**LPWA COLOMBIA**

# IoT: Tecnologías, aplicaciones, regulaciones y desarrollo futuro en las redes LPWA en Colombia

**Miller Fabian Ortiz Jerez**

**Monografía presentada como requisito para optar al título de:**

**Especialista en Telecomunicaciones**

**Director:**

**PhD. Julián Gustavo Rodríguez Ferreira**

**Codirector**

**Efrén Darío Acevedo Cárdenas**

**Universidad Industrial De Santander**

**Facultad De Ingenierías Físico-Mecánicas**

**Escuela De Ingeniería Eléctrica, Electrónica Y De Telecomunicaciones**

**Especialización En Telecomunicaciones**

**Bucaramanga**

**2020**

## Tabla de Contenido

**Pág.**

# Lista de figuras

**Pág.**

# Lista de tablas

**Pág.**

## Lista de Apéndices

**(Ver apéndices adjuntos en el CD y pueden visualizarlos en la Base de Datos de la Biblioteca UIS)**

## Lista de abreviaturas

**2G** *Second Generation*

**3G** *Third Generation*

**3GPP** *3rd Generation Partnership Project*

**4G** *Quarter Generation*

**AES** *Advanced Encryption Standard*

**AFE/RFE** *analog forward extreme/radio frecuency extreme*

**API RESTful** *Application Programming Interface Representational State Transfer*

**BPSK** *Binary Phase Shift Keying*

**CEA IoT** *Centro de Excelencia de Internet de las Cosas*

**CEMOS** *Control, Electrónica, Modelado y Simulación*

**CEO** *Chief Executive Officer*

**CFR** *Code of Federal Regulations*

**COPPA** *Children's Online Privacy Protection Act*

**CSS** *Chirp Spread Spectrum*

**DBPSK** *Differential Binary Phase Shift Keying*

**DL** *Download*

**DPSK** *Differential Phase Shift Keying*

**DRX** *Discontinuous Reception*

**EC-GSM** *Extended Coverage-Global System for Mobile communications*

**eDRX** *extended Discontinuous Reception*

**eGPRS** *extended General Packet Radio Service*

**ETSI** *European Telecommunicatios Standards Institute*

**FCC** *Federal Communications Commision*

**FDD** *Frequency División Duplexing*

**FEC** *Forward Error Correction*

**FHSS** *Frequency Hopping Spread Spectrum*

**FPGA** *Field-programmable Gate Array*

**FSK** *Frequency Shift Keying*

**FTC** *Federal Trade Commission*

**GFSK** *Gaussian Frequency Shift Keying*

**GLBA** *Gramm-Leach-Bliley Act*

**GPRS** *General Packet Radio Service*

**GSM** *Global System for Mobile communications*

**HD** *Hybrid Duplexing*

**HHS** *Health and Human Services*

**HSM** *Hardware Security Module*

**IoT** *Internet of Things*

**IPSEC** *Internet Protocol security*

**ISM** *Industrial Scientist Medical*

**LPWA** *Low Power Wide Area*

**LPWAN** *Low Power Wide Area Network*

**LTE** *Long Term Evolution*

**LPWA COLOMBIA**

| | |
|---|---|
| **LTE-M** | *Long Term Evolution cat M* |
| **M2M** | *Machine to Machine* |
| **MAC** | *Media Access Control* |
| **MTU** | *Maximum Transmission Unit* |
| **OEM** | *Original Equipment Manufacturer* |
| **OFDM** | *Orthogonal Frequency Division Multiplexing* |
| **OFDMA** | *Orthogonal Frequency Division Multiple Access* |
| **PKI** | *Public key inalambric* |
| **PSK** | *Phase Shift Keying* |
| **RF** | *Radio Frequency* |
| **RFID** | *Radio Frequency IDentification* |
| **RPMA** | *Random Phase Multiple Access* |
| **SC-FDMA** | *Single Carrier Frequency Division Multiple Access* |
| **SNO** | *Sigfox Network Operator* |
| **SSL** | *Secure Socket Layer* |
| **STM32** | *Semicondcutors Thomson 32 bits* |
| **TLS** | *Transport Layer Security* |
| **UL** | *Upload* |
| **UIT** | *Unión Internacional de Telecomunicaciones* |
| **UNB** | *Ultra Narrow Band* |
| **WIFI** | *Wireless Fidelity* |

## Resumen

**Título:** IoT: Tecnologías, aplicaciones, regulaciones y desarrollo futuro en las redes LPWA en Colombia*

**Autor:** Miller Fabian Ortiz Jerez**

**Palabras Clave:** LPWA, IoT, conectividad, eficiencia energética, escalabilidad, cobertura.

**Descripción:**

Acorde a las nuevas tecnologías, nuevos desarrollos y tendencias para aprovechar al máximo la red de la internet, las tecnologías LPWA llegan para generar una nueva visión de la interconexión con el mundo del internet de las cosas, IoT. Contando con sus principales características de tamaño, cobertura, eficiencia energética y procesamiento de datos en la nube; estas tecnologías aportan soluciones que otras no cuentan con la capacidad o tienen un costo mayor para su implementación, como lo serían el bluetooth o el WIFI. Que son tecnologías que cuentan con una menor cobertura y mayor despliegue de hardware.

En el apartado regulatorio colombiano, actualmente no se cuentan con normas que permitan el libre desarrollo y comercialización de estas tecnologías, solo se incluyen ciertas bandas de frecuencia de libre uso, solo para proyectos no comerciales, es decir esencialmente estudios académicos. Posteriormente se realiza un análisis a las diferentes regulaciones que cuenta Estados Unidos y se aconseja adquirir este modelo para el desarrollo de las normativas en Colombia. Acorde con lo anterior mencionado, se realiza un modelo metodológico que beneficie el desarrollo de aplicaciones IoT y trabajos futuros al interior de la Universidad Industrial de Santander, con miras al desarrollo a nivel regional y nacional.

---

* Monografía

** Facultad de Ingenierías Físico-Mecánica. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Codirector: Efrén Acevedo Cárdenas. Director: PhD. Julián Rodríguez Ferreira.

## Summary

**Title:** IoT: Technologies, applications, regulations and future development in LPWA networks in Colombia*

**Author:** Miller Fabian Ortiz Jerez

**Keywords:** LPWA, IoT, connectivity, energy efficiency, scalability, coverage.

**Description:**

In line with new technologies, new developments and trends to make the most of the Internet network, LPWA technologies come to generate a new vision of interconnection with the world of the Internet of Things, IoT. Having its main characteristics of size, coverage, energy efficiency and data processing in the cloud; These technologies provide solutions that others do not have the capacity or have a higher cost for their implementation, such as bluetooth or WIFI. Which are technologies that have less coverage and greater deployment of hardware.

In the Colombian regulatory section, there are currently no standards that allow the free development and commercialization of these technologies, only certain free-use frequency bands are included, only for non-commercial projects, that is, essentially academic studies. Subsequently, an analysis is made of the different regulations that the United States has and it is advisable to acquire this model for the development of regulations in Colombia. In accordance with the aforementioned, a methodological model is carried out that benefits the development of IoT applications and future work within the Industrial University of Santander, with a view to development at the regional and national level.

---

* Monograph

** Faculty of Physical-Mechanical Engineering. School of Electrical Engineering, Electronic and Telecommunication. Specialization in Telecommunication. Codirector: Efrén Acevedo Cárdenas. Director: PhD. Julián Rodríguez Ferreira.

# Introducción

La visión que sostiene IoT es usar las tecnologías LPWA para interconectar a los objetos con la internet en todo momento que sea necesario. El IoT se ha convertido en una temática emergente para los proyectos de investigación en la academia y para los sectores de la industria, esto se debe a las diferentes opciones de desarrollo que esta genera. Cualquier escenario que permita el desarrollo de aplicaciones IoT debe poseer compatibilidad con dispositivos y tecnologías desarrolladas y desplegadas, debido a que la idea principal de IoT es de conectar a millones de cosas a la internet (Augustin, 2016).

El IoT suministra una relación entre los mundos virtual y físico, por medio de procesos haciendo uso de lenguajes de programación en aplicaciones de software que permiten respuestas instantáneas con el objetivo de recopilar información que sea procesada en pro de la aplicación. Esto sobrelleva a una nueva era de definiciones en los temas de gestión de la cadena de suministros, industria, energía, transporte, logística, agricultura, hogar, comercio y educación. De esta manera, es un factor decisivo para el continuo desarrollo de aplicaciones que generan valor a la sociedad, dando oportunidad de mejoramiento de sistemas ya existentes y el nacimiento de nuevos modelos tecnológicos (Bor, Vidler y Roeding, 2016).

IoT ha modificado la interconexión entre las personas en una escala global, apresurando la evolución de la tecnología que depende de la interconexión de los objetos para crear entornos inteligentes. Solo en el 2011, 9 millones de dispositivos se encontraban interconectados a nivel

global, proyectando una expectativa de la interconexión a miles de millones de dispositivos en el 2020 (Indelmar, 2018).

Las aplicaciones LPWA se caracterizan por la conectividad de dispositivos de bajo consumo, bajos requerimientos de ancho de banda y operar a grandes distancias. Diseñados para entornos M2M (Machine To Machine), las LPWA permiten una grado más amplio de aplicaciones M2M que las redes de telefonía celular. Las tasas de transferencia de datos son muy bajas, por lo que poseen un alto grado de eficiencia energética por su bajo consumo. Las tecnologías LPWA representan la solución de la industria a la creciente necesidad del mercado de una conectividad de bajo costo y de bajo ancho de banda para sus aplicaciones, que no son apropiadas para las opciones inalámbricas de escasa cobertura como el WiFi, Bluetooth o ZigBee. Aparte de la cobertura, las aplicaciones IoT requieren un componente de expansión más simple que las tecnologías tradicionales de corto alcance, porque estas dependen de redes locales más estructuradas y complejas, lo que involucra la gestión de protocolos de seguridad, la interconexión de fabricantes y la calidad de conexión. Las tecnologías LPWA poseen el potencial para facilitar el despliegue de redes de dispositivos de bajo consumo, ideales para muchas aplicaciones de Smart City alineados con la cuarta revolución industrial (Petajajarvi, 2015).

En conclusión, alrededor de esta temática es válido plantearse las siguientes inquietudes:

- ¿Cuál es el estado actual de las aplicaciones LPWA para el internet de las cosas?,
- ¿Qué oportunidades presenta para el desarrollo en el grupo de investigación CEMOS?

El presente documento busca realizar aportes y obtener resultados a la resolución de estas problemáticas, construyendo una base para posteriores proyectos afines al interior del grupo de investigación CEMOS, que permitan desarrollar de manera analítica y conceptual esta temática en el contexto del área estratégica de las Telecomunicaciones de la Universidad Industrial de Santander.

Con la realización de esta monografía se busca realizar aportes a los posibles desarrollos e inquietudes en la realización de diferentes aplicaciones en las diferentes tecnologías LPWA para el internet de las cosas, en el grupo de investigación CEMOS. Por lo tanto, se muestra en esta monografía, la panorámica actual de las aplicaciones más utilizadas en IoT y su impacto en el día a día.

La presente monografía titulada “IoT: tecnologías, aplicaciones, regulaciones y desarrollo futuro en las redes PLWA en colombia” está dividida en 4 capítulos de la siguiente manera:

En el capítulo I se reseña un breve marco teórico y conceptual que permite contextualizar al lector sobre las diferentes tecnologías LPWA existentes en la actualidad y emergentes. Adjunto al documento en el apendice A, se muestran las principales características para tener en cuenta para su comparación.

En el capítulo II se hace una recopilación de algunos proyectos LPWA que actualmente se encuentran en funcionamiento en Colombia, su cobertura IoT y se registra el estado de las regulaciones en las tecnologías IoT en relación con los Estados Unidos.

En el capítulo III Se realiza un análisis y proyección a mejora a través de las tecnologías LPWA, a tres proyectos de grado presentados ante la Universidad Industrial de Santander que contemplan la implementación de tecnologías IoT con el fin de resolver la problemática planteada.

En el capítulo IV se desglosan los factores o aspectos para tener en cuenta al realizar un diseño metodológico que proceda a una identificación de una o varias tecnologías LPWA que mayor se ajuste a la solución del problema y se describe un modelo de Universidad Inteligente, donde se plantea una implementación de un "Campus laboratorio", a través del grupo de investigación CEMOS.

# 1. Objetivos

## 1.1 Objetivo general

Realizar una revisión bibliográfica de las aplicaciones de los sistemas LPWA y sus implicaciones normativas dentro de la regulación colombiana, para el enfoque IoT al interior de la Universidad Industrial de Santander.

## 1.2 Objetivos específicos

- Proporcionar una visión general de las aplicaciones en sistemas “Low Power Wide Area” para el internet de las cosas.
- Comparar las diferentes tecnologías de LPWA existentes y emergentes.
- Identificar las principales implicaciones normativas dentro de las recomendaciones nacionales para el uso del espectro radioeléctrico en Colombia.
- Analizar las posibles aplicaciones para el desarrollo de proyectos de implementación para el grupo de investigación CEMOS.

# 2. Tecnologías LPWA

Este capítulo contiene los fundamentos teóricos de las tecnologías LPWA (*Low Power Wide Area)* existentes y emergentes, con una comparativa entre ellas.

## 2.1 Alianza LoRa

LoRa es un sistema de telecomunicaciones inalámbricas de largo alcance, baja potencia y tasa de bits, desarrollado para una solución de infraestructura para el Internet de las cosas: los dispositivos de uso final LoRa usan un único salto inalámbrico para comunicarse con las Gateway, conectadas a Internet y que sirven como canales que retransmiten mensajes entre estos dispositivos de uso final y un servidor de red principal. LoRa cuenta con una capa física desarrollada por Semtech que usa el método de modulación spread spectrum, el cual genera un mayor enlace y una mejor resistencia a la interferencia de otras señales (Augustin, 2016). LoRa es una forma de modulación Chirp Spread Spectrum (Bor, Vidler y Roedig, 2016).

En el uso cotidiano los dispositivos de uso final LoRa, se comunica sin licencia en las bandas ISM por debajo de la frecuencia 1 GHz. En Europa, en las frecuencias de 433 MHz y 868 MHz están disponibles, con 868MHz siendo más comúnmente utilizado por su mayor cobertura y contiene sub-bandas con un ciclo de trabajo más sutil. La topología que se utiliza es la red estrella jerárquica, donde se trasmiten mensajes a un servidor principal utilizando Gateway.

La tasa de transmisión de datos puede ir de 300 bps a 50 Kbps utilizando agregación de canales. En pruebas realizadas para determinar su cobertura en (Petajajarvi, 2015) y (Aref y Sikora, 2014) indican que los dispositivos LoRa puede tener una cobertura de hasta 5 km en zonas urbanas,

con una recuperación del 85% de paquetes, hasta 30 km de cobertura en línea de vista, y una cobertura de 8 km en zonas rurales recuperando el 100% de los paquetes, configurado para adquirir mayor velocidad de datos y encriptación AES de 128 bits.

En la figura 1, se puede apreciar una red LoRaWAN basada en seguridad AES de 128 bits.

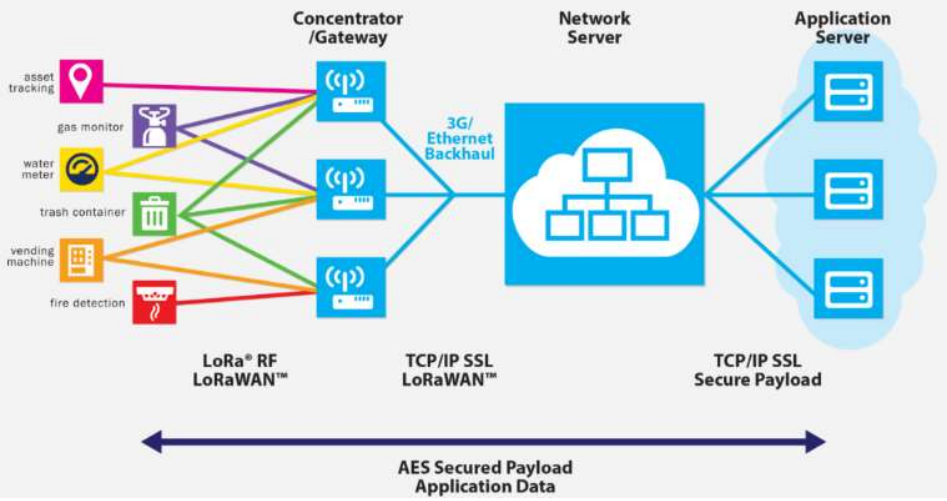


*Figura 1.* Red LoRaWAN. Nota. Tomado de Indelmar. "¿Qué es LoRa y LoRaWAN?". 330ohms. Una tecnología LPWAN para IoT". Mayo 11 de 2018. Recuperado de: https://www.indelmar.com/?p=1174.

## 2.2 SigFox

SigFox es una tecnología LPWA francesa creada en el 2009, que proporciona el servicio de red de cobertura para la red IoT, una tecnología inalámbrica y fue desarrollada para que trabaje e interactúe con dispositivos IoT que cuentan con un alto grado de eficiencia energética y con transferencias de archivos de hasta 12 bytes (330ohms, 2017).

La red SigFox funciona en base a la tecnología de transmisión UNB, que permite usar canales estrechos del espectro de frecuencias para obtener gran cobertura con un bajo consumo de potencia (330ohms, 2017). Para su Uplink, se utiliza un esquema BPSK que funciona a 100bps fijos debido a su eficiencia espectral y máximo de 300bps. Para el Downlink, se usa un esquema que opera a 500bps en un segmento de espectro de 600Hz, se admiten cargas de 12 bytes para Uplink. Se admiten 8 bytes para Downlink (Andreev, 2015).


*Figura 2.* Red SigFox. Nota. Tomado de RedGPS. "RedGPS se integra con SIGFOX". Mayo 30 de 2018. Recuperado de: https://www.redgps.com/blog-noticias/sigfox-en-redgps-106.

Sigfox divide la sub-banda que utiliza 868.180MHz a 868.220MHz en 400 sub-bandas separadas de 100Hz, cuarenta de que están reservados. Una estación base Sigfox puede cubrir un rango de 20-50 km. en zonas rurales, y 3-10km en zonas urbanas (Libelium, 2015).

**2.3 RPMA**

RPMA es una tecnología LPWA inalámbrica diseñada y desarrollada para el internet de las cosas. Esta tecnología fue desarrollada por Ingenu, anteriormente conocida como On-Ramp Wireless, los primeros desarrollos en IoT. Esta tecnología LPWAN utiliza la banda de frecuencia ISM de 2,4 GHz sin licencia y disponible en todo el mundo. Acorde con la banda de frecuencia 2,4 GHz, se implementa en cualquier parte del mundo. La tecnología ofrece características como otras tecnologías como el bajo consumo de la energía, canal de transmisión independiente para actualizaciones rápidas de firmware, rangos mejorados dentro de edificaciones urbanas y rurales, y proceso de encriptación AES de 128 bits para una gran parte de aplicaciones IoT (EverythingRF, 2018).

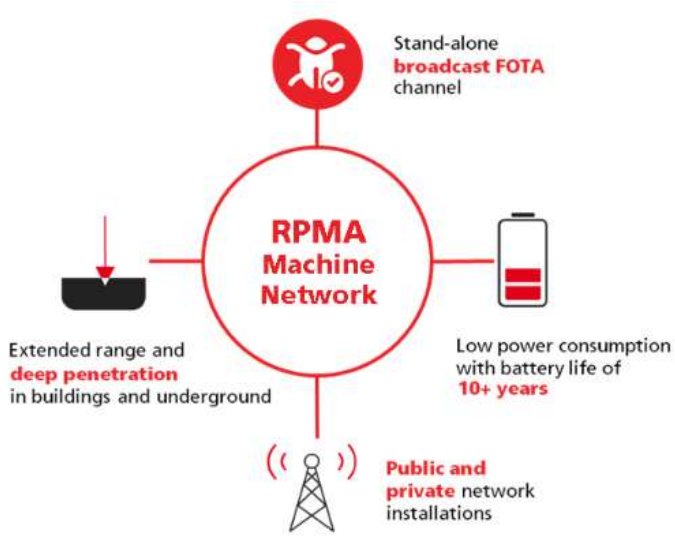


*Figura 3.* RPMA. Nota. Tomado de "¿Qué es la tecnología RPMA?" Equipo editorial - todo RF. 8 de febrero de 2018. Recuperado de: https://www.everythingrf.com/community/what-is-rpma-technology.

Los dispositivos con tecnología RPMA cuentan con velocidades de downlink de 31 kbps y velocidad de uplink de 15.6 kbps. Es similar a NB-IoT, pero con una pérdida de acoplamiento máxima de 167 dB, la distribución de señales llega a las diferentes edificaciones. Esta tecnología

cuenta con las características de bajo consumo energético que permite la duración de sus baterías hasta por 10 años con una sola carga (EverythingRF, 2018). Esto lo hace propicio para aquellos dispositivos que deben situarse en ubicaciones rurales, remotas o espacios de difícil acceso donde no cuentan con una conexión a la red eléctrica, como se muestra en la figura 3.

## 2.4 LTE-M

LTE-M es una de las nuevas tecnologías LPWA que fue desarrollada para aplicaciones del internet de las cosas (IoT). Se define como un protocolo para comunicaciones vía celular de ancho de banda estrecho, que interconecta la red de la internet con dispositivos que transmiten bajas cantidades de datos en extensos periodos de tiempo, con un consumo más eficiente de energía. LTE-M propone de un mayor ancho de banda, el cual permite una comunicación con una velocidad mayor de transferencia de datos, un menor retardo y un posicionamiento del dispositivo mucho más preciso (Orange, 2017).

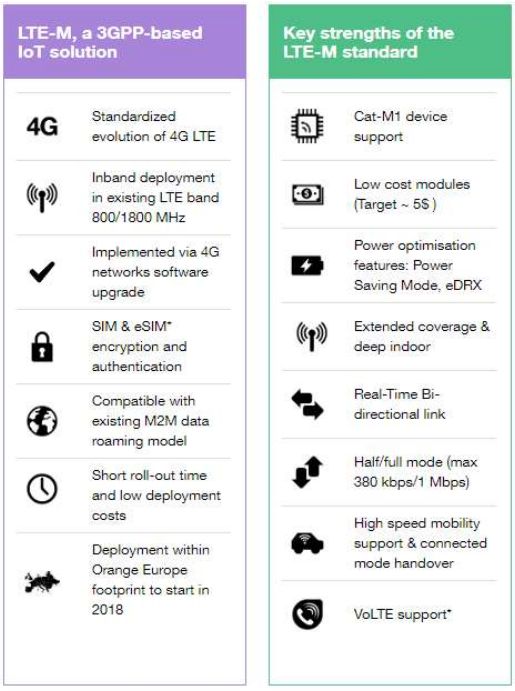


*Figura 4.* Características LTE-M. Nota. Tomado de "LTE-M, la evolución de las máquinas". Recuperado de: https://accent-systems.com/es/ltem/.

LTE-M permite los envíos por voz y movilidad, una gran cobertura y es clave para las comunicaciones M2M y aplicaciones que utilicen dispositivos IoT. Es el elemento fundamental para optimizar el uso eficiente de los recursos (Orange, 2017) y otras características de la tecnología como se aprecia en la figura 4.

## 2.5 NB IoT

Narrowband-IoT (NB-IoT) es una de las tecnologías que se centran en interconectar la internet con los objetos cotidianos que requieren pequeñas cantidades de datos en períodos de tiempo largos (Accent, 2019).

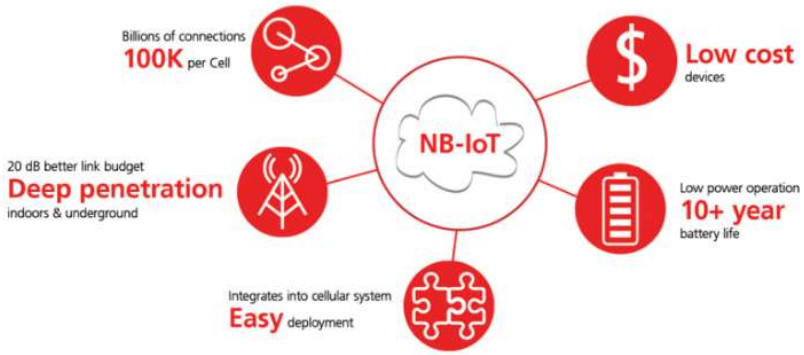


*Figura 5.* NB IoT. Nota. Tomado de "What is NBIoT?". DeCode Staff. Agosto 21 de 2019. Recuperado de: https://medium.com/decodein/what-is-nbiot-7d4cebd753cf.

NB IoT ha sido desarrollada para permitir comunicaciones eficientes y con una gran duración de carga de la batería, para dispositivos distribuidos masivamente. Utiliza la ya existente red móvil celular para interconectar todos los objetos. Está diseñado para mejorar el futuro en pro de la conectividad IoT de una manera más segura y confiable. Es propicio para los dispositivos que constantemente están trasmitiendo información en su entorno y según pruebas realizadas con una vida útil de dispositivo de diez años, con una capacidad de la batería de 5Wh (Accent, 2019).

El enlace descendente de NB-IoT se basa en OFDMA, con 15 kHz espaciado entre subportadoras y reutiliza la misma numerología OFDM como LTE (Wang, 2017). Tanto el tono único como el multitono son compatibles en el enlace ascendente Multitono se basa en SC-FDMA con 15 kHz espaciado de subportadora Con un solo tono, el espaciado de subportadora puede ser 15kHz o 3.75kHz (Lin, Adhikary y Wang, 2016).

En términos de eficiencia energética, NB-IoT, como LTE, usa productos discontinuos recepción (DRX), que evita monitorear el canal de control continuamente para conservar energía,

tiene ciclos DRX hasta 2.56s (Ratasuk, 2016). La versión 13 introdujo DRX extendido (eDRX) ciclos para los modos inactivo y conectado, que extienden ciclos a 43,69 minutos y 10,24 segundos respectivamente (Rico, 2016), Incrementando aún más la energía conservada.

## 2.6 EC-GMS-IoT

La EC-GSM-IoT es una tecnología 2G basada en la existente eGPRS, y diseñada como un sistema que funciona bajo la comunicación móvil celular, con una alta capacidad con bajo consumo de energía y muy buena cobertura. Su objetivo es desarrollar aportes al IoT, y puede implantarse en las redes GSM que actualmente están en funcionamiento solo con una actualización de software. Cuenta con una velocidad de transmisión de 70 Kbps, que son aprobados por el ente regulador de comunicaciones móviles, 3GPP. La EC-GSM-IoT ha sido diseñada para ofrecer cobertura a dispositivos M2M en zonas de difícil acceso y comunicación (Teldat, 2017).

| | EC-GSM-IoT |
|---|---|
| Deployment | In-band GSM |
| Coverage* | 164 dB, with 33dBm power class<br>154 dB, with 23dBm power class |
| Downlink | TDMA/FDMA, GMSK and 8PSK (optional), 1 Rx |
| Uplink | TDMA/FDMA, GMSK and 8PSK (optional) |
| Bandwidth | 200kHz per channel. Typical system bandwidth of 2.4MHz [smaller bandwidth down to 600 kHz being studied within Rel-13] |
| Peak rate (DL/UL) | For DL and UL (using 4 timeslots): ~70 kbps (GMSK), ~240kbps (8PSK) |
| Duplexing | HD, FDD |
| Power saving | PSM, ext. I-DRX |
| Power class | 33 dBm, 23 dBm |

*Figura 6.* Resumen de características EC-GMS-IoT. Nota. Tomado de “Rise of the machines, and the options for connecting them”. L. Brian. Agosto 16 de 2018. Recuperado de:

https://www.ciena.com/insights/articles/Rise-of-the-connected-machines-and-the-options-for-connecting-them.html.

Se definen clases de cobertura, con diferentes números de transmisiones totales para diferentes canales lógicos. La cobertura prevista de 164 dB para la potencia de 33 dBm y 154 dB para la clase de potencia de 23 dBm (Nokia, 2015). Su desempeño en el ahorro de la energía se define en la Versión 12 y eDRX que también son compatibles con dispositivos EC-GSM, aumentando aún más la eficiencia energética. EC-GSM posee un modo inactivo, el cual permite un mayor ahorro de energía en donde no se trasmiten comunicaciones celulares. La duración de la batería de los nodos EC-GSM es de aproximadamente 10 años con una batería de 5 W/h (3GPP, 2015).

## 2.7 Weightless

Weightless es una tecnología LPWA de comunicación inalámbrica de última generación orientada a M2M y cuenta con tres pilares fundamentales, su bajo costo, eficiencia energética y buena cobertura en su propagación de onda. Actualmente su desarrollador tiene 3 bases de esta tecnología, que son Weightless-N, cuya prioridad es el bajo coste, Weightless-W, con cobertura de su espectro utilizado anteriormente por frecuencias de espacio en blanco de TV y Weightless-P, que se enfoca en un alto rendimiento. Esta sección se centrará en Weightless-P, ya que es el estándar más recientemente definido y es más similar al de otras tecnologías LPWA cubiertas en este documento (Bliznakoff, 2014).

Weightless-P es una tecnología de banda estrecha en el rango de frecuencias de 1GHz en las bandas ISM. Este divide el espectro en la frecuencia de los 12.5kHz, que posee una asignación

flexible de canales, cuenta con velocidades de transferencia de datos adaptativas de 200bps a 100kbps y estaciones base sincronizadas en el tiempo que permite el uso eficiente del espectro, cuenta también con el uso racional de energía transmitida y programación previa de recursos para la optimización de recursos, los cuales generan una duración de la batería mayor, así como recursos de red. QoS Weightless-P puede soportar una cobertura aproximada de 2-5 km en zonas urbanas entornos y todo el tráfico se encripta con AES-128/256 (Bliznakoff, 2014).

## 2.8 DASH7

Dash7 es una tecnología diseñada para aplicaciones de red de sensores inalámbricos para IoT. D7AP es un protocolo de full stack, que incluye la aplicación y capas de presentación, que funcionan sobre las bandas de frecuencia ISM de 1 GHz sin licencia [21]. Las señales trasmitidas por los dispositivos se realizan en forma de escritura o lectura en un archivo remoto, los nodos centrales se describen y se pueden configurar con diferentes propiedades percibidas de cada proceso, que se pueden usar junto con identificadores en la agrupación de solicitudes de datos remotos para diferentes aplicaciones. Se desarrolla una API para facilitar la comunicación con las redes D7AP sobre cualquier interfaz (Weyn, 2015) y (Ergeerts, 2015).

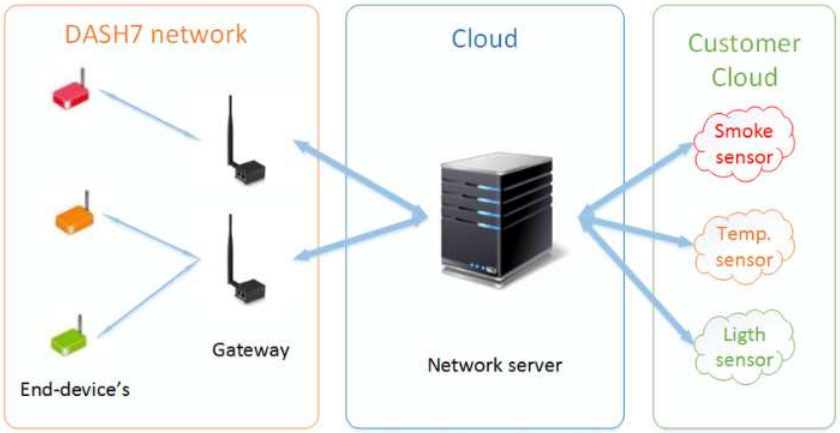


*Figura 7*. DASH7 Alliance Protocol Architecture. Nota. Tomado de Ayoub, Wael & Samhat, Abed Ellatif & Nouvel, Fabienne & Mroue, Mohamad & Prévotet, jean-christophe. (2018). Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and Supported Mobility. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2018.2877382.

Las redes D7AP utilizan comúnmente la topología tipo árbol, y sin el uso de subcontroladores, se utiliza la topología estrella. De este modo, las aplicaciones de las comunicaciones móviles son compatibles con esta tecnología, ya que los diferentes nodos se pueden comunicar con cualquier gateway que se encuentre disponible. Los dispositivos cuentan con una comunicación interna, y las gateway pueden comunicarse con los dispositivos para consultar información de interés. Los dispositivos transmiten de manera asincrónica a la puerta de enlace sin importar condición, y analiza en intervalos constantes los dispositivos para escuchar las transmisiones de enlace descendente. D7AP proporciona tres diferentes velocidades de datos definidas acorde a su tipo de 9.6 kbps, 55.555 kbps y 166.667 kbps, y la distancia entre puntos finales puede alcanzar hasta 5 kilómetros (Finnegan y Brown, 2018). Para sus sistemas de codificación Dash7 utiliza generalmente2-(G) FSK y en el cifrado de sus datos AES-128 (Finnegan y Brown, 2018).

El esquema de modulación utilizado es 2- (G) FSK, la codificación PN9 es se utiliza para el blanqueamiento de datos y está disponible la codificación 1/2 FEC. El tamaño máximo del paquete es de 256 bytes. De manera similar a 802.15.4, AES-CBC se utiliza para autenticación y AES-CCM para autenticación y encriptación.

## 2.9 Green OFDM

Esta tecnología da solución a la relación que encuentra en el pico y el promedio de la potencia de las modulaciones OFDM, que impone altas restricciones al amplificador de potencia de transmisión, lo que conlleva un enorme consumo de energía y un costo de hardware para el transceptor OFDM. Green-OFDM supera el camino para que la tecnología sea de bajo coste, alta velocidad de procesamiento y una gran cobertura para el IoT (EuroCPS, 2018).

Green OFDM cuenta con una plataforma llamada MGIoT que se enfoca en las comunicaciones en la banda de frecuencia subGhz para la nueva generación de aplicaciones para en internet de las cosas y su alta velocidad de trasmisión de datos para las redes inalámbricas de baja potencia. Este incluye una tarjeta FPGA programable que implementa un módem digital flexible greenOFDM, un microcontrolador STM32 para el software de la capa MAC y un conversor analógico / radiofrecuencia analógico. Específicamente, crear una red de objetos que conste de una cámara y un módulo greenOFDM que posee una velocidad de comunicación de 1Mb/s por aire con un servidor de aplicaciones a través de una gateway greenOFDM (EuroCPS, 2018).

## 2.10 Symphony Link

Symphony Link es una red inalámbrica de área amplia y baja potencia (LPWAN) que permite el monitoreo y la comunicación bidireccional con dispositivos sensores (Scott, 2015). Link Labs menciona que puede admitir hasta 250,000 puntos finales en cada puerta de enlace y rangos de hasta 7 millas (Rethink, 2016). Además, Symphony Link admite la actualización de firmware de forma inalámbrica y permite enviar y recibir mensajes de confirmación bidireccionales comprimidos. Symphony Link pone un enfoque más fuerte en industrial aplicaciones y proporciona una solución para eliminar los límites del ciclo de trabajo mediante el salto de frecuencia (RedGPS, 2018).

Dentro de sus características principales, se encuentran (LinkLabs, 2016):

- Recepción de mensajes garantizada
- Control de potencia y velocidad de datos en tiempo real
- Coexistencia de múltiples puertas de enlace
- Reconocimiento de mensaje bidireccional
- Evitación de interferencias
- Infraestructura de clave pública (PKI)
- Firmware por aire
- Intercambio de claves del Estándar de cifrado avanzado (AES) en tiempo real.
- Seguridad de nivel de transporte (TLS) de grado bancario para el tráfico de red.
- Velocidad de datos adaptativa en tiempo real
- Sin límite de ciclo de trabajo

- Calidad de servicio
- MTU fija de 256 bytes.

En la figura 8, se muestra la tecnología Snapshot de Symphony Link, la cual utiliza hardware de LoRa para su uso comercial.

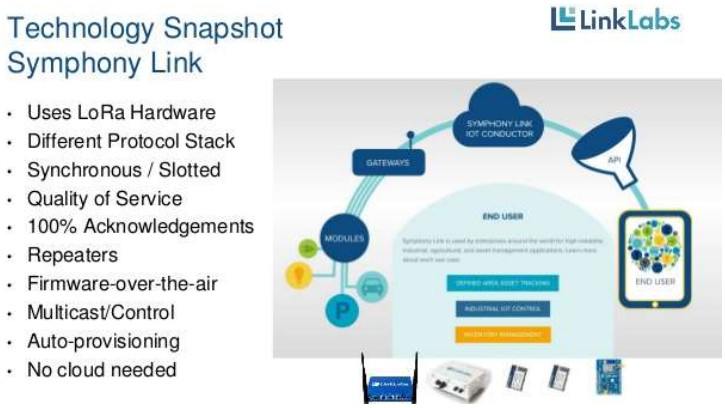


*Figura 8.* Tecnología Snapshot Symphony Link. Nota. Tomado de "Symphony Link™ A revolutionary wireless system for wide-area IoT networks". LinkLabs. 17 septiembre de 2016. Recuperado de: https://www.link-labs.com/symphony.

## 2.11 ThingPark Wireless

ThingPark Wireless es una tecnología LPWA de carácter bidireccional de largo alcance para aplicaciones IoT. La solución ThaPark IoT Enabler resuelve los conflictos relacionados con la gran variedad de protocolos industriales disponibles en dispositivos que están interconectados a la red. Los componentes incluyen Cocoon (solución de software integrada para proveedores de pasarela); ThingPark Cloud (interfaz de desarrollo de aplicaciones y almacenamiento de big data); y ThingPark Store (mercado en línea dedicado a M2M y IoT) (Actility, 2019).


*Figura 9.* ThingPark Wireless Technology. Nota. ThingPark. (2020). Wireless Technology. Tomado de "Actility: ThingPark Wireless". Recuperado de: https://lpwanmarket.com/shop/platforms/actility-thingparkwireless/.

Dentro de sus características primarias, posee una arquitectura de red horizontal central escalable que permite hasta 150Kbps y aproximadamente 10 millones de gateway por clúster, contiene servicio de roaming a nivel de usuario y dirección de capa MAC para optimizar la capacidad de la red y la vida útil de la batería. Fiabilidad de plataforma de nivel de usuario, conexión para las plataformas y aplicaciones de nube de IoT. Aplicaciones de back office para admitir y facilitar la incorporación y gestión de dispositivos y gateway. Cuenta con API RESTful. Gestión para la mejora del ciclo de vida del dispositivo (activación simplificada, actualización de firmware por aire - FUOTA) (Actility, 2019).

En la capa MAC se cuenta con seguridad de tipo criptográfica AES128, que es compatible con el protocolo desarrollado por LoRa, LoRaWAN. Incluye cifrado e integridad de datos. En la capa de transporte cuenta con las opciones de túnel IPSEC y TLS entre gateway y red central.

Protección de las claves raíz del dispositivo a través de HSM e Integración con marcos de autenticación estándar (Actility, 2019).

## 2.12 WAVIOT

WAVIoT es una tecnología LPWA que implementa su solución, NB-Fi (Narrowband Fidelity) que es un protocolo de banda estrecha que posee una comunicación en las sub-bandas de frecuencia ISM sub 1GHz. NB-Fi trabaja en la banda de frecuencia de 500 kHz en cinco mil canales, y cada una de las señales se transmite en la frecuencia de 50 Hz con un ancho de banda con un bit mínimo de tasa de 50 bod. Se usa la modulación DBPSK como esquema de procesamiento en la capa física. Las gateway WAVIoT proporcionan -154 dBm de sensibilidad para el receptor, y cobertura de aproximadamente un millón de nodos. En los dispositivos desarrollados por WAVIoT, pequeñas tramas de datos cortas usan 50mA de corriente en su proceso. Los dispositivos cuentan con una vida útil de hasta 20 años y un enlace de 176 dBm. WAVIoT posee dentro de sus opciones para su distribución, tres redes de diferentes tipos: público, privado (despliegue en toda la ciudad) y empresa (despliegue en todo el campus) (dgmatics, 2016).

NB-Fi cuenta con su operación interna con una topología en estrella y puede lograr un rango de cobertura de aproximadamente 16 km en zonas urbanas y más de 50 km en zona rural. El uplink promedio cuenta con una latencia de 30 segundos, y la latencia promedio de uplink es de 60 segundos. Los datos enviados a través de las gateway se almacenan en la nube y se puede acceder a esta información desde una plataforma IoT y se puede redirigir fácilmente y modificando los

datos mediante el uso de una API. Todos los datos están encriptados bidireccionalmente desde el dispositivo al servidor utilizando un XTEA Clave de 256 bits (Joseph, 2018).

## 2.13 NWAVE

El protocolo homónimo de Nwave es, como Sigfox, basado alrededor de comunicaciones de banda ultra estrecha en las frecuencias sub 1GHz bandas ISM sin licencia (Nwave, 2016). Los nodos de Nwave poseen una cobertura de 10 km en entornos urbanos, y 30 km en zonas rurales, y pueden operar para 20 años con una sola batería de litio AA, proporcionando una velocidad de datos de 100bps (Nwave, 2015).

## 2.14 Telensa

Telensa también proporciona una solución de banda ultra estrecha en las bandas ISM sub 1GHz sin licencia (Telensa, 2016). A diferencia de la mayoría de las tecnologías LPWA, Telensa posee un protocolo que puede proporcionar comunicación bidireccional para facilidad de comunicación entre dispositivos. Una estación base de Telensa puede conectarse a 5000 nodos, y cuenta con una cobertura 2 km en áreas urbanas y 4 km en zonas rurales. Los nodos individuales continúan funcionando según lo programado incluso si la conexión a su la estación base se pierde, tiene una vida útil estimada de 20 años (ACSWireless, 2016).

En la figura 10, se muestra la solución Wireless IoT que implementa en sus campos de acción donde se han desplegado.

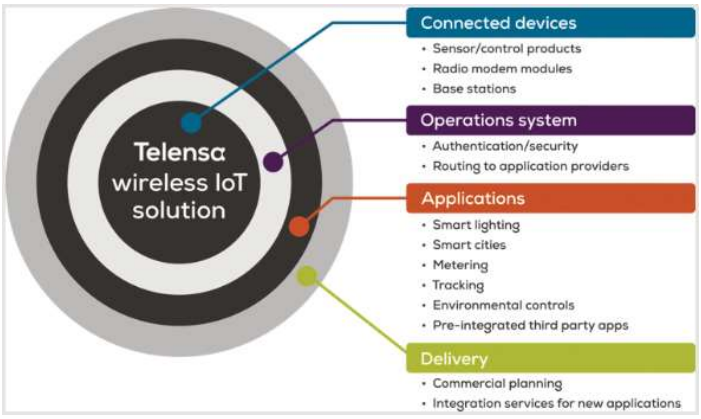


*Figura 10.* Telensa's complete IoT solution. Nota. Tomado de Telensa's complete IoT solution. Recuperado de: https://www.iot-now.com/2015/07/07/34596-building-smarter-cities-with-low-power-radio-networks/.

Telensa ya actualmente tiene en campo millones de nodos en más de 50 redes de Smart City en todo el mundo, principalmente en el Reino Unido, pero tienen participación en ciudades como Shanghai, Moscú y Sao Paulo (Joseph y Stephen, 2018).

### 2.15 Tablas comparativas de tecnologías LPWA.

Ver Apendice A.

## 3. Despliegue de redes LPWA en colombia

En este capítulo se mencionará la cobertura actual Iot en Colombia, algunos desarrollos en proyectos y pilotos a nivel nacional en tecnologías LPWA y regulaciones gubernamentales.

### 3.1 Sigfox lleva su red IoT a Colombia

Colombia se convierte en el tercer país de Latinoamérica donde se despliega la red SigFox para las comunicaciones inalámbricas del Internet de las Cosas. Los países iniciales con estos despliegue son Brasil y México. Las encargadas de proceder con estos despliegues en latinoamérica es la empresa WND y Phaxsi Solutions. El anuncio del despliegue en territorio nacional de la red SigFox, coincide con el lanzamiento de una alianza nacional de universidades, líderes tecnológicos y compañías con el nombre de Centro de Excelencia y Apropiación del Internet de las Cosas (CEA-IoT). Este proyecto inicialmente ya recibió una inversión de 1,8 millones de dólares en 2016 con el objetivo de emplear y propiciar estas tecnologías para fortalecer el desarrollo económico y social de Colombia (TyN, 2016).

El anuncio coincide con el lanzamiento de una alianza nacional de universidades, líderes tecnológicos y compañías conocida como Centro de Excelencia y Apropiación del Internet de las Cosas (CEA-IoT). Esta iniciativa ya recibió una inversión inicial de 1,8 millones de dólares en 2016 con el objetivo de emplear estas tecnologías para fortalecer el desarrollo económico de Colombia (TyN, 2016). Entre potenciales casos de uso para la plataforma se destaca el monitoreo de activos, gestión de cadena de suministros, sistemas de alarma y aplicaciones para ciudades inteligentes, entre otras (TyN, 2016).

### 3.2 Telefónica

Para incentivar el emprendimiento del sector IoT y generar nuevas oportunidades de progreso en tecnología en Colombia, como lo menciona reiteradamente el plan MinTic. El día 30 de octubre de 2019 se inaugura en Bogotá el primer laboratorio IoT para emprendedores gracias a una alianza entre las empresas Telefónica Movistar, Wayra, CEmprende, el campus para el desarrollo de emprendimiento e innovación de América Latina, iNNpulsa y el Ministerio de Comercio, Industria y Turismo que permitió la consolidación del proyecto (eltiempo, 2019).

El 29 de noviembre de 2019, junto con Accenture, se inaugura en Medellín otro laboratorio IoT para emprendedores, el cual da lugar a la incursión dentro de las cuatro tecnologías más innovadoras: internet de las cosas, big data, blockchain e inteligencia artificial. También se anuncia la llegada de un tercer laboratorio IoT con otra empresa de tecnología y que se inaugurará en marzo del 2020, el cual tiene como principales involucrados como Facebook y Google y la empresa de telecomunicaciones Claro. En la actualidad, Telefónica provee de 600.000 servicios de Internet de las cosas a unos 14.000 clientes empresariales de Colombia, y con la nueva red, denominada LPWA espera ampliar este mercado (eltiempo, 2019).

### 3.3 Claro

En el marco del Congreso de Andesco (*Asociación nacional de empresas de servicios públicos y comunicaiones*), que se desarrolló en junio de 2019 en Cartagena, Claro Colombia presentó soluciones basadas en su red NB-IoT (Narrowband Internet of Things por sus siglas en inglés, o Banda Estrecha de Internet de las Cosas, en español), la cual está enfocada para las soluciones de iluminación inteligente, acueductos, ciudades inteligentes y agricultura conectada, entre otros, que

la compañía viene desarrollando en diferentes ciudades y empresas del país. Para su implementación, la compañía invierte una cifra superior a los 5.1 millones de dólares.

NB-IoT es una evolución de las redes móviles existentes, que abre todo un mundo de oportunidades para las empresas en Colombia que quieren o están implementando soluciones basadas en IoT a sus procesos, por ejemplo, la mejora en el consumo de energía en sensores y actuadores que les permite tener mayores eficiencias y optimizaciones, sin invertir en despliegues de redes de baja potencia. Usar una red estándar a nivel mundial y que trabaje en Colombia sobre espectro licenciado les va a permitir crear un ecosistema robusto, seguro y escalable debido a que no coexiste con otras señales y tecnologías (Portafolio, 2019).

### 3.4 Grupo T&T y CODENSA

Se basa en dos proyectos: 1) EIoT para Sistemas de Energía y 2) Monitoreo Inteligente de Refrigeración Industrial. En el caso del proyecto EIoT (Electrical Internet of Things) se busca establecer una mayor eficiencia en el monitoreo de los elementos de los sistemas eléctricos de potencia ubicados en diferentes puntos y pertenecientes a todas las etapas de la cadena como lo son la generación, distribución, transmisión y consumo. Para el proyecto de Refrigeración Industrial, se procede a conectar sensores dentro de los refrigeradores industriales para monitorear y ofrecer servicios de valor agregado como tarifas especiales, recomendaciones y warnings, dependiendo del uso que se le está dando a los equipos (T&T, 2018).

Inicialmente se trabajó en dar solución al problema de la conectividad remota y a las grandes distancias que existen entre cada nodo del sistema. Po lo tanto, se plantea el uso de las LPWAN tecnologías de comunicación inalámbrica, que cuentan con su principal característica de eficiencia energética y gran cobertura en zonas remotas. Se realizaron diferentes pruebas y alternativas para los despliegues de comunicación, y las tecnologías con mejores resultados fueron LoRa y NB-IoT (T&T, 2018).

En el mediano plazo, el propósito de Codensa junto a T&T es (T&T, 2018):

- Implementación de tecnologías de comunicación para el IoT.
- Consolidar un centro de investigación e innovación para soluciones académicas e industriales con tecnologías LoRa y NB-IoT.
- Extender las soluciones IoT a múltiples entornos industriales integrando ambas tecnologías LoRa y NB-IoT.

### 3.5 Redes a nivel regional

Con el desarrollo de estas nuevas tecnologías, se han venido trabajado en diferentes pilotos de prueba para comprobar su correcto funcionamiento en diferentes ciudades del país. Estos despliegues han arrojado resultados satisfactorios, tanto en ubicación estratégica, antenas y gateways, que permiten una muy buena cobertura en zonas urbanas pobladas.

Para este documento, entraremos a revisar un piloto realizado en la ciudad de Bucaramanga como se aprecia en la figura 11. Este proyecto arrojo resultados de cobertura de aproximadamente 5 km a 10 km. Pruebas rurales han demostrado una cobertura de radios en el rango de 18 km a 20 km con la posibilidad de ampliar este rango manteniendo las condiciones de conectividad deseadas. Estos pilotos se han concentrado en demostrar y presentar pruebas óptimas para que sean tomadas en cuenta por las empresas de servicios públicos, en un mejoramiento de las prestaciones a nivel de comunicaciones, seguridad y confiablidad de las redes existentes. En estas redes de prueba LPWA, se han conectado a diferentes tipos de sistemas de medida o medidores, contadores de energía, gas y agua. Dentro de los principales resultados que arrojaron de las pruebas, se ha confirmado el bajo consumo de potencia de estos dispositivos que permite que los sistemas de medida de gas y agua tengan una autonomía de más de 7 años, resultados que no se pueden obtener con tecnologías similares (Penagos, 2017).

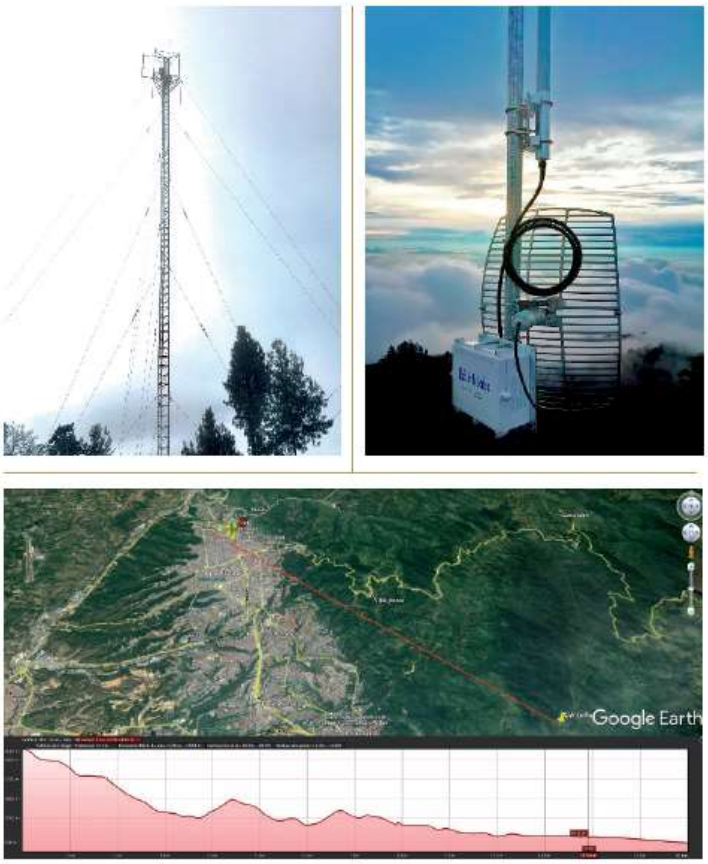


*Figura 11.* Fotos del despliegue del Gateway LoRa a 14 km de Bucaramanga. Mapa de Google Maps mostrando ubicación del Gateway y las unidades de medición de prueba**.** Nota. Tomado de P. Juan Carlos. "Smart Grid, Medición Inteligente e Internet de las Cosas Palancas críticas de competitividad y progreso en Colombia". Orion Infinity. Revista CIDET. Noviembre de 2017.

En base a las pruebas piloto realizadas en la ciudad de Bucaramanga, se obtiene un campo para el desarrollo de múltiples aplicaciones dentro de las limitaciones tecnológicas que aún se tienen a nivel nacional. Cabe resaltar que con el apoyo de empresas privadas y el auge de nuevas tecnologías en el ambiente IoT, se está incrementando el desarrollo de prototipos nacionales y la posibilidad de un crecimiento empresarial en dicho mercado de las telecomunicaciones M2M.

### 3.6 Cobertura IoT en Colombia

Acorde con el plan TIC 2018 – 2022, El futuro digital es de todos, la penetración de nuevas tecnologías a nivel nacional con un 9% en IoT, robótica 1.5%, impresoras 3D, 2.2%, Big Data 3.22%, Inteligencia Artificial (IA) 1.2%, ver Figura 12. Resultados que muestran que se necesita animar la adopción productiva de estas nuevas tecnologías, ya que son pilares para el desarrollo de procesos de transformación digital (MinTic, 2018).

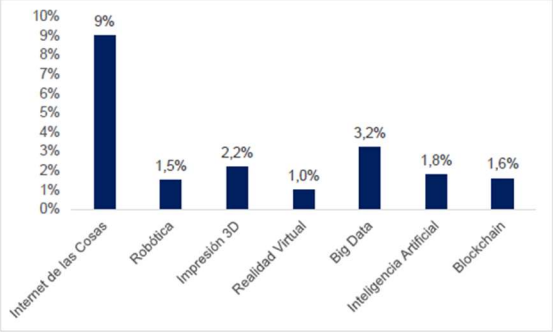


*Figura 12*. Penetración de tecnologías avanzadas. Nota. Tomado de MinTIC. "MinTIC revela los primeros resultados del Observatorio de Economía Digital. Recuperado de https://www.mintic.gov.co/portal/604/w3-article-61929.html". 2017b.

En el proceso de modernización de de los servicios públicos y según el índice de Desarrollo de Gobierno Electrónico (IDEG), en el año 2018 Colombia tuvo una puntuación de 0.68 sobre 1, ocupando la posición número 61, de los 193 países miembros de las naciones unidas. Con esta posición, el país se desplomó 4 posiciones respecto a la medición del año 2016, manteniendo la tendencia negativa presentada en las mediciones anteriores a la de 2018 (UN, 2018), como se muestra en la figura 13.

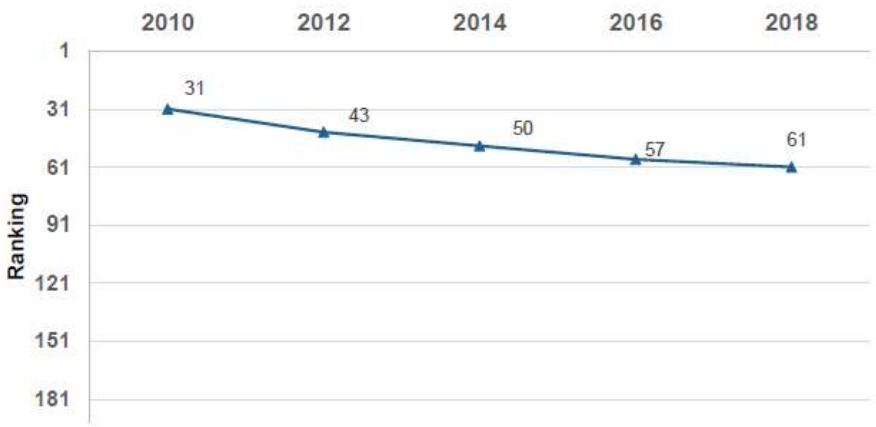


*Figura 13.* Posición de Colombia en el mundo según el índice de Desarrollo de Gobierno Electrónico de Naciones Unidas. Nota. Tomado de Naciones unidas. UN E-Goverment Knowledgebase. 2018. Recuperado de: https://publicadministration.un.org/egovkb/en-us/#.WgMZJq-GO71.

Con soporte de los estudios anteriormente enunciados y la visión del MinTIC que describe (MinTic, 2020): "*El exponente crecimiento de la demanda de un país interconectado la cual promueve el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida y el incremento sostenible del desarrollo*", se debe que propiciar la implantación de nuevas redes e infraestructura tecnológica para la propagación del internet de las cosas, IoT.

Para fijar un punto de referencia IoT en Colombia, se hace énfasis a la proveedora de servicio IoT que alberga mayor cobertura a nivel mundial, SIGFOX (SigFox, 2020). La cual cuenta con una cobertura en Colombia en zonas urbanas (Principal objetivo) y rurales como se puede apreciar en la figura 14. Red que cuenta con compatibilidad con tecnologías Bluetooth, GPS, 2G, 3G, 4G y WiFi.

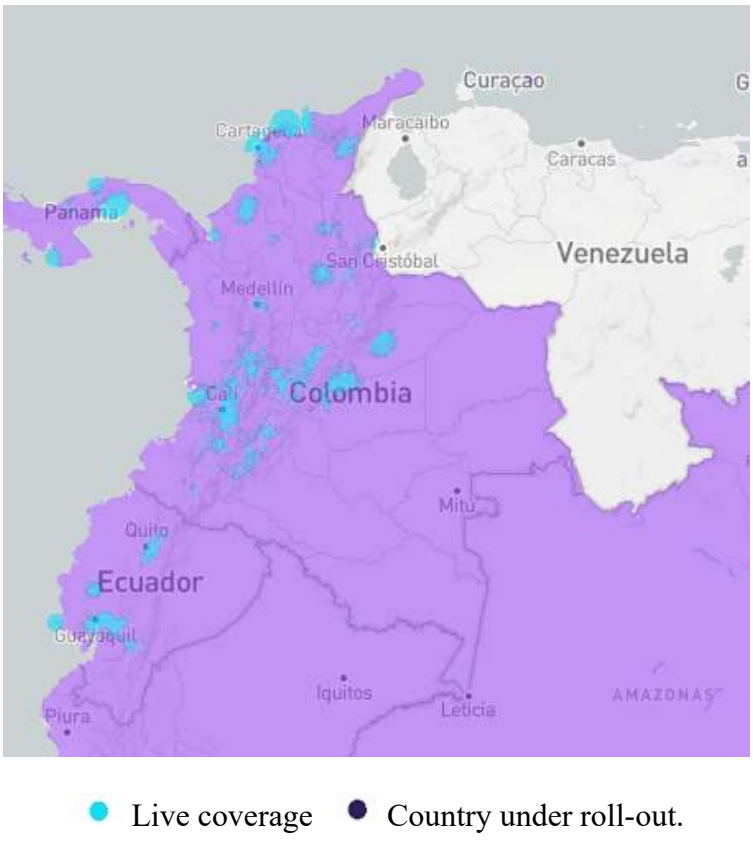


*Figura 14.* Cobertura SIGFOX Colombia. Nota. Tomado de "The world's leading service provider for Internet of Things (IoT)". Enero de 2020. Recuperado de: https://www.sigfox.com/en.

## 3.7 Regulaciones gubernamentales

En este apartado, se sitúa a Estados Unidos como referencia principal para desarrollar un modelo regulatorio para el internet de las cosas (IoT) en Colombia, en cual no existe a la fecha de realización del documento.

**3.7.1 Estados Unidos.** Descripción de normas y leyes que se encuentran adjuntas a la regulación de IoT en Estados Unidos. Inicios, actualidad y futuro.

***3.7.1.1 Selección de radiofrecuencia***. Para ser parte de Internet de las cosas, los dispositivos IOT deben poder conectarse a Internet u otros dispositivos. Los dispositivos pueden hacerlo a través de un cable o una conexión inalámbrica, aunque la mayoría de los dispositivos IoT lo harán comunicarse a través de conexiones inalámbricas. Por lo tanto, los dispositivos necesitarán usar espectro electromagnético, que la Comisión Federal de Comunicaciones (FCC) regula. Las regulaciones del espectro fueron diseñadas, en parte, para minimizar la "interferencia perjudicial", donde una señal procedente de un dispositivo interrumpe la señal de otro dispositivos que usan las mismas frecuencias (FCC, 2002) o las vecinas. Al mismo tiempo, estas regulaciones buscan alentar competencia e innovación (Cf, 2014).

Para lograr sus objetivos de gestión del espectro, la FCC ofrece dos tipos de espectro: con licencia y sin licencia. Las personas interactúan con ambos tipos de espectro diariamente. La conexión a una red inalámbrica con Wi-Fi requiere el uso de espectro sin licencia; conectando a un operador de telefonía móvil requiere el uso de espectro con licencia. Ambos tipos tienen beneficios e inconvenientes, que se mencionan abajo. Los OEM (Original Equipment Manufacturer) deben decidir si usarán sin licencia o espectro con licencia. Además, deben determinar si su dispositivo requiere Autorización de equipo de la FCC (Cf, 2014).

***3.7.1.2 Espectro sin licencia o con licencia***. Los dispositivos que usan espectro sin licencia pueden hacerlo sin autorización expresa de la FCC para acceder a las frecuencias, los consumidores usan espectro sin licencia diariamente. Las computadoras portátiles, por ejemplo, se

conectan a internet a través de Wi-Fi, que se comunica sin licencia en bandas de 2.4 GHz o 5 GHz (Hanbury y Maltas. 2017).

Mientras que las reglas y políticas de la FCC para dispositivos sin licencia no requieren autorización para ocupar espectro de radio, la FCC requiere condiciones de operación y varias formas de aprobación previa para los propios dispositivos. En mercado los equipo que utilizan espectro sin licencia, los OEM deben aceptar cualquier interferencia que reciban sus dispositivos y deben evitar causar interferencias perjudiciales. Los OEM también deben asegurarse de que sus dispositivos cumplan con la Parte 15 de la FCC regulaciones (Hanbury y Maltas. 2017).

Las dos frecuencias predominantes sin licencia que los OEM pueden diseñar sus dispositivos son 2.4 y de 5 GHz. Dispositivos que se comunican en los 5 GHz la banda puede enviar mayores cantidades de información a través de distancias más cortas con menos penetración en el edificio, y los dispositivos requieren antenas más pequeñas (Musey, 2013). Dispositivos que usan las frecuencias de 5 GHz corren el riesgo de incompatibilidad con enrutadores Wi-Fi porque los enrutadores más antiguos no están equipados para recibir esta frecuencia. Los dispositivos que usan 2.4 GHz se comunican con menos información sobre distancias algo más largas con mayor penetración en edificaciones, aunque estos dispositivos exigen antenas más grandes (Musey, 2013). El alcance de las señales de 2.4 GHz significa que la banda puede congestionarse más rápido que la banda de 5 GHz (Hanbury y Maltas. 2017).

Los OEM pueden desear equipar sus dispositivos para que sean compatibles con múltiples frecuencias y agregar capacidades adicionales. Si bien, hacerlo aumenta la interoperabilidad,

también impone requisitos de hardware adicionales en el dispositivo. OEM debe tener en cuenta cualquier restricción en el tamaño del dispositivo cuando deciden qué frecuencias usará el dispositivo. Los fabricantes de equipos originales que utilizan espectro con licencia reciben un servicio más confiable (señal), aunque tendrán que pagar por ello. Para usar espectro con licencia, los OEM generalmente se asociarán con una empresa que tenga una licencia y posea la infraestructura requerida, como Verizon o T-Mobile. Sin embargo, los OEM necesitarán pagar al titular de la licencia lo necesario para comprar el espectro y construir, mantener y operar la infraestructura. El espectro con licencia es más confiable que la variedad sin licencia porque recibe protección legal de interferencias perjudiciales (Armand, 2013). Los grandes OEM también pueden comprar espectro con licencia que el gobierno subasta o en el mercado secundario (FCC, 2013).

La Parte 15 de las regulaciones de la FCC establece las condiciones y requisitos para dispositivos que usan frecuencias sin licencia. Eso tiene ocho subpartes (Hanbury y Maltas. 2017):

- **La Subparte A** establece regulaciones generales sobre dispositivos que usan espectro sin licencia. Esta parte incluye disposiciones que restringen los dispositivos que envían interferencia perjudicial y explica otros requisitos técnicos generales (FCC, 2017).

- **La subparte B** regula los radiadores no intencionales, tales como computadoras, televisores y dispositivos con discapacidad Wi-Fi, Relojes digitales. Radiadores no intencionales intencionalmente generan energía de radiofrecuencia, pero eso sí, no tiene la intención de emitir las señales a través de la radiación o inducción (C.F.R, §§ 15.1–15.38).

- **La Subparte C** establece los requisitos para radiadores intencionales, como teléfonos celulares, walkie-talkies y cualquier cosa que use conectividad Bluetooth. Estos son los dispositivos que generan y emiten intencionalmente energía de frecuencia por radiación o inducción (C.F.R, §§ 15.41–15.78).

- **La Subparte D** regula las bandas sin licencia. Dispositivos de servicio de comunicación, que son radiadores intencionales que funcionan en 1.9 GHz banda de frecuencia que proporciona una "amplia gama de servicios de comunicaciones fijas móviles y auxiliares a particulares y empresas " (C.F.R. §§ 15.201–257).

- **La Subparte E** regula a los nacionales sin licencia. Dispositivos de infraestructura de información, como inalámbricos ISP. Estos dispositivos son radiadores intencionales. operando en 5.15–5.35 GHz y 5.470–5.85 Bandas de GHz que "usan modulación digital de banda ancha técnicas y proporcionan una amplia gama de velocidad de datos móviles y comunicaciones fijas para individuos, empresas e instituciones" (C.F.R. §§ 15.301–323).

- **La Subparte F** establece los requisitos técnicos para dispositivos que utilizan operaciones de banda ultra ancha, como periféricos para PC, monitores inalámbricos y comunicaciones de dispositivo a impresora. Estos dispositivos transmiten grandes volúmenes de datos en distancias cortas sin interferencia sustancial o demandas de energía (C.F.R. §§ 15.401–407).

- **La Subparte G** incluye regulaciones para el acceso banda ancha sobre líneas eléctricas (C.F.R. §§ 15.501–525).

- **La subparte H** se refiere a dispositivos de espacio en blanco, que operan en espectros de transmisión no utilizados (C.F.R. §§ 15.601–615). Cualquier dispositivo puede estar equipado para usar espacios en blanco de espectro, estos dispositivos pueden ser equipados para usar wifi.

***3.7.1.3 Autorización de equipo***. FCC exige que todos los dispositivos de radiofrecuencia (dispositivos de RF) estén autorizados según la Parte II de sus reglamentos antes de su comercialización e importación en los Estados Unidos (C.F.R. §§ 15.701–717). Los fabricantes de equipos originales deben determinar primero si sus dispositivos son dispositivos de RF y, de ser así, deben completar el procedimiento de aprobación necesario (Hanbury y Maltas. 2017).

Los dispositivos de RF son "capaces de emitir energía de radiofrecuencia por radiación, conducción u otros medios" (C.F.R. §§ 2.1–1400). Casi todos los dispositivos electrónicos son capaces de emitir energía de RF y, por lo tanto, deben demostrar el cumplimiento de las normas de la FCC (FCC, 2017). Los productos pueden contener más de una RF y, como resultado, puede requerir completar las tres aprobaciones enumeradas a continuación (EA y FCC, 2017). Los dispositivos de RF se agrupan en las siguientes cuatro categorías: radiadores incidentales, radiadores no intencionales, radiadores intencionales y equipos industriales, científicos y médicos (EA y FCC, 2017).

1. **Los radiadores incidentales** son dispositivos como bombas de pozo, lámparas de detección de movimiento y máquinas fotocopiadoras, que no están diseñados para usar, generar o emitir energía de radiofrecuencia de más de 9 kHz intencionalmente (C.F.R. § 15.3(n).). Los radiadores incidentales no requieren autorización del equipo, aunque deben cumplir con 47 CFR § 15.5 (EA y FCC, 2017).
2. **Los radiadores no intencionales** son dispositivos como computadoras con Wi-Fi, televisores y relojes digitales. Estos radiadores usan "lógica digital, señales eléctricas que operan en frecuencias de radio para su uso dentro del producto, o envían señales de radiofrecuencia por conducción al equipo asociado a través del cableado de conexión, pero no están destinados a emitir energía de RF de forma inalámbrica por radiación o inducción". Los productos que contienen solo lógica digital pueden estar exentos de una autorización de equipo (EA y FCC, 2017).

3. **Los radiadores intencionales** son dispositivos como teléfonos celulares, micrófonos inalámbricos y apertura de puertas de garaje. “Generan y emiten intencionalmente energía de radiofrecuencia por radiación o inducción que puede funcionar sin una licencia individual” (EAP y FCC, 2017).

4. **Los equipos industriales, científicos y médicos** son dispositivos como equipos de resonancia magnética, equipos de diatermia médica y equipos de calefacción industrial. Utilizan energía de RF para usos distintos de las telecomunicaciones. Los OEM pueden recibir la autorización del equipo para su dispositivo a través de uno de los tres

procedimientos de aprobación: certificación, declaraciones de conformidad y verificación (EAP y FCC, 2017).

5. **La certificación** es el proceso de aprobación más riguroso, reservado para dispositivos con la mayor probabilidad de interferencia dañina, como teléfonos móviles, walkie-talkies y transmisores de control remoto (C.F.R. §§ 2.1031–1060). La certificación requiere que los solicitantes presenten una solicitud por escrito y datos de prueba, recopilados por un laboratorio de pruebas acreditado por la FCC a un organismo de certificación de telecomunicaciones (US.GOV, 2015).

6. **La Declaración de conformidad** es el procedimiento que requiere el uso de un laboratorio de pruebas acreditado por la FCC para garantizar que el dispositivo cumpla con los estándares técnicos apropiados. Los dispositivos sujetos a una declaración de conformidad incluyen: computadoras personales, dispositivos de interfaz de TV y hornos de microondas (EAP y FCC, 2017). Las empresas no necesitan solicitar la aprobación de la FCC, pero deben demostrar el cumplimiento si la FCC pregunta (C.F.R. §§ 2.1031–1060).

7. **La verificación** requiere que los operadores confíen en las mediciones que ellos u otra parte tomen en su nombre para garantizar que el dispositivo cumpla con los estándares técnicos. Los dispositivos sujetos a verificación incluyen equipos ISM no destinados al consumidor, receptores de TV y FM y equipos informáticos empresariales (EAP, 2015). Los OEM no necesitan usar un laboratorio de pruebas acreditado por la FCC, ni deben

enviar datos a la FCC. La empresa debe demostrar el cumplimiento si la FCC pregunta (C.F.R. §§ 2.951–955).

***3.7.1.4 Privacidad***. La promesa de Internet de las cosas va más allá de los dispositivos que pueden comunicarse: también se trata del volumen de datos que se pueden recopilar, usar y analizar para generar nuevas ideas sobre el mundo (US.GOV, 2015). Porque Internet de las cosas hace que los dispositivos pueden recopilar y transmitir información sobre individuos, estos dispositivos pueden implicar privacidad y preocupaciones. Los OEM deben entender el panorama legal en los Estados Unidos con respecto a la privacidad (Hanbury y Maltas. 2017).

El principal regulador de privacidad en los Estados Unidos es la Comisión Federal de Comercio (FTC). La FTC administra varios estatutos que tienen requisitos específicos, pero más en general, la FTC regula las prácticas de privacidad a través de su autoridad de la Sección 5. La Comisión Federal de Comercio La ley prohíbe los "actos o prácticas injustas o engañosas" (FCC, 2008). Injusto se define como prácticas que causan o son o es probable que cause daños sustanciales a los consumidores, lo cual es razonablemente no evitable por los propios consumidores y no compensado por los beneficios compensatorios para los consumidores o a la competencia" (FCC, 2008). El engaño no está definido legalmente, aunque la FTC afirma que considera el engaño como un representación material, omisión o práctica que es probable que engañe a los consumidores razonables. La autoridad de la Sección 5 de la FTC no es la única ley que protege la privacidad en los Estados Unidos: el Congreso también aprobó varias leyes de privacidad que se aplican a industrias específicas, ciertas prácticas comerciales, y grupos vulnerables. Además, la ley estatal podría imponer requerimientos adicionales (Miller, 1983).

**Actos o prácticas injustas o engañosas:** Los OEM deben observar los procedimientos de ejecución de la FTC para comprender mejor lo que espera de las empresas, como la Comisión carece de autoridad proactiva para la reglamentación. Las decisiones de ejecución de la FTC son una forma de precedente para comprender la aplicación de la privacidad (Daniel, 2014). Para evitar acusaciones de actos engañosos, los OEM deben divulgar sus prácticas de privacidad y evitar hacer tergiversaciones (Hanbury y Maltas. 2017). La FTC ha iniciado procedimientos basado en prácticas engañosas de privacidad en muchos casos, incluyendo lo siguiente:

1. una empresa no pudo proporcionar consumidores con aviso adecuado sobre la función (FTC, 2011).
2. una compañía afirmó falsamente que los consumidores podrían optar por no participar de seguimiento mediante el uso de una configuración en el navegador (OAS y FTC, 2011).
3. la compañía hizo muchas tergiversaciones sobre la privacidad, incluyendo que cumplió con los EE. UU. Marco de Puerto seguro (US-EU, 2015).
4. una empresa actuó en contra de su política de privacidad cuando compartió información con anunciantes (MS y FTC, 2012).

Para evitar acusaciones de actos injustos, los OEM deben consultar asesoramiento sobre si se requiere el consentimiento del consumidor para recopilar y compartir información. La FTC solo tiene cabida a enjuiciar a las empresas por actos de privacidad injustos, entonces el estándar es relativamente incipiente. Un ejemplo de la La FTC es que inicia procedimientos contra una

empresa por injustas prácticas de privacidad en cuanto la FTC procesó a una empresa para rastrear a los consumidores sin recibir información consentimiento (VIZIO, 2017).

***3.7.1.5 Información protegida***. Además de la prohibición general de la FTC sobre prácticas injustas o engañosas, la ley de los Estados Unidos también establece requisitos de privacidad para ciertas industrias y tipos de información. Los OEM deben tomar nota si manejan alguna de la siguiente información (Hanbury y Maltas. 2017).

1. **Información personal sobre niños menores de 13 años**: los dispositivos OEM que fabrican dispositivos dirigidos a niños menores de 13 años o que recopilan deliberadamente información personal sobre niños menores de 13 años deben cumplir con la Ley de Protección de Privacidad en Línea para Niños (COPPA). Se aplica COPPA a "cualquier servicio disponible a través de Internet, o que se conecte a Internet o a una red de área amplia" (COPPA, 2015). La FTC administra el estatuto.

2. **Información de finanzas personales para el consumidor**: las empresas que "participan de manera significativa en la provisión de productos o servicios financieros", así como sus filiales y proveedores de servicios, deben proteger la información de finanzas personales del consumidor de conformidad con la Ley Gramm-Leach-Bliley (GLBA) (FI y CI, 2006). Los fabricantes de equipos originales deben cumplir con los GLBA, si lo hacen, están afiliados a cualquier persona que lo haga o brinden servicios a cualquiera que realice cualquiera de las siguientes actividades: (1) prestar, intercambiar, transferir, invertir para otros o proteger dinero o valores, (2) proporcionar servicios financieros , servicios de

asesoramiento económico o de inversión, (3) corretaje o servicio de préstamos, (4) cobro de deudas, (5) prestación de servicios de liquidación de bienes inmuebles y (6) asesoramiento profesional de personas que buscan empleo en servicios financieros (Hanbury y Maltas. 2017). La FTC administra la Ley Gramm-Leach-Bliley.

3. **Información de salud personal:** Dos agencias imponen protecciones de privacidad para la información de salud personal: el Departamento de Salud y Servicios Humanos de los EE. UU. (HHS) y la FTC (Hanbury y Maltas. 2017).

   - ✓ Las empresas como los planes de salud, los centros de intercambio de información médica, los proveedores de atención médica que transmiten información médica en forma electrónica en relación con las transacciones enumeradas y los socios comerciales de todo lo anterior deben cumplir con la Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA) enmendada por Tecnología de la información sanitaria para la salud económica y clínica (HITECH) (HIPAA, 2013).
   - ✓ HIPAA protege toda la información de salud individualmente identificable, también conocida como información de salud protegida o PHI. HHS administra HIPAA (HIPAA, 2013).
   - ✓ Todos los proveedores de registros de salud personales, entidades relacionadas con PHR y proveedores de servicios externos que HIPAA no cubre deben cumplir con los requisitos de notificación de incumplimiento de HITECH. El requisito, que administra la FTC, exige que las entidades cubiertas divulguen cuando ha habido

un " adquisición no autorizada de información de salud identificable por PHR que no es segura y se encuentra en un registro de salud personal " (FTC y HBNR, 2010).

4. **Informes del consumidor**: los OEM podrían considerarse proveedores bajo la Ley de Crédito e Informes Justos (FCRA) y, por lo tanto, podrían enfrentar obligaciones legales según la Regla del Proveedor (C.F.R. §§ 660.1–4). FCRA protege los informes de crédito del consumidor y regula a las compañías que regularmente brindan información al consumidor para los informes de crédito agencias (§ 15 U.S.C. 1681s-2). La FTC administra FCRA.

**Preocupaciones adicionales, correos electrónicos y mensajes de texto**: Los OEM pueden considerar comunicarse con los consumidores mediante el uso de mensajes de texto o mensajes de correo electrónico por una variedad de razones, como notificar a los consumidores sobre las prácticas de privacidad. Al hacerlo, deben tener en cuenta dos leyes que regulan estas acciones: CAN-SPAM y la Ley de Protección al Consumidor Telefónico (TCPA) (Hanbury y Maltas. 2017).

1. **Comunicaciones comerciales por correo electrónico**: CAN-SPAM regula los correos electrónicos enviados con fines de marketing. El estatuto se aplica a los mensajes comerciales, que se definen como "cualquier mensaje de correo electrónico cuyo propósito principal es la publicidad comercial o promoción de un producto o servicio comercial" (CAN-SPAM, 2009). La FTC administra CAN-SPAM.

2. **Mensajes de texto marcados automáticamente**: La TCPA prohíbe los mensajes de texto marcados automáticamente a menos que (1) el consumidor haya dado su consentimiento o (2) el mensaje se envíe con fines de emergencia. Los textos comerciales requieren el consentimiento del consumidor por escrito, mientras que el consentimiento oral es suficiente para otros fines (Avoiding, 2016). La FCC administra el TCPA.

***3.7.1.6 Ciberseguridad***. En 2016, cientos de miles de IOT sin garantía los dispositivos infectados con malware fueron coordinados para tomar bajar sitios web importantes (Hilton, 2016). Este incidente, también conocido como el incidente de Dyn, trajo la seguridad del dispositivo IOT al destacar. Los OEM deben comprender la evolución legal del panorama con respecto a la seguridad del dispositivo IOT. Al igual que la privacidad, la FTC es el principal regulador de seguridad para Dispositivos IOT. La FTC regula estas prácticas principalmente a través de su autoridad de la Sección 5, aunque el Congreso tiene también faculta a la Comisión y otras agencias, para hacer cumplir los requisitos de seguridad para las entidades que manejan ciertos tipos de información (Hanbury y Maltas. 2017).

**Injusto o engañoso**. Los procedimientos de ejecución de la FTC también arrojan luz sobre las expectativas para la seguridad del dispositivo IOT. Sin embargo, esta área está evolucionando, por lo que los informes del personal de la FTC y otras formas de orientación también es perspicaz. Para evitar acusaciones de prácticas engañosas, los OEM deben asegurarse de que tengan prácticas razonables para cumplir con su representaciones sobre la seguridad del dispositivo. Representaciones pueden derivar de promesas abiertas a los símbolos en el embalaje. Ejemplos de procedimientos de la FTC que alegan las prácticas engañosas de ciberseguridad incluyen: (1) una

empresa proporcionando monitores para bebés con acceso a Internet descritos de sus cámaras como "seguras", pero tenían un software defectuoso que permitía a cualquiera ver las imagenes en línea (FTC, 2014); (2) una empresa tergiversó tanto que sus dispositivos son seguros como que tenía un procedimiento para proteger dispositivos de personas no autorizadas acceso (D-Link, 2017); y (3) una empresa tergiversó que su entorno "en la nube" era seguro y no pudo adoptar medidas de seguridad razonables para mantener su entorno seguro (ASUS, 2016). Muchas otras medidas relacionadas con la seguridad existen en varios procedimientos (OAM, 2016).

Para evitar acusaciones de prácticas injustas, los OEM deben también adoptan prácticas de seguridad razonables proporcionales con "la cantidad y la sensibilidad de los datos recopilados, el sensibilidad de la funcionalidad del dispositivo y los costos de remediando las vulnerabilidades de seguridad" (FTC, 2015). La FTC tiene inició procedimientos de injusticia contra empresas en el siguientes ejemplos: (1) un laboratorio clínico que no logró adoptar medidas de seguridad razonables para proteger información personal (LabMD, 2016); y (2) una empresa que vende dispositivos para proteger las redes no pudo tomar razonable pasos para asegurar sus dispositivos (D-Link, 2017). En LabMD, la compañía estaba manejando información confidencial de salud. La FTC denuncia que identificó varias actividades relacionadas con la seguridad, como la implementación de "detección de intrusos sistema (s) o monitoreo de integridad de archivos, monitoreo de tráfico cruzando sus firewalls, ofreciendo capacitación en seguridad de datos a sus empleados y eliminar cualquiera de los datos del consumidor " la empresa recauda (LabMD, 2016).

La FTC parece estar atendiendo a la brecha entre el vida útil de un dispositivo y la vida útil de su software. Así, la FTC ha recomendado que las empresas "sean francas en sus

representaciones sobre proporcionar seguridad continua actualizaciones y parches de software. Revelando la longitud de las compañías de que tiempo planean apoyar y lanzar software y las actualizaciones para una determinada línea de productos que ayudarán a los consumidores comprender mejor las "fechas de vencimiento" seguras para sus dispositivos básicos conectados a Internet "(FTC, 2006).

**Información protegida**: Al igual que lo hace para la privacidad, la ley de los Estados Unidos establece requisitos de seguridad para ciertas industrias y tipos de información. Los OEM deben tomar nota si manejan alguna de la siguiente información (Hanbury y Maltas. 2017).

1. **Información personal sobre niños menores de 13 años**: COPPA requiere que las entidades cubiertas “establezcan y mantengan procedimientos razonables para proteger la confidencialidad, seguridad e integridad de la información personal recopilada de niños” (COPPR, 2017). La guía de la FTC recomienda que los OEM minimicen los datos recopilados, compartan datos con solo los proveedores y terceros "capaces de mantener su confidencialidad, seguridad e integridad" conservan la información solo durante el tiempo que sea "razonablemente necesario para el propósito que se recopiló" y eliminan la información de forma segura una vez que ya no es una razón legítima para retenerlo (COPPR, 2017).

2. **Información de finanzas personales del consumidor:** La Norma de Salvaguardia de la FTC requiere que las entidades cubiertas "garanticen la seguridad y confidencialidad" de la información de finanzas personales del consumidor mediante la adopción de medidas

como el desarrollo de "un plan de seguridad de la información por escrito que describa su programa para proteger la información del cliente y que sea apropiado para el tamaño y complejidad de la empresa, la naturaleza y el alcance de sus actividades, y la sensibilidad de la información del cliente" (FIC, 2006).

3. **Información de salud personal**: la Regla de Seguridad de HIPAA requiere que las entidades cubiertas adopten "salvaguardas administrativas, físicas y técnicas apropiadas para garantizar la confidencialidad, integridad y seguridad de la información de salud electrónica protegida" (TSR, 2017).

***3.7.1.7 Estado del espectro IMT 5G***. Desde 2014, la Comisión Federal de Comunicaciones - FCC, trabaja en el reordenamiento del espectro radioeléctrico de alto rango para servicios móviles. En octubre de 2014, el regulador emitió un aviso de consulta para examinar el potencial de las bandas por encima de los 24 GHz para la provisión de servicios móviles. Con esta acción, la FCC se convirtió en el primer organismo regulador del mundo en iniciar formalmente procedimientos para el espectro 5G. La consulta incluyó preguntas relacionadas con el uso compartido de espectro y la opción de licencia en las siguientes bandas (Hanbury y Maltas. 2017):

- 24 GHz: 24.25-24.45 GHz y 25.05-25.25 GHz
- Banda LMDS: 27.5-28.35 GHz; 29.1-29.25 GHz y 31-31.3 GHz
- 39 GHz: 38.6-40 GHz
- 37/42 GHz: 37.0-38.6 GHz y 42.0-42.5 GHz
- 60 GHz: 57-64 GHz y 64-71 GHz (extensión)

- 70/80 GHz: 71-76 GHz; 81-86 GHz y 92-95 GHz.

Un año después, en octubre 2015, la FCC publicó un Aviso de Propuesta de Reglamentación (NPRM) para el uso del espectro superior a 24 GHz. El regulador propuso reglas para las siguientes cuatro bandas superiores a 24 GHz para el servicio móvil y solicitó comentarios sobre las reglas de servicio propuestas autorizando las operaciones móviles y de otro tipo en esas bandas (5GAMERICAS, 2019).

- 27.5-28.35 GHz
- 38.6-40 GHz
- 37-38.6 GHz
- 64-71 GHz

La NPRM propuso los siguientes regímenes de licencias para las siguientes bandas (Hanbury y Maltas. 2017):

- Licenciadas
    - 27.5-28.35 GHz
    - 38.6-40 GHz
- Licencia híbrida
    - 37-38.6 GHz
    - Outdoor: licenciado
    - Indoor: libre para dueños de propiedades

- Sin licencia
    - 64-71 GHz

- Tamaño de Área de licencia para 28 GHz, 39 GHz y outdoor 37 GHz Bands
    - Condado (existen 3.143 condados en EEUU).
- Término de la licencia: 10 años

La FCC continuó con la publicación de nuevas regulaciones. En noviembre de 2017 emitió un Segundo Aviso Adicional de Propuesta de Reglamentación para Espectro Milimétrico Superior a los 24 GHz. Sintéticamente, la nueva reglamentación incluye (FCC, 2017):

- Disponibilidad de espectro adicional de onda milimétrica (mmW) de 1700 MHz para uso inalámbrico terrestre 5G.
- Mantiene el uso sin licencia de la banda de 64-71 GHz
- Mantiene espectro en las bandas 48.2-50.2 GHz y 40-42 GHz para uso de satélite.
- Rechaza limitar la cantidad de espectro en las bandas de 24 GHz y 47 GHz que un postor puede adquirir en una subasta, e incorpora estas dos bandas en el umbral del espectro mmW previamente adoptado para revisar las transacciones propuestas del mercado secundario.

Además, el texto de reglamentación propone:

- Permitir un uso más flexible del SFS (servicio fijo por satélite) de la banda de 24,75-25,25 GHz
- Buscar comentarios sobre otra opción para los licenciatarios de mmW terrenales para cumplir con las obligaciones de desempeño, que podrían acomodar las implementaciones de IoT y otros servicios innovadores
- Eliminar el límite de la cantidad de espectro en las bandas de 28, 37 y 39 GHz que un postor puede adquirir en una subasta.

Ya en junio de 2018, la FCC volvió a emitir regulaciones bandas superiores a 24 GHz (FCC, 2018). Básicamente estableció reglas adicionales para bandas de espectro de ondas milimétricas previamente identificadas, designadas para uso flexible. Esto incluye adoptar un requisito de operabilidad para toda la banda de 24 GHz, un marco de compartición para permitir el uso de una parte de la banda de 24 GHz para operaciones terrenales inalámbricas y estaciones terrenas del Servicio fijo por satélite, un plan de banda para la banda inferior de 37 GHz, y reglas de agregación de espectro aplicables a ciertas bandas. La FCC, además, busca comentarios sobre 2,75 GHz de espectro adicional en las bandas de 26 GHz y 42 GHz disponibles para servicios inalámbricos de próxima generación; establece mecanismos de coordinación para facilitar el uso compartido de la banda Lower 37 GHz entre usuarios federales y no federales (Hanbury y Maltas. 2017).

Entre otras medidas, la FCC está reconsiderando su política para la banda de 3.55-3.7 GHz, espectro que en la actualidad se utiliza para “Citizens Broadband Radio Service”, pero podría estar disponible para 5G en un futuro. El regulador también considera una consulta sobre la banda 5.925–7.125 GHz para uso sin licencia. La FCC inició en noviembre de 2018 la Subasta 101 que

incluye la banda de 28 GHz (FCC, 2018) y concluyó el 25 de enero de 2019. En total se recaudaron poco más de US$ 702 millones y se asignó el 97% de las licencias disponibles (FCC, 2019). En el caso de la banda de 28 GHz, operadores nacionales en Estados Unidos adquirieron bloques de espectro a través del mercado secundario.

La Subasta 102 inició en marzo de 2019 para colocar la banda de 24 GHz (24,25 GHz-24,45 GHz / 24,75 GHz-25,25 GHz) que abarca más licencias que la Subasta 101. La fase de reloj concluyó el 18 de abril de 2019 con una recaudación de casi USD$ 2,000 millones (Telegeography, 2019), nivel que puede incrementar durante la fase de asignación de bloques. En esta fase se reportan ofertas ganadoras en el 99,8% de las áreas cubiertas por las licencias (Auctiondata, 2019). El 3 de mayo de 2019 inició la fase de asignación de los bloques que se prevé concluya el 28 de mayo tentativamente. La FCC planea asignar más espectro de bandas altas (FCC, 2018), tentativamente a partir de 2019, en los segmentos de 37-39 GHz y la banda de 47 GHz46 y en cuanto a capacidad disponible en la banda de 3,5 GHz no hay planes para licitarla antes de 2020.

***3.7.1.8 Futuro***. La Comisión Federal de Comunicaciones tiene una estrategia completa para facilitar la supremacía de los Estados unidos en las tecnologías 5G, esta estrategia fue denominada "Plan 5G FAST". Esta estrategia incluye tres actividades clave para su desarrollo (Hanbury y Maltas. 2017):

1. Introducción de más espectro. La FCC está propiciando medidas para hacer que parte del espectro esté disponible para las tecnologías 5G. Como bandas de frecuencia bajas de 600 MHz, 800 MHz, y 900 MHz. Bandas de frecuencia media de 2,5 GHz, 3,5 GHz, y 3,7 – 4,2 GHz, y

bandas de frecuencia altas de 24 GHz, 26 GHz, 28 GHz, 37 GHz, 39 GHz, 42 GHz y 47 GHz. Acorde con lo anterior mencionado, la FCC está pujando para la generación de nuevas asignaciones de estas bandas (Hanbury y Maltas. 2017).

2. Introducción de más espectro. La FCC está propiciando medidas para hacer que parte del espectro esté disponible para las tecnologías 5G. Como bandas de frecuencia bajas de 600 MHz, 800 MHz, y 900 MHz. Bandas de frecuencia media de 2,5 GHz, 3,5 GHz, y 3,7 – 4,2 GHz, y bandas de frecuencia altas de 24 GHz, 26 GHz, 28 GHz, 37 GHz, 39 GHz, 42 GHz y 47 GHz. Acorde con lo anterior mencionado, la FCC está pujando para la generación de nuevas asignaciones de estas bandas (Hanbury y Maltas. 2017).

3. Remodelar las normativas antiguas. La FCC está remodelando las normativas antiguas para impulsar el despliegue de backhaul para las redes 5G (Hanbury y Maltas. 2017).

**3.7.2 Colombia**. Para implementar las tecnologías IoT en Colombia, primero se debe acoger a las recomendaciones globales dadas por la Union Internacional de Telecomunicaciones – UIT, que es el organismo especializado en telecomunicaciones para la conectividad internacional de redes, la cual Colombia forma parte de esta unión desde el año 1914. Para la regulación de estas tecnologías a nivel nacional, la encargada del tema le compete a la Agencia Nacional del Espectro – ANE.

***3.7.2.1 Unión Internacional de Telecomunicaciones – UIT***. La Unión Internacional de Telecomunicaciones – UIT, es una organización de carácter internacional de conectividad de las

redes de comunicaciones, la cual está comprometida con conectar la población desde cualquier parte del mundo y cualesquiera que sean sus medios (UIT, 2020).

La UIT cuenta con tres tareas principales, que son organizadas en sectores que desarrollan sus actividades por medio de conferencias con la activa participación de los países miembros de la organización. Cada sector realiza sus estudios por sector para determinar factores importantes, constituidas por distintos tipos de profesionales. El principal objetivo de estas comisiones de estudio es el establecimiento de normas técnicas o recomendaciones. Por tanto, en mayo de 2015, se creó el Grupo Temático sobre las particularidades de red de las IMT 2020 para analizar cómo será la interacción de las tecnologías 5G emergentes en las redes futuras, como estudio previo sobre las adecuaciones y actualizaciones de red necesarias para soportar el desarrollo de los nuevos sistemas 5G (MinTic, 2019).

En la fecha de septiembre de 2016 fue publicada por la IUT, la Recomendación UIT-R M.2083-0 (UIT-R M.2083-0, 2017) "*Concepción de las IMT – Marco y objetivos generales del futuro desarrollo de las IMT para 2020 y en adelante*", la principal meta de esta recomendación es conceptualizar las IMT para 2020 y futuro posterior, mediante la definición de las posibles tendencias en el usuario final y las aplicaciones interconectadas a la red mundial, del crecimiento del flujo de información, de los desarrollos tecnológicos y de la incursión en el espectro (IUT, 2018.

Dentro de los retos que enfrentan los entes reguladores para facilitar el despliegue de esta tecnología se tienen (MinTic, 2019):

- Despliegue de redes más ágil (infraestructura)
- Gestión y planificación del espectro radioeléctrico (Bandas bajas, medias y altas)
- Una regulación orientada a la seguridad y privacidad de servicios y aplicaciones.
- Calidad de servicio y derechos de usuario.
- Redes de fibra óptica.
- Desarrollo de marco jurídico para incentivar y facilitar inversiones

Se debe enfatizar que la ITU divide al mundo en su Reglamento de radiocomunicaciones con el propósito de administrar el espectro electromagnético global. Cada región posee su propio conjunto de asignación de frecuencias, lo cual es la principal razón para definir las regiones. Ver Figura 15.

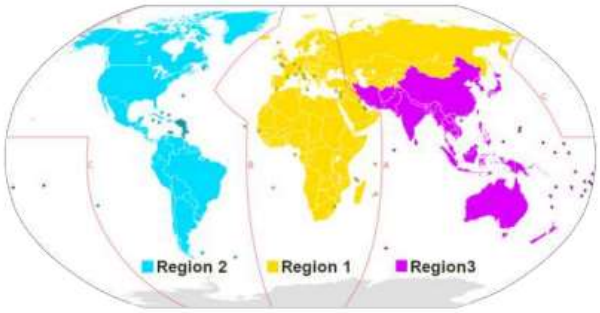


*Figura 15.* División de regiones por asignación de frecuencias. Nota. Tomado de Song, S. Rey-Moreno, C. Jensen, M. "Innovaciones en la gestión del espectro". Internet society.

De manera ilustrativa se realiza un diagrama el cual muestra las Instituciones encargadas de la normalización internacional en Telecomunicaciones, ver Figura 16. El trabajo de estos grupos de estudio es realizar investigación y normalización en temas regulatorios y técnicos.

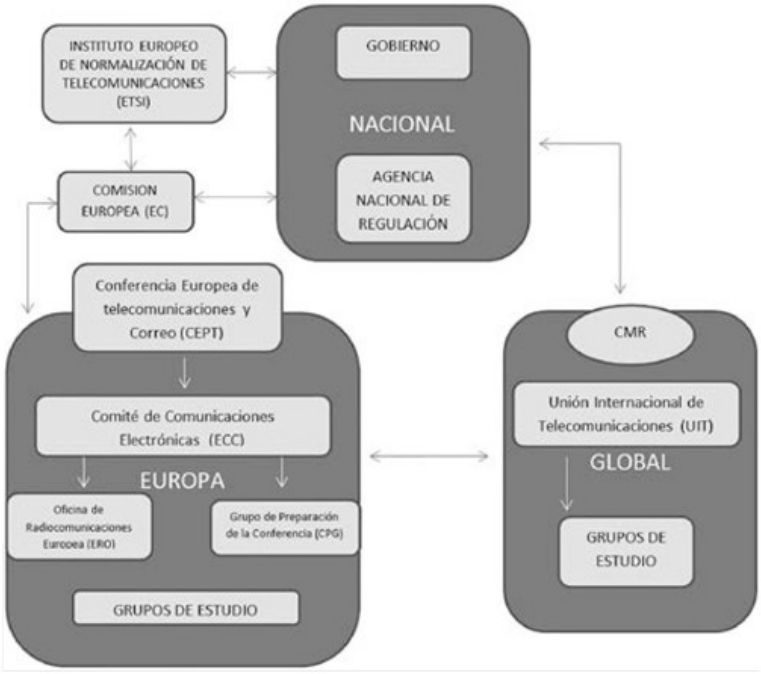


*Figura 16.* Instituciones encargadas de la normalización internacional de telecomunicaciones. Nota. Tomado de Cave, M., Doyle, C., & Webb, W. (2007). Essentials of modern spectrum management. New York: Cambridge; New York. Cambridge University Press.

***3.7.2.2 Plan Nacional de Desarrollo – PND***. Lo que contempla el plan nacional de desarrollo es estructurar el territorio para la sostenibilidad, el desarrollo y la equidad territorial en municipios, departamentos y áreas metropolitanas. Indaga propuestas para formular proyectos de largo plazo para las aglomeraciones y corredores urbanos de las ciudades y la formulación de decretos para el plan de ordenamiento territorial. En el PND prevalecen los proyectos que generen el desarrollo sostenible de las ciudades (DNP, 2015).

En el mencionado PND se contempla también la implementación de un proyecto llamado "Observatorio de Ciudades" con el fin de realizar estudios de seguimiento a la Política del Sistema

de Ciudades y apoyar en el ordenamiento del territorio nacional para la sostenibilidad, el desarrollo y la equidad territorial en municipios, departamentos y áreas metropolitanas, a partir de los datos compilados y la articulación de los datos para tomar decisiones que den a lugar (DNP, 2015).

El índice de Indicadores de las Ciudades Modernas fue creado por el DNP para medir 36 indicadores en 6 aspectos: Ciencia, Equidad e inclusión social, Productividad, Tecnología e Innovación, Participación e Instituciones y Sostenibilidad, Competitividad y Complementariedad; Seguridad, Gobernanza (DNP, 2015).

Por su parte el MinTIC ya realizó un primer reporte al marco de ciudades inteligentes en el 2014, a través de un oficio basado en las políticas nacionales. El oficio plantea los objetivos y recomendaciones que se deberán tener en cuenta en la implementación de una política de ciudades inteligentes en Colombia, así como un plan de acción que define las pautas o pilares para llevar a cabo su puesta en marcha (MinTIC, 2014).

Sin embargo, luego de una revisión de los proyectos actuales, no hay objetivos y planes concretos para las ciudades inteligentes a nivel nacional, solo se observan algunas iniciativas locales. Se destacan por ejemplo esfuerzos como los de Medellín, con iniciativas como Ruta N (Ruta N, 2020), el cual es un centro de innovación y negocios, una corporación creada por la alcaldía de Medellín, UNE y EPM para promover el desarrollo de negocios innovadores basados en la transferencia de conocimiento y tecnología, que incrementen la competitividad de la ciudad y de la región, a través del cual se fortalecen proyectos.

***3.7.2.3 Agencia Nacional del Espectro – ANE***. La Agencia Nacional del Espectro – ANE, es el organismo del gobierno colombiano encargado de orientar al Ministerio de las Tecnologías de la Información y las Comunicaciones en relación con la planeación, control y gestión de la vigilancia del espectro en Colombia (ANE, 2020).

La ANE en el año 2018, bosquejó los parámetros técnicos para promover el IoT en Colombia, donde se analizó el aumento del canal de internet que da soporte a los sistemas inteligentes, programables, con la capacidad de interactuar con el usuario final. También el estudio involucró el análisis para implementar las ciudades inteligentes donde puede existir un impacto muy positivo para el beneficio de los sectores industriales. Dado los estudios parciales realizados por la ANE, mostró las siguientes condiciones para la implementación de la internet de las cosas en Colombia (Guzman, 2019):

- Control de interferencias y las propagaciones de la señal en ambientes interiores y exteriores.
- Se debe colocar una banda de frecuencia exclusiva que permita la conectividad.
- Ampliar la potencia del espectro y de la transmisión de la señal.
- Utilizar las bandas de frecuencia que estén de uso libre y que permitan registrarse para el uso de la IoT.
- Monitoreo de la ocupación del espectro, densidad de los dispositivos conectados por áreas y regiones.

Dicho lo anterior, actualmente Colombia no cuenta con un marco normativo vigente que regule a la implementación de tecnologías IoT. Por lo tanto, se plantea en este documento unas recomendaciones o puntos específicos a la ANE para tener en cuenta a la hora de articular dicha reglamentación.

1. **Gestión**

- Conocimiento, aceptación y apropiación del internet de las cosas.
- Visión y misión por parte de los entes nacionales implicados en el tema.
- Lograr un nivel óptimo de desarrollo económico-social y fortalecimiento de ciudades con altos niveles de desigualdad y pobreza en temas de infraestructura donde se puedan implementar las tecnologías.
- Inversión tecnológica, administración de datos, seguridad, estándares internacionales.

2. **Parte técnica**

- Capa física
  - ✓ Identificar e implementar protocolos y arquitecturas escalables.
  - ✓ Configuración de sensores, sincronización en tiempo real.

- Capa de red
  - ✓ Diseño de tecnologías que se adapten a los lineamientos que disponga la ANE para la transmisión de datos. (Bandas licenciadas, no licenciada e híbridas)

- Capa de Gestión de servicio
    - ✓ Almacenamiento y procesamiento de datos en tiempo real.
    - ✓ Interoperabilidad.
    - ✓ Modelo de sistema de gestión. (Calidad)

- Capa de aplicaciones
    - ✓ Integración de internet de las cosas con los sistemas existentes TIC.
    - ✓ Dar valor agregado a los datos a través de aplicaciones que resulten útiles para la población en general.

Por último y no menos importante, se le recomienda a la ANE, implementar toda esta tecnología teniendo como referencia a las regulaciones y restricciones ya establecidas por la Federal Communications Commision - FCC en los estados unidos, que se evidencian en el numeral 2.7.1 del presente capítulo.

## 4. Posibles aplicaciones para el desarrollo de proyectos de implementación para el grupo de investigación CEMOS.

En este capítulo se realiza un análisis de tres proyectos de grado, en los cuales se presenta como base fundamental el IoT; presentados ante la escuela de ingenierías eléctrica, electrónica y de telecomunicaciones de la Universidad Industrial de Santander.

## 4.1 Implementación de un sistema de seguridad IoT.

Retomando el apartado de recomendaciones del proyecto "Implementación de un sistema de seguridad IoT" (Ray, 2019) se evidencia que, para una posible implementación en el sector de seguridad y protección, se requiere de una estructura tanto en software como hardware que cumpla con los requisitos que se exige en los reglamentos técnicos en lo que respecta a sistemas contraincendios, detección de intrusos y demás aplicables en este ámbito.

Por lo tanto, es acertado implementar una de las soluciones LPWA presentadas en este documento, respetando la metodología expuesta en el capítulo 5. Para mencionar algún proyecto para tener en cuenta para este tipo de soluciones se pueden encontrar el siguiente ejemplo:

- ***Nest Protect*** (Nest, 2020): Tiene un sensor de humo de calidad industrial, se prueba automáticamente y dura hasta una década. Ver figura 17.

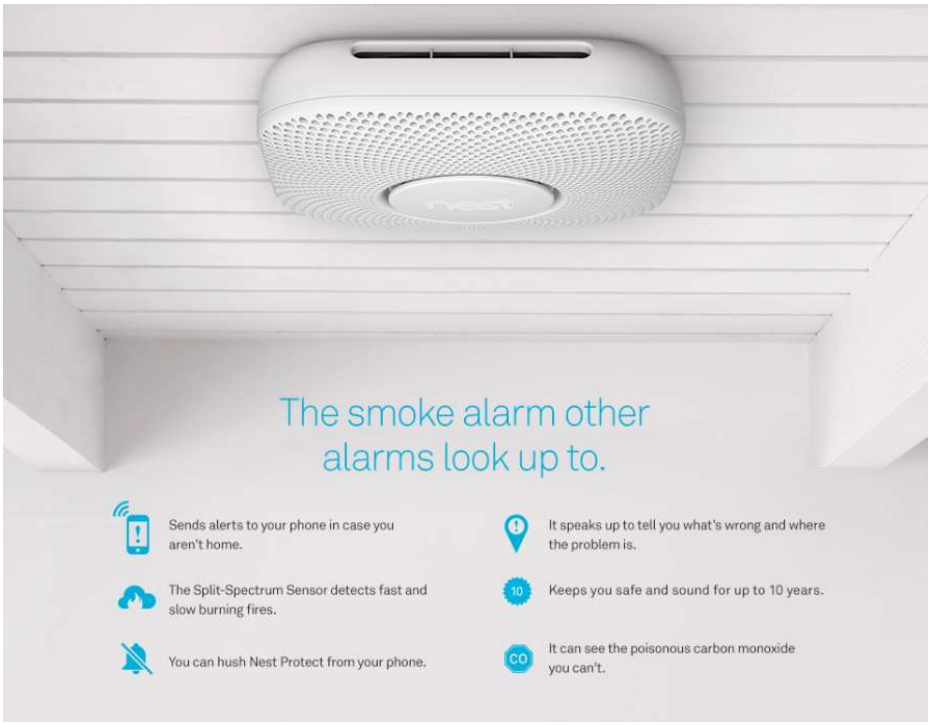


*Figura 17.* Características de Nest protect. Nota. Tomado de "Nest Protect (Battery) 2nd Generation". 2020. Recuperado de: https://es.verizonwireless.com/products/nest-protect-smoke-and-carbon-monoxide-alarm-battery/

Cuenta con comunicación inalámbrica a través de un dispositivo móvil con conexión a internet, para transmitir alarmas de humo al usuario, identificación de zona en peligro, desactivación de alarma sonora y notificación de batería baja. Se complementa con otros dispositivos de la marca como el ***Nest Thermostat*** y la videocámara con ***Wi-Fi Nest Cam***, que se utilizan para tener acceso y control de la temperatura e imagen en tiempo real.

## 4.2 Monitoreo, adquisición y transmisión de datos en tiempo real, mediante IoT, de las variables medidas por un prototipo de caracterización de paneles fotovoltaicos y de medición de variables meteorológicas.

“Monitoreo, adquisición y transmisión de datos en tiempo real, mediante IoT, de las variables medidas por un prototipo de caracterización de paneles fotovoltaicos y de medición de variables meteorológicas” (Angulo y Muñoz, 2019). Teniendo en cuenta la eficiencia energética que se viene tratando en las diferentes tecnologías presentadas en este documento, y la eficiencia energética que requieren los sistemas fotovoltaicos en la conversión de energía solar a eléctrica. Vale mencionar la aplicación de módulos IoT que cuenten con características de las tecnologías LPWA para el monitoreo, adquisición y transmisión de datos en tiempo real; teniendo en cuenta el consumo de los diversos dispositivos electrónicos del prototipo y la fuente regulada de tensión que se requiere para su operación. Una de las principales características de las tecnologías LPWA, es su autonomía en lo que respecta a sus fuentes de alimentación, ya que dependiendo del módulo que se implemente para dicha solución, se generará una mayor independencia de la red eléctrica debido a sus baterías de larga duración y bajo consumo.

### 4.3 Diseño e implementación de un sistema de monitoreo en estanques piscícolas basado en internet de las cosas (IoT).

En base a las pruebas y resultados obtenidos en el prototipo de monitoreo en el “Diseño e implementación de un sistema de monitoreo en estanques piscícolas basado en internet de las cosas (IoT) (Lozano, 2019), cabe resaltar el uso de la tecnología LPWA LoRa, la cual cuenta con características idóneas para proyectos en zonas rurales como se aprecia en la tabla A 1. Para una posible expansión y mejora en cobertura se podría migrar a la tecnología SIGFOX, ya que cuenta con un rango de cobertura mayor que se encuentra entre 20-50 km, la cual tendría un plus dentro de sus beneficios y así siendo atractiva para el mercado piscícola a grandes escalas.

También se realiza la observación del cambio de la tarjeta raspberry Pi 3B+ por un microcontrolador de propósito específico, ya que esta tarjeta de desarrollo es multipropósito y tendría un valor económico más elevado para un desarrollo comercial.

Para mencionar algún proyecto que cubra las mayores necesidades y posea mayor autonomía se puede encontrar el siguiente ejemplo, que comparte la visión de los proyectos "Monitoreo, adquisición y transmisión de datos en tiempo real, mediante IoT, de las variables medidas por un prototipo de caracterización de paneles fotovoltaicos y de medición de variables meteorológicas" y "Diseño e implementación de un sistema de monitoreo en estanques piscícolas basado en internet de las cosas (IoT)":

- ***Libelium-Thing+ LoRaWAN Smart Fish Farming Solution Kit***. cuenta con una variedad de sensores que mejoran y simplifican el monitoreo remoto del estado en que se encuentra el agua. Experimentos realizados en favorecer la productividad de la acuicultura, enumeran diferentes tipos de parámetros. El pH y los niveles de oxígeno disuelto hacen parte fundamental de estos parámetros. Además, se recomiendan otros rangos químicos dentro de cada estanque para proteger la vida de los peces, como el amonio y el nitrito, que son los primordiales cuadros de toxicidad creados por las heces de los propios peces (Marketplace, 2020).

*Figura 18*. LibeliumThing LoRaWAN Smart Fish Farming Solution Kit. Nota. Tomado de The IoT Marketplace. "Libelium-Thing+ LoRaWAN Smart Fish Farming Solution Kit" Recuperado de: https://www.the-iot-marketplace.com/libelium-thing-lorawan-smart-fish-farming-solution-kit.

# 5. Red IoT para fortalecer los sistemas LPWAN aplicado a las competencias investigativas dentro de la universidad industrial de santander.

En este capítulo se procede a realizar un modelo para una red IoT que cuente como base para la implementación de un campus laboratorio IoT en la Universidad Industrial de Santander para el desarrollo de nuevas aplicaciones.

## 5.1 Factores para tener en cuenta en la evaluación de tecnologías en el diseño de sistemas IOT.

Para realizar un diseño de manera efectiva de un producto conectado, los implicados deben primero la consideración de cómo manejará las transformaciones que la tecnología del IoT impone en el diseño de los productos dependiendo de su función en la cadena de comunicación. Esos nuevos requerimientos pueden, dar como resultado un cambio en la mentalidad del diseño final, las responsabilidades, las actividades de trabajo del diseño y de la administración (Avan, Jassawalla y Sashittal, 1998).

Para acoplarse a estas variaciones, la organización necesita avanzar, lo cual se puede lograr trabajando en: las personas, procesos, y tecnología. Es relevante prever que los cambios que transcurran en la organización no necesariamente deber ser exclusivos a un solo pilar. Más aún, con la gran auge de la innovación que estamos viviendo, se pueden cubrir estos tres aspectos, y cada una puede relacionarse con las otras (Brenna, Greg, Jonathan y Bob, 2016).

1. **Crecimiento**. Realizar una proyección de los costos iniciales y de la escalabilidad. Para la elección de la tecnología debe ser no sólo en el costo inicial, sino también en los nuevos costos de las tecnologías y dispositivos sean funcionales entre sí (Brenna, Greg, Jonathan y Bob, 2016).

2. **Avances tecnológicos**. Debe contar con un sistema que evolucione al pasar el tiempo, ya que se tendrían unos equipos obsoletos y perdida de capital invertido. Incurriendo en una nueva adquisición de un nuevo sistema y generando mayores costos de inversión (Brenna, Greg, Jonathan y Bob, 2016).

3. **Misión del sistema.** En sistemas de misiones críticas no se debe de depender de un solo fabricante, por lo que se debe contar a la mano otras opciones de marcas para los equipos a adquirir. Se debe evitar estar sujetos a las disposiciones del fabricante (Brenna, Greg, Jonathan y Bob, 2016).

Aparte de los ya nombrados, otro factor a tener en cuenta en el diseño de un sistema IoT y en la evaluación de las tecnologías a utilizar, es la comunicación. Esta comunicación está relacionada con muchos aspectos que dependen de su buen desempeño, se menciona principalmente la importancia de la capacidad de almacenamiento de energía para su correcto actuar. Los aspectos para considerar son los siguientes (Gonzales, 2017):

- Distancia entre el emisor y el receptor
- Naturaleza de los obstáculos
- Distorsión del ruido
- Regulaciones gubernamentales

De acuerdo con estos aspectos, tendremos que elegir las tecnologías y protocolos adecuados a cada contexto. En el caso de que solo necesitemos comunicarnos dentro de un edificio (dependiendo del tamaño), podemos usar las tecnologías Zigbee o WiFi. Lo cual es diferente si se habla de Smart Citys, o aplicaciones en las que las distancias entre dispositivos son del orden de kilómetros. Por lo tanto, se elige una tecnología LPWA (Gonzales, 2017).

## 5.2 Modelo de implementación de campus laboratorio en la Universidad industrial de Santander.

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

Acorde con la densa población estudiantil que alberga el campus universitario y la problemática que existe en relación con movilidad, control de accesos, estacionamientos (automóviles, motocicletas, bicicletas) y control de inventarios (biblioteca, equipos), entre otros. Radica la necesidad de plantear soluciones a cada una de ellas en base a las tecnologías presentadas en el presente documento. Por ejemplo, las bicicletas las cuales tiene un flujo de entrada al campus de aproximadamente 1011 bicicletas y de salida alrededor de 829 bicicletas por día, según datos recopilados en (Acosta y Merchan, 2017). Actualmente se cuenta con un sistema de ticket de papel impreso en cada una de las porterías, el cual se entrega con registro a lapicero, el color de la bicicleta y el género del propietario de la bicicleta al momento de entrar a las instalaciones de la universidad. Se ve la necesidad de realizar este proceso de una manera óptima y eficaz para ambas partes implicadas, ya que proceso genera:

1. **Basura**. Por lo que no son reutilizables (no cuidado con el medio ambiente).
2. **Perdida de ticket**. Las cuales incurren en realizar un proceso de toma de datos por parte del encargado al portador de la bicicleta, incurriendo así en pérdida de tiempo para las diferentes partes implicadas.

3. **¿Seguridad?** No hay verificación clara de propiedad del vehículo.

Para mejorar y optimizar este tipo de actividades, se proyecta “campus laboratorio” el cual desarrollaría soluciones para dichas problemáticas, así generando nuevos campos de acción e investigación para la universidad el cual se proyectaría a nivel regional y nacional.

Antes de entrar en materia de implementación es pertinente contemplar las bandas de frecuencias de operación de los diferentes dispositivos que son permitidas en el territorio colombiano. A continuación, se nombran las bandas de frecuencia a las cuales los diferentes entes de regulación tienen destinadas para las comunicaciones de este tipo.

**Banda de uso libre**: De acuerdo con el artículo 11 de la Ley 1341 de 2009 dispone que el Gobierno nacional podrá establecer bandas de frecuencias de uso libre, de acuerdo con las recomendaciones de la UIT (MinTic, 2009). Que la Resolución 2190 de 2003 del Ministerio de Tecnologías de la Información y las Comunicaciones atribuyó unas frecuencias radioeléctricas para su uso libre por parte del público en general, en aplicaciones de baja potencia y corto alcance de operación itinerante, y definió las características técnicas de operación para su utilización (MinTic, 2003).

Que la Resolución número 689 de 2004 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic, 2004), atribuyó unas bandas de frecuencia para su libre utilización dentro del territorio nacional, mediante sistemas de acceso y redes inalámbricas de área local que utilicen tecnologías de espectro ensanchado y modulación digital, de banda ancha y baja potencia.

Bandas de frecuencia: Se atribuyen dentro del territorio nacional a título secundario, para operación sobre una base de no interferencia y no protección de interferencia, los siguientes rangos de frecuencias radioeléctricas, para su libre utilización por sistemas de acceso y redes inalámbricas de área local, que empleen tecnologías de espectro ensanchado y modulación digital, de banda ancha, baja potencia, en las condiciones establecidas por esta resolución (MinTic, 2004).

a) Banda de 902 a 928 MHz

b) Banda de 2 400 a 2 483,5MHz

c) Banda de 5 150 a 5 250MHz

d) Banda de 5 250 a 5 350 MHz

e) Banda de 5 470 a 5 725 MHz

f) Banda de 5 725 a 5 850 MHz

Bandas de frecuencia para servicio móvil: Estas bandas son de uso privado por tal motivo es necesario contratar un servicio con alguno de los operadores, para el caso de Colombia son Claro, Movistar, Tigo, Etb, etc (MinTic, 2004).

Estos operadores funcionan sobre las bandas de:

a) Banda de 850MHz

b) Banda de 1900MHz

c) Banda AWS 1700/2100MHz

d) Banda 2500MHz

e) Banda 2500/2690MHz

Bandas de telemetría y control: Las condiciones operativas y las frecuencias y bandas de frecuencia para aplicaciones de telemetría y telecontrol se consulta en la resolución 711 de 2016 de la agencia nacional del espectro, ANE.

**5.2.1 Campus laboratorio.** Para acotar y dar una vía a las tecnologías IoT que actualmente se están trabajando a nivel nacional y que poseen características que sobresalen dentro de la geografía colombiana, se procede a plantear a LoRa, como las principal propuesta para el desarrollo del internet de las cosas al interior del campus universitario.

**5.2.2 Grupo de investigación CEMOS.** Por parte del grupo de investigación CEMOS, se plantea la creación de un "campus laboratorio", en el cual se permita crear aplicaciones que den solución a la problemáticas planteadas en el numeral 4.2 y demás no contempladas que tengan cabida en este tipo de soluciones tecnológicas. Por tal motivo se proyecta la creación de una red IoT que involucre routers, módulos IoT y cosas que constantemente estén comunicadas entre sí, para proporcionar información detallada de acuerdo con su actividad. Esta red IoT se gestionará a través de la red LAN de la universidad, que describe según (UIS, 2020) que cuenta con:

> *"una topología estrella, la cual contiene un switch core de alta capacidad que interconecta por medio de enlaces de fibra óptica los centros de cableado en cada uno de los edificios del campus y sedes de la universidad, los cuales a su vez cuentan con switches de borde y equipos access point outdoor e indoor para la conectividad de los usuarios. A la fecha, la red LAN institucional cuenta con aproximadamente 5000*

*computadores para profesores, estudiantes y empleados, 150 switches de borde, 90 Access Points's y 70 equipos servidores".*

**5.2.2.1 Implementación Campus Laboratorio.** Modelo en general de la implementación de Campus Laboratorio en la Universidad Industrial de Santander.

*5.2.2.1.1 Gateway.* Para la implementación de la red IoT se dispondrán de tres Gateways ubicados estratégicamente para dar cobertura al campus. El primer Gateway (Amarillo) estaría ubicado en el edificio de la facultad de ingenierías fisicomecánicas, el cual daría cobertura a la zona oeste. El segundo Gateway (Azul) estaría ubicado en el edificio de Biblioteca, el cual daría cobertura a la zona media y el tercer Gateway (Rojo) estaría ubicado en el auditorio Luis A. Calvo, dando cobertura a la zona este de la universidad, como se aprecia en la figura 19.

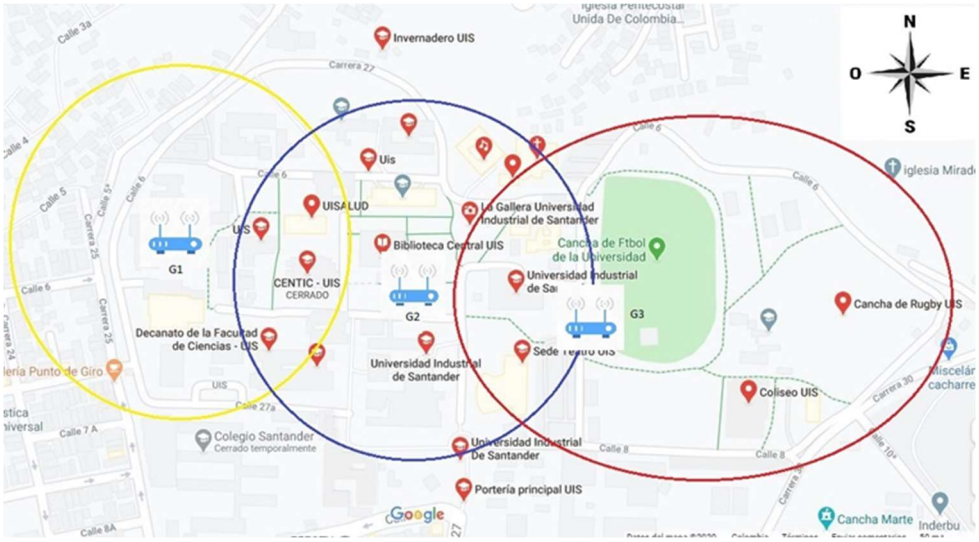


*Figura 19.* Ubicación de dispositivos en plano de la UIS. Nota. Tomado de Google. (2020) "mapa de la Universidad Industrial de Santander". Recuperado de: https://www.google.com/maps y modificado por el autor.

El Gateway 3 se plasma con una mayor cobertura hacia la zona de la cancha de Rugby debido a que la onda de propagación viaja con mayor facilidad, ya que no encuentra a su paso obstáculos como grandes edificios, los cuales si se encuentran en el radio de cobertura de los Gateways 1 y 2. Se estima el área del campus en Google Maps de aproximadamente 0.3 Kilometros cuadrados, los cuales constan de zonas verdes y carreteras. Los dispositivos G1, G2 Y G3 se ubican estratégicamente para dar cobertura a los módulos que se encuentra en los diferentes edificios. Toda esta red se controla mediante un centro de control. Cabe aclarar que, para el correcto funcionamiento de los Gateways, las directivas de la universidad deben facilitar un punto de conexión de internet de alto ancho de banda, debido a las grandes velocidades que se presentarán en el tráfico de información de los diferentes módulos.

A continuación, se muestra en la figura 20 el Gateway seleccionado y en la tabla 1 se expone las especificaciones técnicas.

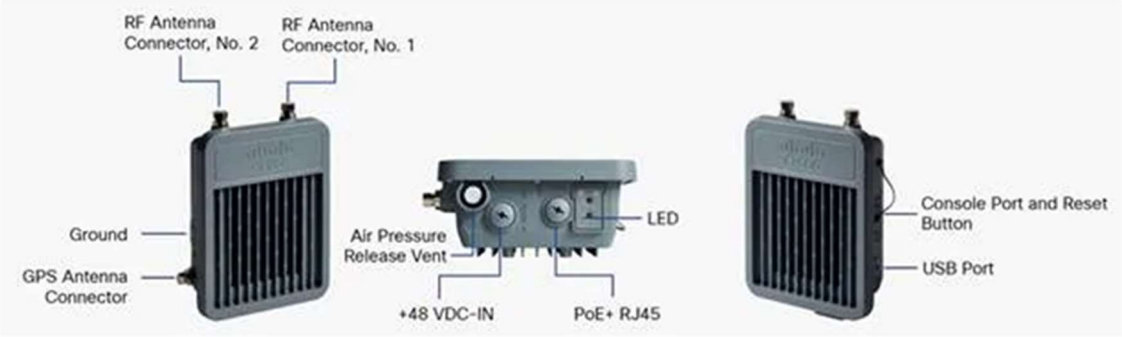


*Figura 20.* Cisco Wireless Gateway IXM-LPWA-900-16-K9. Nota. Tomado de Cisco. (2019) "Cisco Wireless Gateway for LoRaWAN Data Sheet. Recuperado". de: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheetc78737307.html

Especificaciones técnicas:

Tabla 1. Características de Gateway Cisco Wireless Gateway IXM-LPWA-900-16-K9.

| **Gateway** | *Cisco Wireless Gateway IXM-LPWA-900-16-K9* |
|---|---|
| **Tecnología** | LoRa |
| **Factor de Protección** | Exterior<br>IP 67 |
| **Sistema Operativo** | Linux Version 4.4.52 |
| **CPU** | 1.33 GHz, single core |
| **Memoria** | 1 GB DDR4 RAM |
| **Ethernet** | 1x 10/100 Mbps Fast Ethernet (RJ-45)<br>Support for PoE+ (802.3at) PD |
| **USB** | 1x USB 2.0, conector type A |
| **Consumo de potencia** | 30 Watts máximo |
| **Antena ANT-LPWA-DB-O-N-5** | Omnidireccional<br>5 dBi de ganancia<br>Rango de frecuencia de 863 - 928 MHz |
| **WI-FI** | 2.4 GHz/5 GHz 802.11n |

*Nota:* Tomado de Cisco. (2019) "Cisco Wireless Gateway for LoRaWAN Data SheetRecuperado". de: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheetc78737307.html y modificado por el autor.

*5.2.2.1.2 Módulos.* Para la implementación de los módulos IoT se debe realizar un previo análisis del tipo de variables a procesar, tamaño, velocidad de recepción y trasmisión, por lo tanto, se muestran a continuación módulos actualmente comerciales, unos más robustos que otros.

- LILYGO® TTGO T-Call V1.3 ESP32 Wireless Module GPRS Antenna SIM Card SIM800L Module

*Figura 21.* LILYGO® TTGO T-Call V1.3 ESP32 Wireless Module GPRS Antenna SIM Card SIM800L Module. Nota. Tomado de AliExpress. (2020). "LILYGO® TTGO T-Call V1.3 ESP32 Wireless Module GPRS Antenna SIM Card SIM800L Module" Recuperado de: https://www.aliexpress.com/item/33045221960.html?srcSns=sns_WhatsApp&tid=white_background_101&spreadType=socialShare&tt=sns_WhatsApp&image=H021e681b6d8c4fe6838b9af0bed11bc1r.jpg&aff_request_id=4edf4aaae2204f74be55122464653b6e158904168747404824_d7Vwm2r&aff_platform=default&sk=_d7Vwm2r&aff_trace_key=4edf4aaae2204f74be55122464653b6e158904168747404824_d7Vwm2r&businessType=ProductDetail&title=COP+50%2C973.21++5%EF%BC%85+dto.+%7C+LILYGO%C2%AETTGO+tcall+V1.3+ESP32+m%C3%B3dulo+inal%C3%A1mbrico+GPRS+antena+SIM+tarjeta+SIM800L+m%C3%B3dulo&platform=AE&terminal_id=75c26a7d0cb544e8844334e3cce8c114

Tabla 2. Características de LILYGO® TTGO T-Call V1.3 ESP32 Wireless Module GPRS Antenna SIM Card SIM800L Module.

| Módulo | LILYGO® TTGO T-Call V1.3 ESP32 Wireless Module GPRS Antenna SIM Card SIM800L |
|---|---|
| Sistema Operativo | FreeRTOS |
| CPU | ESPRESSIF-ESP32 240MHz Xtensa® single-/dual-core 32- LX6 microprocesador |
| Memoria | FLASH: QSPI flash 4MB / PSRAM 8MB<br>SRAM: 20 kB SRAM |
| Protocolos | IPv4, IPv6, SSL, TCP/UDP/HTTP/FTP/MQTT |
| USB | Tipo-C |
| Consumo de potencia | 5 Watts máx |
| Encriptado | AES/RSA/ECC/SHA |
| WI-FI Backhaul | 802.11 b/g/n(802.11n, speed up to150Mbps)A-MPDU and A-MSDU: polymerization, support 0.4μS Protection interval |

*Nota:* Tomado de AliExpress. (2020). "LILYGO® TTGO T-Call V1.3 ESP32 Wireless Module GPRS Antenna SIM Card SIM800L Module" Recuperado de:https://www.aliexpress.com/item/33045221960.html?srcSns=sns_WhatsApp&tid=white_background_101&spreadType=socialShare&tt=sns_WhatsApp&image=H021e681b6d8c4fe6838b9af0bed11bc1r.jpg&aff_request_id=4edf4aaae2204f74be55122464653b6e158904168747404824_d7Vwm2r&aff_platform=default&sk=_d7Vwm2r&aff_trace_key=4edf4aaae2204f74be55122464653b6e158904168747404824_d7Vwm2r&businessType=ProductDetail&title=COP+50%2C973.21++5%EF%BC%85+dto.+%7C+LILYGO%C2%AETTGO+tcall+V1.3+ESP32+m%C3%B3dulo+inal%C3%A1mbrico+GPRS+antena+SIM+tarjeta+SIM800L+m%C3%B3dulo&platform=AE&terminal_id=75c26a7d0cb544e8844334e3cce8c114 y modificado por el autor.

*Módulos de marcas más comerciales.* En otra perspectiva de implementación de módulos con funcionalidades IoT, nombramos a las tarjetas de desarrollo de tipo general como Arduino y

Raspberry Pi, que cuentan con una programación sencilla y gran variedad de sensores y actuadores que facilitan su despliegue en proyectos a bajo costo.

- Aduino nano 33 IoT.

*Figura 22.* Arduino Nano 33 IoT. Nota. Tomado de Arduino. (2020). "ARDUINO NANO 33 IOT". Recuperado de: https://store.arduino.cc/usa/nano-33-iot.

Especificaciones técnicas:

Tabla 3. Características de Arduino nano 33 IoT.

| **Módulo** | **ARDUINO NANO 33 IOT** |
|---|---|
| **Pines** | 33 |
| **CPU** | SAMD21 Cortex®-M0+ 32bit low power ARM MCU |
| **Memoria** | CPU Flash Memory 256KB<br>SRAM 32KB |
| **Interfaz de Comunicación** | USB UART SPI I2C |
| **Conectores** | Native in the SAMD21 Processor |
| **Consumo de potencia** | 0.2 Watts |
| **Bluetooth** | Bluetooth module based on ESP32 |
| **Conversor** | Analog Input Pins: 8 (ADC 8/10/12 bit)<br>Analog Output Pins: 1 (DAC 10 bit) |
| **WI-FI** | 802.11 b/g/n wireless LAN |

*Nota:* Tomado de Arduino. (2020). "ARDUINO NANO 33 IOT". Recuperado de: https://store.arduino.cc/usa/nano-33-iot

- Raspberry Pi Zero W.

Figura 23. Raspberry Pi Zero W. Nota. Tomado de Raspberry Pi. (2020). "Raspberry Pi Zero W". Recuperado de: https://www.raspberrypi.org/products/raspberry-pi-zero-w/

Tabla 4. Características de Raspberry Pi Zero W.

| **Módulo** | **Raspberry Pi Zero W** |
|---|---|
| **Pines** | HAT-compatible 40-pin header |
| **CPU** | 1GHz, single-core |
| **Memoria** | 512MB RAM |
| **Comunicación** | TCP y UDP |
| **Conectores** | Mini HDMI and USB On-The-Go ports<br>Micro USB power<br>CSI camera connector |
| **Consumo de potencia** | 1.19 Watts |
| **Bluetooth** | Bluetooth 4.1<br>Bluetooth Low Energy (BLE) |
| **WI-FI** | 802.11 b/g/n wireless LAN |

Nota: Tomado de Raspberry Pi. (2020). "Raspberry Pi Zero W". Recuperado de: https://www.raspberrypi.org/products/raspberry-pi-zero-w/

Por otro lado, se pueden encontrar en el mercado dispositivos como los enunciados en el capítulo 3, que ayudarían a un mejor cuidado y protección de la vida humana y animal. Estos podrían implementarse dentro de la red al servicio del sistema de prevención y control de incendios (Nest Protect), que actualmente algunos edificios no cuentan con las instalaciones exigidas por la norma NSR-10 Título J. Con el Libelium-Thing+ LoRaWAN Smart Fish Farming Solution Kit, tendría un impacto positivo en el sensado de los niveles de Ph y niveles de oxígeno de los estanques, ya que en ocasiones emanan olores fuertes que generan desagrado a la comunidad universitaria.

*5.2.2.1.3 Configuración*. Consiste básicamente en la configuración de los módulos a través de los puertos por los cuales permita la comunicación vía WI-FI integrado a cada dispositivo, por el cual se ejecuta la comunicación con internet. También se requiere de la configuración del Gateway, en la recepción y transmisión de datos de los módulos y posterior envío a la nube IoT.

A continuación, se muestra en la figura 21 un diagrama de conexión el cual sirve como modelo para ejemplificar la comunicación entre dispositivos.

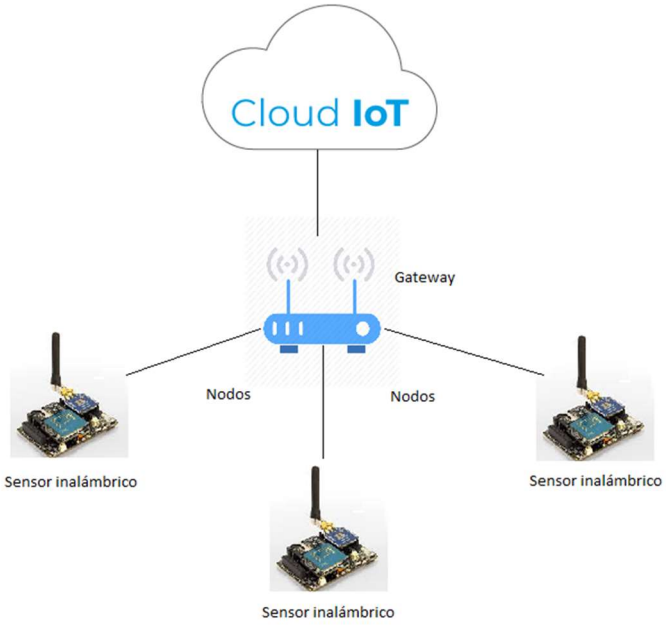


*Figura 24.* Diagrama de comunicación entre dispositivos. Nota. Tomado de Sanchez, M. (2015). "Redes de sensores inalámbricos (sector cuaternario)". Recuperado de: https://migueysanchez.wordpress.com/2015/09/29/redesdesensoresinalambricossectorcuaternario/ y modificado por el autor.

Nota: Para un análisis detallado acerca de la programación de Gateways, módulos, nodos y demás dispositivos que intervengan en la proyección de la red IoT al interior de la Universidad Industrial de Santander queda a disposición de trabajos de grado futuros, ya que no es el alcance de este proyecto de grado.

*5.2.2.1.4 Plataforma Web*. Consiste en implementar una plataforma web administrativa, la cual cumpla la función de la gestión de datos provenientes de la nube IoT. Esta plataforma contendría un registro de usuario e inicio de sesión, los cuales se les permita obtener información detallada de los datos contenidos en la nube, para posterior análisis mediante gráficos o tablas. También incluir la configuración remota de gateways para su administración.

# 6. Conclusiones

Dentro de las características principales de cobertura, nivel de madurez y bandas de frecuencia de las tecnologías LPWA descritas en el capítulo I, y los despliegues de redes en Colombia mencionados en el capítulo II, las tecnologías SigFox, LoRa y NB-IoT, son las más apropiadas de acuerdo a sus características, pero LoRa sobresale por sus múltiples dispositivos de robustez variada para la implementación proyectos IoT en la república de Colombia.

Una universidad inteligente es aquella que a través de la tecnología busca optimizar el uso de los recursos físicos, económicos y ambientales y mejorar la calidad de vida de sus habitantes. Por tanto, más que definir el término universidad inteligente, el objetivo es que sea gente inteligente, entendiendo el término como la posibilidad de que la persona acceda a los servicios que ofrece la tecnología de manera equitativa y que ésta resulte útil y confiable para facilitar sus tareas y problemas diarios.

Como conclusión final de este proyecto, se crea un modelo a grandes razgos de red IoT que sirve de guía al grupo de investigación CEMOS, en fortalecer e innovar en el desarrollo de proyectos a nivel científico en el tema del internet de las cosas (IoT) dentro de los parámetros legales; ya que uso comercial no se encuentra regulado.

## 7. Investigaciones Futuras

El planteamiento de Universidad Inteligente se da a partir de la visión de expandir y escalar estos tipos de proyectos, ya que la Universidad Industrial de Santander es referencia a nivel regional y nacional. Con Aportes de las diferentes universidades que trabajan en la temática de IoT y con un trabajo en conjunto, se podrían desarrollar grandes proyectos que generen desarrollo social, económico, educativo y empresarial, lo cual cumple con los objetivos expresados por el MinTIC de implementación de ciudades inteligentes.

## Referencias bibliografícas


§ 15 U.S.C. 1681s-2. (2015). "*Equipment Authorization*, *FED. COMM. COMM'N"*. Oct. 21, 2015. Recuperado de: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

16 C.F.R. §§ 660.1–4. (2015). *"Equipment Authorization, FED. COMM. COMM'N"*. Oct. 21, 2015. Recuperado de: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

330ohms. (2017). *¿Qué es SigFox y cómo funciona?* Recuperado de https://blog.330ohms.com/2017/05/11/que-es-sigfox-y-como-funciona/

330ohms. (2018). *"¿Qué es LoRa y LoRaWAN?. Una tecnología LPWAN para IoT*". Recuperado de https://www.indelmar.com/?p=1174

3GPP. (2015). "*TR 45.820: Cellular system support for ultralow complexity and low throughput Internet of Things (CIoT)".*

47 C.F.R. § 15.3(n). (2015). *"Equipment Authorization, FED. COMM. COMM'N".* Oct. 21, 2015. Recuperado de: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

5GAMERICAS. (2019). *"Espectro en américa latina y el caribe para 5G: Bandas medias y altas."* Mayo de 2019.

accent-systems. (2017). La revolución del mundo conectado ¿qué es narrowband-iot?. Recuperado de https://accent-systems.com/es/nb-iot/

Accessing Spectrum. (2017). "*FED. COMM. COMM'N"*. Recuperado de: https://www.fcc.gov/general/accessing-spectrum (last accessed July 3, 2017).

ACSWireless. (2016). *"Telensa Street Light Controls".* Recuperado de: http://www.advanced-cx.com/telensa.

Actility: ThingPark Wireless. (2020). Recuperado de https://lpwanmarket.com/shop/platforms/actility-thingparkwireless/

AliExpress. (2020). "LILYGO® TTGO T-Call V1.3 ESP32 Wireless Module GPRS Antenna SIM Card SIM800L Module" Recuperado de: https://www.aliexpress.com/item/33045221960.html?srcSns=sns_WhatsApp&tid=white_backgroup_101&spreadType=socialShare&tt=sns_WhatsApp&image=H021e681b6d8c4fe6838b9af0bed11bc1r.jpg&aff_request_id=4edf4aaae2204f74be55122464653b6e158904168747404824_d7Vwm2r&aff_platform=default&sk=_d7Vwm2r&aff_trace_key=4edf4aaae2204f74be55122464653b6e-1589041687474-04824-_d7Vwm2r&businessType=ProductDetail&title=COP+50%2C973.21++5%EF%BC%85+dto.+%7C+LILYGO%C2%AETTGO+tcall+V1.3+ESP32+m%C3%B3dulo+inal%C3%A1mbrico+GPRS+antena+SIM+tarjeta+SIM800L+m%C3%B3dulo&platform=AE&terminal_id=75c26a7d0cb544e8844334e3cce8c114

Andreev, S. (2015). "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap". In: IEEE Communications Magazine 53.9, pp. 32–40.

Andreev, S. (2015). "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap". In: IEEE Communications Magazine 53.9, pp. 32–40.

ANE. Agencia nacional del espectro. Colombia. (2020). Recuperado de: https://www.mintic.gov.co/portal/inicio/Ministerio/InstitucionesRelacionadas/Agencia-Nacional-del-Espectro-ANE/

Angulo. C y Muñoz. E. (2019). "Monitoreo, adquisición y transmisión de datos en tiempo real, mediante IoT, de las variables medidas por un prototipo de caracterización de paneles fotovoltaicos y de medición de variables meteorológicas". Universidad Industrial de Santander.

Arduino. (2020). "ARDUINO NANO 33 IOT". Recuperado de: https://store.arduino.cc/usa/nano-33-iot

Aref, M and Sikora, A. (2014). “Free space range measurements with Semtech Lora technology”. In: 2nd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems, pp. 19–23.

ASUS. Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk, FED. TRADE COMM’N. Feb. 23, 2016, Recuperado de: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

Auctiondata. 14 de mayo de 2019. Recuperado de https://auctiondata.fcc.gov/public/projects/auction102

Augustin, A. (2016). “A Study of LoRa: Long Range & Low Power Networks for the Internet of Things”. In: Sensors 16.9.

Avan R. and Sashittal, C. (1998). “An examination of collaboration in high-technology new product development processes”. Journal of Product Innovation Management 15(3), pp. 237–54.

Bliznakoff, D. (6 de noviembre de 2014). IoT: Tecnologías, usos, tendencias y desarrollo futuro, pp.20-21.

Bor, M., Vidler, J. and Roedig, U. (2016). “LoRa for the Internet of Things”. En: Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks. EWSN’16. pp. 361–366.

Brian, L. (Agosto 16 de 2018). “Rise of the machines, and the options for connecting them”. Recuperado de https://www.ciena.com/insights/articles/Rise-of-the-connected-machines-and-the-options-for-connecting-them.html

CAN-SPAM Act: A Compliance Guide for Business, FED. TRADE COMM’N Sep. 2009, Recuperado de: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

Cave, M., Doyle, C., & Webb, W. (2007). Essentials of modern spectrum management. New York: Cambridge; New York. Cambridge University Press.

Cisco. (2019) “Cisco Wireless Gateway for LoRaWAN Data SheetRecuperado”. de: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/datasheet-c78-737307.html

Commission Finds LabMD Liable for Unfair Data Security Practices, FED. TRADE COMM’N. July 29, 2016, Recuperado de: https://www.ftc.gov/news-events/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices;

Complying with COPPA: Frequently Asked Questions, FED. TRADE COMM’N. Mar. 20, 2015, Recuperado de: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

Complying with the FTC’s Health Breach Notification Rule, FED. TRADE COMM’N Apr. 2010, Recuperado de: https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

De miguel, F. (12 septiembre 2017). Tecnologías LPWA en el contexto del IoT, EC-GSM-IoT: mayor cobertura GSM para el Internet de las cosas. Recuperado de https://www.teldat.com/blog/es/tecnologias-lpwa-en-el-contexto-del-iot/

D-Link. Case alleges inadequate Internet of Things security practices, FED. TRADE COMM’N. Jan. 5, 2017, Recuperado de: https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internetthings-security.

D-Link. case alleges inadequate Internet of Things security practices, FED. TRADE COMM’N. Jan. 5, 2017. Recuperate de: https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet things-security.

DNP. “Departamento Nacional de Planeación, Plan Nacional de Desarrollo” 2014-2018: Todos por un nuevo país, vol. Tomo 1 y 2, G. d. C. y. R. Públicas, Ed., Bogotá, 2015.

e.g. Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users’ Profile Information, FED. TRADE COMM’N (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state charges-resulting; Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data, FED. TRADE COMM’N (Jan. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/dental-

practice-software-provider-settles-ftc-charges-it-misled; Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates, FED. TRADE COMM'N. Dec. 21, 2015, Recuperado de: https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java.

E.g., VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent, FED. TRADE COMM'N. Feb. 6, 2017, Recuperado de: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

Egomexico. ¿Cómo funciona la tecnología de identificación por radio frecuencia RFID?01 de noviembre de 2016. Recuperado de: http://www.egomexico.com/tecnologia_rfid.htm

Ekaterina, N. (03 de junio de 2018). "Proyectos IoT que cambiarán el mundo". Recuperado de https://apiumhub.com/es/tech-blog-barcelona/proyectos-iot/. Tendencias tecnológicas.

El Grupo T&T y CODENSA se preparan para enfrentar el despliegue masivo del IoT. (28 de septiembre de 2018). Universidad Nacional de Colombia, sede Medellín, Grupo T&T. Investigación en teleinformática y teleautomática. Recuperado de http://grupotyt.medellin.unal.edu.co/noticias/72-el-grupo-t-t-y-codensa-se-preparan-para-enfrentar-el-despliegue-masivo-del-iot

El primer laboratorio de IoT en Colombia abre sus puertas. (31 de octubre de 2019). Redacción Tecnósfera. Recuperado de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/asi-es-el-primer-laboratorio-de-internet-de-las-cosas-que-funciona-en-colombia-429252

Ellatif, A., Fabienne N., Mohamad, M., jean-christophe, P. and Wael, A. (2018). "Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and Supported Mobility. IEEE Communications Surveys & Tutorials". PP. 10.1109/COMST.2018.2877382.

Equipment Authorization – RF Device, FED. COMM. COMM'N. Oct. 21, 2015. Recuperado de: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

Equipment Authorization – RF Device, FED. COMM. COMM'N., last accessed June 20, 2017. Recuperado de: https://www.fcc.gov/oet/ea/rfdevice.

Equipment Authorization Procedures, FED. COMM. COMM'N. Oct. 21, 2015. Recuperado de: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

Equipment Authorization Procedures, FED. COMM. COMM'N., last accessed June 20, 2017. https://www.fcc.gov/general/equipment-authorization-procedures#sec1

Equipment Authorization Procedures, FED. COMM. COMM'N., last accessed June 20, 2017. Recuperado de: https://www.fcc.gov/general/equipment-authorization-procedures#sec1

Ergeerts, G. (2015). "DASH7 Alliance Protocol in Monitoring Applications". In: 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp. 623–628.

ETSI. Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods. 2012. Recuperado de: http://www.etsi.org/deliver /etsie/300200300299/30022001/02.04.0140/en30022001v020401o.pdf.

F Institutions and C. Information: Complying with the Safeguards Rule, FED. TRADE COMM'N. Apr. 2006, Recuperado de: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutionscustomer-information complying#how.

FCC, Auction 101: Spectrum Frontiers – 28 GHz. 2018. Recuperado de: https://www.fcc.gov/auction/101/factsheet#keydates

FCC, Tercer Informe y Orden, Opinión y Orden de Memorándum, y Tercer Nuevo Aviso de Propuesta de Establecimiento de Reglas. 14 de mayo de 2019. Recuperado de: https://auctiondata.fcc.gov/public/projects/auction101

FCC, Tercer Informe y Orden, Opinión y Orden de Memorándum, y Tercer Nuevo Aviso de Propuesta de Establecimiento de Reglas. 2018. Recuperado de: https://docs.fcc.gov/public/attachments/FCC-18-73A1.pdf

FCC. A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, FED. TRADE COMM'N July, 2008, Recuperado de: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

FCC. Avoiding Spam: Unwanted Email and Text Messages, FED. COMM. COMM'N. Feb. 22, 2016, Recuperado de: https://transition.fcc.gov/cgb/consumerfacts/canspam.pdf.

FCC. Fourth Report and Order. 2018. Recuperado de: https://docs.fcc.gov/public/attachments/FCC-18-180A1.pdf

FCC. Segundo Aviso Adicional de Propuesta de Reglamentación para Espectro Milimétrico Superior a los 24 GHz. 2017. Recuperado de: https://docs.fcc.gov/public/attachments/FCC-17-152A1.pdf

FCC. The FCC's 5G FAST Plan. Washington. 2018. Recuperado de: https://www.fcc.gov/5G

Final Rule in the Matter of Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions, No. 12-268, 79 FR 48441, 48444 (Aug. 15, 2014).

Financial Institutions and Customer Information: Complying with the Safeguards Rule, FED. TRADE COMM'N. Apr. 2006, Recuperate de: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (quotation marks omitted).

Finnegan, J. and Brown, S. (12 de febrero de 2018). "A Comparative Survey of LPWA Networking". Maynooth University.

FIWOO. Plataformas IoT. 28 de noviembre de 2016. Recuperado de: https://secmtic.com/plataforma-iot

FTC. Approves Final Order Settling Charges Against TRENDnet, Inc., FED. TRADE COMM'N. Feb. 7, 2014, Recuperado de: https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

FTC. Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network, FED. TRADE COMM'N. Mar. 30, 2011. Recuperado de: https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

FTC. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, FED. TRADE COMM'N. June 2017, Recuperado de: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step6.

Google. (2020) "mapa de la Universidad Industrial de Santander". Recuperado de: https://www.google.com/maps

Goursaud, C. and Gorce, J-M. (Oct. 2015). "Dedicated networks for IoT: PHY / MAC state of the art and challenges". In: EAI endorsed transactions on Internet of Things.

Hacking linux. WiMAX que es y para qué sirve? 9 de abril de 2009. Recuperado de: https://hackinglinux.wordpress.com/2009/04/09/wimax-que-es-y-para-que-sirve/

HHS. The Security Rule, U.S. DEP'T OF HEALTH & HUMAN SERV. May 12, 2017, Recuperado de: https://www.hhs.gov/hipaa/for-professionals/security/index.html.

Internet of Things: Privacy & Security in a Connected World, FED. TRADE COMM'N 31–32. Jan. 27, 2015, Recuperado de: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

IoT. Manual pc. ¿Qué es 5G? 29 de agosto de 2019. Recuperado de: http://www.manualpc.com/que-es-5g/

IoT. Temas tecnologicos. ¿Que son las redes móviles? 05 de octubre de 2016. Recuperado de: http://www.temastecnologicos.com/redes-moviles.html

IUT. Recomendación UIT-R M.2083-0. Concepción de las IMT – Marco y objetivos generales del futuro desarrollo de. Ginebra.

IUT. Sentando las bases para la 5G: Oportunidades y desafíos. Ginebra. Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-S.pdf

J. Armand, The Spectrum Handbook, Summit Ridge Group 12 Aug. 2013.

James C. Miller III, FTC Policy Statement on Deception, FED. TRADE COMM'N. Oct. 14, 1983, Recuperado de: https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf

K 47 C.F.R. §§ 2.1–1400. Equipment Authorization, FED. COMM. COMM'N. Oct. 21, 2015. Recuperado de: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

Ley 1341 de 2009. (2009). MinTIC. Recuperado de https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009

Libelium. (2015). Waspmote Sigfox Networking Guide.

Lin, A. X., Adhikary, Y. P. and Wang, E. (2016). "Random Access Preamble Design and Detection for 3GPP Narrowband IoT Systems". In: IEEE Wireless Communications Letters 5.6, pp. 640–643.

Llamazares, J. C. eco joven. 12 de agosto de 2016. Recuperado de: http://www.ecojoven.com/dos/03/RFID.html

Low Power networks hold the key to IoT. (16 June 2015). Rethink Research. Rethink Technology Research Ltd. Recuperado de https://rethinkresearch.biz/report/low-power-networks-hold-the-key-to-iot/

Lozano, M. (2019). "Diseño e implementación de un sistema de monitoreo en estaciones piscícolas basado en el internet de las cosas (IoT)". Universidad Industrial de Santander.

LTE-M, la evolución de las máquinas. (2017). accent-systems. Recuperado de https://accent-systems.com/es/ltem/.

LTE-M. (2017). LTE-M in a nutshell, LTE-M at a glance. Orange Developer. Recuperado de https://developer.orange.com/orange_explains/lte-m-in-a-nutshell/

M. Michael. “The Internet of Things”. 2014.

MB/S GREEN-OFDM IOT. (05 de Abril de 2018). Eurocps. Recuperado de https://www.eurocps.org/innovators-projects/ongoing-projects/mbs-green-ofdm-iot/

Medium. (2019). What is NBIoT?. DeCode Staff. Recuperado de https://medium.com/decodein/what-is-nbiot-7d4cebd753cf

Millonaria inversión de Claro a soluciones IoT en servicios públicos. (27 de junio de 2019). Portafolio. Recuperado de https://www.portafolio.co/negocios/millonaria-inversion-de-claro-a-soluciones-iot-en-servicios-publicos-531053

MinTIC, “Política de Tecnologías de la Información y las Comunicaciones para Ciudades y/o Territorios Inteligentes”, Bogotá, 2014.

MinTIC. (2017). “MinTIC revela los primeros resultados del Observatorio de Economía Digital”. Recuperado de https://www.mintic.gov.co/portal/604/w3-article-61929.html”.

MinTIC. (2018). “Plan TIC 2018 – 2022, El futuro digital es de todos”. Recuperado de https://www.mintic.gov.co/portal/604/articles-101922_Plan_TIC.pdf

MinTIC. (2020). “Todos por un nuevo país. Paz, equidad y educación”. Misión y Visión. Recuperado de https://www.mintic.gov.co/portal/inicio/3870:Mision-y-Vision

Musey, J. A. (11 Aug. 2013). “The Spectrum Handbook”. Summit Ridge Group.

Myspace Settles, FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers, FED. TRADE COMM’N. May 8, 2012, Recuperado de:

https://www.ftc.gov/news-events/press-releases/2012/05/myspace-settles-ftc-charges-it-misled-millions-users-about.

Naciones unidas. (2018). “UN E-Goverment Knowledgebase”. Recuperado de: https://publicadministration.un.org/egovkb/en-us/#.WgMZJq-GO71

Navarro, J., Jimenez, L., Huerta, F., Jimenez, C., Rodriguez. y N., Huerta, F. (2016). “Predicciones de Tecnología, Medios de Comunicación y Telecomunicaciones”. Deloltte University Press. Pág 77.

NB-Fi LPWAN Technology - Products and Tech Description. (2016). Recuperado de http://dgmatics.com/wp.pdf.

Nest Protect (Battery) 2nd Generation. (2020). Verizonwireless. Recuperado de https://es.verizonwireless.com/products/nest-protect-smoke-and-carbon-monoxide-alarm-battery/

Nokia. LTE-M - Optimising LTE for the Internet of Things. 2015.

NW1000 Data Sheet. (2015). Nwave. Recuperado de http://nwave.io/wp-content /uploads/2015/09/NWave1000Datasheet0r3.pdf.

Nwave: How it works. (2016). Nwave. Recuperado de http://www.nwave.io/how-it-works/

Online Advertiser Settles FTC, Charges ScanScout Deceptively Used Flash Cookies to Track Consumers Online, FED. TRADE COMM’N. Nov. 8, 2011, Recuperado de: https://www.ftc.gov/news-events/press-releases/2011/11/online-advertiser-settles-ftc-charges-scanscout-deceptively-used.

Penagos, J. (Noviembre de 2017). “Smart Grid, Medición Inteligente e Internet de las Cosas Palancas críticas de competitividad y progreso en Colombia”. Orion Infinity. Revista CIDET.

Petajajarvi, J. (2015) “On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology”. In: 14th International Conference on ITS Telecommunications (ITST), pp. 55–59.

process for US companies to satisfy the EU’s data protection requirements so as to be eligible to receive personal information about EU data subjects. The Framework required companies to self-certify that they fulfilled 7 principles: notice, choice, onward transfer, security, data integrity, access, and enforcement. The FTC policed companies who claimed they complied with US-EU Safe Harbor through its Section 5 authority. On October 6, 2015, the European Court of Justice invalidated the Safe Harbor framework. The Safe Harbor framework has since been replaced with the Privacy Shield framework. See also, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, FED. TRADE COMM’N. Nov. 29, 2011, Recuperate de: https://www.ftc.gov/news events/press-releases/2011/11/facebook-settles-ftc-charges-itdeceivedconsumers-failing-keep 45

Raspberry Pi. (2020). “Raspberry Pi Zero W”. Recuperado de: https://www.raspberrypi.org/products/raspberry-pi-zero-w/

Ratasuk, R. (2016). “NB-IoT system for M2M communication”. In: IEEE Wireless Communications and Networking Conference, pp. 1–5.

Ray, T. (2019). “Implementación de un sistema de seguridad IoT”. Universidad Industrial de Santander.

Raza, U., Kulkarni, P. and Sooriyabandara, M. (2017). “Low Power Wide Area Networks: An Overview”. In: IEEE Communications Surveys Tutorials PP.99, pp. 1

RedGPS se integra con SIGFOX. (Mayo 30 de 2018). RedGPS. Recuperado de https://www.redgps.com/blog-noticias/sigfox-en-redgps-106

Report of the Interference Protection Working Group, FED. COMM. COMM’N. SPECTRUM POLICY TASK FORCE 1. (Nov. 15, 2002). FCC. Recuperado de https://transition.fcc.gov/sptf/files/IPWGFinalReport.pdf.

Resolución 2190 de 2003. (2003). MinTIC. Recuperado de https://www.mintic.gov.co/portal/inicio/6604:Resolucion-2190-de-2003

Resolución 689 de 2004. (2004). MinTic. Recuperado de https://normograma.mintic.gov.co/mintic/docs/resolucion_mincomunicaciones_1689_2007.htm

Reynders, B., Meert, W. and Pollin, S. (2016). “Range and coexistence analysis of long-range unlicensed communication”. In: 23rd International Conference on Telecommunications (ICT), pp. 1–6.

RF. (2018). “¿Qué es la tecnología RPMA?”. Equipo editorial - todo RF. Recuperado de https://www.everythingrf.com/community/what-is-rpma-technology.

Rico, A. A. (2016). “An overview of 3GPP enhancements on machine to machine communications”. In: IEEE Communications Magazine 54.6, pp. 14– 21.

S. Daniel, H. Woodrow, The FTC and the New Common Law of Privacy, 114 COLUMBIA L. REV. 583 (2014), Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

S. Hilton, Dyn Analysis Summary of Friday October 21 Attack, DYN. Oct. 26, 2016, Recuperate de: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

Sanchez, M. (2015). “Redes de sensores inalámbricos (sector cuaternario)”. Recuperado de: https://migueysanchez.wordpress.com/2015/09/29/redes-de-sensores-inalambricos-sector-cuaternario/

Schatsky, D. and Trigunait, A. (2016). “Internet of Things, Dedicated networks and edge analytics will broaden adoption”. Deloltte University Press. Pág 3.

Scott, D. (13 December 2016). The Baltimore Sun. "Annapolis-based Link Labs raises $5.7 million to grow 'the Internet of things". Recuperado de https://www.baltimoresun.com/business/bs-bz-link-labs-20150821-story.html

See generally, In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, FED. COMM. COMM’N., Mar. 21, 2013. Recuperado de: https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-34A1.pdf.

Sigfox lleva su red IoT a Colombia. (29 de agosto de 2016). TyN Magazine. Recuperado de http://www.tynmagazine.com/sigfox-lleva-su-red-iot-a-colombia/

Sniderman, B., Gorman, G., Holdowsky J., Mariani, J. and Dalton, B. (September 12, 2016). "The design of things: Building in IoT connectivity. The Internet of Things in product design" Deloitte University Press.

Song, S. Rey-Moreno, C. Jensen, M. "Innovaciones en la gestión del espectro". Internet society

Summary of the HIPAA Privacy Rule, U.S. DEP'T OF HEALTH & HUMAN SERV. July 26, 2013, Recuperado de: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Symphony Link™ A revolutionary wireless system for wide-area IoT networks. (17 septiembre de 2016). link-labs. Recuperado de https://www.link-labs.com/symphony.

Technology Assessment: Internet of Things, U.S. GOV. ACC. OFFICE at 4–5.

Technology Assessment: Internet of Things, U.S. GOV. ACC. OFFICE at 4–5. 2015.

Tecnología. RFID. 12 de julio de 2016. Recuperado de: http://www.areatecnologia.com/electronica/rfid.html

Telegeography. Clock phase of FCC 24GHz concludes; falls just short of USD2bn. Recuperado de: https://www.telegeography.com/products/commsupdate/articles/2019/04/18/clock-phaseof-fcc-24ghz-concludes-falls-just-short-of-usd2bn/

Telensa's complete IoT solution. (2015). iot-now. Recuperado de https://www.iot-now.com/2015/07/07/34596-building-smarter-cities-with-low-power-radio-networks/

The IoT Marketplace. (2020). "Libelium-Thing+ LoRaWAN Smart Fish Farming Solution Kit". Recuperado de https://www.the-iot-marketplace.com/libelium-thing-lorawan-smart-fish-farming-solution-kit

The world's leading service provider for Internet of Things (IoT). (Enero de 2020). SigFox. Recuperado de https://www.sigfox.com/en.

ThingPark Wireless: IoT network platform for operators, the market leading, most complete, powerful and flexible multi-technology LPWA IoT Network platform. (15 de enero de 2019). Actility. Recuperado de https://www.actility.com/public-iot-connectivity-solutions/

UIS. (2020). "Infraestructuta tecnológica" Recuperado de: https://www.uis.edu.co/webUIS/es/administracion/serviciosInformacion/infraestructuraTecnologica.html

UIT. All about the Technology. 04 de abril de 2011. Recuperado de: http://www.itu.int/osg/spu/ni/3G/technology/

UIT. ITU global standard for international mobile telecommunications ´IMT-Advanced´. julio de 2016. Recuperado de: http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-adv/Pages/default.aspx

UIT. Unión Internacional de Telecomunicaciones. 2020. Recuperado de: https://www.itu.int/es/Pages/default.aspx

UNB Wireless. (2016). Telensa. Recuperado de http://www.telensa. com/unb-wireless/.

Wang, Y. P. E. (2017). "A Primer on 3GPP Narrowband Internet of Things". In: IEEE Communications Magazine 55.3, pp. 117–123.

Weyn, M. (2015). "DASH7 alliance protocol 1.0: Lowpower, mid-range sensor and actuator communication". In: IEEE Conference on Standards for Communications and Networking (CSCN), pp. 54–59.