8. INTERNET DE LAS COSAS

Autores: Lic. Hernán Bramati – Ing. José Gallardo

8.1 INTRODUCCIÓN

Las recientes innovaciones de la electrónica, la informática y las tecnologías de la información y la comunicación (**TIC**) han propiciado, por una parte, un crecimiento exponencial de la capacidad de procesamiento de los sistemas de información y por otra, han permitido la miniaturización de microprocesadores, con una reducción sustancial de los costos.

Desde hace tiempo, existen soluciones de automatización y control. Ya en 1970 se comenzaron a utilizar dispositivos para el monitoreo de la distribución eléctrica de centrales, usando líneas telefónicas. A partir de ahí se implementaron distintas soluciones de telemetría, monitoreo, automatización y control, mayoritariamente en las industrias manufacturera, de producción de petróleo y automotriz con **SCADA** (Supervisory Control And Data Acquisition) (supervisión, control y adquisición de datos), que evolucionaron a finales de los ‘90 con la interacción «Máquina-a-Máquina» **M2M** (Machine-to-Machine).

En simultáneo, el proceso continuo de expansión de Internet y gestación de nuevas tecnologías, servicios y plataformas ha permitido la emergencia del fenómeno conocido como «**Internet de las Cosas**» (**Internet of Things**, habitualmente denominado por sus siglas inglesas **IoT**), que supone la evolución de Internet, desde una red de ordenadores interconectados hasta una red de objetos interconectados.

Por ello, en sociedades tecnológicamente más avanzadas, IoT es desde hace unos años una realidad puesto que hoy en día Internet intercomunica no sólo ordenadores, teléfonos inteligentes o las tabletas, sino también otros muchos tipos de «objetos»: desde relojes, lentes de realidad aumentada, electrodomésticos (heladeras, aire acondicionado), televisores, videoconsolas, automóviles, elementos de edificios (cámaras de seguridad, controles de acceso, sensores de temperatura, etc), hasta grandes infraestructuras públicas como puentes, autopistas o ciudades.

IoT se constituye así en un concepto tecnológico que impacta cultural, técnica y económicamente en nuestra sociedad con un efecto transformador. Asimismo, en el mundo actual, IoT es un pilar fundamental para la cuarta revolución industrial que generará una gran transformación llamada “Industria 4.0” como muestra la Figura 1.

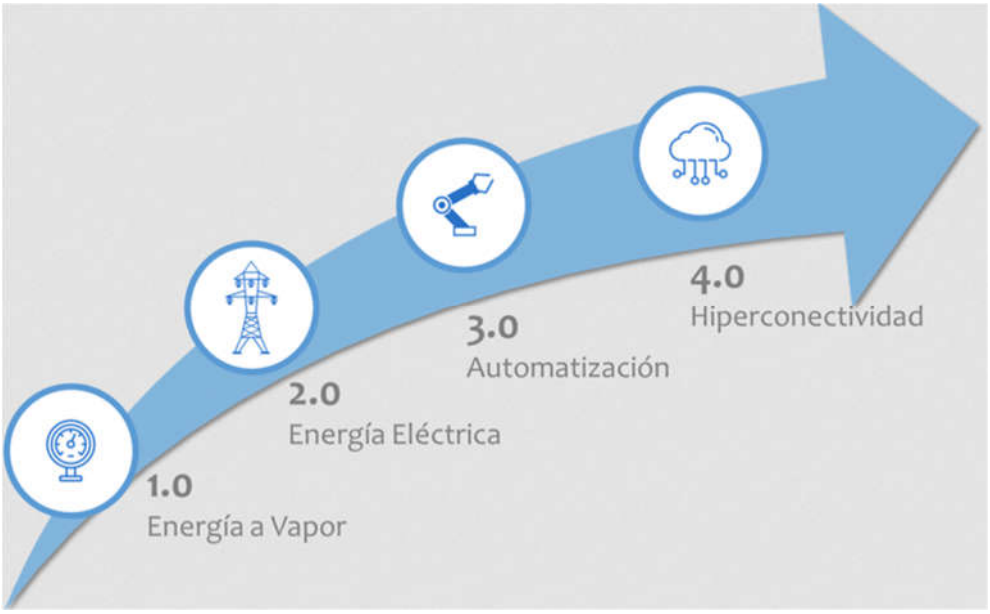

Figura 8.1 - Evolución histórica de la Industria.

8.2 CONCEPTO Y DEFINICIONES DE IoT

En Internet de las Cosas las cosas u objetos tienen conexión a Internet en cualquier momento y lugar. En un sentido técnico, consiste en la integración de sensores y dispositivos dentro de objetos cotidianos que quedan conectados a Internet a través de redes fijas e inalámbricas. Dado su tamaño, costo y consumo de energía, diminutos sensores son fácilmente integrables en hogares, entornos de trabajo y lugares públicos. De esta manera, cualquier objeto se puede conectar y manifestarse en la red. Por ello, IoT implica que todo objeto puede ser una fuente de datos. Esto está empezando a transformar la forma de hacer negocios, la organización del sector público y el día a día de millones de personas.

8.2.1 Definiciones

En este contexto podemos dar una primera definición conceptual de los que es y representa IoT: “**Internet de las Cosas** hace referencia a una tecnología basada en la conexión de objetos cotidianos a Internet que intercambian, agregan y procesan información sobre su entorno físico, para proporcionar servicios de valor añadido a los usuarios finales. También reconoce eventos o cambios, y tales sistemas pueden reaccionar de forma autónoma y adecuada”.

Sin embargo, no existe una definición formal única y universalmente aceptada para el término IoT. Diferentes grupos utilizan diferentes definiciones para describir una visión particular de lo que significa IoT y sus atributos más importantes. A continuación, se presentan dos definiciones.

La Unión Internacional de Telecomunicaciones (**UIT**) publica en 2012 la Recomendación ITU-T Y.2060 “Overview of the Internet of Things” como la “Infraestructura mundial para la sociedad de la información, que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras”. Se discute el concepto de interconectividad, pero no vincula a la IoT específicamente con Internet.

La segunda definición fue incluida en una convocatoria de trabajos para una edición de la revista del Instituto de Ingenieros Eléctricos y Electrónicos **IEEE** Communications Magazine, y vincula a la IoT con los servicios en la nube: “La Internet de las Cosas es un marco en el que todas las cosas tienen una representación y una presencia en Internet. Más específicamente, la IoT tiene como objetivo ofrecer nuevas aplicaciones y servicios que sirvan de puente entre el mundo físico y el virtual, en que las comunicaciones M2M representan la comunicación básica que permite las interacciones entre las cosas y las aplicaciones en la nube”.

8.3 ARQUITECTURA DE INTERNET DE LAS COSAS

Aunque se han propuesto diferentes arquitecturas para IoT, no existe un consenso generalizado, con modelos de arquitectura que recogen con mayor o menor detalle los diferentes aspectos de IoT. A continuación, se muestran algunas de las arquitecturas más relevantes.

8.3.1 Arquitectura de 3 niveles

Una de las arquitecturas más básicas, es la arquitectura de tres niveles: de percepción, de red y de aplicación.

- El **nivel de percepción** es el nivel físico, donde los sensores recogen información del entorno.
- El **nivel de red** es el responsable de conectar los sensores y servidores entre sí para transmitir y procesar los datos recogidos por los sensores.
- El **nivel de aplicación** es donde IoT puede ser desplegado en diferentes áreas de aplicación.

8.3.2 Arquitectura de 5 niveles

Formada por los niveles de percepción, transporte, proceso, aplicación y nivel de negocio. En este modelo de arquitectura los niveles de percepción y aplicación son

los mismos que en la arquitectura de tres niveles (Figura 2). En cuanto al resto de niveles:

- El **nivel de transporte**, transfiere los datos de los sensores mediante redes 3G, red de área local LAN, Bluetooth, RFID (Radio Frequency Identification) y NFC (Near Field Communication), desde el nivel de percepción al nivel de proceso y viceversa.
- El **nivel de proceso** almacena, analiza y procesa grandes cantidades de datos procedentes del nivel de percepción. Puede proporcionar y gestionar servicios a los niveles más bajos, utilizando tecnologías de bases de datos, cloud computing y big data.
- El **nivel de negocio** gestiona las aplicaciones, el modelo de negocio y la privacidad.

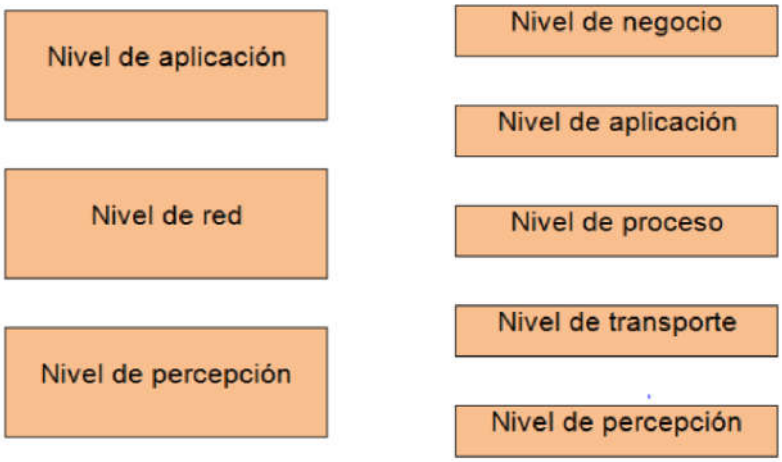

Figura 8.2 - Arquitecturas de 3 Niveles y 5 Niveles.

No obstante, vamos a reducir el modelo de IoT a las siguientes tres capas:

- El hardware de los dispositivos (sensores y actuadores).
- La infraestructura de comunicaciones.
- Las aplicaciones.

8.4 DISPOSITIVOS UTILIZADOS EN IoT.

Sensores y actuadores son piezas fundamentales para IoT al posibilitar que objetos de la vida cotidiana interactúen entre ellos y los seres humanos a través de Internet o redes dedicadas, recopilando información del entorno o interactuando con él.

Estos dispositivos son cada vez de menor tamaño, facilitando su integración en cualquier objeto. La tendencia de estos dispositivos es la miniaturización y la creación de redes inteligentes de elementos simples. La nanotecnología junto a la

miniaturización permite que el tamaño de los dispositivos sea mínimo sin disminuir su velocidad de funcionamiento y capacidad. Junto a la miniaturización, la separación del proceso en elementos hardware con capacidades limitadas, que cuando actúen en conjunto puedan conseguir grandes cosas, de manera que cada elemento se comunique con los otros elementos a su alrededor mediante lenguajes muy básicos.

IoT utiliza dispositivos electrónicos capaces de medir magnitudes físicas o químicas y transformarlas en señales eléctricas (**sensores**). Por otro lado, también utiliza dispositivos capaces de utilizar señales eléctricas para activar un determinado proceso (**actuadores**). Estos dos tipos de dispositivos combinados con la capacidad de conexión forman la capa de hardware de IoT.

8.4.1 Sensores

La información recogida por los sensores es convertida al mundo digital para poder así tratarla, almacenarla y enviarla a otros dispositivos. Los sensores pueden clasificarse de acuerdo a la magnitud vayan a leer en:

8.4.1.1 Físicos: Transforman una magnitud física en información. Entran dentro de esta clasificación los sensores de temperatura, de presión, acelerómetros, galgas extensiométricas, sensores de luz giróscopos, inclinómetros y otros. Ejemplos en Figura 3.

Figura 8.3 - Diferentes sensores.

8.4.1.2 Químicos y bioquímicos: Los sensores químicos miden concentraciones de distintos elementos o moléculas, proporcionando lecturas de la concentración de los elementos o moléculas medidas respecto del entorno. La salida que proporcionan estos sensores es una señal analógica proporcional a la medida, que debe de ser convenientemente adaptada mediante un circuito (Figura 4).

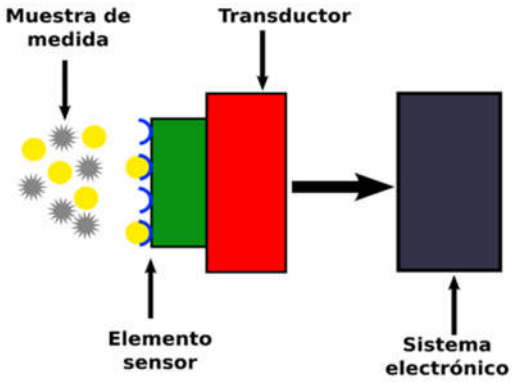

Figura 8.4 - Esquema de sensor bioquímico.

8.4.2 Actuadores

No están tan implantados como los sensores y a diferencia de éstos, los actuadores, a partir de una información digital, actúan en el mundo real.

8.4.2.1 Motores: Dentro de los actuadores, los de uso más común son los motores, existen múltiples tipos y formas diferentes de controlarlos. Habitualmente estos se controlan utilizando modulación por ancho de pulso (**PWM**, Pulse Width Modulation). Se envían pulsos de ancho variable para que el motor gire de forma proporcional a la anchura del pulso.

8.4.2.2 Servomotores: Este tipo de actuadores permite controlar la posición dentro de un rango y mantener fija esta posición. El control se realiza igualmente mediante señales PWM, siendo la duración de los pulsos la que indica la posición o el ángulo de rotación. Si no se envía señal alguna, el servo queda libre (Figura 5).

Figura 8.5 - Servomotores.

8.4.2.3 Motores paso a paso: Son motores que pueden avanzar un determinado número de grados o pasos (steps) respecto de su eje. Se necesita un

circuito y generar señales que se envían al motor, logrando pasos de pocos grados (Figura 6).

Figura 8.6 - Motor paso a paso.

8.4.2.4 Electroválvulas: Válvulas controladas electrónicamente que permiten o impiden el paso de líquidos o gases. Disponen de dos posiciones, abierto o cerrado, por lo que el control es sumamente sencillo (Figura 7).

Figura 8.7 - Electroválvulas de vacío de 2 vías.

8.4.3 Teléfonos móviles (Smartphones)

Los teléfonos móviles en sí mismos pueden ser sensores y actuadores. Además de permitir recibir llamadas y realizarlas, entre otras muchas más funcionalidades, disponen de múltiples sensores y actuadores:

- Acelerómetro: permite medir movimientos y conocer la posición del móvil.
- Magnetómetro: mide el campo magnético de la tierra.
- Giróscopo: mide los movimientos, el ángulo y la velocidad de giro en las tres coordenadas espaciales.
- Sensores de iluminación: registra la cantidad de luz ambiental.

- Sensores de temperatura: temperatura ambiental limitada a un rango de valores habituales (-20º a 50º).
- Sensores acústicos: Están equipados con micrófonos que permiten registrar el sonido.
- Barómetro: mide la presión atmosférica.
- Sensor táctil: recibe entradas múltiples simultáneamente.
- GPS: Proporciona la posición en coordenadas espaciales.

8.4 MODELOS DE COMUNICACIÓN

Desde el punto de vista operativo, es útil pensar en cómo se conectan y comunican los dispositivos de IoT, en términos de sus modelos de comunicación. El Comité de Arquitectura de Internet (IAB) dio a conocer en marzo de 2015 un documento para guiar la creación de redes de objetos inteligentes (RFC 7452), que describe cuatro modelos de comunicación comunes que utilizan los dispositivos de la IoT, que se presentan a continuación.

8.4.1 Dispositivo a dispositivo

El modelo de comunicación dispositivo a dispositivo representa dos o más dispositivos que se conectan y se comunican directamente entre sí y no a través de un servidor de aplicaciones intermediario. Estos dispositivos se comunican sobre muchos tipos de redes, entre ellas las redes IP o la Internet. Sin embargo, para establecer comunicaciones directas de dispositivo a dispositivo, muchas veces se utilizan protocolos como Bluetooth, Z-Wave o ZigBee, como se muestra en la Figura 8.8

Figura 8.8 - Comunicación Dispositivo a Dispositivo

Por lo general, este modelo de comunicación se utiliza en aplicaciones como sistemas de automatización del hogar, que habitualmente utilizan pequeños paquetes de datos para la comunicación entre dispositivos, con requisitos relativamente bajos en términos de la tasa de transmisión. Los dispositivos para la IoT residenciales

(lámparas de luz, interruptores, termostatos y cerraduras) normalmente envían pequeñas cantidades de información, por ejemplo, un mensaje del estado de bloqueo de una puerta o un comando para encender una luz, dentro de un escenario de automatización del hogar.

8.4.2 Dispositivos a nube

En un modelo de comunicación de dispositivo a la nube, el dispositivo de la IoT se conecta directamente a un servicio en la nube, como por ejemplo un proveedor de servicios de aplicaciones, para intercambiar datos y controlar el tráfico de mensajes. Este enfoque suele aprovechar los mecanismos de comunicación existentes (por ejemplo, las conexiones Wi-Fi o Ethernet cableadas tradicionales) para establecer una conexión entre el dispositivo y la red IP, que luego se conecta con el servicio en la nube. (Figura 8.9).

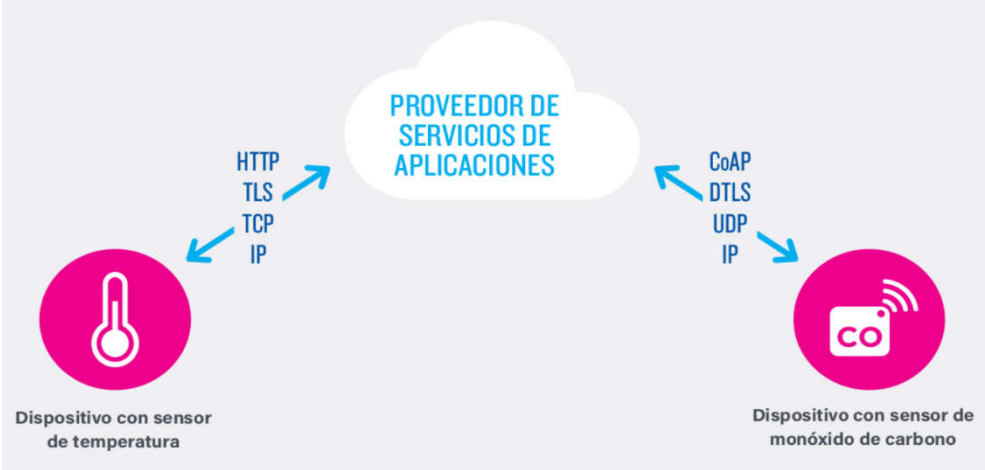

Figura 8.9 - Comunicación dispositivo a nube

8.4.3 Dispositivo a puerta de enlace

En este modelo el dispositivo de IoT se conecta a través de un servicio de puerta de enlace a nivel de aplicación ALG (Application Layer Gateway), como una forma de llegar a un servicio en la nube. Dicho de otra manera, esto significa que hay un software de aplicación corriendo en un dispositivo de puerta de enlace local, que actúa como intermediario entre el dispositivo y el servicio en la nube y provee seguridad y otras funcionalidades, tales como traducción de protocolos o datos. Este modelo se ilustra en la Figura 8.10.

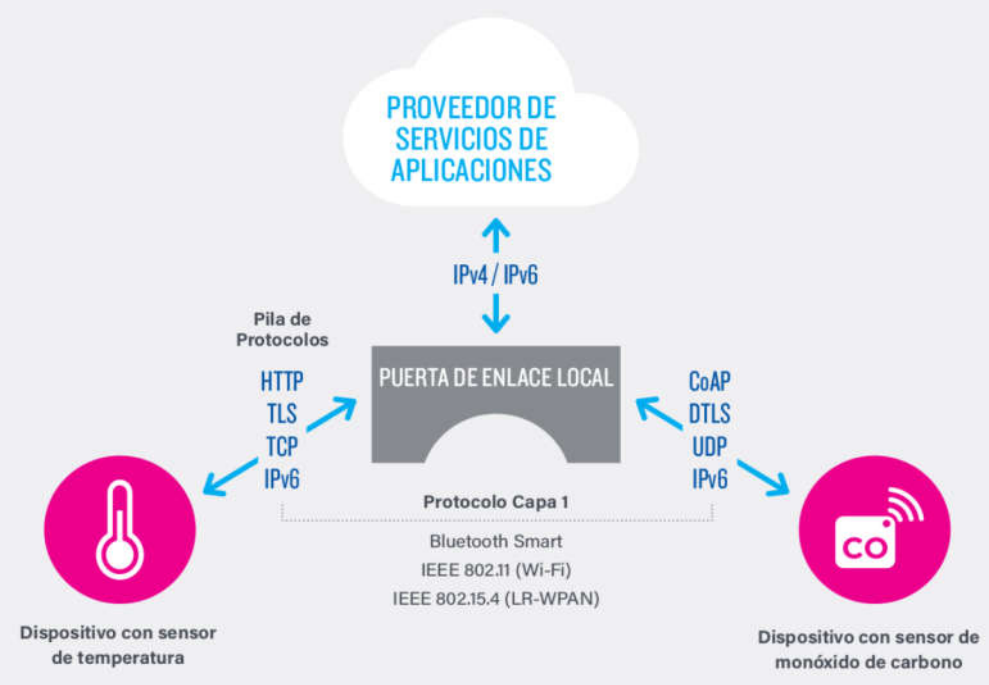

Figura 8.10 - Comunicación dispositivo a Puerta de Enlace.

En dispositivos de consumo se utilizan diferentes formas de este modelo. En muchos casos, el dispositivo de puerta de enlace local es un teléfono inteligente, con una aplicación para comunicarse con un dispositivo y transmitir datos a un servicio en la nube. Esto suele ser el modelo empleado en los artículos de consumo populares como los dispositivos utilizados para llevar registro de la actividad física, que no poseen capacidad nativa para conectarse directamente a un servicio en la nube, por lo que muchas veces utilizan una aplicación para teléfono inteligente como puerta de enlace intermedia.

Otra forma de este modelo es la aparición de dispositivos “hub” en las aplicaciones de automatización del hogar. Se trata de dispositivos que sirven de puerta de enlace local entre los dispositivos individuales de IoT y un servicio en la nube, pero que también pueden reducir los problemas de interoperabilidad entre los propios dispositivos.

8.4.4 Intercambio de datos a través del back-end

Este modelo se refiere a una arquitectura de comunicación que permite que los usuarios exporten y analicen datos de un servicio en la nube, en combinación con datos de otras fuentes. Esta arquitectura permite el acceso a terceros a los datos. Una arquitectura de intercambio de datos a través del back-end permite agregar y analizar los datos obtenidos de un solo dispositivo de IoT.

Para lograr la interoperabilidad de los datos de dispositivos inteligentes alojados en la nube, se requieren interfaces de programación de aplicaciones (**APIs**) en la nube. La Figura 8.11 muestra una representación de este diseño.

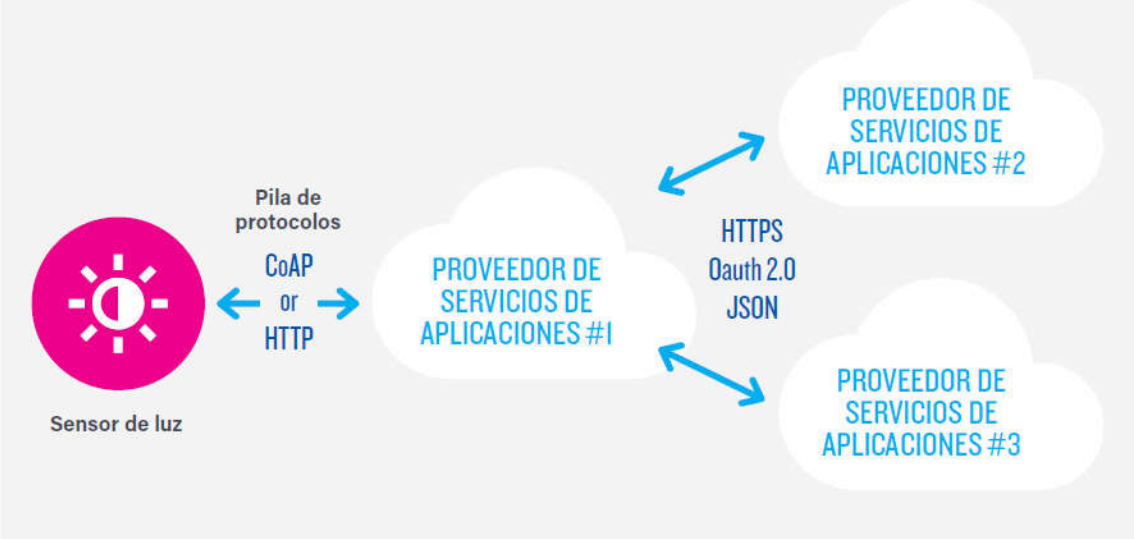

Figura 8.11 - Back-End ó sistema de soporte.

8.5 PROTOCOLOS DE COMUNICACIONES

Como IoT está creciendo rápidamente, una gran variedad de dispositivos se conecta a Internet en un número que aumenta exponencialmente (Figura 12). Estos dispositivos están equipados con baterías, un mínimo de almacenamiento y capacidad de proceso. Debido a estas restricciones la comunicación entre estos dispositivos acarrea varios desafíos:

- Direccionamiento y numeración.
- Comunicaciones con bajo consumo de energía.
- Protocolos de enrutamiento eficientes y bajo requerimiento de memoria.
- Movilidad.

Los dispositivos IoT, generalmente se conectan a Internet a través de la pila **TCP/IP**, esta pila es muy compleja y necesita gran cantidad de memoria y energía. También pueden conectarse localmente a través de redes no IP, en la que el consumo de energía es menor y conectarse a Internet a través de una pasarela (Gateway). Algunas redes no IP, como Bluetooth, RFID y NFC son muy populares, pero con un alcance reducido, por lo que las aplicaciones están limitadas a redes de área personal **PAN** (Personal Area Network). Para aumentar el alcance, es necesario modificar la pila TCP/IP con el objetivo de reducir el consumo de energía.

Figura 8.12 - Dispositivos IoT.

8.5.1 Direcciones y numeración- ipv6

Los dispositivos de IoT requieren una dirección de comunicaciones única y enrutable (que requiere un protocolo amplio de direcciones, tales como IPv6); o requieren hacer uso de redes locales únicamente, para compartir datos con otros dispositivos y recibir instrucciones de un controlador cercano, como una computadora personal o un smartphone, en cuyo caso una dirección globalmente única no es requerida.

Permitir conexiones entre dispositivos de red entre pares **P2P** (Peer-to-Peer) puede aumentar la fiabilidad de las comunicaciones, en relación a las comunicaciones necesarias con una red global grande y compleja. Pero cuando los dispositivos deben ser globalmente accesibles a través de Internet se requiere espacio de direcciones de gran tamaño para identificar individualmente a cada uno.

De hecho, la mayoría de los observadores coinciden en que, de aquí al año 2025, se conectarán a Internet miles de millones de nuevos dispositivos, desde sensores industriales hasta electrodomésticos y vehículos.

Así, el número de direcciones no asignadas para la versión actual del protocolo de Internet (IPv4 con 32 bits) es extremadamente limitado, por lo que se propone emplear la nueva versión IPv6 que con 128 bits tiene suficientes direcciones ha sido desplegada globalmente.

8.5.2 Tecnologías lpwan

Una red de área amplia de baja potencia **LPWAN** (Low Power Wide Area Network) es un tipo de red de telecomunicaciones inalámbrica diseñada para permitir

comunicaciones de largo alcance con una tasa baja de datos y consumiendo poca energía entre dispositivos ó “cosas”, como sensores que funcionan con batería.

A continuación, se presenta en la Tabla 8.1 un cuadro de tecnologías LPWAN disponibles:

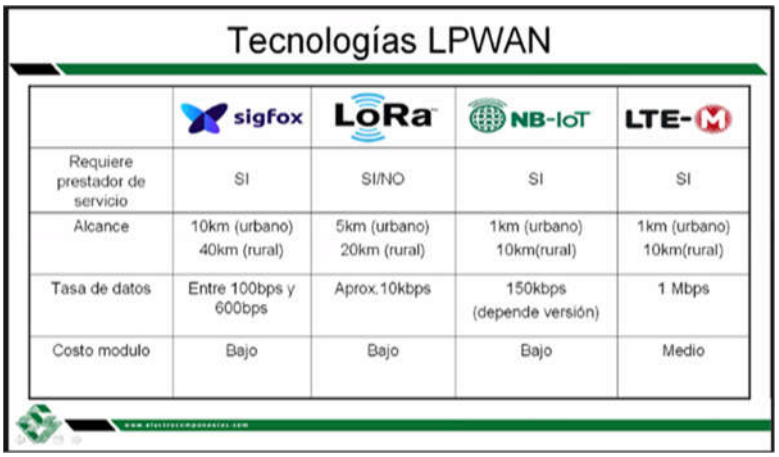

Tabla 8.1 Tecnologías LPWAN

El despliegue de redes LPWAN es realizado normalmente por dos tipos de proveedores. Por un lado, proveedores que despliegan sus propias redes inalámbricas basadas en estándares que utilizan frecuencias no licenciadas (equivalentes a la del Wifi que tenemos en nuestras casas), entre los que se destacan Sigfox y LoRa, y por el otro, las mismas empresas de telefonía móvil actualizando sus redes pueden brindar estos servicios orientados a IoT, como NB-IoT y LTE-M.

Sigfox es un operador de red global y creador de la **red 0G** que implementa redes inalámbricas para conectar dispositivos de bajo consumo como pueden ser medidores eléctricos, centrales de alarmas o relojes inteligentes, que necesitan estar continuamente encendidos y enviando pequeñas cantidades de datos. En nuestro país Sigfox, WND (su socio para América Latina), y Velocom (su operador local), anunciaron en 2017 su plan para desplegar la red de Sigfox en Argentina.

LoRa (Long Range, Largo Alcance) es una técnica de modulación inalámbrica basada en espectro expandido (spread spectrum), desarrollada por la empresa fabricante de chips de radio Semtech por lo que todos los chips LoRa son fabricados por esta compañía, y son importantes para IoT por 3 factores: largo Alcance, bajo consumo y baja tasa de bits, como lugares de poca cobertura suburbanos.

LoRa representa la capa física dentro de una red **LoRaWAN**. Por lo tanto, el término LoRaWAN hace referencia a una red de nodos LoRa que se comunican a través de puerta de enlaces (gateways) y cuyos mensajes son gestionados por un servidor de red (network server)

LoRaWAN es el protocolo de red que usa tecnología LoRa para redes de baja potencia y área amplia, empleado para comunicar y administrar dispositivos LoRa. Esta tecnología es útil para aplicaciones de monitoreo

Las tecnologías **LTE-M** (Long Term Evolution for Machine), conocida como **CAT-M1**, y **NB-IoT** (Narrow Band IoT) trabajan sobre bandas licenciadas sin riesgos de interferencias y bajo los estándares de la **3GPP** (3rd Generation Partnership Project), que aseguran compatibilidad y economía de escala.

LTE-M es una tecnología bajo el estándar LTE diseñada para soluciones que requieren bajo ancho de banda, alta vida útil de batería y movilidad.

En cambio, NB-IoT es una tecnología diseñada para soluciones estáticas, con una cantidad de transmisiones limitadas y pequeñas lo que hace que requieran un ancho de banda muy bajo soportando una latencia mayor. En este caso el foco está en que la vida útil de la batería sea muy alta.

En la Tabla 8.2 se presenta un cuadro comparativo de ambas tecnologías.

Especificaciones generales	LTE-M	NB-IoT
Vida útil de la batería	5 años	10 años
Velocidad de conexión	1Mbps	64 kbps
Movilidad	Si	No
Tipo de conectividad	Frecuente	Eventual
Frecuencias	B28 (700Mhz)	B4 (1700/2100Mhz) y B28 (700Mhz)

Tabla 8.2 Tecnologías LTE-M y NB-IoT.

La diferencia con las otras tecnologías para LPWAN, LoRa y SigFox, es que utilizan bandas de frecuencia no-licenciadas. Para acceder a un servicio LoRa se requiere de una infraestructura propia, aunque en algunos países se brinda como un servicio por medio de un operador. En el caso de SigFox es necesario adquirir un servicio de un operador específico sí o sí.

Si bien hay otras características técnicas que diferencian a LTE-M/NB-IoT/SigFox/LoRa, la tendencia actual lleva a que dependiendo del escenario estas tecnologías pueden ser complementarias o alternativas entre sí.

8.6 APLICACIONES DE IoT

IoT supone un avance para disminuir el espacio existente entre el usuario y la máquina, al impulsar la comunicación entre máquinas y sistemas que cooperan entre sí, realimentando y evolucionando proactivamente los procesos y permitiendo un control sobre nuestro entorno cada vez más efectivo. Así IoT cambiará nuestro día a día, mediante dispositivos que se conectan entre sí y a la red. La información sobre

nuestro entorno estará disponible y en tiempo real, de forma que pueda enriquecer nuestra experiencia y facilitar la actividad cotidiana, mediante aplicaciones y servicios que pueden ir desde la optimización del uso energético hasta aplicaciones de seguridad, salud y ciudades inteligentes.

Sus posibilidades de aplicación son muy variadas, abarcando diversos campos de actividad. A continuación, se describen algunos de mayor protagonismo y evolución.

8.6.1 Casas Inteligentes (Smart Homes)

Uno de los campos de aplicación en el que se han desarrollado más proyectos es el de las casas inteligentes, con sensores de temperatura, actuadores para apertura y cierre de persianas, electrodomésticos inteligentes, como ejemplos de los elementos utilizados en IoT, como muestra la Figura 8.13.

Figura 8.13 - Casa Inteligente (Smart Home).

En una Smart Home los sensores son los encargados de dar información de la casa. Cada habitación necesita aportar una determinada información, tales como temperatura, presencia, estado de ventanas, persianas y puertas. En este tipo de entornos, es donde el uso de distintas tecnologías de comunicación de corto alcance (Bluetooth, Zigbee) para recolección de datos de los dispositivos y de largo alcance (LPWAN) para transportar estos datos a la nube, se hace presente y donde el desarrollo de estándares debe permitir que diferentes tecnologías puedan interactuar entre sí.

8.6.2 Ciudades Inteligentes (Smart Cities)

Ciudades inteligentes son aquellas ciudades que aplican las tecnologías de información y de comunicación (TIC) para proveerlas de infraestructuras que garanticen: desarrollo sostenible, incremento de la calidad de vida, mayor eficacia de los recursos disponibles y fomentar la participación ciudadana activa.

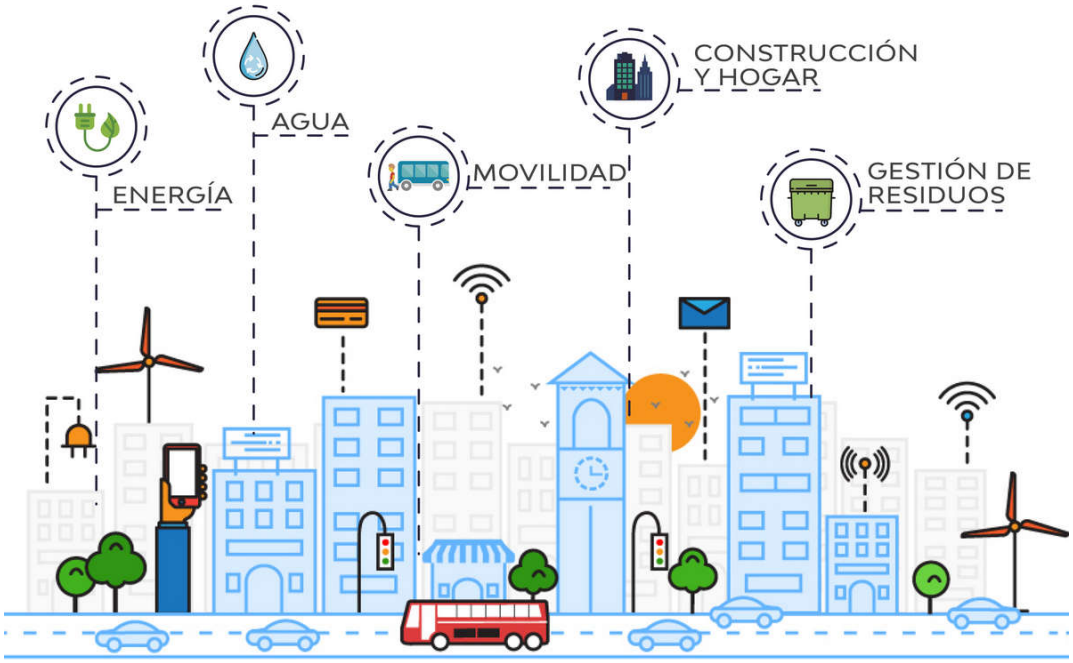

Figura 8.14 - Ciudad Inteligente (Smart City).

Smart City es otro campo en el que IoT está muy presente, a través de dispositivos que recopilan la mayor cantidad de datos para facilitar la vida al ciudadano (Figura 8.14). Las aplicaciones pueden ir desde el estacionamiento inteligente (Smart Parking), indicando donde existe estacionamiento libre, o indicar que una plaza de minusválido está siendo ocupada por un vehículo no autorizado, el tráfico inteligente (Smart Traffic) para informar en tiempo real del tráfico y proponer rutas alternativas, gestión eficiente del alumbrado, etc. Así pueden convertirse las ciudades en un ecosistema más inteligente y conectado.

8.6.3 Agricultura y ganadería

El sector agrícola se ha percatado del gran potencial que las tecnologías de vanguardia tienen para facilitar el trabajo diario, reducir pérdidas o mejorar el rendimiento y la calidad del producto. Obtener información en tiempo real de diferentes parámetros de agua, suelo o aire de cualquier campo, permite tomar decisiones estratégicas para ahorrar recursos y optimizar los rendimientos. Las

aplicaciones van desde el control automático del riego hasta medición de radiación solar (Figura 8.15).

Figura 8.15 - IoT en agricultura.

8.6.4 Tecnología Ponible ó Llevable (Wearable Technology)

Uno de los tipos de dispositivos que están tomando gran popularidad son los wearables. Se trata de dispositivos que nos monitorizan durante todo el día determinados parámetros de nuestro cuerpo y entorno más cercano, mostrando esa información en nuestro Smartphone (Figura 8.16). En la actualidad estos dispositivos pueden encontrarse en las áreas de salud, deporte, entretenimiento, industrial y militar.

Figura 8.16 - Tecnología Ponible.

8.6.5 IoT Industrial (IIoT)

IIoT consiste en el uso de tecnologías de IoT en la fabricación de productos, o en la industria en general. Incorpora, además de las propias e IoT, tecnologías de

aprendizaje automático (machine learning) y big data (Figura 8.17). Se trata de una tendencia emergente y todavía no existe ninguna plataforma que domine el sector, de momento las posibilidades de IIoT se basan en:

- Computación basada en sensores: Gestión de datos en tiempo real, para fabricantes, servicios públicos y minería. Plataformas de recolección de datos de sensores y control de procesos para la mejora del rendimiento, ahorro de energía.
- Analítica industrial: Información analítica para evitar el tiempo de inactividad del equipamiento, optimizar los beneficios y gestionar los riesgos.
- Aplicaciones inteligentes: Desarrollo ágil de aplicaciones para productos conectados.

Figura 8.17 - IoT en la Industria.

8.7 REGULACIÓN JURÍDICA. PRIVACIDAD Y PROTECCIÓN DE DATOS

La gama de temas legales, reglamentarios y de derechos relacionados con Internet de las Cosas es amplia y variada. Los dispositivos de IoT crean nuevos desafíos legales y de políticas que no existían anteriormente y que amplifican muchos de los desafíos ya existentes. Por ejemplo, algunos tipos de dispositivos de IoT pueden plantear nuevos desafíos en cuanto a la accesibilidad para personas con discapacidades, sin dejar de lado la compatibilidad con los estándares y directrices de accesibilidad existentes. Por otra parte, la enorme cantidad de dispositivos inalámbricos de IoT y el ruido de radiofrecuencia (RF) y las interferencias que producen son ejemplos de cómo los dispositivos de IoT amplifican la dificultad que existe para regular el uso del espectro de RF.

Otros desafíos emergentes para los dispositivos de IoT son las preocupaciones legales y reglamentarias con respecto a la propiedad intelectual, las cuestiones ambientales (por ejemplo, cómo desechar los dispositivos) y la propiedad legal de

dispositivos (por ejemplo, ¿los dispositivos serán propiedad del usuario o serán alquilados?).

A las complejidades de decidir las estrategias apropiadas de regulación para los problemas de la IoT se suma la complejidad de decidir qué lugar de la arquitectura de un sistema de la IoT es el mejor para conseguir los resultados deseados. ¿Dónde se deben colocar los controles regulatorios? ¿En el dispositivo, en el flujo de datos, en la puerta de enlace, en el usuario o en la nube en que se almacenan los datos? Las respuestas a estas y otras preguntas dependen de la perspectiva desde la cual se analice la situación. Cada vez más, los análisis regulatorios de los dispositivos de la IoT se realizan desde una perspectiva legal general y tecnológicamente neutra, como por ejemplo las leyes y reglamentos de protección al consumidor. Entre otras cosas, evaluar las implicancias legales de los dispositivos de la IoT desde la perspectiva de la prevención de prácticas desleales o engañosas contra los consumidores puede ayudar a informar las decisiones sobre privacidad y seguridad.

IoT genera desafíos únicos para la **privacidad** que van más allá de los problemas que existen en la actualidad. Es necesario desarrollar estrategias para respetar las opciones de privacidad individuales considerando un amplio espectro de expectativas, sin dejar de fomentar la innovación en nuevas tecnologías para la IoT.

En la Internet tradicional, la **interoperabilidad** es el valor central más básico; el primer requisito de la conectividad a Internet es que los sistemas “conectados” deben poder “hablar el mismo idioma” en cuanto a protocolos y codificaciones.

Una interoperabilidad eficaz y estándares de la IoT bien definidos para los dispositivos puede fomentar la innovación y ofrecer eficiencias a quienes fabrican dispositivos, aumentando así el valor económico total del mercado, la competencia y la elección de los servicios por parte del usuario.

8.7.1 Seguridad en IoT

Las soluciones IoT, en su gran mayoría están formadas por componentes, que deben incorporar medidas de seguridad para permitir la protección contra diferentes vulnerabilidades. Estos componentes se ejecutan en tres niveles distintos:

- Nivel de Dispositivos/Gateways: En este nivel se protege contra elementos maliciosos que pretenden adquirir los datos enviados por los dispositivos.
- Nivel de Red/Transporte: La protección contra dispositivos que envían datos falsos con el objetivo de interferir los datos persistentes de la aplicación.
- Nivel de aplicaciones: En este nivel la protección se centra en evitar el uso inválido de los datos o la manipulación de los procesos que los analizan dentro de la aplicación.
- Es precisamente en este nivel donde los dispositivos IoT exponen a los posibles atacantes la mayor superficie de ataque. El nivel de aplicación incluye todos

los dispositivos que tengan conectividad con los dispositivos IoT incluyendo además aplicaciones, tanto locales como basadas en la nube y móviles.

En el desarrollo de aplicaciones para IoT, una parte intrínseca del ciclo de vida de desarrollo es la seguridad, en las etapas de diseño, desarrollo y pruebas. En la etapa de diseño de la aplicación, se debe de realizar una evaluación formal de los requerimientos de seguridad y privacidad.

La Tabla 8.3 describe brevemente cada nivel y las consideraciones de seguridad en las que se deben enfocar los desarrolladores.

Estas consideraciones de seguridad son fundamentales para el diseño y desarrollo de aplicaciones para IoT, donde todo lo que se fabrica puede considerarse un candidato para la conectividad, añadiendo características que proporcionan a los usuarios acceso directo o remoto a información proporcionada por diferentes dispositivos.

Las aplicaciones IoT, se alejan del paradigma tradicional de desarrollo, por lo que presenta una dificultad adquirir la experiencia necesaria para llevar a cabo todas las etapas necesarias para desarrollar un producto IoT. Es de vital importancia comprender completamente los diferentes requisitos hardware, software y de certificación necesarios para el diseño de la aplicación.

Nivel	**Descripción**	**Consideraciones**
Aplicación	Despliegue de aplicaciones IoT	• Seguridad de la aplicación • Llamada API segura. • Seguridad de Node-RED • Descifrado de mensajes • Mensaje verificación de checksum
Red/Transporte	Plataforma de mensajería IoT	• Autenticación de dispositivos • Autorización • Seguridad de la API • Configuración de seguridad • Transporte seguro
Dispositivos/ Gateways	Los dispositivos (directamente o a través de gateways) publican los datos del sensor y reciben las instrucciones para ejecutar las funciones de control.	• Autenticación • Cifrado del mensaje de carga • Suministro y verificación de certificados • Transporte seguro • Arranque seguro • Firewalls • Actualizaciones firmware y parches

Tabla 8.3 - Consideraciones de Seguridad por Niveles.

Estas consideraciones de seguridad son fundamentales para el diseño y desarrollo de aplicaciones para IoT, donde todo lo que se fabrica puede considerarse un candidato para la conectividad, añadiendo características que proporcionan a los usuarios acceso directo o remoto a información proporcionada por diferentes dispositivos.

Las aplicaciones IoT, se alejan del paradigma tradicional de desarrollo, por lo que presenta una dificultad adquirir la experiencia necesaria para llevar a cabo todas las etapas necesarias para desarrollar un producto IoT. Es de vital importancia comprender completamente los diferentes requisitos hardware, software y de certificación necesarios para el diseño de la aplicación.

8.8 CONCLUSIONES

IoT (Internet de las Cosas) se introduce rápidamente en nuestra vida cotidiana proporcionando calidad de vida mediante la conexión de dispositivos, tecnologías y aplicaciones. La automatización y conexión de todo lo que nos rodea requiere de una serie de tecnologías, protocolos y aplicaciones que son la base de sustento de IoT.

La arquitectura, los diferentes componentes y protocolos que constituyen IoT, necesitan de una visión global, que permitan por un lado comprender los diferentes aspectos de este nuevo paradigma y a su vez permitir abordar algunos de los desafíos y problemas relacionados con las tecnologías, su diseño y el despliegue de IoT.

Uno de los aspectos a tener en cuenta es el desarrollo de nuevas tecnologías de comunicación que permitan la comunicación de decenas de miles de dispositivos con limitaciones de consumo de energía a grandes distancias, lo que abre nuevos mercados e impulsa el desarrollo de otras tecnologías, por parte de otros actores ya consolidados, para obtener cuota de mercado y aprovechar la infraestructura existente.

En las capas más bajas de la arquitectura, las tecnologías se encuentran en un estado de desarrollo muy avanzado, con sensores, actuadores y controladores, no obstante, hay mucho más por desarrollar en el resto de las capas, desarrollo que impactará en la vida humana de formas insospechadas en las próximas décadas.

Por último, IoT está creando una demanda de una amplia gama de puestos de trabajo en el área de TICs y oportunidades interesantes en otros campos emergentes.