de las tecnologías de la capa física y de la capa de enlace, el IEEE lanzó la iniciativa de IoT como una plataforma para que la comunidad técnica colaborara sobre las tecnologías que hacen avanzar IoT. Junto con esta iniciativa, muchas de los estándares relacionados con IoT se han completado o están en curso" (60).

IETF

"El IETF ha sido fundamental en la definición y estandarización de los protocolos de Internet, incluyendo IPv4 e IPv6, así como numerosos protocolos de enrutamiento (por ejemplo, OSPF, RIP, PIM, BGP), protocolos de aplicación (por ejemplo, HTTP, LDAP, SMTP), y protocolos de seguridad (por ejemplo, TLS, IPSec, IKE)" (60). En 2006, empezó a trabajar en una serie de normas para IoT. Actualmente, hay cinco Grupos de trabajo de la IETF centrados en tecnologías relacionadas con IoT.

ITU

"La Unión Internacional de Telecomunicaciones (ITU) es un organismo de las Naciones Unidas (ONU) con más de 190 estados miembros y más de 700 miembros de la industria, además de universidades e institutos de investigación y desarrollo. Ha participado intensamente en la definición y el desarrollo de estándares de telecomunicaciones" (60).

La UIT publicó uno de los primeros informes sobre "la Internet de las Cosas" en 2005 y ha participado en el desarrollo de IoT desde entonces, produciendo múltiples documentos normativos.

IPSO Alliance

"La Alianza para el Protocolo de Internet para Objetos Inteligentes (IPSO) es un grupo abierto de interés especial sin ánimo de lucro que promueve el uso del protocolo IP para conectar objetos inteligentes a la red. Se formó en 2008 e incluye miembros de empresas de tecnología y comunicaciones, además de empresas verticales de la industria (por ejemplo, de energía). La alianza complementa la labor de otros órganos de definición de normas, como el IETF, el

IEEE y el ETSI, promoviendo las tecnologías de IoT mediante la publicación de libros blancos y la celebración de seminarios web, eventos de interoperabilidad y desafíos" (60).

OCF

"Open Connectivity Foundation (OCF) es un grupo industrial que se centra en desarrollar estándares y certificaciones para dispositivos de IoT basados en el protocolo CoAP de la IETF. Se formó en julio de 2014 por Intel, Broadcom y Samsung Electronics bajo el nombre de Open Interconnect Consortium. El consorcio cambió su nombre a OCF en febrero de 2016. Actualmente tiene más de 80 compañías asociadas incluyendo General Electric, Cisco Systems, Microsoft y Qualcomm. El OCF está definiendo un marco para el descubrimiento sencillo de dispositivos y la conectividad confiable entre cosas. En septiembre de 2015, publicó la primera versión de la especificación de este marco. El OCF también está trabajando en la aplicación de referencia de código abierto de la especificación, que se llama *IoTivity*" (60) .

IIC

"El Industrial Internet Consortium es una organización sin ánimo de lucro que tiene por objeto acelerar el desarrollo y la adopción de máquinas y dispositivos, análisis inteligentes y personas interconectados. Fue fundada por AT&T, Cisco, General Electric, IBM e Intel en marzo de 2014. El IIC no desarrolla estándares para IoT; más bien, proporciona requisitos a otras organizaciones que definen estándares. El IIC se centra en la creación de casos de uso, arquitecturas de referencia, marcos y bancos de pruebas para aplicaciones reales de IoT a través de diversos entornos industriales. El IIC también establece entre sus objetivos facilitar foros abiertos para compartir e intercambiar ideas y prácticas del mundo real, y conocimientos, además de crear confianza en torno a nuevas e innovadoras enfoques de la seguridad. El trabajo del IIC no incluye a los consumidores; más bien está dirigido a los negocios verticales como la energía, la atención sanitaria, el transporte y la fabricación" (60).

ETSI

"The European Telecommunication Standards Institute (ETSI) es una organización independiente sin ánimo de lucro que define normas. El ETSI fue una de las primeras organizaciones en desarrollar un conjunto de estándares que definen una capa de servicio horizontal completa para las comunicaciones M2M.

Los estándares M2M del ETSI especifican componentes arquitectónicos para IoT, incluyendo dispositivos (cosas), pasarelas con interfaces asociadas, aplicaciones, tecnologías de acceso, así como la Capa de Capacidades de Servicio M2M (middleware). También incluyen características de seguridad, programación del tráfico, descubrimiento de dispositivos y gestión del ciclo de vida" (60).

El ETSI también está investigando varias aplicaciones de las tecnologías M2M, incluyendo electrodomésticos inteligentes, medición inteligente, ciudades inteligentes, redes inteligentes, eSalud, sistemas de transporte inteligentes y automatización industrial inalámbrica.

oneM2M

"En julio de 2012, siete organizaciones de elaboración de normas (TIA y ATSI de los EE.UU., ARIB y TTC del Japón, CCSA de China, ETSI de Europa y TTA de Corea) crearon una organización mundial para definir y normalizar conjuntamente las funciones horizontales comunes de la capa de servicios de aplicación de IoT en el marco del Proyecto de Asociación OneM2M . Los fundadores acordaron transferir y detener su propio trabajo sobre la capa de servicios de aplicación de IoT que se superponía. La asociación ha crecido hasta incluir, además de los siete órganos de normalización, cinco foros mundiales de tecnología de la información y las comunicaciones y más de 200 empresas" (60).

AllSeen Alliance

"La Alianza AllSeen se formó en diciembre de 2013 como un Proyecto de Colaboración de la Fundación Linux.

Es un consorcio abierto sin ánimo de lucro que tiene como objetivo promover IoT basada en el proyecto de código abierto AllJoyn. AllJoyn es un marco de software abierto, seguro y programable destinado a la conectividad y los servicios. Permite que los dispositivos descubran, conecten e interactúen directamente con otros productos habilitados por AllJoyn. El proyecto fue creado originalmente por Qualcomm y lanzado al dominio del código abierto.

Consiste en un kit de desarrollo de software de código abierto (SDK) y una base de código de marcos de servicio que permiten funciones básicas de IoT como el descubrimiento, la incorporación, la gestión de la conexión, el enrutamiento de mensajes y la seguridad, garantizando así la interoperabilidad entre los sistemas" (60).

Thread Group

"El grupo de trabajo Thread se formó en julio de 2014 e incluyó a la filial de Google Nest, Samsung, ARM Holdings, Freescale, Silicon Labs, Big Ass Fans, y la compañía de cerraduras Yale. El propósito del grupo es promover Thread como el protocolo para el hogar conectado y certificar los productos que apoyan este protocolo. El protocolo Thread es un protocolo libre de derechos de autor de documentación cerrada que se ejecuta en la parte superior de IEEE 802.15.4 y 6LowPAN. Añade funciones como la seguridad, el enrutamiento, la configuración y el encendido del dispositivo para maximizar la duración de la batería. El hilo compite con otros protocolos ya existentes en este espacio como Bluetooth Smart, Z-Wave y ZigBee" (60).

ZigBee Alliance

"La ZigBee Alliance fue formada en 2002 por Motorola, Philips, Invensys, Honeywell y Mitsubishi para desarrollar, mantener y publicar el estándar ZigBee. Desde entonces, la alianza ha crecido hasta incluir a más de 170 miembros participantes y más de 230 empresas adoptantes, incluyendo ABB, Fujitsu, British Telecom, Huawei, Cisco, etc. La alianza publica 'perfiles de aplicación' que permiten a los proveedores crear productos interoperables. La especificación inicial de ZigBee se centraba en la automatización del hogar, pero desde entonces su alcance se ha ampliado para incluir la automatización de grandes edificios, aplicaciones de venta al por menor y la supervisión de la salud" (60).

TIA

"La Asociación de la Industria de las Telecomunicaciones (TIA) elabora normas industriales para las tecnologías de la información y las comunicaciones y representa a más de 400 empresas en este ámbito. El comité de ingeniería de la TIA TR-50 fue creado en 2009 para desarrollar estándares de interfaz programática de aplicaciones (API) para la supervisión y la comunicación bidireccional entre los dispositivos inteligentes y otros dispositivos, aplicaciones o redes. El comité incluye a muchos actores de la industria, entre ellos Alcatel Lucent, AT&T, CenturyLink, Cisco, Ericsson, ILS Technology, Intel, LG, Nokia Siemens Networks, Numerex, Qualcomm, Sprint, Verizon y Wyless" (60). Incluso antes de la TR-50, la TIA estaba involucrada en los estándares M2M, con varios de sus comités de ingeniería trabajando en comunicaciones de dispositivos inteligentes

Z-Wave Alliance

"La Alianza Z-Wave es un consorcio industrial de más de 300 compañías que crean productos y servicios de IoT sobre el protocolo Z-Wave. Z-Wave es un protocolo inalámbrico de corto alcance, inicialmente desarrollado por una pequeña empresa danesa llamada Zensys. Z-Wave es un protocolo integrado verticalmente, que funciona a través de su propia capa de radio. Las capas de acceso físico y de enlace de Z-Wave fueron ratificadas por la Unión Internacional de Telecomunicaciones (UIT) como la norma internacional G.9959. A menudo se considera que Z-Wave es el principal competidor de ZigBee, pero a diferencia de ZigBee, sólo se centra en las aplicaciones del entorno doméstico" (60).

5.2 Principales empresas a nivel internacional

> ***Se espera que el mercado global de IoT alcance un valor de 1.386.06 mil millones de dólares para 2026 desde 761.4 mil millones de dólares en 2020 a una tasa compuesta anual del 10,53%, durante el período 2021-2026.***

> "Se espera que el mercado global de IoT alcance un valor de 1.386.06 mil millones de dólares para 2026 desde 761.4 mil millones de dólares en 2020 a una tasa compuesta anual del 10,53%, durante el período 2021-2026. Con el desarrollo de tecnologías de redes inalámbricas, la aparición de análisis de datos avanzados, una reducción en el costo de los dispositivos conectados, un aumento en la adopción de la plataforma en la nube, se espera que el mercado crezca a un ritmo positivo" (61)

Con esta perspectiva de crecimiento, el panorama de empresas que se dedican a IoT a nivel internacional es también cada vez mayor. En muchas ocasiones, se trata de pequeñas empresas de reciente creación que ofrecen productos/servicios de nicho novedosos, y son capaces de competir con grandes multinacionales. Por supuesto, las grandes empresas de Internet y de TI como Google, Amazon, Apple, Microsoft, etc. también están intentando explotar este negocio que supone IoT, desarrollando y evolucionando constantemente sus productos y servicios.

En esta sección se presentan algunas de las empresas que tiene mayor presencia o relevancia en el entorno IoT a nivel internacional, se incluyen las referencias (40), (41), (42), (43) y (62). El criterio seguido para elegir estas empresas ha sido considerar compañías consolidadas y con largo recorrido en el panorama internacional, referentes en el mercado, de tamaño medio y grande, y que tiene productos, servicios o soluciones IoT en producción. Estas compañías pueden ser representativas para empresas que se estén planteando iniciar desarrollos en el ámbito de IoT, bien como ejemplos o referentes, o para ser utilizadas como base sus operaciones, productos y servicios.

Empresa	URL
Alibaba IoT Cloud Solutions	Plataforma de IoT de la empresa China Alibaba para la generación de aplicaciones, recolectar, procesar y analizar datos procedentes de diferentes dispositivos https://www.alibabacloud.com/solutions/IoT
Altizon	Plataformas de computación orientadas a la fabricación, como Datonis Industrial IoT, Manufacturing y Edge. https://altizon.com
ARM	Plataforma IoT para la gestión de la conectividad, gestión de dispositivos y gestión de datos. Dispositivos IoT. https://www.arm.com/solutions/iot
Prodea	Solución end-to-end mediante la plataforma Arrayent Connect Platform de Prodea http://prodea.com/platform/
Atos	Plataforma de servicios inteligentes para soluciones IoT Atos Codex. https://atos.net/en/solutions/atos-codex-connected-intelligence/atos-codex-iot
AWS IoT	Conjunto de servicios de la arquitectura propuesta por AWS para IoT. https://aws.amazon.com/es/iot/
Ayla IoT Platform	Empresa y plataforma que permite la incorporación de datos de dispositivos Edge, la gestión de los mismos y la construcción de aplicaciones. https://www.aylanetworks.com/
Bosch	Plataforma Bosch IoT Suite para conectar y gestionar dispositivos, sensores y gateways. https://www.bosch-iot-suite.com
Braincube	Plataforma IoT que ofrece una infraestructura Big Data, integración y estructuración de la información desde sistemas IT y OT en formato Edge y Cloud. https://braincube.com/solutions/iiot-platform/
Bsquare	Suite de productos que abarcan el ámbito Edge y Cloud para proporcionar soluciones que reducen el Time-to-Market. https://www.bsquare.com/products-and-services/iot-software-services/
Cisco	Soluciones de redes, gateways, gestión de datos y seguridad para soluciones IoT. https://www.cisco.com/c/es_es/solutions/internet-of-things/overview.html
Davra	Plataforma para soluciones IoT en el ámbito industrial. https://davra.com
Ericsson IoT Platform	Solución de plataforma IoT de Ericsson para la conectar dispositivos de forma global. https://www.ericsson.com/en/internet-of-things/platform
Eurotech	Produce dispositivos IoT funcionales. También suministra una plataforma de integración de IoT basada en una arquitectura de microservicios, conocida como Everyware Cloud. https://www.eurotech.com/en/products/iot/
Evrythng	Solución IoT Cloud en producción para grandes clientes https://evrythng.com/

Exosite	Software de IoT industrial, a través e la plataforma Murano, para monitorizar remotamente la condición de equipos, máquinas y activos de alto valor. https://www.exosite.com
Fiware	Plataforma open-source en continua evolución y muy utilizada en el panorama nacional. https://www.fiware.org/
Flutura	Sistemas IoT para la industria pesada. Plataforma Flutura Celebra. https://www.flutura.com
GE Digital	A partir de Predix, la plataforma IoT de GE, se habilitan entornos de prueba, modelado de procesos, optimización de la distribución y soluciones analíticas para implementar soluciones IoT. https://www.ge.com/digital
Google Cloud	Solución de Google orientada al ámbito IoT. https://cloud.google.com/
Hitachi	Soluciones de aplicaciones IoT y de análisis Lumada. También es fabricante de muchos de los equipos que las industrias ya utilizan, como motores, refrigeradores, controladores, etc. https://www.hitachivantara.com/en-us/products/iot.html
Hitachi Vantara - Lumara	Solución de Hitachi mediante su plataforma Lumara para proporcionar conectividad a dispositivos IoT. https://www.hitachivantara.com/es-latam/products/iot.html
HPE Universal IoT Platform	HPE proporciona una amplia gama de hardware específico para soluciones IoT muy enfocadas al ámbito Edge más que al Cloud. https://www.hpe.com/emea_europe/en/solutions/iot-platform.html
HQ Software Lab	Desarrollo de dispositivos y sensores, análisis de datos, diseño de UI/UX y desarrollo de aplicaciones móviles. https://hqsoftwarelab.com
Huawei	Soluciones inteligentes sectoriales. https://e.huawei.com/es/solutions/technical/iot
IBM	Entre otros servicios, ofrece la plataforma Watson IoT que incorpora tecnologías de inteligencia artificial. https://www.ibm.com/es-es/watson
IoTivity	Plataforma open-source que proporciona conectividad a dispositivos IoT https://iotivity.org/
IoTSens	Empresa con soluciones y enfocadas a cuatro verticales: agua, ciudades, industria y desarrollos personalizados IoT. https://www.iotsens.com/es/
Kaa IoT Platform	Plataforma genérica Cloud y Gateway IoT de largo recorrido en el sector. https://www.kaaproject.org/
Litmus Automation	Frameworks LoopEdge y DeviceHub, para conseguir soluciones IoT más gestionables. https://litmus.io
Microsoft - Azure IoT Hub	Conjunto de servicios de Microsoft a través del cloud de Azure para el ámbito IoT https://azure.microsoft.com/es-es/services/iot-hub/

Octoblu	Plataforma multiprotocolo para la creación segura de servicios IoT. https://octoblu.github.io/
Oracle	Plataformas de IoT orientadas a la fabricación inteligente, el mantenimiento predictivo o la logística inteligente. https://www.oracle.com/es/internet-of-things
PTC	Plataforma de IoT Industrial ThingWorx. https://www.ptc.com/es/products/thingworx
QIO Technologies	Soluciones de IoT basadas en la aplicación de la inteligencia artificial. https://qio.ai/
RootCloud	Solución madura y con amplio recorrido en el sector por la que se utilizan en diversas verticales. http://en.rootcloud.com/
Samsung SDS	Orientación de Samsung hacia el ámbito IoT muy orientado a la domótica. https://www.samsungsds.com/us/iot/iot.html?referrer=https://www.google.com/
SAP Leonardo IoT	Solución de SAP orientada a IoT. https://help.sap.com/viewer/product/SAP_Leonardo_IoT/1904b/en-US
Schneider Electric - Wonderware Industrial IoT	Solución de Schneider Electric/Wonderware para la conectividad de dispositivos IT y OT muy centrada en la industria. https://www.wonderware.es/internet-de-las-cosas-industrial-iiot/
Siemens	Plataforma IoT MindSphere de Siemens en constante evolución y muy ligada a sus productos y soluciones IT y OT. Ha realizado importantes adquisiciones de software para extender sus servicios y facilidades en el ámbito IoT. https://siemens.mindsphere.io
Software AG	Ofrece todo tipo de servicios, desde suites de software integradas diseñadas para la supervisión de empresas hasta plataformas en la nube que facilitan la creación de sistemas de IoT a medida, por ejemplo, la plataforma de IoT Cumulocity. https://www.softwareag.com
ThinSpeak	Solución para proyectos IoT con capacidades de recolección de datos y analítica de los mismo utilizando la potencialidad de Matlab. https://thingspeak.com/
Verizon - ThingSpace	Espacio dentro de IoT de la empresa Verizon a través de su plataforma Thingspace y con capacidades de gestión de software. https://thingspace.verizon.com/index.html

Tabla 7: Empresas IoT a nivel internacional.

6. INFOGRAFÍA RESUMEN

Internet of Things (IoT) se define como la **capacidad de los objetos de transferir datos** por Internet sin necesidad de interacciones por parte de los usuarios.

Internet of Everything (IoE) extiende este concepto a la **interconexión de dispositivos, personas y procesos**.

ANDALUCÍA CONECTADA

ARQUITECTURA

La arquitectura de referencia de IoT la componen **diferentes capas de tecnologías** que dan soporte a la implementación de soluciones.

- Sensores
- Servicios
- Comunicación
- Aplicaciones

En 2025, habrá en el mundo 75.000 Millones de dispositivos conectados

El volumen de datos generados por IoT en 2025 se estima en 79,5 Zettabytes

CASOS DE USO

Las aplicaciones de Internet de las Cosas (IoT) se están extendiendo cada vez más. Entre los **sectores con mayor nivel de implantación de IoT destacan la industria manufacturera y la salud**.

- Industria
- Hogares
- Salud
- Smart Cities

ELEMENTOS TÉCNICOS

Los elementos técnicos de una solución IoT **se relacionan y combinan entre sí** para ofrecer el resultado esperado.

- Comunicación
- Actuadores
- Sensores
- Plataformas

En 2020, el 80% de la industria manufacturera cuenta ya con algún tipo de tecnología IoT

En 2020, el 60% de los dispositivos IoT se instalarán en hogares

TENDENCIAS Y OPORTUNIDADES

La irrupción de tecnologías IoT han sido **pioneras en el crecimiento de nuevos negocios** y con la llegada del 5G se espera un repunte en la adopción de estas tecnologías.

- Innovación en sensores
- Edge Computing
- IA
- Blockchain

7 REFERENCIAS

1. *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges*. Keyur K Patel, Sunil M Patel. 5, s.l. : International Journal of Engineering Science and Computing, 2016, Vol. 6.

2. Misra. Sensors and Actuators in IoT | Enabling Industrial Automation. [Online] 2017. https://bridgera.com/sensors-and-actuators-in-iot/.

3. Beniamino Di Martino, Kuan-Ching Li, Laurence Tianruo Yang, Antonio Esposito. *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*. s.l. : Springer, 2018.

4. *Securing the Internet of Things: Challenges, threats and solutions*. Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios. s.l. : Elsevier, 2019, Internet of things, Vol. 5.

5. *A gap analysis of internet-of-things platforms*. Julien Mineraud, Oleksiy Mazhelis, Xiang Su, Sasu Tarkoma. 2016, Computer Communications, Vol. 89.

6. Michele Albano, Erkki Jantunen, Gregor Papa, Urko Zurutuza. *The MANTIS Book: Cyber Physical System Based Proactive Collaborative Maintenance*. s.l. : River Publishers , 2019.

7. *Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases*. Tiago M. Fernández-Caramés, Paula Fraga-Lamas. 2020, Sensors (Basel).

8. *A Review of Security Concerns in Internet of Things*. Leloglu, . 1, 2017, Journal of Computer and Communications, Vol. 5.

9. *Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends*. Anna Triantafyllou, Panagiotis Sarigiannidis , Thomas D. Lagkas. 2018, Wireless Communications and Mobile Computing, Vol. 2018.

10. William Stallings, Lawrie Brown. *Computer Security: Principles and Practice*. s.l. : Pearson, 2017.

11. *Security, privacy and trust in Internet of Things: The road ahead*. Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini. 2015, Computer Networks, Vol. 76.

12. Cavoukian, . *Privacy by Design - The 7 Foundational Principles*.

13. Agencia Española Protección de Datos. Guía de Privacidad desde el Diseño. [Online]

Octubre 2019. https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf.

14. *Advanced encryption standard*. Rijmen, V., Daemen, J. 2001, Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology.

15. *ISO/IEC 29192-1:2012 INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - LIGHTWEIGHT CRYPTOGRAPHY - PART 1: GENERAL*. 2012.

16. *Toward Standardizing Lightweight Cryptography.* McKay, K., Feldman, L., Witte, G. 2017, ITL Bulletin .

17. Mikel Cañizo, Xabier De Carlos, Felix Larrinaga. *QU4LITY - Digital Reality in Zero Defect Manufacturing. D4.9 Report on Equipment Interworking and Interoperability.* 2020.

18. *From a literature review to a conceptual framework of enablers for smart manufacturing control.* Rojas, R.A., Rauch, E. 2019, The International Journal of Advanced Manufacturing Technology , Vol. 104, pp. 517-533.

19. *Interoperability in Internet of Things: Taxonomies and Open Challenges*. Noura, M., Atiquzzaman, M., Gaedke, M. 3, 2019, Mobile Networks and Applications, Vol. 24.

20. Hans van der Veer, Anthony Wiles. *Achieving Technical Interoperability - ETSI*. European Telecommunications Standards Institute. 2008.

21. IEC. *IEC TC 65/290/DC, Device Profile Guideline, TC65: Industrial Process Measurement and Control*. 2002.

22. *A Cloud-Based Infrastructure to Support Manufacturing Resources Composition*. Giovanni Di Orio, Diogo Barata, André Rocha, José Barata. 2015. DoCEIS 2015: Technological Innovation for Cloud-Based Engineering Systems.

23. *Towards a semantic administrative shell for industry 4.0 components*. Irlán Grangel-González, Lavdim Halilaj, Gökhan Coskun, Sören Auer, Diego Collarana, Michael Hoffmeister. 2016. IEEE Tenth International Conference on Semantic Computing (ICSC). pp. 230–237.

24. *Communication Models in Internet of Things: A Survey*. Santosh Kulkarni, Sanjeev Kulkarni. 11, s.l. : IJSTE - International Journal of Science Technology & Engineering, 2017, Vol. 3.

25. *Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios*. Centenaro M., Vangelista L., Zanella A., Zorzi M. 5, 2016, IEEE Wireless Communications, Vol. 23, pp. 60-67.

26. *Internet Protocol for Smart Objects (ipso) Alliance*. Hui, . 2009.

27. Cruz, Juan Carlos. ZigBee para IoT. [Online] 2018. https://medium.com/an%C3%A1lisis-de-

la-tecnolog%C3%ADa-zigbee-para-su-uso-en-el/zigbee-para-iot-12666b636821.

28. Edgar. Wi-Fi 6 is Set to Change the Future of IoT. [Online] 2020. https://www.electronicdesign.com/technologies/iot/article/21136114/wifi-6-is-set-to-change-the-future-of-iotheres-why.

29. *A comparative study of LPWAN technologies for large-scale IoT deployment*. Mekki, et al. 2019, ICT Express.

30. EMnify. What is 5G IoT and how will it change connectivity? [Online] 2020. https://www.emnify.com/blog/what-is-5g-how-will-it-change-iot-connectivity.

31. Sáez, Ignacio Porro. IoT: protocolos de comunicación, ataques y recomendaciones. [Online] 2019. https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones.

32. *Software-defined networking for internet of things: A survey*. Bera, Samaresh, Sudip Misra, and Athanasios V. Vasilakos. 2017, IEEE Internet of Things Journal.

33. *A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV.* Alam, Iqbal, et al. 2020, ACM Computing Surveys.

34. A. Rayes, S. Salam. The Things in IoT: Sensors and Actuators. *Internet of Things From Hype to Reality*. 2019.

35. Avnet. Pressure sensors: The design engineer's guide. [Online] https://www.avnet.com/wps/portal/abacus/solutions/technologies/sensors/pressure-sensors.

36. Henessy. Sensor Technology Handbook. 10.

37. John Carey, Larson Davis. Sensor Technology Handbook. 18.

38. Kantarci. What is an IoT platform? Benefits, Features & Top Vendors. [Online] 2020. https://research.aimultiple.com/iot-platform/.

39. Gartner. Magic Quadrante for Industrial IoT Platform. [Online] Octubre 2020. https://braincube.com/resource/download-the-gartner-2020-magic-quadrant-for-industrial-iot-platforms/.

40. Hasan, . Choose the Right IoT Platform: Top 20 IoT Cloud Platforms Reviewed. [Online] https://www.ubuntupit.com/choose-the-right-iot-platform-top-20-iot-cloud-platforms-reviewed/.

41. ONTSI: Onbservatorio Nacional de las Telecomunicaciones y de la SI. *Interoperabilidad de Plataformas de Gestión de Ciudades Inteligentes*. 2016.

42. Jose Luis Izkara, Alberto Armijo, Asier Mediavilla, Urmo Lehtsalu, Iñaki Arenaza, Felix Larrinaga, Patxi Saez de Viteri, Ana Quijano, Jose Luis Hernandez, Irune Badiola, Álvaro Arroyo, Sonia Montané, Magdalena Rozanska, Patricia Pérez Tarancón. *Smartencity*

Deliverable 6.1: CIOP Functional and Non-Functional Specifications. 2016.

43. Gartner. Industrial IoT Platforms Reviews and Ratings. [Online] 2021. https://www.gartner.com/reviews/market/industrial-iot-platforms.

44. Jose Luis Izkara, Alberto Armijo, Asier Mediavilla, Iñaki Arenaza. *SmartEnCity. Deliverable 6.1: CIOP Functional and Non-Functional Specifications.* 2016.

45. Beniamino Di Martino, Kuan-Ching Li, Laurence T. Yang, Antonio Esposito. *Internet of Things: Technology, Communications and Computing.* 2018.

46. Fiware Catalogue. [Online] 2020. https://www.fiware.org/developers/catalogue/.

47. Holst. Statista. [Online] 20 Enero 2021. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

48. Turck. Growing Pains: The 2018 Internet of Things Landscape. [Online] 2018. https://mattturck.com/iot2018/.

49. Omale. Gartner Identifies Top 10 Strategic IoT Technologies and Trends. [Online] https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

50. Rose. Top 14 IoT Trends to Expect in 2020. [Online] https://towardsdatascience.com/top-14-iot-trends-to-expect-in-2020-fa81a56e8653.

51. Seriun. Big Data, The Internet of Things (IoT) and Artificial Intelligence (AI). [Online] 2017. https://www.seriun.co.uk/iot-big-data-ai.

52. Jain. Can blockchain accelerate Internet of Things (IoT) adoption? [Online] https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html#.

53. Talluri. Why edge computing is critical for the IoT. [Online] 2017. https://www.networkworld.com/article/3234708/why-edge-computing-is-critical-for-the-iot.html.

54. Keith Shaw, Josh Fruhlinger. What is a digital twin and why it's important to IoT. [Online] 2019. https://www.networkworld.com/article/3280225/what-is-digital-twin-technology-and-why-it-matters.html.

55. *IoT ethics challenges and legal issues.* Ahmed Abo Bakr, Marianne A. Azer. 2017. 12th International Conference on Computer Engineering and Systems (ICCES).

56. Amitranjan Gantait, Joy Patra, Ayan Mukherjee. Defining your IoT governance practices. [Online] 2018. https://developer.ibm.com/technologies/iot/articles/iot-governance-01.

57. Lea, . IoT Security – Physical and hardware security. [Online] 2019. https://www.embedded.com/iot-security-physical-and-hardware-security/.

58. Umanenko, . Considering the User Experience in the Internet of Things. [Online] 2018.

https://onix-systems.com/blog/user-experience-in-iot.

59. Vilmate LLC. THE INTERNET OF THINGS FUTURE IS COMING: 7 IOT TRENDS FOR 2020. [Online] Vilmate , 2018 (Actualizado 2020). https://vilmate.com/blog/the-internet-of-things-future-is-coming-5-iot-trends-for-2018/.

60. A. Rayes, S. Salam. Industry Organizations and Standards Landscape. *Internet of Things From Hype to Reality*. 2019.

61. Mordor Intelligence. [Online] 2021. https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry.

62. Geletska. Best IoT companies for all things smart. [Online] 2020. https://thinkmobiles.com/blog/best-iot-companies/.

8 ACRÓNIMOS

Término	Definición
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
ADSL	Asymmetric Digital Subscriber Line
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
APT	Advanced Persistent Threat
ASIC	Application-specific integrated circuit
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
CPS	Cyber Physical System
CRM	Customer Relationship Management
CSP	Cloud Service Provider
CSV	Comma Separated Values
DTLS	Datagram Transport Layer Security
EA	Enterprise Architecture
ERP	Enterprise Resource Planning
FPGA	Field Programmable Gate Array
GDPR	General Data Protection Regulation
HTML	HyperText Markup Language
IA	Inteligencia Artificial
IaaS	Infrastructure as a Service
IDPS	Intrusion Detection and Prevention System
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoE	Internet of Everything
IoMT	Internet of Military Things
IoP	Internet of People
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISM	Industrial, Scientific and Medical Radio Bands
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation

Término	Definición
LAN	Local Area Netwok
LoRaWAN	Long Range Wide-area network
LPWAN	Low Power Wide Area Network
LR-WPAN	Low Rate Wireless Personal Area Network
LWM2M	OMA Lightweight M2M
M2M	Machine to Machine
MIT	Massachusets Institute of Technology
MiTM	Man in the Middle
MQTT	MQ Telemetry Transport
MQTT-S	MQ Telemetry Transport for Wireless Sensor Networks
NB-IoT	Narrowband IoT
NIST	National Institute of Standards and Technology
OPC-UA	Open Platform Communications Unified Architecture
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PoE	Power over Ethernet
QoS	Quality of Service
REST	REpresentational State Transfer
RPC	Remote Procedure Call
RPL	IPv6 Routing Protocol for LLNs
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
S7	STEP 7
SaaS	Software as a Service
SDK	Software Development Kit
SDN	Software Defined Networks
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Service-Oriented Computing
TLS	Transport Layer Security
TPM	Trusted Platform Module
URI	Uniform Resource Identifier
UX	User eXperience
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WiFi	Wireless Fidelity
WSN	Wireless Sensor Network
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

< ANDALUCÍA CONECTADA >

Andalucía
se mueve con Europa

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

Junta de Andalucía