DISEÑO DE UN ESQUEMA DE INTEGRACIÓN DE TECNOLOGÍAS IOT DE LOS SISTEMAS DE SEGURIDAD ELECTRÓNICA

AUTORES

MARCO ANDRÉS ANGULO TELLO
FREDDY CANDELO VELÁSQUEZ

UNIVERSIDAD DEL PACÍFICO
PROGRAMA DE INGENIERÍA DE SISTEMAS
BUENAVENTURA – VALLE DEL CAUCA
2107

DISEÑO DE UN ESQUEMA DE INTEGRACIÓN DE TECNOLOGÍAS IOT DE LOS SISTEMAS DE SEGURIDAD ELECTRÓNICA

AUTORES

MARCO ANDRÉS ANGULO TELLO
FREDDY CANDELO VELÁSQUEZ

MODALIDAD
TESIS DE GRADO

ASESOR

ENGELBERTO SOLÍS CAICEDO

UNIVERSIDAD DEL PACÍFICO
PROGRAMA DE INGENIERÍA DE SISTEMAS
BUENAVENTURA – VALLE DEL CAUCA
2107

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE GRÁFICOS

Pág.

LISTA DE ANEXOS

Pág.

AGRADECIMIENTOS

A Dios, a mi madre, hermanos y docentes de la Universidad del Pacífico.

Freddy Candelo Velásquez

Primeramente, a Dios por darme sabiduría y permitir terminar esta investigación.

A mi familia por su apoyo en cada etapa de este proyecto y de mi desarrollo personal y profesional logrando avanzar cada día más en mi formación.

Al director de Tesis Engelberto Solís por su colaboración y guía en el desarrollo de este proyecto.

A la Universidad del Pacifico por la enseñanza brindada, con su nivel de formación y pluriculturalidad me hizo crecer como persona y profesional.

Marco Andrés Angulo Tello

RESUMEN

La presente investigación se basa en un estudio del marco general que abarca el Internet de las Cosas, su ecosistema, las principales tecnologías, las capas básicas que están involucradas, el impacto que se impone en la sociedad y en las empresas los factores determinantes en el futuro de esta tecnología.

Se investigó sobre las tecnologías de comunicación en relación con Internet de las Cosas. De igual forma, se realizó una descripción de los dispositivos más relevantes de los sistemas de seguridad IoT, los nuevos paradigmas de computación en la nube, las plataformas IoT, entre otros aspectos relevantes del IoT y los sistemas de seguridad electrónica.

Luego de analizar las tecnologías y componentes, se presenta un esquema de integración tecnologías IoT de los sistemas de seguridad electrónica.

Palabras Claves

Internet de las Cosas, IoT, Sistemas de Seguridad Electrónica, Esquemas, Integración.

INTRODUCCIÓN

En la actualidad Internet está estandarizada en gran parte por los protocolos de comunicación (IP, TCP, UMTS, LTE) y los dispositivos de conectividad remota. Bajo este contexto, los equipos técnicos y tecnológicos que se utilizan a diario están cada vez más enfocados a ser administrados y controlados remotamente, permitiendo procesar cada uno de los datos que serán convertidos en información, y así lograr que se visualice en tiempo real desde cualquier parte del mundo a través de dispositivos que se encuentran conectados a internet.

El internet de las cosas (IoT) logra ser de gran importancia al permitir que se dé la primera evolución real de Internet. Un salto que conducirá hacia el desarrollo de aplicaciones revolucionarias con el potencial de mejorar drásticamente la manera en que las personas viven, aprenden, trabajan y se entretienen. El internet de las cosas ya ha logrado que Internet sea sensorial (temperatura, presión, vibración, luz, humedad, entre otros), lo que nos permite ser más proactivos y menos reactivos [1].

Por otra parte, con la llegada de IoT los usuarios tendrán más control sobre la información permitiendo que las ciudades, las empresas y los hogares sean sitios más agradables, útiles y provechosos que contribuyan a mejorar el nivel de vida de las personas y lograr hacerla más fácil.

Este trabajo consiste en la elaboración de un *diseño de un esquema de integración de tecnologías IoT de los sistemas de seguridad electrónica***,** basándose en una investigación previa del contexto de IoT, sus tecnologías, protocolos y dispositivos, la importancia que tiene este para la sociedad, su impacto y los sectores donde este puede ser aplicado.

En el capítulo 1 se explicará el concepto de IoT, su ecosistema, arquitectura básica compuesta por 3 capas principales, las principales tecnologías de IoT, sus diversos sectores, la importancia y los beneficios que trae para la sociedad y qué tan seguro es IoT.

En el capítulo 2 se describen las diferentes tecnologías de comunicación, protocolos, y dispositivos (3G, 4G, 5G, GPS, WIMAX, WIFI, Z-WAVE, ZIGBEE, BLUETOOTH, RFID, NFC, sensores, actuadores, entre otros); que son implementadas en IoT, además de los nuevos paradigmas computacionales

conocidos como *Cloud computing, Fog computing*, integración de sistemas de seguridad electrónica y *Big Data*,

Por otra parte, se procede a construir un esquema de integración para los sistemas de seguridad electrónica IoT, presentando las características de los dispositivos IoT a implementar fabricados por la importante empresa de tecnología Libelium que serán administrados a través de la plataforma de IBM Bluemix.

En el capítulo 3 se describe como el Internet de las Cosas constituye grandes oportunidades para las empresas a través de la representación de datos y encuestas tomadas por importantes compañías de tecnología, y cuáles son sus niveles de aceptación dependiendo de su aplicabilidad y campo de acción para las principales regiones del mundo (Asia, América Latina, América de Norte y Europa)

Bajo el mismo esquema que denota las oportunidades que trae consigo IoT se hace la contextualización para el caso de Colombia, evaluando cuales son los beneficios esperados, las expectativas y el impacto. Además de ello se presenta un estado de arte de cómo se encuentra la infraestructura de conexión a internet y servicios móviles acondicionada para recibir a IoT en Colombia y Buenaventura y la participación que tienen las principales empresas prestadoras de servicio de internet en el contexto de las TIC’s.

1. JUSTIFICACIÓN

La importancia de diseñar de un esquema de integración de tecnologías IoT de los sistemas de seguridad electrónica consiste en mejorar los ya existentes, permitiendo que sean más proactivos, que estén siempre disponibles y se comuniquen mutuamente sin necesidad de intervención humana.

Lo anterior se fundamenta en la construcción de una propuesta basada en una investigación previa de cómo se lleva a cabo la integración de los sistemas de seguridad electrónica IoT aprovechando los nuevos avances tecnológicos del mismo (protocolos, servicios, tecnologías y plataformas), ya que IoT además de ser un elemento de carácter I+D[1] para las empresas resulta de gran beneficio para la recolección de información, procesamiento de datos y la obtención de respuestas y acciones automáticas lo que permite cumplir con los 3 principios TI fundamentales que son: disponibilidad, integridad y confidencialidad.

Internet se ha vuelto omnipresente, ha tocado casi todos los rincones del mundo y está incidiendo en la vida humana de formas inimaginables. Sin embargo, el viaje está lejos de haber terminado. Ahora estamos entrando en una era de conectividad aún más propagada donde una gran variedad de aparatos estará conectados a la web, de acuerdo con Cisco Systems [2] 50 billones de dispositivos para el 2020; constituyendo la era de la "Internet de las Cosas" (abreviado como IoT). Los dispositivos IoT equipados con sensores integrados, actuadores, procesadores y transceptores no son considerados una sola tecnología; sino una aglomeración de diversas tecnologías que trabajan en conjunto [3].

De acuerdo con la guía; The Dzone guide to Internet of Things Volumen III – 2016 [4] en su encuesta aplicada a 797 profesionales TI reveló que el 76% de los encuestados consideró que IoT será relevante para las organizaciones en el futuro y 24% restante respondió que no. En cuanto a la participación de los profesionales en proyectos de IoT la encuesta reveló que un 30% había participado, un 26% no y el 40% restantes manifestó no haber trabajado, pero si estar interesado en participar en proyectos a futuro.

En el contexto empresarial Según el IDC Analyze the Future en su artículo: “Índice de innovación de la Sociedad (QuISI – Ene 2016 aplicado para Colombia)” el valor de inversión en IoT y de TI en Colombia se encuentra en un grado de madurez bajo con tan solo el 0,1%, un valor no mayor a US$ 484 Millones en comparación

[1] Investigación y Desarrollo: hace referencia, según el contexto, a la investigación en ciencias aplicadas o bien ciencia básica utilizada para el desarrollo de ingeniería, que persigue con la unión de ambas áreas un incremento de la innovación que conlleve un aumento en las ventas de las empresas.

con USA que abarca el 27% con US$ 210 Mil millones y China el 26% con US$ 204 Mil Millones y el 46% restante, otros países desarrollados, han invertido alrededor de US$ 354,5 Mil Millones.

En ese sentido es de suma importancia que las empresas piensen desde ahora en innovar e invertir en IoT dado que es un sistema cibernético-físico donde se integran dispositivos y tecnologías con su entorno y que puede estar presente en todas partes al mismo tiempo, procesando y analizando datos en tiempo real.

2. ANTECEDENTES

Al hablar de Internet de las cosas es importante conocer el origen del término y quienes fueron algunas de las personas y los proyectos más influyentes e importantes que ayudaron a la transición que partió de visionar el término y su campo de acción a volverlo una tendencia tecnológica actual.

- 1832: Un telégrafo electromagnético fue creado Baron Schilling en Rusia, y en 1833 Carl Friedrich Gauss y Wilhelm Weber inventaron su propio código para comunicarse a una distancia de 1200m dentro de Göttingen, Alemania.

- 1844: Samuel Morse envía el primer mensaje telegráfico del código morse "¿Qué ha hecho Dios?" Desde Washington, DC hasta Baltimore.

- 1926: Nikola Tesla en una entrevista con la revista Colliers:

  "Cuando la tecnología inalámbrica se aplique perfectamente, toda la tierra se convertirá en un enorme cerebro, todas las cosas son partículas de un conjunto real y rítmico y los instrumentos a través de los cuales vamos a ser capaces de hacer esto serán increíblemente simples en comparación con nuestros teléfonos actuales. Un hombre será capaz de llevar uno en el bolsillo de su chaleco."

- 1950: Alan Turing en su artículo Computing Machinery and Intelligence en el Oxford Mind Journal:

  "... También puede sostenerse que es mejor proveer a la máquina con los mejores órganos sensoriales que el dinero pueda comprar, y luego enseñarla a entender y hablar inglés. Este proceso podría seguir la enseñanza normal de un niño".

- 1964: En Understanding Media Marshall McLuhan declaró:

  "... *mediante medios eléctricos, establecemos una dinámica por la que todas las tecnologías anteriores -incluidas las ciudades- se traducirán en sistemas de información*".

- 1966: Karl Steinbuch, pionero de la informática alemana, dijo: "Dentro de unas décadas, las computadoras estarán entretejidas en casi todos los productos industriales".

- 1969: Se envió el primer mensaje a través de ARPANET, red operativa origen de la Internet global.

- 1979: Se probó el TCP/IP, los protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.

- 1989: Tim Berners-Lee propone la World Wide Web.

- 1990: Considerado el primer dispositivo IoT. John Romkey, creó una tostadora que estaba conectada a una computadora con redes TCP / IP que se podía encender y apagar a través de Internet para la conferencia INTEROP de octubre de 1989.

- 1990: Berners-Lee implementó la primera comunicación exitosa entre un cliente Hypertext Transfer Protocol (HTTP) y un servidor a través de Internet, había inventado la World Wide Web. Él mismo, un año más tarde, creó la primera página web. A partir de ese momento el desarrollo tecnológico es vertiginoso, comienza la revolución de Internet.

- 1991: Se escribe el artículo científico americano de Mark Weiser sobre la informática omnipresente llamado "La computadora para el siglo XXI".

- 1995: Se incorpora Amazon y Echobay (Ebay).

- 1997: Se publica el artículo de Paul Saffo "Sensores: La próxima ola de innovación - Infotech".

- 1998: Google se incorpora.

- 1999: Kevin Ashton, impartió una conferencia en Procter & Gamble donde habló por primera vez del concepto de Internet de las Cosas. " The Internet of Things".

- 1999: Neil Gershenfeld hablaba sobre cosas similares del Laboratorio de Medios del MIT en su libro When Things Start to Think y al establecer el Centro de Bits y Atoms en 2001:

  "En retrospectiva, parece que el rápido crecimiento de la World Wide Web puede haber sido sólo la carga de disparo que ahora está desencadenando la verdadera explosión, ya que las cosas empiezan a utilizar la red".

- 1999: Auto-ID Labs se abre, que es el sucesor orientado a la investigación del MIT Auto-ID Center, fundado originalmente por Kevin Ashton, David Brock y Sanjay Sarma. Ellos ayudaron a desarrollar el Código de Producto Electrónico o EPC, un sistema global de identificación de artículos basado en RFID destinado a reemplazar el código de barras UPC.

- 1999: Neil Gross in la Business Week:

  "En el próximo siglo, el planeta tierra pondrá una piel electrónica, utilizará Internet como un andamio para sostener y transmitir sus sensaciones. Esta piel ya está siendo cosida. Está formada por millones de dispositivos de medición electrónicos incorporados: termostatos, medidores de presión, detectores de contaminación, cámaras, micrófonos, sensores de glucosa, EKGs, electroencefalogramas que sondearán y monitorearán ciudades y especies en peligro, la atmósfera, nuestros barcos, carreteras y flotas de camiones, nuestras conversaciones, nuestros cuerpos".

- 2005: La agencia de las Naciones Unidas International Telecommunications Union ITU publica el primer estudio sobre el tema. A partir de ese momento Internet de las Cosas adquiere otro nivel.

  "*Una nueva dimensión se ha agregado al mundo de las tecnologías de información y la comunicación (TIC): a cualquier hora, en cualquier lugar, ahora vamos a tener conectividad para cualquier cosa. Las conexiones se multiplican y crearán una nueva red dinámica de redes con redes, una Internet de las Cosas*".

- 2005: Comienza la aventura de Arduino.

- 2006: Se comercializa el Nabaztag (liebre en armenio) originalmente fabricado por la empresa francesa Violet. Se trata de un pequeño conejo que se conecta a Internet por ondas wifi. Se comunica con su usuario emitiendo mensajes vocales, luminosos o moviendo sus orejas. Difunde informaciones como la meteorología, la Bolsa, la calidad del aire, el estado de la circulación, llegada de los correos electrónicos, etc.

- 2006-2008: Reconocimiento de la UE y celebración de la Primera Conferencia Europea de la IoT.

- 2008: Un grupo de empresas lanzó la Alianza IPSO para promover el uso del Protocolo de Internet (IP) en redes de "objetos inteligentes" y para permitir la Internet de las Cosas. La alianza de IPSO ahora cuenta con más de 50 empresas miembro, incluyendo Bosch, Cisco, Ericsson, Intel, SAP, Sun, Google y Fujitsu.

- 2008-2009: Se contempló el nacimiento oficial del Internet de las Cosas.

- 2010: El primer ministro chino Wen Jiabao dijo que IoT era la clave de la industria para China.

- 2011: Se lanzó el nuevo protocolo IPV6. Samsung, Google, Nokia y otros fabricantes anuncian sus proyectos NFC. Se crea la iniciativa IoT-GSI Global Standards para promover la adopción de estándares para IoT a escala global. China continúa invirtiendo e impulsando el desarrollo y la investigación en Internet de las Cosas con instituciones como Shanghai Institute o la Chinese Academy of Sciences [5].

- 2015: Boo-Keun Yoon, presidente de Samsung, anuncia que en 2020 todos los productos de su empresa serán inteligentes. Desde las aspiradoras hasta los microondas, todos estarán conectados a Internet. Además de afirmar lo siguiente:

  "Samsung entiende que IoT va a transformar la sociedad, la economía e incluso nuestras propias vidas. Es una revolución que involucra a todas las industrias. Pero para hacer realidad este nuevo estilo de vida es fundamental la colaboración de las empresas y la creación de un ecosistema abierto donde los dispositivos IoT puedan hablar entre sí.

  En efecto, el gran desafío de IoT es el "idioma" y, aunque existe el argumento compartido de que es imprescindible la interoperabilidad de los dispositivos, a día de hoy son muy pocas las empresas que colaboran en este objetivo común" [6].

3. PLANTEAMIENTO DEL PROBLEMA

En la actualidad es poco el conocimiento que se tiene sobre las oportunidades y ventajas que ofrece IoT, en primera instancia por ser un término relativamente nuevo y poco explorado; en el ámbito tecnológico, son pocas las tecnologías integradas que hablen todas un mismo "idioma" basadas en IoT, que den soluciones de primera mano a las necesidades del sector empresarial y productivo.

La cantidad de dispositivos que estarán conectados a internet en los próximos años se distribuirán en varios lugares diferentes: ciudades, vehículos, hogares, empresas, espacios comerciales y en personas. La seguridad seguirá siendo una prioridad máxima para asegurar el crecimiento sostenido de IoT.

En este sentido los sistemas de seguridad electrónica IoT actuales no son completamente proactivos, ya que aún requieren de algún tipo de intervención humana ya sea para su funcionamiento, monitorización, almacenamiento y/o procesamiento de datos recolectados.

3.1. PREGUNTA DE INVESTIGACIÓN

¿Cómo los sistemas de seguridad electrónica IoT pueden brindar soluciones inteligentes, confiables y efectivas para las empresas?

4. OBJETIVOS

4.1. GENERAL

Diseñar un esquema de integración de tecnologías IoT de los sistemas de seguridad electrónica como propuesta para ser aplicado en el sector empresarial.

4.2. ESPECÍFICOS

- Conocer el contexto de IoT como sistema de integración de dispositivos y sus distintos campos de aplicación.
- Identificar y categorizar las tecnologías y dispositivos IoT aplicados en los sistemas de seguridad electrónica.
- Identificar la importancia de los sistemas de seguridad electrónica IoT en las empresas y cómo se pueden brindar soluciones inteligentes confiables y efectivas.

5. MARCO DE REFERENCIA

5.1. MARCO TEÓRICO

5.1.1. Internet de las Cosas.

Internet de las Cosas (IoT) describe el creciente estado de las cosas activadas por Internet (por ejemplo, objetos, entornos, vehículos y prendas de vestir) que pueden comunicar la información asociada a otros dispositivos similares (M2M: máquina a máquina) como parte de la Internet [7].

El término ha llegado a describir una serie de tecnologías y disciplinas de investigación que permiten a Internet llegar al mundo real de los objetos físicos. Se trata de cosas que tienen identidades y personalidades virtuales, operando en espacios inteligentes usando interfaces inteligentes para conectarse y comunicarse dentro de contextos sociales, ambientales y de usuarios.

IoT en la forma más básica es una manera de conectar las funciones diarias con el mundo. Dado que se ha transformado con el tiempo, éste se ha dividido en seis secciones diferentes y distintivas: detección; medición; interpretación; conexión; análisis, predicción y aprendizaje; actuación y optimización [8].

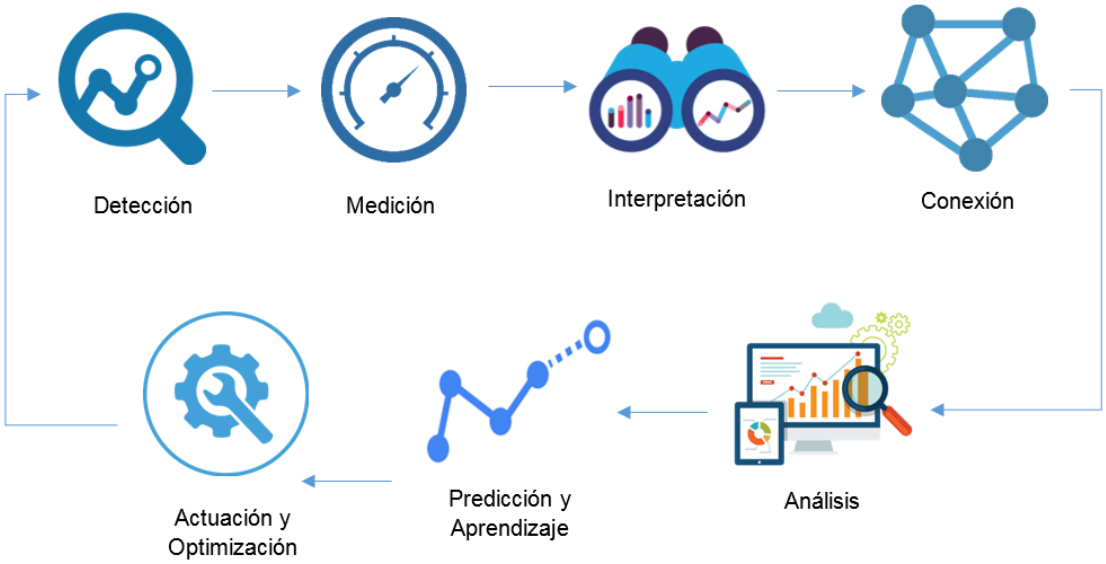


Figura 1 Interacción IoT [Autores]

5.1.2. Plataformas IoT.

Al igual que el término IoT, una plataforma IoT es un concepto muy amplio. Puede tratarse de simples plataformas que sirven para almacenar datos y ofrecen interfaces estándares al usuario, hasta sistemas más completos que permiten el uso de herramientas para hacer predicciones, analíticas o para crear interfaces más complejas.

Una plataforma IoT debe de permitir recoger los datos enviados desde los diferentes dispositivos conectados, además de los datos de otras fuentes como pueden ser los datos del tiempo, mapas etc. Por otro parte, debe de facilitar la creación de aplicaciones, tanto móviles como para otros dispositivos, que visualicen de manera clara los datos recibidos de los dispositivos IoT conectados a la plataforma, además de los datos sobre los que se ha trabajado [9].

Algunas de las plataformas IoT más famosas que se pueden encontrar en el mercado son las siguientes:

PLATAFORMA	DESCRIPCIÓN
AMAZON WEB SERVICE IOT	Se trata de una plataforma que sirve para conectar diferentes dispositivos a la nube de Amazon Web Service. Además, permite la conexión entre dispositivos, trabajar sobre los datos enviados por los dispositivos conectados y crear aplicaciones para interactuar con los estos. AWS IoT permite la conexión y el envío de mensajes mediante los protocolos MQTT, HTTP y WebSockets. Para la fácil conexión Amazon proporciona un SDK, éste está disponible en C y JavaScript.
IBM BLUEMIX	BlueMix es una plataforma Cloud, basada en open-standards, para construir, gestionar y ejecutar aplicaciones de todos los tipos (web, mobile, big data, dispositivos inteligentes). Entre sus capacidades se incluye Java, desarrollo de mobile backend, monitorización de aplicación, así como otras capacidades que vienen del ecosistema de partners y open source - todo a través del modelo cloud as-a-service.
IOT-TICKET	IoT-Ticket es una plataforma completa de Internet de las Cosas (IoT) que cubre la adquisición de datos, reportes, tablero de instrumentos y análisis. Permite la eficiencia operativa y la innovación de modelos empresariales para distintas empresas. La plataforma soporta monitoreo de supervisión, control, automatización y funciones avanzadas de generación de informes.

MICROSOFT AZURE SUITE	Microsoft ofrece un conjunto de aplicaciones IoT de Azure que permite crear escenarios de IoT desde cero o desde soluciones pre-configuradas. Microsoft propone como plataforma IoT a Azure IoT Suite. Esta plataforma basada en Azure, incluye además un servicio llamado Azure IoT Hub, que permite la comunicación fiable y bidireccional entre los dispositivos IoT y la plataforma.
ORACLE IOT	Oracle proporciona un servicio de IoT llamado Oracle Internet of Things Cloud Service. Este proporciona la posibilidad de conectar dispositivos en tiempo-real a la nube. Además, permite el análisis de los datos enviados y la integración de los datos con otras aplicaciones.
SENSORUP IOT PLATFORM	SensorUp hace accesible la información de todos los diferentes tipos de sensores en una sola plataforma, utilizando estándares abiertos para conectar los sensores. La Plataforma IoT es la primera y más completa que cuenta con la implementación de la API de SensorThings de OGC.
THINGWORX	ThingWorx es la una plataforma para empresas que permite a los innovadores desarrollar e implementar rápidamente soluciones inteligentes y conectadas para Internet de las Cosas.

Tabla 1. Plataformas IoT [9]

5.1.3. IoT en los Sistemas de Seguridad Electrónica.

Los sistemas de seguridad electrónica han venido evolucionando al pasar de los tiempo todos gracias al Internet de las Cosas. En la actualidad existen diferentes soluciones IoT implementadas en los sistemas de seguridad electrónica listadas en la siguiente tabla:

Nombre del Producto	Tipo de Producto	Area	Sitio Web
Meshdynamics	Surveillance Hardware Networking	Security, Monitoring, Industrial IoT, Smart Grid	meshdynamics.com
Remforce Boiler and Leak Monitoring	Sensors	Home Automation	remforce.com
VersaSense	Sensors	Home Automation	versasense.com
Calliope Meter	Sensors	Home Automation, Utilities	calliopewater.com
Casa Jasmina	Sensors	Home Automation	casajasmina.arduino.cc/
EKOOR Green IoT	Sensors, Beacons	Utilities, Home Automation	ekoor.io
Helium Smart Sensors	Sensors	Home Automation, Environmental, Analytics	helium.com
Lagoon	Sensors	Home Automation, Industrial IoT	golagoon.com
leakSMART Platform	Sensors	Home Automation, Industrial IoT	getleaksmart.com
Sense Home Energy Monitor	Sensors	Home Automation, Utilities	sense.com
Scanalytics Floor Sensors	Sensors	Analytics, Industrial IoT	scanalyticsinc.com

Tabla 2. The Dzone guide to volume III Internet of Things, Solutions Directory [4]

Las soluciones seleccionadas son incluidas basándose en varios criterios imparciales, incluyendo la madurez de la solución, la innovación técnica, la relevancia y la disponibilidad de datos.

Como la evolución que ha demostrado la industria de la seguridad física, el consumidor y la tecnología de TI ha tenido un profundo efecto en la conducción de la innovación y el cambio con la industria de la seguridad, HDTV, Cámaras IP y Power over Ethernet. Con esto en mente el Internet de las cosas también está establecido para tener profundas ramificaciones en la seguridad y la industria de video vigilancia.

IoT permitirá a las cámaras conectadas a internet pensar de forma independiente y tomar decisiones inteligentes por su cuenta. Como ejemplo, se puede implementar una malla de cámaras de red que se correspondan entre sí para alertar a la siguiente cámara de una persona u objeto que entra a una locación.

Son tantas las capacidades individuales de los dispositivos IoT en el mundo de la seguridad y donde el aspecto más importante de esta tendencia es cómo todos los componentes trabajan juntos para resolver un desafío tangible. En primer lugar, los sistemas basados en IoT deben ser fáciles de diseñar, instalar, mantener y utilizar. Esto supone todo un reto tecnológico.

Para maximizar el potencial de IoT se requiere que los proveedores de servicios de sistemas de seguridad y video vigilancia:

1) Entiendan cómo cada característica o componente trabaja en conjunto.

2) Puedan diseñar una solución que se puede utilizar para resolver desafíos específicos.

3) Los servicios ofrecidos sean capaces de entregarlos como una oferta integrada cuyo valor a largo plazo tiene más valor que la suma de sus partes.

Por otra parte, las soluciones de seguridad se mueven mucho más allá de solo la implementación de cámaras. De hecho, en gran parte debido a la llegada de IoT, en ese aspecto, los límites tradicionales del sector de la seguridad y video vigilancia continúan difuminados. Por ejemplo, las cámaras de red pueden utilizarse para la gestión de información de edificios e incluso saltar a la investigación científica con análisis en tiempo real de los patrones de tráfico y movimientos de multitudes. IoT permitirá que los sistemas combinados integren dispositivos previamente dispares como cámaras de video vigilancia, detectores de humo, paneles de control de acceso y altavoces en una consola de administración común, proporcionando una vista panorámica en edificios y sitios enteros.

El resultado es una gran oportunidad para soluciones de seguridad diseñadas específicamente para compartir datos útiles con otros dispositivos conectados, todos los cuales pueden monitorearse de forma remota. Esta conectividad entre

dispositivos proporcionará a los usuarios finales una conciencia situacional más completa en múltiples ubicaciones.

Con la creciente cantidad de datos generados, compartidos a través de la red y, en muchos casos, almacenados y accedidos a través de modelos de computación en nube, existe una creciente necesidad de concentrarse en la protección de todos estos datos y activos que existen "virtualmente". Por tal razón, están surgiendo nuevas tecnologías y métodos para mejorar la seguridad cibernética específicamente para sistemas de seguridad en red y basados en la nube. Esto es fundamental para protegerse contra vulnerabilidades, como la piratería informática, y será un aspecto importante de cómo se diseñan e implementan las soluciones de seguridad física y vigilancia.

De acuerdo con Axis Comunication, Líder en cámaras de red y otras soluciones TI en su guía Hardening Guide afirma que la responsabilidad de asegurar una red, sus dispositivos y los servicios que soporta caen en toda la cadena de suministro del proveedor, así como en la organización del usuario final. Un entorno seguro depende de sus usuarios, procesos y tecnología.

Sobre las cámaras de seguridad en un entorno de red: La amenaza más evidente para una cámara de red es el sabotaje físico, el vandalismo y la manipulación. Para ello desde una perspectiva de TI / red, la cámara es un punto final de red similar a las computadoras portátiles, computadores de escritorios y dispositivos móviles.

Acerca de los niveles de protección

Los diferentes niveles de protección varían según el tamaño y las necesidades del sistema. Cada nivel supone que se sigan las recomendaciones del nivel anterior. Ver tabla 3.

Nivel de Protección	Recomendado para	Procedimiento
0 Protección por defecto	Sólo se recomienda para fines de demostración y escenarios de prueba.	N/A
1 Protección Estándar	Recomendado para niveles mínimos de protección. Este nivel es adecuado para pequeñas empresas o instalaciones de oficina donde, por lo general, el operador también es el administrador.	- Comprobar el firmware - Actualizar el firmware - Restablecer los valores predeterminados de fábrica - Establecer la contraseña de root - Establecer permisos de usuario - Ajustar la configuración básica de la red - Establecer fecha y hora - Desactivar audio
2 Protección Empresarial	Configuración recomendada para corporaciones que tienen un administrador de sistema dedicado.	- Habilitar el cifrado - Crear una cuenta de administrador de copia de seguridad - Crear cuenta de cliente de vídeo - Deshabilitar AVHS - Desactivar los servicios de detección - Ajustar la configuración de red avanzada - Desactivar SOCKS - Desactivar QoS - Deshabilitar vídeo de multidifusión - Deshabilitar SSH - Establecer filtro de dirección IP
3 Protección empresarial administrada	Infraestructura de red de gran tamaño con un departamento de TI / IS. Para entornos en los que las cámaras necesitan integrarse en una infraestructura de red empresarial.	- Acceso a la red IEEE 802.1x - Configurar la supervisión SNMP - Registro remoto del sistema

Tabla 3. Niveles de Protección [10]

:

5.1.4. Redes de Sensores Inalámbricos.

Para entender las redes de sensores inalámbricos, en inglés: Wireless Sensor Networks (WSN), es útil examinar brevemente su historia. Al igual que muchas tecnologías avanzadas, el origen de las WSN se puede ver en aplicaciones militares e industriales, lejos de las aplicaciones actuales que consisten en dispositivos distribuidos que utilizan sensores para monitorear las condiciones físicas con sus aplicaciones extendidas a la infraestructura industrial, automatización, salud, tráfico y muchas áreas de consumo. La primera red inalámbrica que tiene semejanza real con una WSN moderna es el Sistema de Vigilancia de Sonido (SOSUS), desarrollado por el Ejército de los Estados Unidos en los años 50 para detectar y rastrear submarinos soviéticos [11] [12].

Línea de tiempo

- 1970's: Sensores con cables conectados a la ubicación central.
- 1980's: Redes de sensores cableados distribuidos.
- 1993: Proyecto: Sensores de red integrados inalámbricos en UCLA.
- 1999-2003: Proyecto DARPA SensIT: UC Berkeley, USC, Cornell, etc.
- 2000: Adaptive Multi-domain Power Aware Sensors program at MIT.
- 2001: Laboratorio de Investigación de Intel en Berkeley centrado en WSN, NASA Sensor Webs.
- 2002: Centro NSF para la detección en red integrada.
- 2001-2002: Emergencia de la industria de redes de sensores; Empresas de lanzamiento como Sensoria, Crossbow, Ember Corp, SensiCast más establecidos: Intel, Bosch, Motorola, General Electric, Samsung.
- 2003-2004: Norma IEEE 802.15.4, Zigbee Alliance [13].

El objetivo de muchas de estas iniciativas y organizaciones de estándares es permitir el despliegue de alto volumen de WSNs en aplicaciones industriales y de consumo, reduciendo el costo y la energía por sensor, simplificando al mismo tiempo las tareas de desarrollo y mantenimiento.

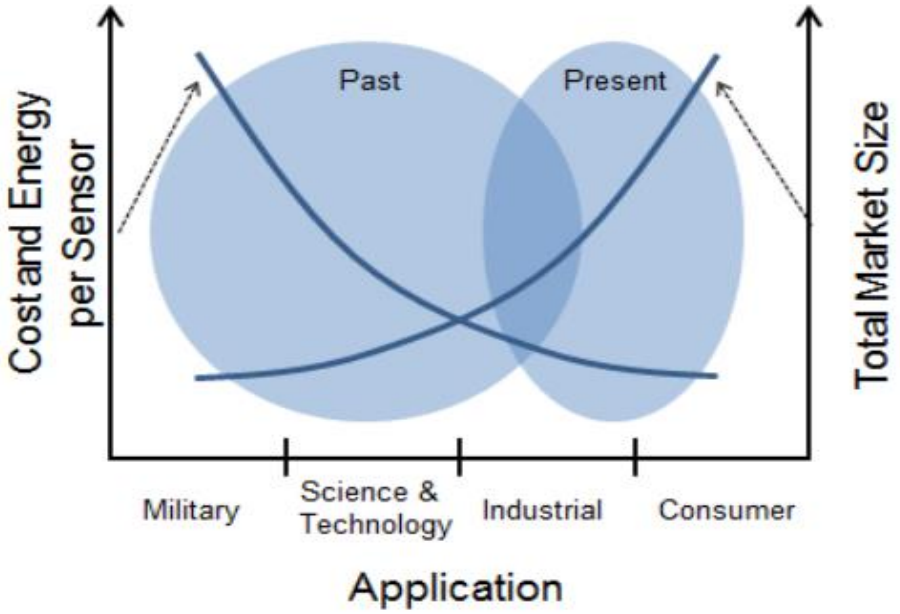


Gráfico 1. WSNs Ganan Tracción en el Mercado con disminución en los costos de los sensores. [13].

Reducir los costos de implementación de WSN y aumentar la funcionalidad implica grandes avances en cuatro áreas tecnológicas clave: sensores, dispositivos semiconductores, protocolos de redes y tecnología de almacenamiento / generación de energía. La culminación de este esfuerzo es el despliegue de redes de sensores inalámbricos para el emergente Internet de las Cosas (IoT) [13].

5.2. MARCO CONCEPTUAL

Sistema De Información.

Los sistemas de información son componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información para apoyar la toma de decisiones, la coordinación, el control, el análisis y la visualización en una organización y están formados por cinco componentes: hardware, software, datos, personas y procesos [14].

Protección de Datos

La protección de datos se ubica dentro del campo de estudio del Derecho Informático. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización, almacenamiento, organización y acceso. En algunos países la protección de datos encuentra reconocimiento constitucional, como derecho humano y en otro simplemente legal [15].

Confidencialidad.

Se refiere a la protección de datos frente a la difusión no autorizada. Se espera que la información sea accesible únicamente por las entidades autorizadas [16].

Disponibilidad.

Se refiere a la continuidad operativa de la entidad, capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran [16].

Integridad.

Asegurar que los datos no sufran cambios no autorizados, Es la cualidad de un mensaje, comunicación o archivo, que permite comprobar que no ha sido alterado. Busca mantener los datos libres de modificaciones no autorizadas [16].

Autenticación o Autentificación.

Es la propiedad que permite identificar el generador de la información. La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice.

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. Se suele realizar mediante un usuario o login y una contraseña o password [17].

Sensores.

Un sensor es un dispositivo capaz de detectar diferentes tipos de materiales, con el objetivo de mandar una señal y permitir que continúe un proceso, o bien detectar un cambio; dependiendo del caso que éste sea. Es un dispositivo que, a partir de la energía del medio, proporciona una señal de salida que es función de la magnitud que se pretende medir [18].

Actuadores.

Se denominan actuadores a aquellos elementos que pueden provocar un efecto sobre un proceso automatizado, modificando los estados de un sistema. Su función es generar el movimiento de los elementos según las órdenes dadas por la unidad de control. El actuador recibe la orden de un regulador o controlador y da una salida necesaria para activar un elemento final de control, transformando la energía de entrada en energía de salida utilizable para realizar una acción [19].

Controladores.

Un controlador es un dispositivo que almacena y ejecuta los programas de control, activa o desactiva actuadores de acuerdo con los datos positivos que los sensores le emiten [20].

Sistemas de Seguridad Electrónica.

Un sistema de seguridad electrónica es la interconexión de recursos, redes y dispositivos (Medios técnicos activos) cuyo objetivo es precautelar la integridad de las personas y su entorno previniendo de peligros y presiones externas.

Las principales funciones de un Sistema de Seguridad Electrónica son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico (personas, paquetes, correspondencia, vehículos, etc.), la vigilancia óptica mediante fotografía o circuito cerrado de televisión (*CCTV*) y la intercomunicación por megafonía y protección de las comunicaciones [21].

Control de Acceso.

El control de acceso consiste en un mecanismo que permite verificar la identidad de un usuario u ordenador con el fin de autorizar el ingreso o acceso a recursos físicos o lógicos.

Determinar el acceso a dichos recursos es fundamental, ya que permite que su manejo responda a las finalidades con que fueron destinados; para la implementación de esto, se identifican tres componentes:

- Mecanismo de autenticación: Puede ser una clave, lector biométrico, mapa o contraseña.
- Mecanismo de autorización: Tras la autenticación es la que permite o no el acceso.
- Mecanismo de trazabilidad: Complementa el mecanismo de autorización en los casos que este puede fallar.

Adicionalmente los controles de acceso se clasifican en dos tipos:

- Sistemas de control de acceso autónomos: Este tipo de sistemas permiten el control de puertas, horarios o identificación mediante claves o biometría.
- Sistemas de control de acceso en red: Estos logran integrarse mediante el uso de un software que permite obtener un registro de todas las actividades realizadas en un sistema [22].

CCTV.

CCTV es una sigla en inglés "*Closed Circuit Televisión*" que traducido al español es "circuito cerrado de televisión", consiste en una o más cámaras de vigilancia conectadas a uno o más monitores de vídeo o televisores que reproducen las imágenes transmitidas por las cámaras. Las imágenes vistas por la cámara se transmiten por cables coaxiales o una red inalámbrica.

El sistema se caracteriza por ser cerrado, lo cual indica que las imágenes grabadas por la cámara no se transmiten sino se almacena en un dispositivo para su visualización o para ser usadas como evidencia, como, por ejemplo: en el caso de un robo o asesinato, las imágenes grabadas pueden ser de gran ayuda para

las autoridades para encontrar a responsables de hechos ilícitos o criminales. Además, es un sistema para ser utilizado por un número limitado de espectadores [23].

Sensor de Movimiento.

Los sensores de movimiento son dispositivos basados en la tecnología de los rayos infrarrojos o las ondas ultrasónicas para poder captar en tiempo real los movimientos que se generan en un espacio determinado. Estos sensores de movimiento, adscritos sobre todo a cámaras de seguridad, puertas en almacenes y centros comerciales, etc.; son uno de los dispositivos más reconocidos e importantes dentro de la seguridad electrónica, que tanto ha apostado por, sobre todo, dos aspectos fundamentales: el tamaño y la funcionalidad de cada uno de los equipos que se usan durante el proceso.

Pero los sensores también están siendo adaptados a todo tipo de electrodomésticos, haciendo mucho más eficaces los niveles de protección o de vigilancia a los que un recinto puede llegar. Se ven sensores de movimiento ya instalados en algunas lámparas, por ejemplo, o hasta en relojes despertadores, siendo esta la última generación de sensores de movimiento que funcionan por intermedio de ondas ultrasónicas [24].

Sistema de alarmas.

Un sistema de alarma es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas.

Por ejemplo, la intrusión de personas, inicio de fuego, el desbordamiento de un tanque, la presencia de agentes tóxicos, cualquier situación que sea anormal para el usuario.

Son capaces además de reducir el tiempo de ejecución de las acciones a tomar en función del problema presentado, reduciendo así las pérdidas [25].

Gateway.

Un Gateway (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Una puerta de enlace o Gateway es normalmente un equipo informático configurado para hacer posible a las máquinas de una red local (LAN) conectadas

a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: *Network Address Translation*). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP *Masquerading* (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y, por tanto, una única dirección IP externa [26].

Detector de Gas.

Un detector de gas es un dispositivo que detecta la presencia de gas en el aire y que, a una determinada concentración, emite una señal óptica –acústica de aviso los del Tipo B y los del Tipo A, además, pueden poner en funcionamiento un sistema de corte automático de gas. El Corte automático de gas es un sistema que permite el corte del suministro de gas al recibir una determinada señal procedente de un detector, de una central de alarmas o de cualquier otro dispositivo previsto como elemento de seguridad en la instalación receptora, siendo la reapertura del suministro únicamente posible mediante un rearme manual [27].

Lector de Reconocimiento Biométrico

Los dispositivos de reconocimiento biométrico son tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, como, por ejemplo, la huella digital, el reconocimiento del patrón venoso del dedo o el reconocimiento facial. Estos dispositivos son excelentes sistema de identificación de la persona que se aplica en muchos procesos debido a dos razones fundamentales, la seguridad y la comodidad.

Los sistemas de reconocimiento biométrico pueden ser usados en cualquier aplicación que requiera seguridad, control de acceso, control de presencia e identificación o comprobación del usuario. Básicamente aportan tres ventajas: resistencia física, bajos costes de mantenimiento y ausencia de problemas electroestáticos.

Estos sistemas permiten garantizar o denegar el paso a las personas sin que éstas tengan necesidad de utilizar llaves o tarjetas, ni de memorizar claves, contraseña o códigos. Estos dispositivos ‘leen’ una característica o serie de características físicas (estáticas) de la persona, consideradas suficientes para su identificación: los más usuales son las huellas dactilares, el entramado de venas de la retina, la forma del iris, los patrones faciales, las venas de la mano o la geometría de la misma [28].

M2M (Machine to Machine, “Máquina a Máquina”).

Se trata de un concepto genérico que hace referencia a las tecnologías que permiten el intercambio (bidireccional) de información entre máquinas remotas, sin necesidad de intervención humana, utilizando para ello las comunicaciones inalámbricas o cableadas.

Esta comunicación máquina a máquina hace referencia a las tecnologías que permiten a los sistemas comunicarse con otros dispositivos de las mismas características a través de dispositivos tales como sensores, para capturar un evento y posteriormente transmitir los datos a través de una aplicación de software. Independientemente del tipo de máquina o del tipo de datos, la información fluye generalmente de la misma forma, desde una máquina a través de la red y conducida a través de una puerta de enlace *(Gateway)* a un sistema donde es procesada.

Los dispositivos que mandan y reciben información pueden ser desde pequeños sensores, capaces de realizar medidas e informar de estas a otros sensores o a las estaciones que manejan los datos, hasta vehículos inteligentes capaces de tomar sus “propias” decisiones.

Además de las comunicaciones entre dispositivos, M2M engloba a los componentes de hardware (como sensores que recogen información o módulos de comunicaciones integrados en dispositivos cotidianos), middleware (componentes software que actúan como intermediarios ante otros componentes de software) y software que permiten desarrollar los servicios y aplicaciones M2M [29].

5.3. MARCO CONTEXTUAL

El contexto de la investigación se centra en reconocer inicialmente el ecosistema IoT como sistema de integración entre dispositivos en donde se aglomeran tecnologías y dispositivos inteligentes que pueden ser aplicados en los sistemas de seguridad electrónica en las empresas para las cuales el IoT puede contribuir a fortalecerlos de una manera efectiva.

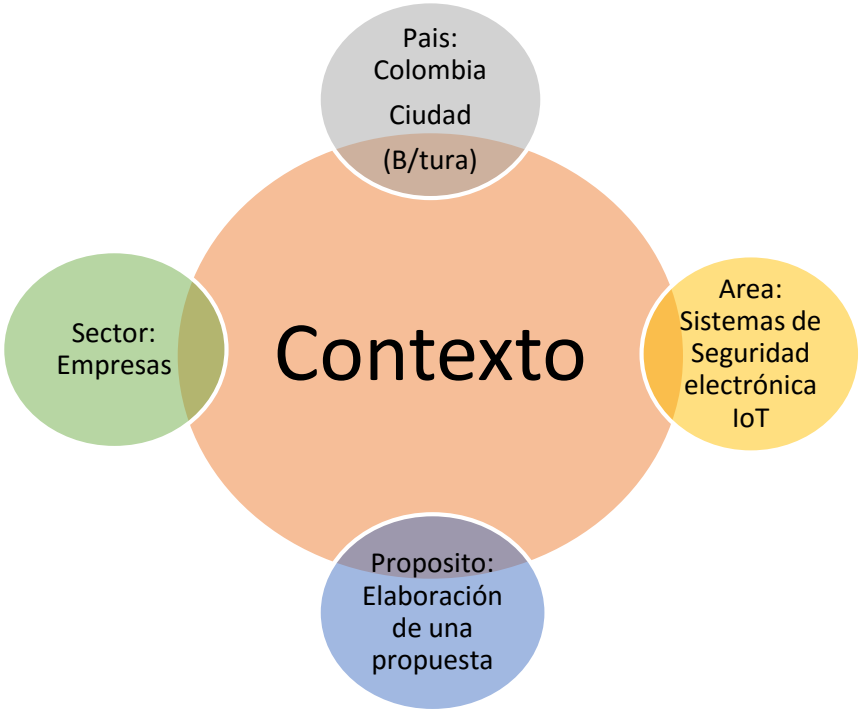


Figura 2 Marco contextual de la Investigación [Autores]

En un contexto global se están desarrollando proyectos tales como FIRE en la Unión Europea, FIND en Estados Unidos de América y AKARI en Japón para el fortalecimiento de Internet en diferentes campos, esto en marco de dos metodologías, la primera con un enfoque evolutivo y otra de enfoque revolucionario. Así mismo El IEEE creó el estándar 1901-2010 para dotar de un marco común para todos los desarrolladores.

En Colombia el Plan Vive Digital mediante la expansión de la infraestructura, la creación de nuevos servicios a precios más bajos, la promoción del desarrollo de aplicaciones y contenidos digitales y el impulso a la apropiación tecnológica por parte de éstos crea un círculo virtuoso en el que existe más demanda de los usuarios, más aplicaciones para éstos, más y mejores servicios a precios más económicos, en una infraestructura moderna.

Para el caso de Buenaventura el índice de penetración de internet en el año 2016 fue de 4.9% con relación a la población existente que sumó un total de 407.539 habitantes y con un total de 19.836 suscriptores a internet en ese año según fuentes del DANE.

5.4. MARCO LEGAL

Este proyecto se regirá bajo las leyes y normas de la constitución Política de Colombia en los siguientes artículos:

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Artículo 23. Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales.

Artículo 74. Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley. El secreto profesional es inviolable [30].

Además, se adicionan las siguientes leyes generales:

LEY 1341 LEY GENERAL DE LAS TICS [31].
LEY 1273 DELITOS INFORMÁTICOS [32].
LEY 1581 PROTECCIÓN DE DATOS [33].

6. CAPÍTULO 1. IOT LA NUEVA REVOLUCIÓN DE INTERNET

6.1. ¿QUÉ ES EL INTERNET DE LAS COSAS?

La frase "Internet de Cosas" (IoT) fue acuñada a principios del siglo 21 por el Centro de Auto-ID del MIT con mención especial a Kevin Ashton y David Brock, como un complejo sistema cibernético-físico, que integra todo tipo de dispositivos, sistemas de detección, identificación, comunicación, redes e informática, y conecta a todas las personas y cosas de manera que cualquiera, en cualquier momento y lugar, a través de cualquier dispositivo y medio, pueda acceder más eficientemente a la información de cualquier objeto y cualquier servicio [34]. "Ubicuo" es la característica distintiva de las tecnologías IoT, por lo que el IoT suele estar relacionado con la identificación, detección omnipresente, computación e Inteligencia ubicua.

6.2. CONCEPTOS Y DEFINICIONES

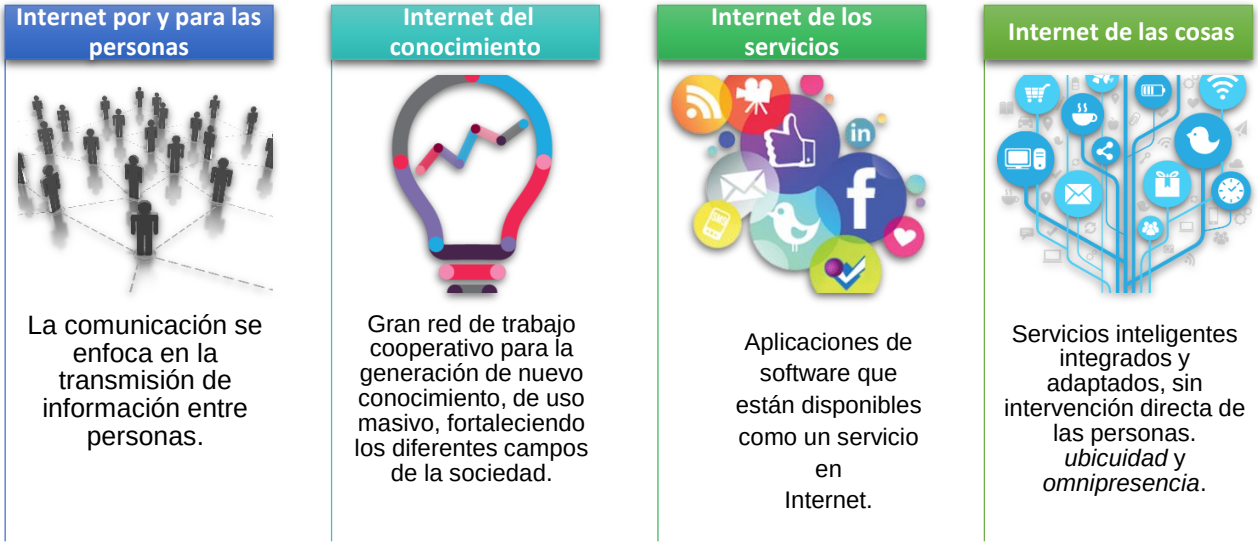


Figura 3 Transición al internet de las cosas [Autores]

Un concepto para el Internet de las Cosas que recoge las ideas de diferentes ámbitos del mundo sería: Una gran red de información, basada en elementos electrónicos con reconocimiento de su entorno e inteligencia propia para facilitar desde tareas cotidianas hasta procesos industriales complejos, generando bienestar en primera instancia al usuario y a nivel macro, a comunidades enteras. En el Internet de las cosas se agrega una nueva dimensión a la comunicación manejada en los sistemas de comunicación actuales, en la que se busca tener comunicación en cualquier momento y lugar, con la incorporación de múltiples dispositivos que tendrán respuestas autónomas, esto genera la nueva dimensión en la cual se tiene comunicación entre los computadores, entre humanos sin computadores, de un humano a una cosa y entre cosas. Las tecnologías involucradas en IoT estas compuestas por sensores, actuadores, inteligencia artificial, entre otras.

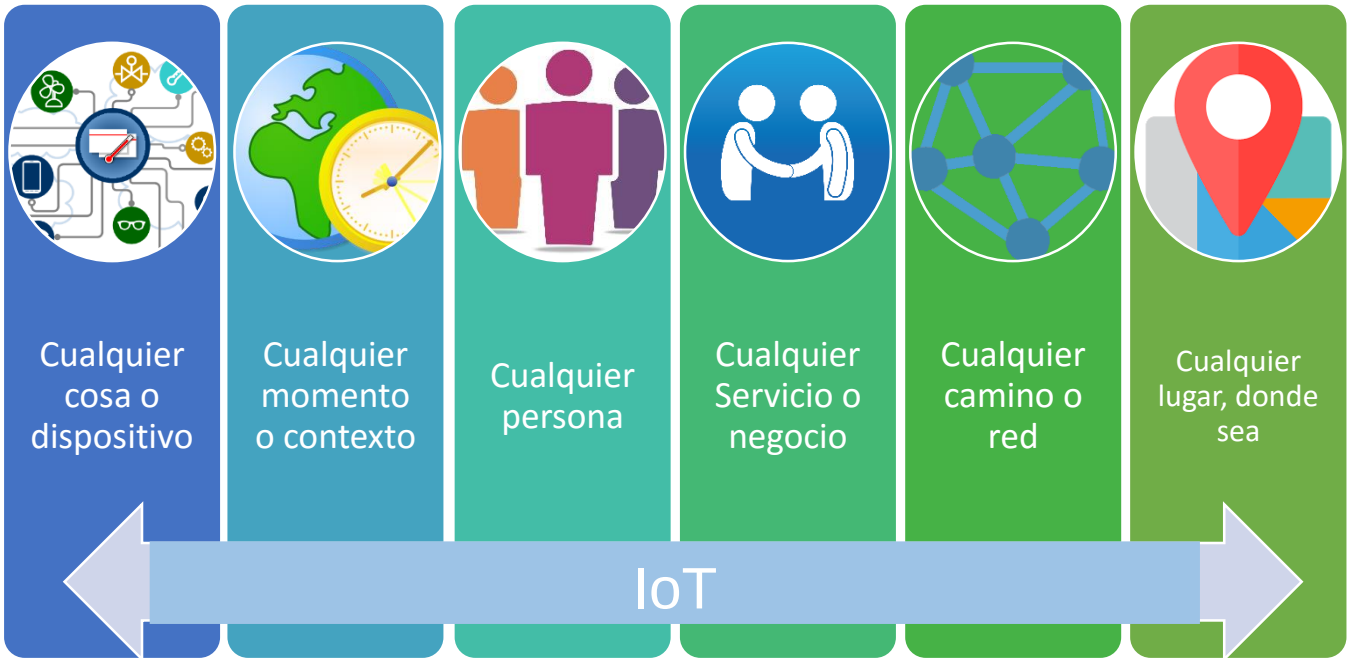


Figura 4 Contexto de IoT [Autores]

6.3. TENDENCIAS DE IOT

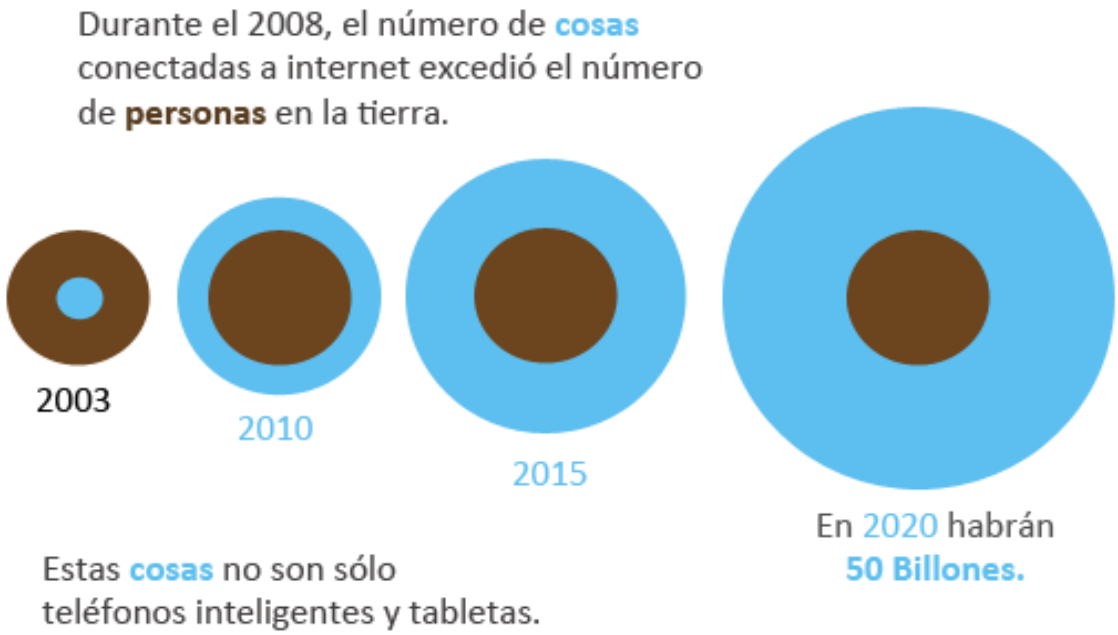


Figura 5 Tendencias IoT [35]

A finales de 2011, 20 hogares típicos generaron más tráfico de Internet que el internet entero en 2008.

Cisco's Planetary Skin Cisco utilizará miles de millones de sensores en red en tierra y en mar que podría monitorear los cambios en el ambiente.

Con el protocolo **IPv6**, se tendrá

340,282,366,920,938,463,463,374,607,431,768,211,456

Posibles direcciones de Internet. Eso es 100 por cada átomo en la faz de la tierra y se leería: *trescientos cuarenta sextillones doscientos ochenta y dos mil trescientos sesenta y seis quintillones novecientos veinte mil novecientos treinta y ocho cuatrillones cuatrocientos sesenta y tres mil cuatrocientos sesenta y tres trillones trescientos setenta y cuatro mil seiscientos siete billones cuatrocientos treinta y un mil setecientos sesenta y ocho millones doscientos once mil cuatrocientos cincuenta y seis.*

Las limitaciones tecnológicas están retrocediendo exponencialmente. Cuando billones de cosas están conectados, hablando y aprendiendo, la única limitación dejada será nuestra propia imaginación.

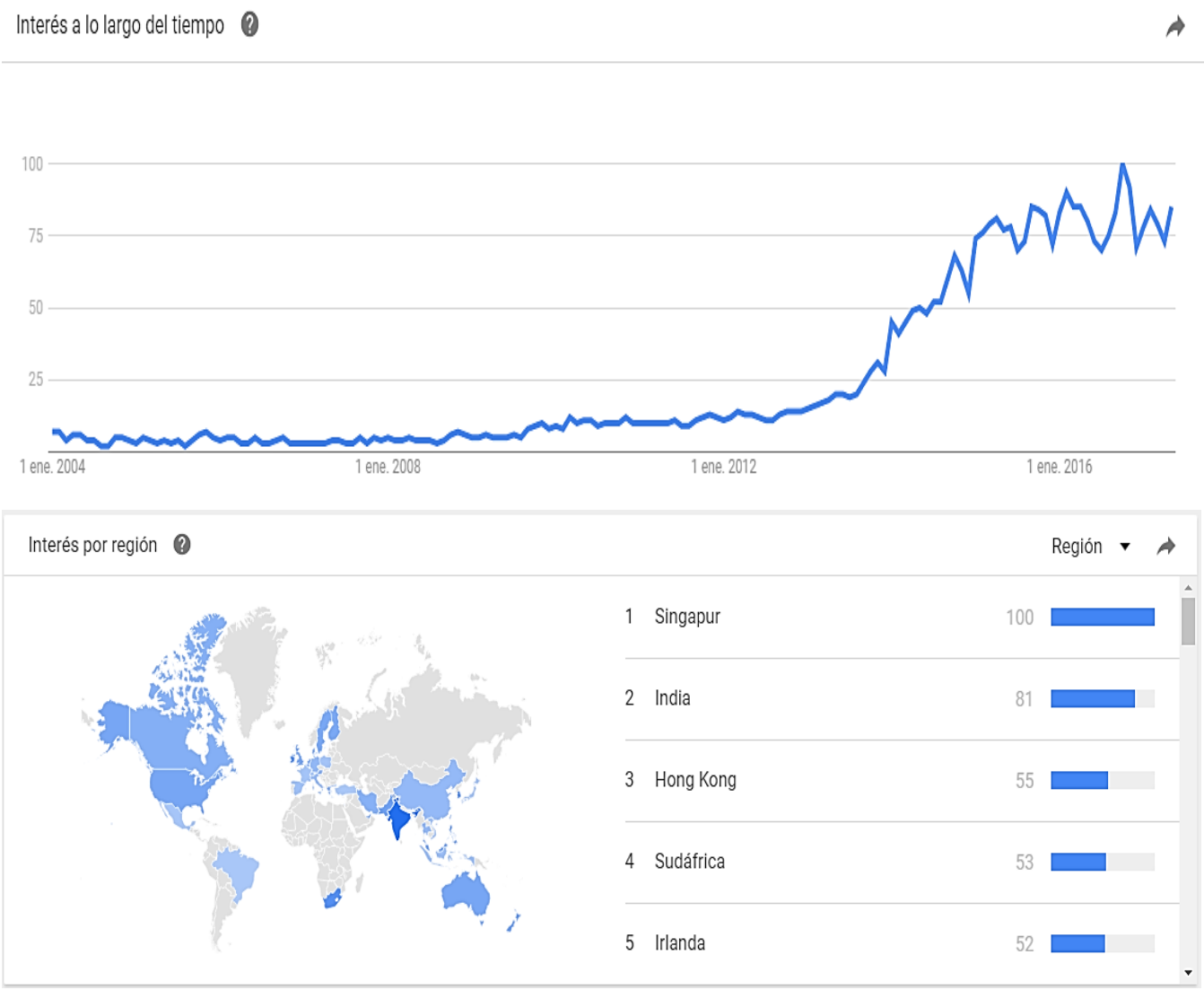


Gráfico 2. Interés a lo largo del tiempo y por región para Internet of Things, 2004-2017 [36]

En la actualidad se están desarrollando proyectos a nivel global tales como FIRE en la Unión Europea, FIND en Estados Unidos de América y AKARI en Japón para el fortalecimiento de Internet en diferentes campos, esto en marco de dos metodologías, la primera con un enfoque evolutivo y otra de enfoque revolucionario, el enfoque evolutivo trata de pasar del estado actual a un nuevo estado el Internet a través de parches incrementales, esto es lo que se

ha venido realizando los últimos 30 años con un gran éxito, pero debido al auge de Internet se ha llegado a un punto donde se presentan grandes dificultades para seguir experimentando con la arquitectura actual por su grado de complejidad [37].

6.4. EL ECOSISTEMA DE IOT

El ecosistema IoT permite a las entidades conectarse y controlar sus dispositivos.

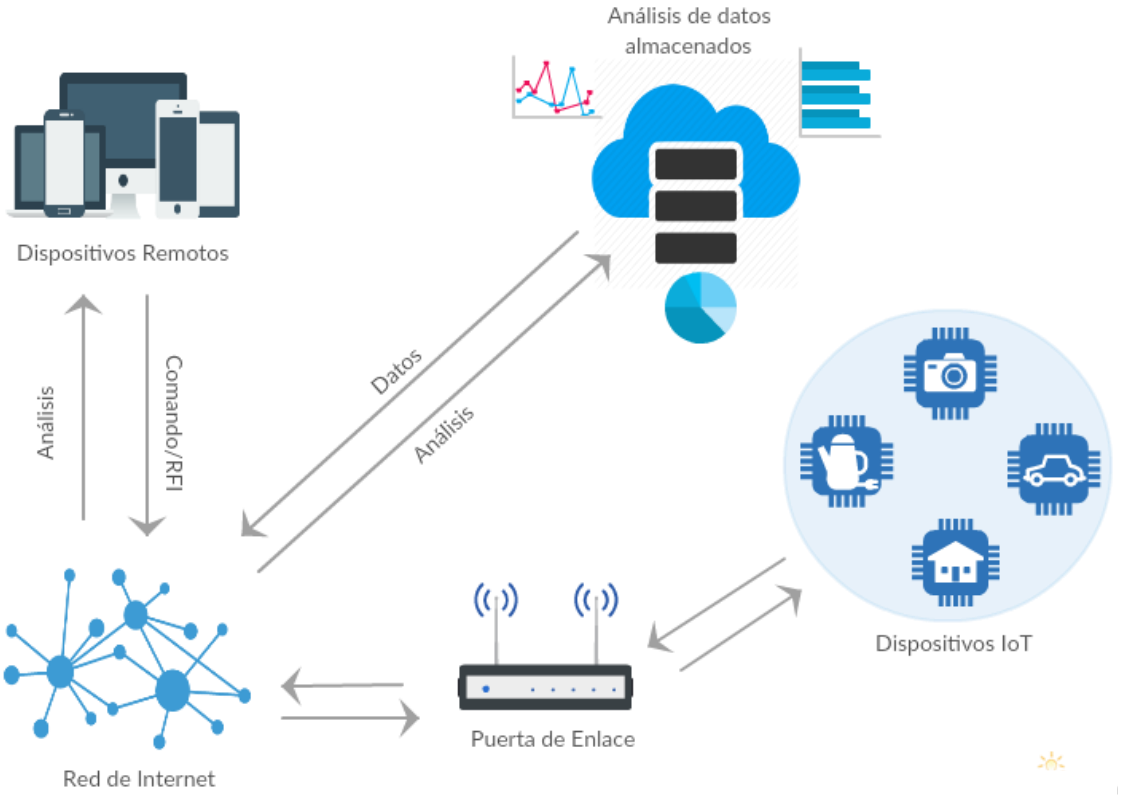


Figura 6 Ecosistema IoT [38]

En el ecosistema IoT, una entidad utiliza un dispositivo remoto (por ejemplo, smartphone, tableta, etc.) para enviar un comando o una solicitud de información a través de una red a un dispositivo IoT. A continuación, el dispositivo realiza el comando y / o envía la información de nuevo a través de la red para ser analizada y mostrada en el mando a distancia. Hay múltiples ubicaciones en las que los datos generados por el dispositivo IoT pueden ser

analizados y almacenados, incluyendo la nube, una base de datos bien sea de forma remota o localmente en los propios dispositivos IoT.

6.5. TAXONOMÍA

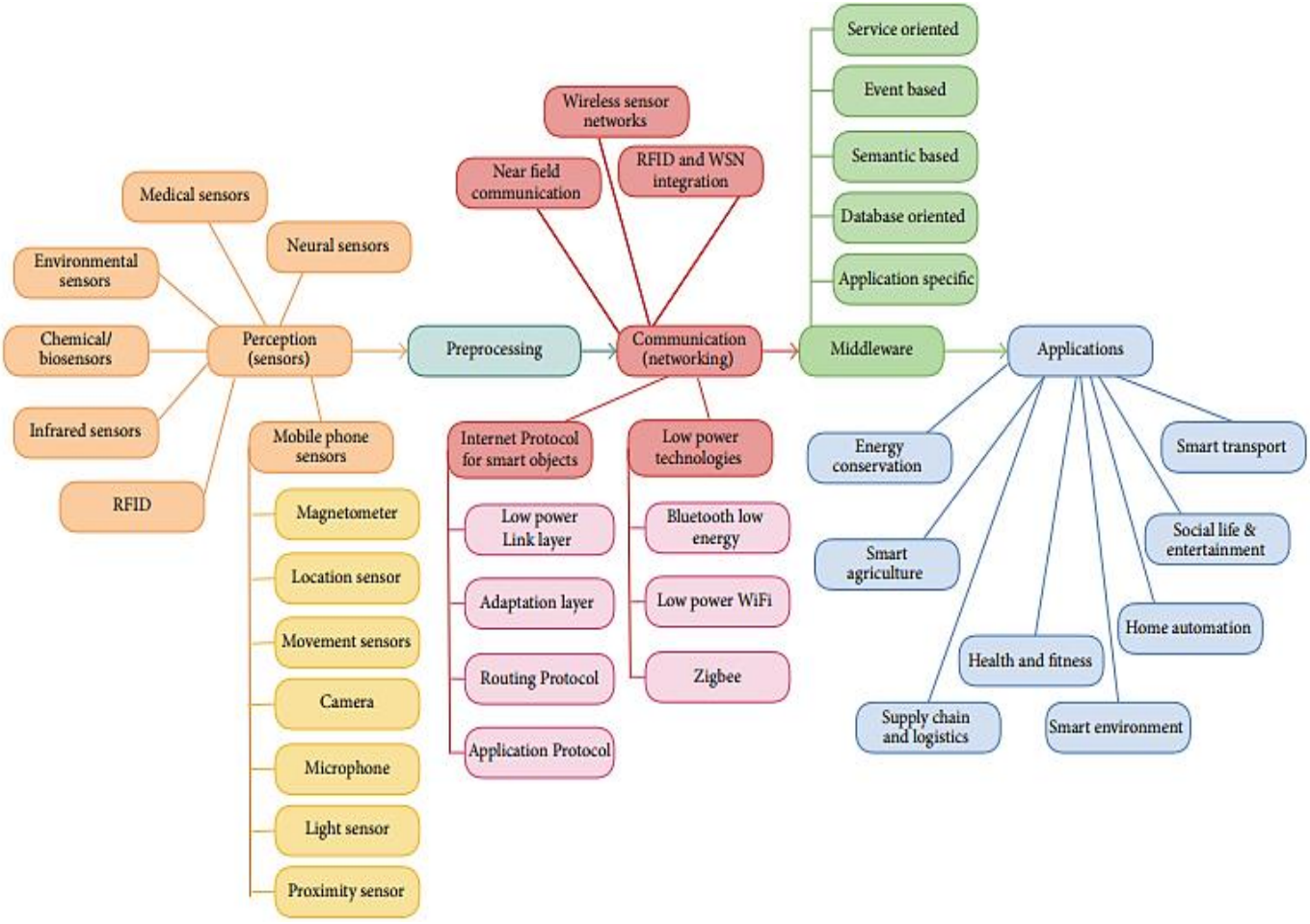


Figura 7 Taxonomía de la investigación en tecnologías IoT [39]

La figura 7 representa la taxonomía de tecnologías IoT. Esta se basa en los elementos arquitectónicos de IoT contenidos en 5 capas (Percepción, pre-procesamiento, comunicación, Middleware y Aplicación).

6.6. ARQUITECTURA BÁSICA DE IoT (LAS 3 CAPAS)

Los casos de uso específicos y las oportunidades a través de diferentes industrias son numerosos, y en muchos sentidos el mundo de IoT está recién comenzando. Lo que emerge de estos escenarios es un conjunto de desafíos y patrones comunes. Los proyectos IoT tienen dimensiones adicionales que aumentan su complejidad en comparación con otras aplicaciones de tecnología centrada en la nube, entre ellas:

- Hardware diverso
- Diversos sistemas operativos y software en los dispositivos
- Requisitos de puerta de enlace de red diferentes.

- **Descripción general de los componentes de nivel superior**

  Aquí dividimos el sistema en tres componentes básicos, el dispositivo, la puerta de enlace y la nube:

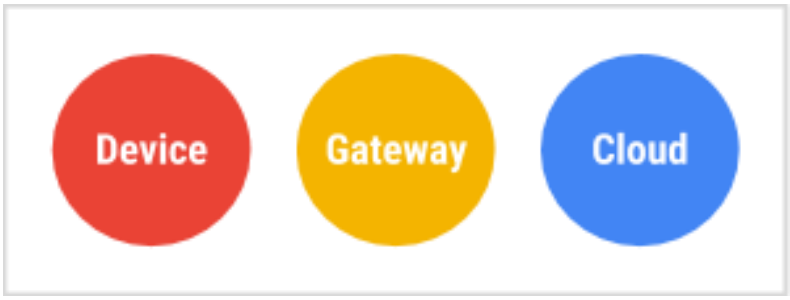


Figura 8 Arquitectura básica IoT [40]

  Un dispositivo incluye hardware y software que interactúa directamente con el mundo. Los dispositivos se conectan a una red para comunicarse entre sí o con aplicaciones centralizadas. Los dispositivos pueden estar conectados directa o indirectamente a Internet.

  Una puerta de enlace permite que los dispositivos que no estén conectados directamente a Internet puedan acceder a servicios en la nube. Aunque el término puerta de enlace tiene una función específica en la creación de redes, también se utiliza para describir una clase de dispositivo que procesa datos en nombre de un grupo o grupos de dispositivos. Los datos de cada dispositivo se envían a una plataforma en la nube, donde se procesa y se combina con datos de otros dispositivos y, potencialmente, con otros datos transaccionales de negocio.

6.7. PRINCIPALES TECNOLOGÍAS DEL INTERNET DE LAS COSAS

Las principales tecnologías sobre las cuales se impulsa el Internet de las Cosas, son la RFID para la identificación de los objetos, los sensores para la captación de los cambios del medio físico, la nanotecnología para que se genere ubicuidad en los sistemas que hace simplemente que sean cada vez menos perceptibles por las personas o usuarios finales y las tecnologías inteligentes para que los objetos puedan generar acciones dependiendo del contexto sin influencia humana, estas cuatro tecnologías se explican de manera general a continuación para tener una idea más clara de que tratan y porque son importantes para el desarrollo de Internet de las cosas.

RFID.

Es una tecnología de identificación automática sin contacto llamada “Radio Frequency Identification” (Identificación por radiofrecuencia). Con esta tecnología se puede lograr la identificación automática de objetos estáticos o dinámicos y personas, la forma más básica del sistema RFID se compone de etiquetas, lectores y antenas, este tipo de tecnología es útil para el Internet de las Cosas porque con ella se logra la identificación de los diferentes objetos que interactúan en el IoT y se logra mayor facilidad para el manejo de la información. [41]

Sensores IoT.

Una pieza clave para lograr llegar al Internet de las Cosas, son los sensores, ya que gracias a estos se logra la recopilación de información sobre el entorno en el que se encuentran las cosas, gracias a los avances en nanotecnología, se ha logrado que el tamaño de los microprocesadores sea cada vez menor sin perdidas de velocidad de procesamiento.

La idea de la miniaturización es que cada vez elementos más comunes pueden interactuar con la red de Internet sin observar cambios considerables en los equipos, esto significa que gracias a los sensores conectados se obtendrán información en tiempo real y se podrá acceder a ella desde otros lugares y a través de esta información se podrán tomar decisiones remotas sobre las acciones a tomar u observar que acciones se realizaron de manera automática. [42]

Nanotecnología.

El estudio de partículas minúsculas se está utilizando para mejorar los productos alrededor de una serie de industrias, incluyendo los sectores de medicina, energía y el transporte. La utilización de nanotecnología hará posible que los objetos que interactúan y se conectan en la red unos con otros, sean lo más pequeños posible con las herramientas tecnológicas actuales e irá disminuyendo su tamaño con los avances en esta tecnología, además de la nanotecnología y la miniaturización de los equipos, en los objetos se pueden crear inteligencia embebida, este tipo de equipos son conocidos como dispositivos inteligentes. [43] [44]

Tecnologías Inteligentes.

Las tecnologías inteligentes son los métodos empleados para lograr cierto propósito mediante el uso de un conocimiento a priori. Objetos que obtienen inteligencia después de la implantación de tecnologías inteligentes, se pueden comunicar con los usuarios activa o pasivamente. El contenido y la orientación de la investigación principalmente incluye: teoría de la inteligencia artificial, tecnologías avanzadas y sistemas de interacción entre humanos y máquinas, tecnologías y sistemas de control inteligente, procesamiento inteligente de señales entre otras. [45]

6.8. IOT EN SUS DIVERSOS SECTORES

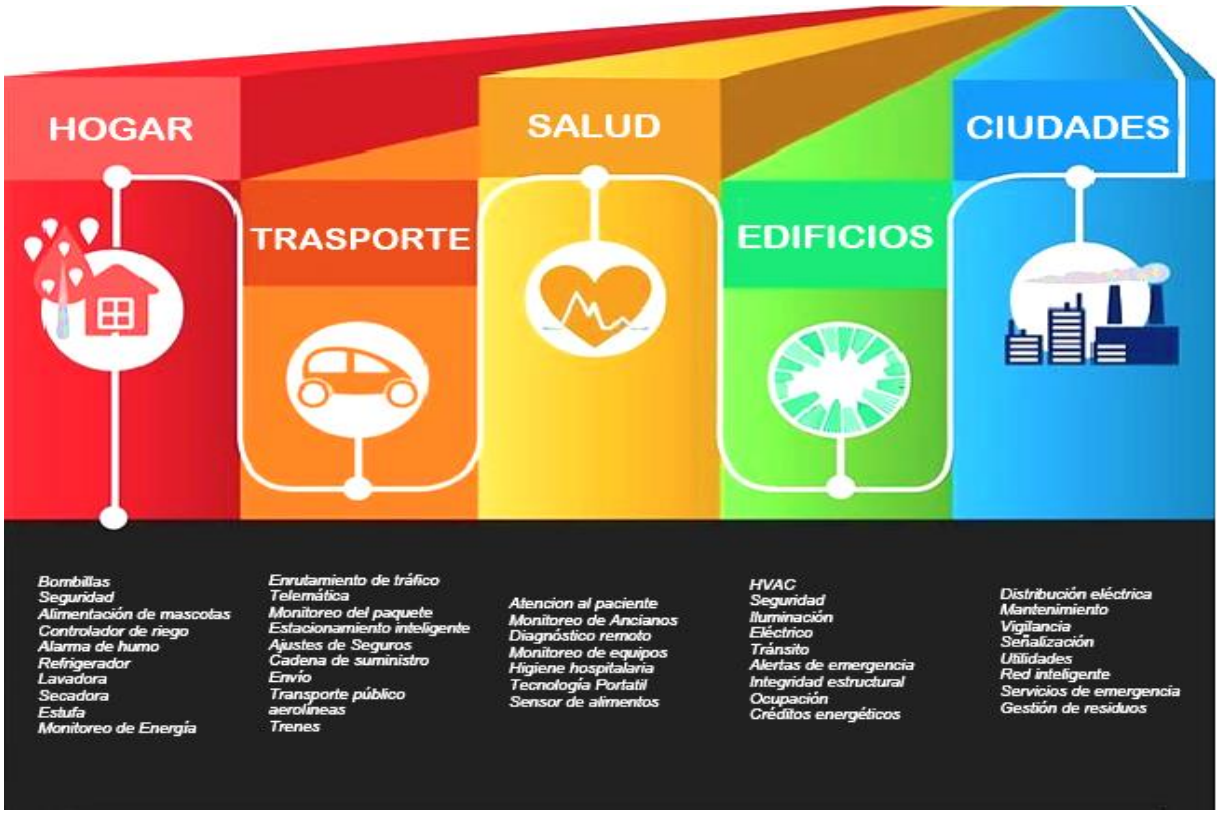


Figura 9 IoT en sus diversos sectores [46]

Ejemplos de aplicación de IoT

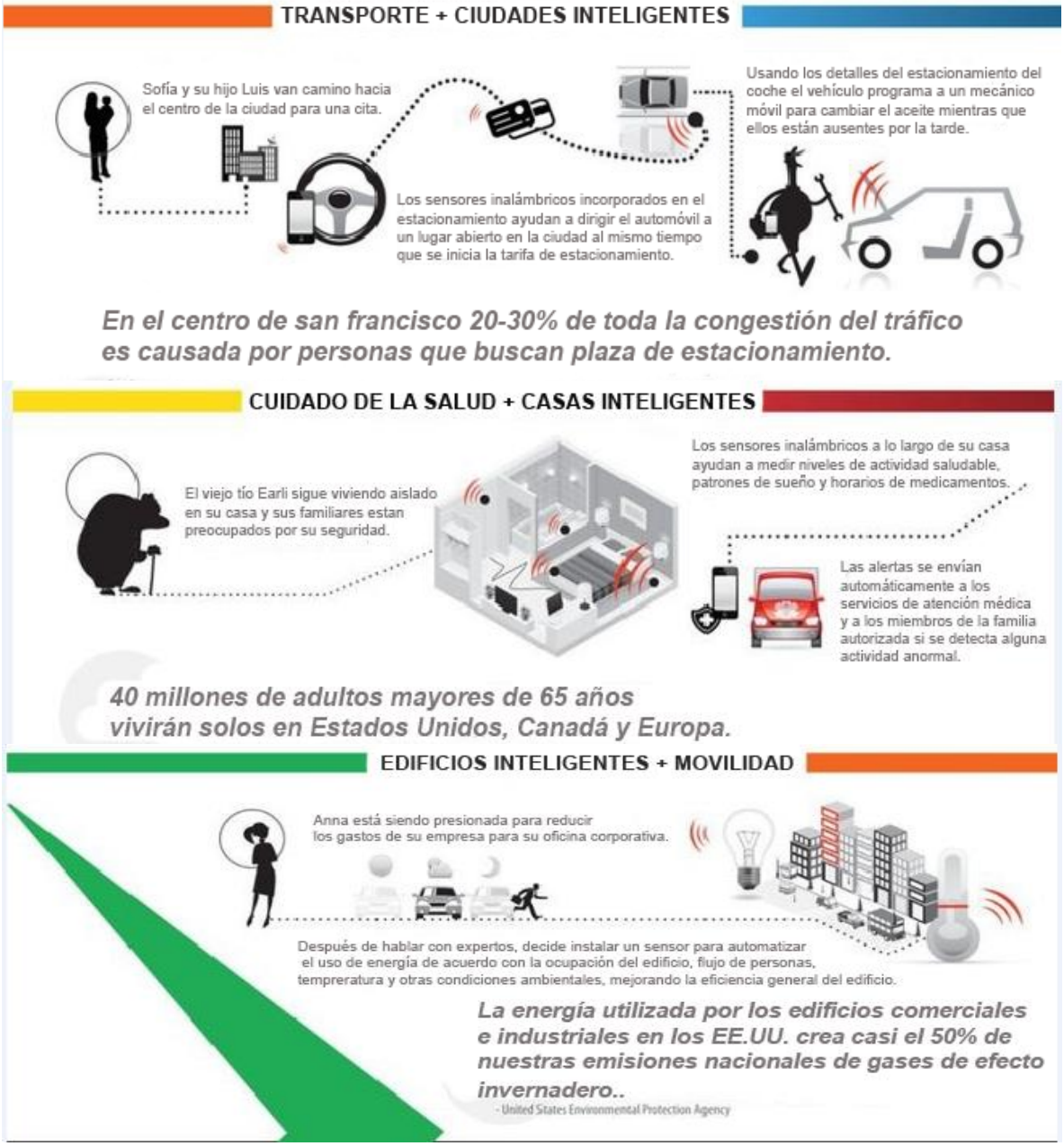


Figura 10. Ejemplos IoT [46]

6.9. LA IMPORTANCIA DE IOT EN LA SOCIEDAD

Figura 11. IoT en la Sociedad [Autores]

Podemos afirmar que la principal importancia que IoT tiene para la sociedad consiste en brindarle un sin número de beneficios, contribuyendo a hacer la vida mucho más fácil en muchas formas diferentes dependiendo del dispositivo que se utilice. Lo anterior se puede obtener integrando: tecnología + innovación + conocimiento, conociendo cuales son los principios de IoT y así lograr transformar los datos en información y la información en conocimiento.

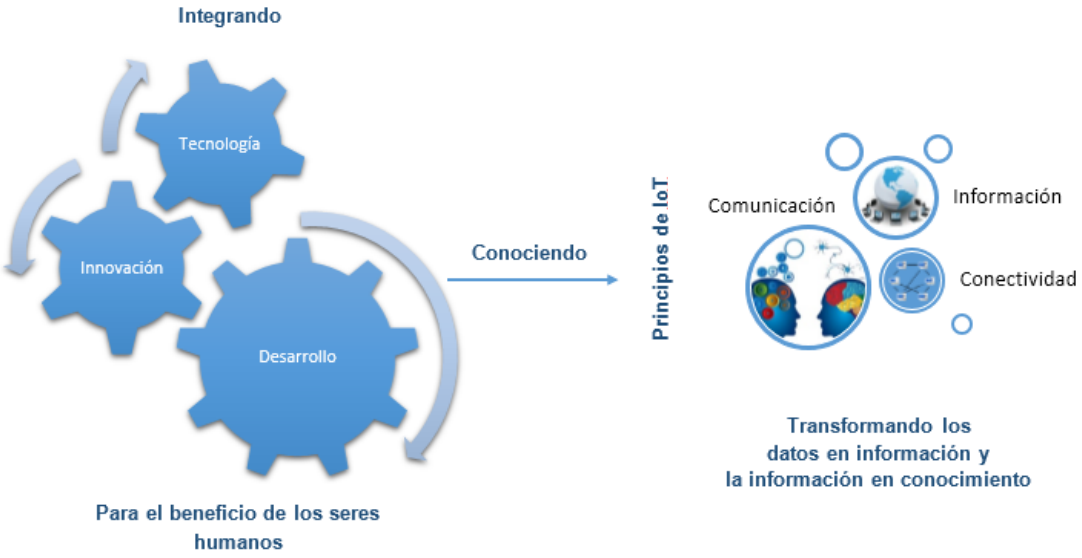


Figura 12 Importancia de IoT en la sociedad y sus principios [Autores]

6.10. LOS BENEFICIOS Y RIESGOS DE IOT

Internet de las Cosas, se trata de problemas reales alrededor de la seguridad, dijo Reichental. “Si un sistema de señal de tráfico no está coordinado, los coches se estrellarán. Si un sistema de disparadores de emergencia no funciona, la policía no recibirá alertas para despachar unidades o las ambulancias no irán al lugar correcto” [47].

Muchos dispositivos conectados y aplicaciones no tienen una política de privacidad absoluta y la seguridad IoT en este punto está dejando sus datos personales en riesgo de un ataque externo. Los datos se convertirán en un objetivo irresistible para terceros.

BENEFICIOS	RIESGOS
Mayor conectividad entre usuarios y cosas	Vendedores de datos
Disponibilidad de los sistemas IoT 24x7x365	Los datos podrían usarse en su contra
Hogares, empresas, autos, ciudades, hospitales e industrias inteligentes	Los hackers podrían utilizar el IoT para burlarse de usted, de su privacidad y seguridad legal de los datos generados
Hacer la vida más fácil	Depender menos de las personas
Mejorar el nivel de vida	Cambios de hábitos de vida (Sedentarismo)
Datos convertidos en conocimiento	Vulnerabilidades de la transmisión de datos a través de la red

Tabla 4 Beneficios y Riesgos IoT.[47]

6.11. LA SEGURIDAD EN IOT

La seguridad, en su aspecto más técnico, se puede definir como aquellas actividades enfocadas a proteger un determinado dispositivo o servicio, así como todo aquello con lo que interactúa e intercambia con otros dispositivos o servicios, ya sea información, datos, señales, etc. Utilizando como base la anterior definición, la seguridad de IoT se podría definir como aquellas actividades encaminadas a la protección de los objetos y sus comunicaciones o interacciones con otros objetos [48].

IoT se constituye como un nuevo paradigma que habilita un sinfín de nuevos servicios y aplicaciones para muchos de los ámbitos de nuestra sociedad. Sin embargo, su seguridad, un punto de especial trascendencia, sigue sin estar del todo claro, lo que supone por un lado un foco importante de riesgos y problemas, pero que al mismo tiempo abre la posibilidad para la generación de nuevas ideas y soluciones.

Los expertos apuntan que una de las principales barreras para la implantación de IoT es precisamente la seguridad y la privacidad. El porqué es bien sencillo: por un lado, las restricciones que imponen los dispositivos y redes de IoT impiden la aplicación directa de soluciones tradicionales de seguridad. En concreto, protocolos tradicionales de seguridad y criptografía requieren una gran cantidad de recursos de memoria y proceso, algo de lo que habitualmente carecen los

dispositivos IoT. Por tanto, la adaptación de soluciones de seguridad a este nuevo paradigma se presenta como un gran desafío. Además, cabe destacar que, a diferencia de otros entornos más tradicionales, los dispositivos IoT suelen trabajar en condiciones de mayor dificultad, en cuanto a los entornos que les rodean, entornos que muchas veces no están controlados e incluso son hostiles o propensos a ataques malintencionados [49].

La consultora Gartner, según uno de sus últimos estudios, asegura que al final del año 2017 más del 20 por ciento de las empresas dispondrá de servicios digitales dedicados a la protección de sus iniciativas empresariales mediante dispositivos y servicios en IoT. Gartner señala que ya existen muchas iniciativas empresariales que están utilizando IoT, por lo que el papel que jugará en los negocios y en la industria obligará a las empresas a tener que invertir en su seguridad [50].

Por otra parte, gracias a IoT, el crecimiento de empleos en el sector de la seguridad informática está viviendo un momento vertiginoso, ya que se están creando miles de puestos de trabajo.

Problemas y retos identificados

Expertos de la Comisión Europea [51], a partir de diversos estudios realizados para identificar los potenciales riesgos en entornos altamente interconectados, señalan como problemas importantes a tener en cuenta, en cuanto a privacidad y protección de datos y seguridad de la información con respecto al IoT, los siguientes:

1. Continuidad y la disponibilidad en la provisión de servicios basados en IoT.
2. Diseño de tecnologías IoT.
3. Trazabilidad / análisis del rendimiento / tratamiento ilícito.
4. Reutilización de los datos / ampliación de la verdadera misión de los datos.
5. Ejercicio de los derechos de protección de datos para las personas y el cumplimento de la legislación para las organizaciones.
6. Pérdida / violación de la privacidad y protección de datos de los individuos.
7. Realización de ataques maliciosos contra los dispositivos y sistemas IoT.
8. Pérdida del control por parte del usuario / dificultad en la toma de decisiones.
9. Lock-in del usuario, en cuanto a que los usuarios se queden “bloqueados” en un proveedor específico de servicios IoT.
10. Legislación aplicable. Los individuos y empresas se enfrentan a una serie de leyes de protección de datos nacionales / regionales que ofrecen distintos niveles de protección.

A continuación, se mostrará un ejemplo claro de vulneración de dos dispositivos que se encuentran conectados a internet implementando un particular motor de búsqueda donde evidencia uno de los tantos retos y riesgos ya mencionados que

existe en IoT y de los cuales desde ya se están tomando medidas para contrarrestarlos.

Ejemplo: Shodan, un temido motor de búsqueda del Internet de las cosas.

Shodan le permite al usuario encontrar iguales o diferentes tipos específicos de equipos (routers, servidores, etc.) conectados a Internet a través de una variedad de filtros. Puede ser utilizada para descubrir cuál de sus dispositivos están conectados a la Internet, donde se encuentran y quién los utiliza.

En el siguiente ejemplo se demostrará cómo a través de este motor de búsqueda se accede a una cámara y a un router que están vulnerables ante cualquier manipulación o acceso no autorizado en la Web.

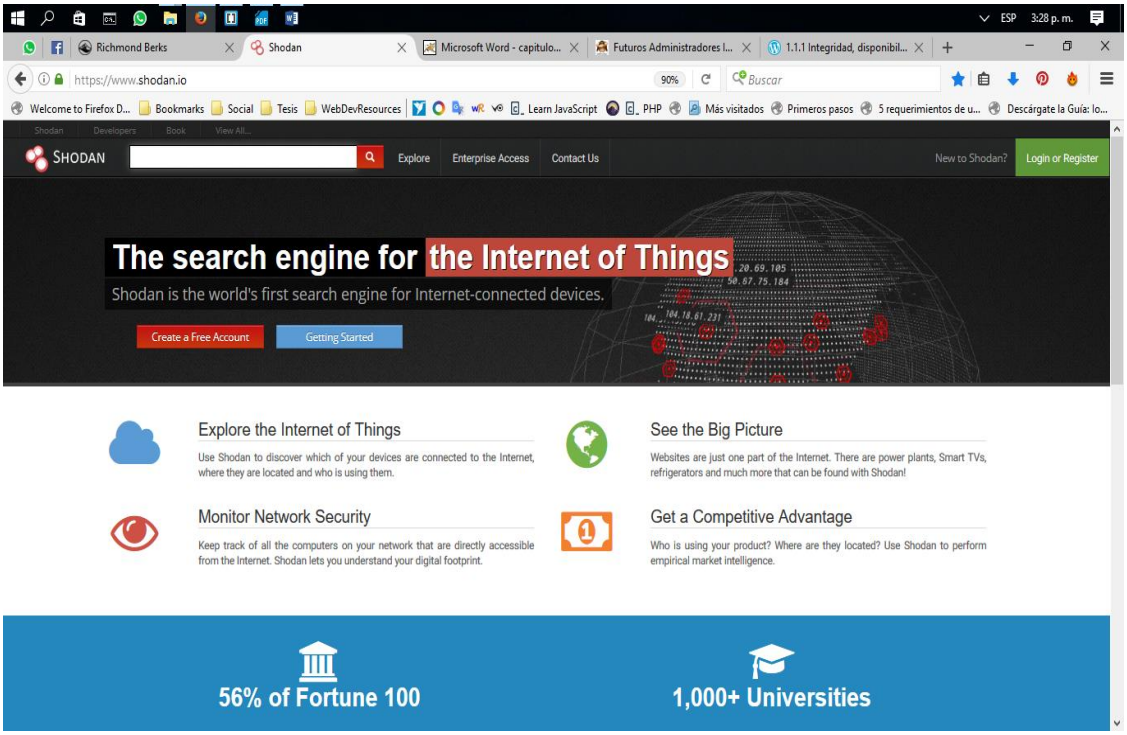


Figura 13 Shodan, página de Inicio, [52]

Caso 1. Cámara IP sin autentificación

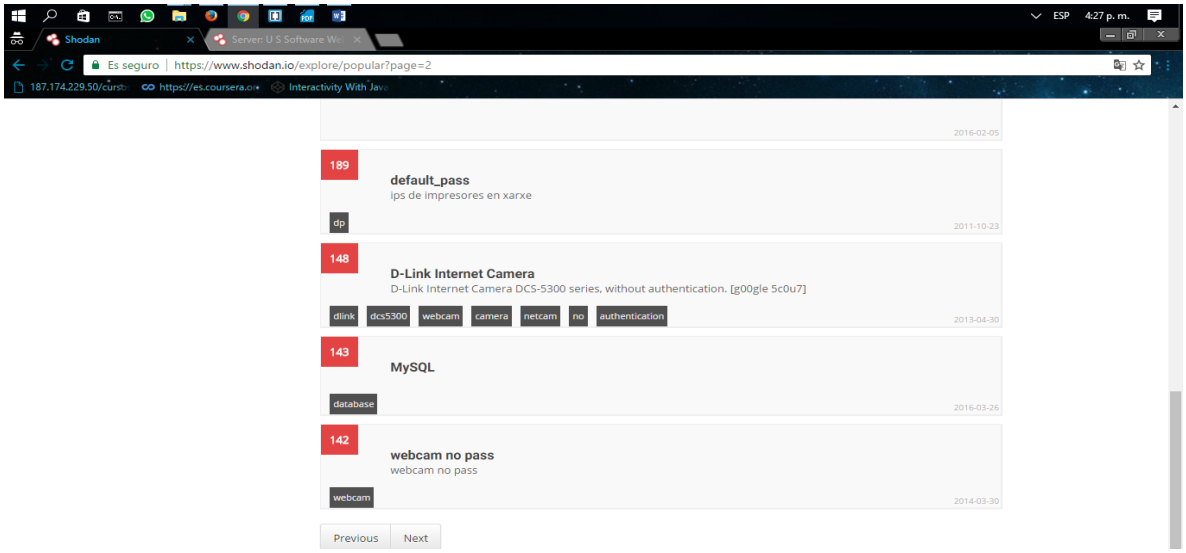


Figura 14. Acceso a webcam no pass – Cámara sin autenticación [52]

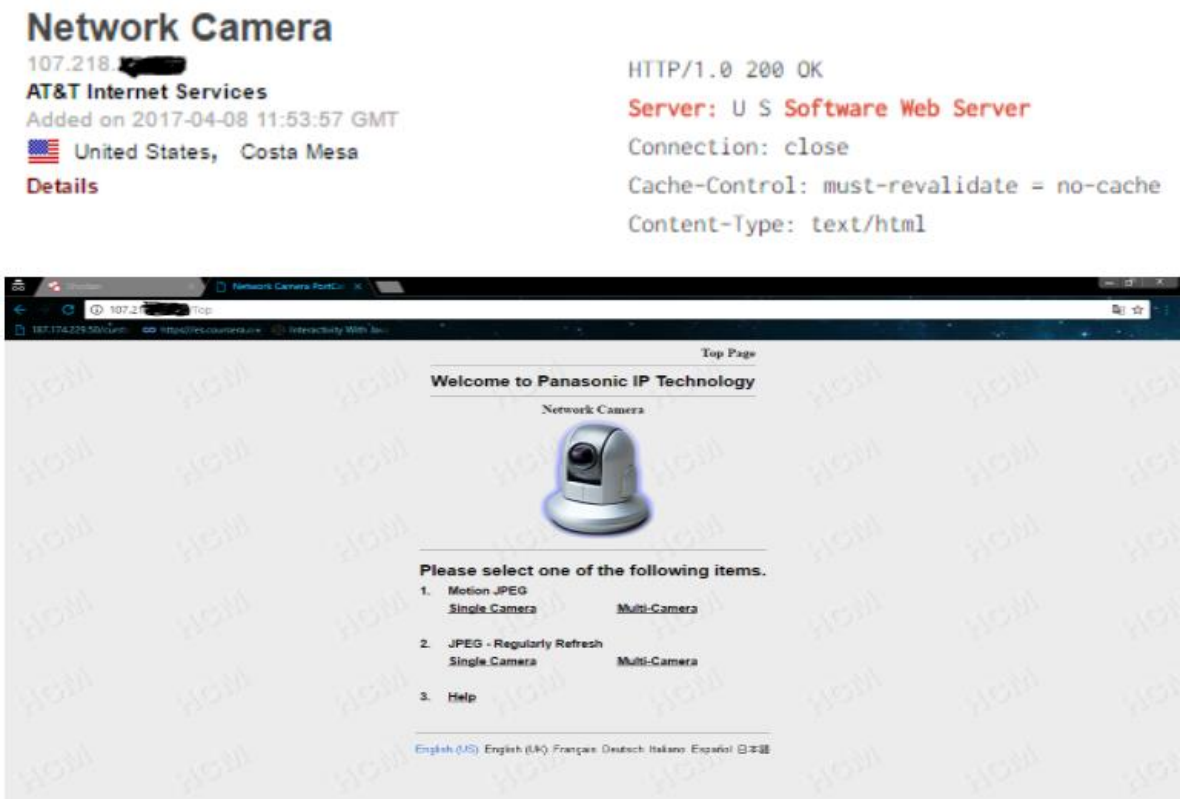


Figura 15. Menú principal del panel de configuración de la cámara [53]

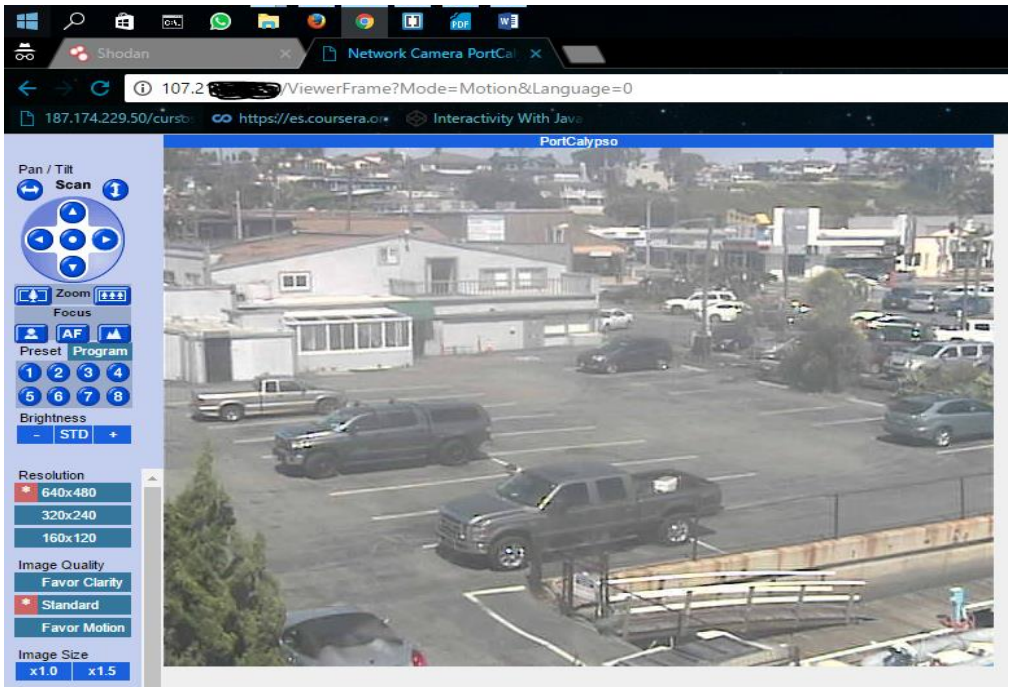


Figura 16. Vista carama en tiempo real [53]

Caso 2: Router con autenticación revelada (user: tmadmin and pass: tmadmin)

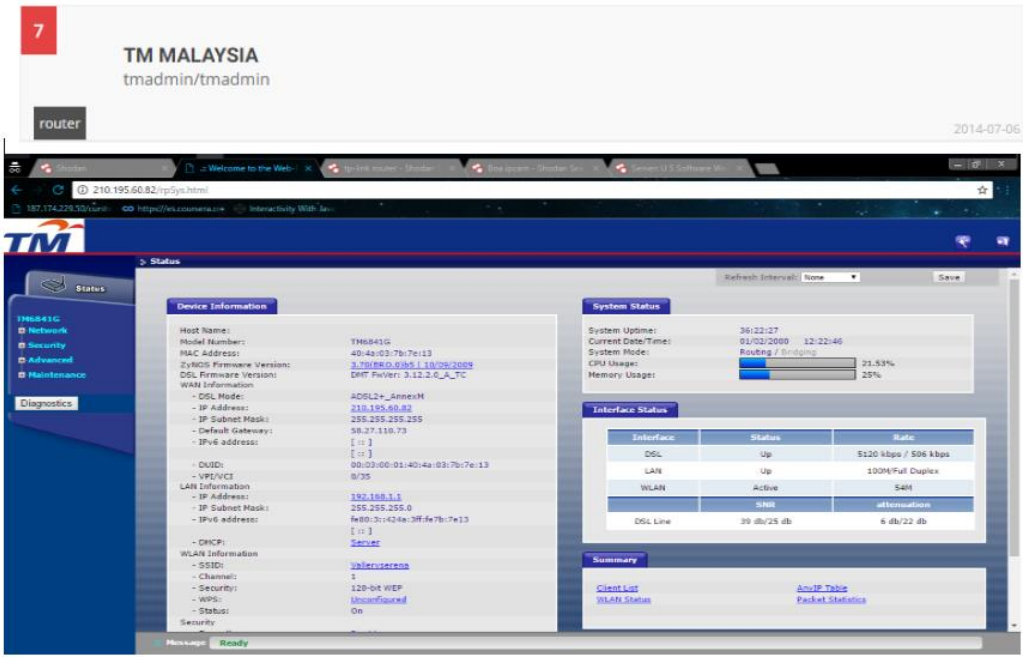


Figura 17. Menú de principal de configuración – sistema penetrado [52]

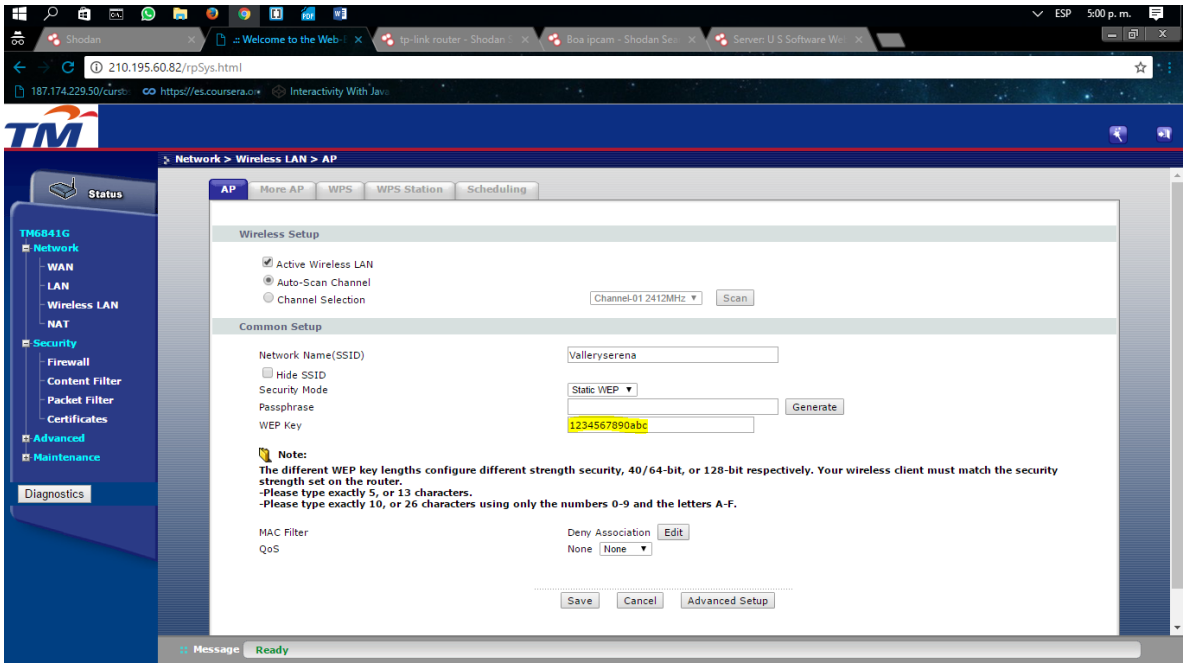


Figura 18. Web Key de router revelada 1234567890abc [52]

Del ejemplo anterior se puede concluir que existen vulnerabilidades en la red como puertos abiertos, interfaces de usuario para aplicaciones sin autenticación, uso de datos de login por defecto o ausencia de cortafuegos que pueden dejar al descubierto quién, cómo, cuando y donde se manipulan los diferentes dispositivos que están conectados a Internet.

Por ello la seguridad en IoT supone un foco importante de riesgos, al mismo tiempo abre la posibilidad para la generación de nuevas ideas y soluciones que contribuyan a tener sistemas más confiables y seguros.

7. CAPÍTULO 2. TECNOLOGÍAS EN RELACIÓN CON IOT

7.1. TECNOLOGÍAS Y PROTOCOLOS DE COMUNICACIÓN.

Las tecnologías de comunicación juegan un papel muy importante en el internet de las cosas, por medio de estas, los dispositivos IoT pueden estar interconectados y compartir información para realizar alguna tarea específica de forma autónoma. Estas tecnologías contienen estándares y protocolos de comunicación que permiten la implementación del IoT.

La siguiente imagen ilustra una serie de tecnologías y protocolos que pueden intervenir a la hora de realizar la comunicación entre dispositivos IoT. Cada una de estas está subdividida de acuerdo a su alcance teniendo como base la clasificación de redes de comunicación de datos.

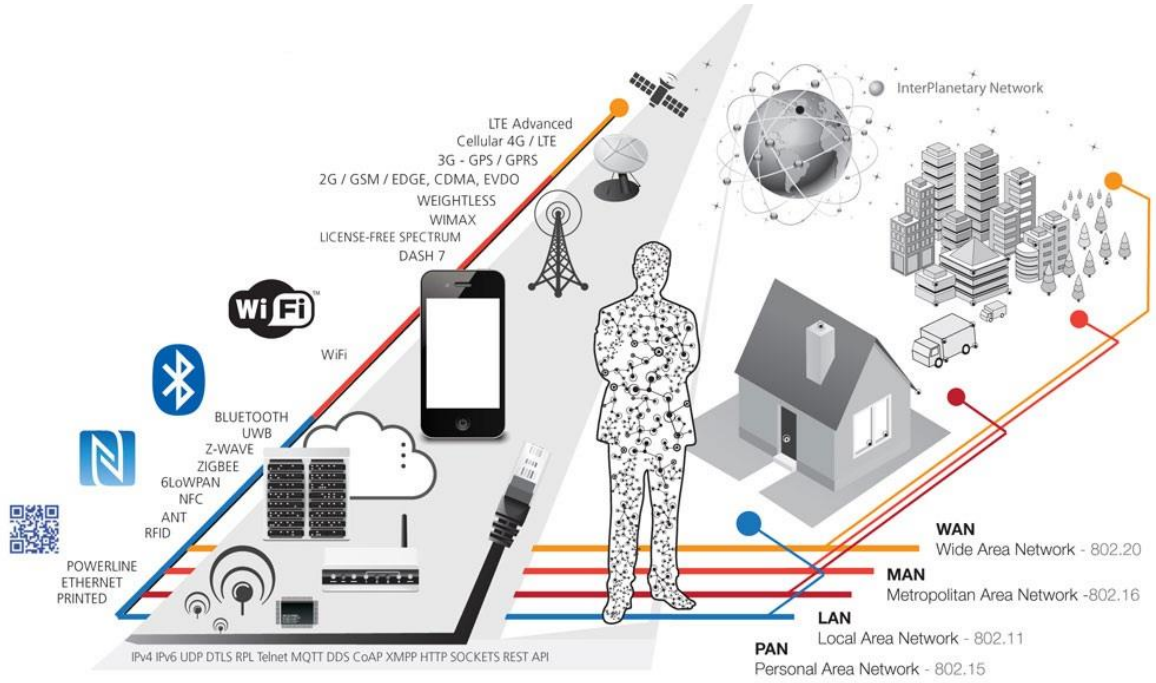


Figura 19. Clasificación de IoT en base al rango de cobertura de los dispositivos [54]

En la clasificación de redes se incluirán solo las WAN, MAN, LAN y PAN por ser las más populares en cuanto a su cobertura. Cada una agrupa un conjunto de tecnologías y protocolos de comunicación algunas necesarias para configuración de una arquitectura IoT, como lo muestra la figura 20.

Figura 20. Clasificación de IoT en base al rango de cobertura de los dispositivos 2 [55]

A continuación, se irán detallando cada una de estas tecnologías con el fin de conocer sus características y aplicación.

Cabe resaltar que se hará énfasis en las tecnologías de comunicación y no en las redes de comunicación de datos ya que estas se utilizarán solo para la clasificación y agrupación de dichas tecnologías y protocolos.

Tecnología WAN

El grupo de tecnologías WAN están conformadas por aquellas que permiten la comunicación inalámbrica de dispositivos interconectados a nivel mundial.
Entre estas tecnologías se encuentran:

Segunda generación de Tecnología Móvil (2G)

La segunda generación de estándares de comunicaciones inalámbrica aplicada a la telefonía celular nació en 1991 y aún sigue en funcionamiento.

Fue la primera en introducir transmisiones 100% digitales con voz y datos, dando lugar a los SMS y MMS. Pese a surgir en los 90, este estándar sigue estando en uso en muchas partes del mundo. Una de las ventajas más evidentes de la naturaleza digital del 2G es que las transmisiones, además de poder comprimirse para que tuvieran un menor tamaño, podrían cifrarse, lo que solucionaba los graves problemas de privacidad de la generación anterior.

El estándar base (estrictamente, 2G) en Europa fue GSM, mientras que en Estados Unidos fue CDMA. Permitían una velocidad máxima teórica de 50 kbps que usualmente se quedaba en unos 10kbps, a la altura de los módems de la época. Posteriormente, las redes 2G mejoraron y podían alcanzar unos 170 kbps con la revisión GPRS (apodado 2.5G) y hasta 384 kbps con la revisión EDGE (apodado 2.75G o 2.9G.

Cabe resaltar que la telefonía móvil 2G no es un estándar o un protocolo sino una forma de marcar el cambio de protocolos de telefonía móvil analógica a digital [56].

Aplicaciones

Telefonía (Voz, *SMS y MMS),* sistemas de seguridad, localizador automático de vehículos, entre otros.

Tercera generación de Tecnología Móvil (3G)

La Tercera Generación *(3G)* de estándares de comunicaciones inalámbrica aplicada a la telefonía celular nació en 2000, en esta generación se transmite voz y datos a través de telefonía móvil mediante el estándar UMTS abreviación de Universal *Mobile Telecommunications System* que traducido Servicio Universal de Telecomunicaciones Móviles*.*

Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir voz y datos (como la descarga de programas, intercambio de correos electrónicos, y mensajería instantánea).

Tras la segunda generación, la industria se puso manos a la obra con el 3G, prometiendo Internet móvil a la altura de las conexiones domésticas. En Europa, Japón y China se adoptó el estándar UMTS, que no dependía de la infraestructura GSM anterior. En EEUU y Corea del Sur, se optó por CDMA- 2000, construidos sobre la infraestructura de las redes 2G. UMTS se implementó principalmente como W-CDMA y ofrecía, en teoría, de 300 kbps a 2 Mbps. A pesar de las mejoras, no tardó en recibir ‘actualizaciones’ que aumentaban aún más su ancho de banda: HSPA (representado como H en el móvil, entre 600 kbps y 10 Mbps) y HSPA+ (representado como H+, puede llegar a los 672 Mbps teóricos, aunque se suele quedar en 100).

La arquitectura de funcionamiento es similar a la tecnología 4G, sin embargo, esta red mantiene la voz mediante una red celular clásica y los datos los transmite mediante una red IP, por lo tanto, son necesarias dos frecuencias de funcionamiento [57].

Aplicaciones

Telefonía, navegación Web, enlaces M2M, contadores inteligentes, control de activos (vehículos, mercancías, etc.)

Cuarta Generación de Tecnología Móvil (4G)

4G LTE *(Long Term Evolution*) es un estándar de comunicaciones inalámbrico de alta velocidad de transmisión para dispositivos en uso desde el año 2008. Está basado en la tecnología de red GSM y HSPA, siendo esta la cuarta generación. La arquitectura principal es común a las anteriores versiones en cuanto a requerir una tarjeta SIM con un contrato y una torreta que dé cobertura al terminal, sin embargo, la gran diferencia de LTE frente a sus predecesoras radica en que las antenas de comunicaciones de las torretas están basadas en redes IP tanto para datos como para voz, permitiendo simplificar los costes de operación y aumentar considerablemente el rendimiento.

Esta modificación de arquitectura ha hecho que las antenas sean incompatibles con 3G y 2G, por lo tanto, todos los dispositivos IoT que pretendan usar LTE deberán tener capacidad multibanda para poder ser utilizados en todo el mundo [58].

Cabe resaltar que esta tecnología por hacer uso de sistemas de telefonía, requiere de un contrato con un operador para poder usar las torretas, por lo tanto, estamos ante dos factores limitantes, el coste por uso y la necesidad de disponer de cobertura LTE en la localización de los dispositivos **I**oT**.**

Aplicaciones

Telefonía, navegación web, enlaces M2M, contadores inteligentes, control de activos (vehículos, mercancías, entre otros)

Quinta Generación de Tecnología Móvil (5G)

La quinta generación de tecnologías móvil por su abreviación 5G es la próxima tecnología de redes inalámbricas. Actualmente se encuentra en desarrollo y sin estandarizar, se espera que su uso común inicie en 2020.

Con la red 5G los usuarios tendrán mayor ancho de banda, y, por tanto, más velocidad, con lo que habrá mayores posibilidades de desarrollar la realidad virtual, descargas de video HD en segundos hasta la presencia de hologramas, en un futuro. Sin embargo, lo más llamativo que tiene 5G, es la capacidad de desplegar el tan esperado "Internet de las Cosas", en diferentes campos variados para los cuales la red 4G no estaba aún preparada. Debido a que 5G hace uso de un espectro de onda más ancho será posible hacer más ágil la transmisión de datos, lo cual es una necesidad dentro del Internet de las Cosas. "Se necesita una red que tenga una latencia de pocos milisegundos, por ejemplo, con la red 4G para que un vehículo autónomo que va a 100 km/h frene se necesitarían tres metros, mientras que con la red 5G solo necesita de unos centímetros", explica el matemático de *Huawei Mérouane Debbah Paris*.

Se puede avizorar que una variedad de aplicaciones de IoT que aprovechan la infraestructura celular podrían ser prevalentes en 2020. Existen oportunidades que van desde medidores de potencia empleados en la Red Eléctrica Inteligente hasta Sistemas Públicos de Alertas que utilizan sensores de detección de terremotos / tsunamis conectados de manera inalámbrica. Todos estos tipos de aplicaciones pueden y están comenzando a desplegarse incluso en las redes celulares de hoy. Sin embargo, se predice que las aplicaciones de la Internet de las Cosas crecerán a un ritmo mucho más veloz que el que quizá puedan manejar de forma óptima las redes y tecnologías celulares existentes. Para dar soporte a los posibles miles de millones de dispositivos IoT, se necesita una infraestructura inalámbrica que no solo sea escalable en términos de su capacidad, sino que además pueda manejar de manera óptima las diferentes necesidades de servicio de diversas verticales de IoT. Ejemplos de distintas necesidades de servicios incluyen distintos requisitos de movilidad, latencia, confiabilidad y fortaleza de las redes. Estos conjuntos diversos de requisitos pueden exigir una re-arquitectura de los componentes clave de la red celular, por ejemplo, para dar soporte a la movilidad a demanda en que la movilidad solamente se suministre a aquéllos dispositivos y servicios que la necesitan. El siguiente ejemplo de casos de uso con Comunicaciones Tipo Máquina (MTC)[2] se convertirá en la norma societaria en torno del año 2020. [59]

[2] *En la industria se usan diferentes términos para describir las comunicaciones máquina a máquina. Entre ellos: IoT, M2M, MTC, etc. En el presente trabajo, los empleamos de manera indistinta.*

Aplicaciones

Realidad Virtual, Realidad aumentada, Internet táctil, Juegos en la nube, redes sensoriales, automatización industrial, vehículos sin conductor, edificios inteligentes, sistemas de seguridad IoT, entre otros.

Figura 21. Sectores de aplicación 5G [60]

Sistema de Posicionamiento Global (GPS)

El Sistema de Posicionamiento Global por sus siglas GPS, aunque su nombre correcto es NAVSTAR-GPS, es un sistema mundial de navegación desarrollado por el Departamento de Defensa de los Estados Unidos. Actualmente este sistema consta de 24 satélites artificiales *(21 regulares más 3 de respaldo)* y sus respectivas estaciones en tierra, proporcionando información para el posicionamiento las 24 horas del día sin importar las condiciones del tiempo.

Los satélites artificiales son utilizados por el G.P.S, como punto de referencia para el cálculo de posiciones de puntos sobre la superficie de la tierra con precisiones cada día mejores.

Desde sus inicios puramente militares en el año 1978, sus aplicaciones han ido incrementándose constantemente en diversas áreas y los equipos receptores de G.P.S han ido disminuyendo tanto en tamaño como en costo.

En el campo de la ingeniería civil, el G.P.S se ha convertido en una herramienta indispensable para profesionales y técnicos en la determinación de posiciones y realización de levantamientos topográficos con rapidez y precisión.

Actualmente la tecnología existente permite manejar los datos obtenidos por medio de G.P.S. con los programas de aplicación en las ramas de ingeniería y geodesia. Este sistema evoluciona dando paso a A-GPS [61].

Aplicaciones

Transporte, topografía, meteorología, telecomunicaciones, sistema de localización, sistemas de seguridad, entre otros.

Tecnología MAN

Este conjunto de tecnologías está caracterizado por ser diseñada para dar cobertura a una distancia menor en comparación de las tecnologías WAN, es decir abarca un área metropolitana.

Weightless

Weightless es una tecnología de comunicación inalámbrica de última generación orientada a M2M y con tres premisas fundamentales, muy bajo coste, muy bajo consumo y buena propagación de onda para aumentar su rango de trabajo.

Actualmente existen dos versiones de esta tecnología, Weightless-W diseñada para el uso de las frecuencias de ruido blando en la señal de televisión y la versión N (en diseño) que hace uso de la banda de frecuencia ISM. El gran atractivo de esta tecnología reside en que los dispositivos tienen un alcance de hasta 5 km, un coste favorable y además una duración estimada de batería de hasta 10 años.

Además de todo ello, al hacer uso de bandas en baja frecuencia consigue alcanzar una alta penetración en edificios y mejora su propagación [62].

Aplicaciones

Dada su alta penetración en edificios, su bajo consumo y bajo coste es ideal para cualquier aplicación IoT en Smart City.

WIMAX

WiMAX es una tecnología de comunicación inalámbrica basada en estándar IEEE 802.16 y está diseñado específicamente para enlaces sin línea de visión directa (NLoS) entre el suscriptor y la estación base, por lo tanto, la hace especialmente útil para entornos urbanos densamente poblados donde es utilizada para el despliegue de última milla de líneas de acceso a internet.

Debido al alto coste de las estaciones y terminales este tipo de tecnología ve reducida su utilidad a aquellas aplicaciones de IoT en las que el número de dispositivos sea bajo y el coste no sea un factor determinante. Sin embargo, el uso del WiMAX si tiene especial interés actuando como nexo de unión entre redes (uniendo por ejemplo un nodo Zigbee con internet).

Tal y como podemos ver en el gráfico 3, se podría considerar el WiMAX como el punto intermedio entre velocidad y movilidad de las tecnologías inalámbricas [63].

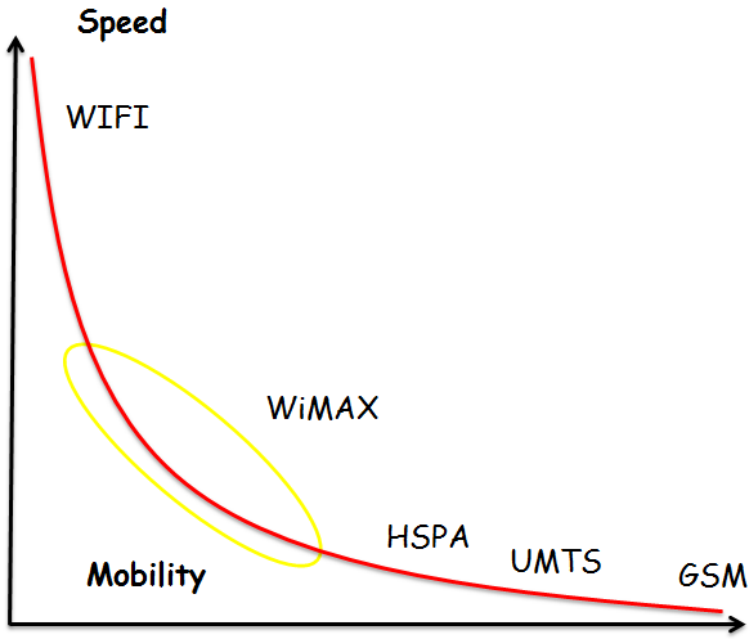


Gráfico 3. Comparación ente velocidad y movilidad de tecnologías inalámbricas. [63]

Aplicaciones

Routers, acceso de internet de última milla, aplicaciones en zonas NLoS.

DASH7

Dash7 es un estándar abierto de comunicación de baja potencia y rango medio diseñado en base al modelo BLAST (*Bursty Light data Asyncronous Stealth Transient*), cuyas particularidades hacen que las transmisiones sean caracterizadas por:

- *Bursty:* la transmisión de datos es abrupta y no contiene audio ni video.
- *Ligera*: los paquetes suelen estar limitados a 256 bits.
- *Asincrónica:* por diseño, la comunicación no requiere saludo ni sincronización de dispositivos.
- *Stealth:* los nodos de conexión pueden escoger comunicarse solo con algunos dispositivos.
- *Transitional:* Al contrario que otras tecnologías Wireless, Dash7 está orientado a la subida de datos por lo que es más sencillo hacer que respondan a ciertos dispositivos [64].

Figura 22 Esquema de características de tecnología DASH7 [64]

Gracias a su diseño y a la duración de la batería (en algunos casos de años) esta tecnología está especialmente adaptada para ser utilizada en redes sensoriales, donde su rendimiento está demostrando que es muy superior al WiFi, ZigBee y tecnologías RFID activas.

Aplicaciones

Información de plazas libres en parkings, dispositivos que presentan información en base a la posición (útil para museos, por ejemplo), o la implementación de un sistema de monitorización de mercancías dentro de almacenes en minutos sin necesidad de cables ni antenas.

Enocean

EnOcean es una tecnología inalámbrica revolucionaria con función de captación de energía. Su principal elemento diferenciador con respecto al resto de competidores consiste en disponer de un sistema de alimentación completamente autónomo (sin batería), lo cual lo hace ideal para aquellas aplicaciones del tipo de redes sensoriales [65].

Existen actualmente tres modelos de captación de energía:

- *Captación de energía mediante movimiento:* Este sistema está basado en la conversión de energía electrodinámica. Mediante el ligero movimiento de un pequeño botón el sistema es capaz de generar energía para enviar tres datagramas con una sola oscilación.
- *Células solares de interior:* Este sistema permite la conversión lumínica en energía, estando especialmente diseñado para funcionar en interiores, con un tamaño de entre 5cm y 3.5cm es fácilmente acoplable a cualquier sensor. Existen dos variantes, una permite la comunicación unidireccional y la otra bidireccional.
- *Conversión térmica:* Mediante estos módulos es posible capturar la energía térmica emitida por radiadores, maquinaria o el propio cuerpo humano y convertirla en energía eléctrica, sumado a todo ello el rango diferencial de temperatura para su correcto funcionamiento es muy bajo, no siendo necesario grandes cambios de temperatura.

Las fusiones de un diseño de protocolo de bajo consumo con captadora de energía hacen que esta tecnología disponga de una gran flexibilidad en cuanto a aplicaciones, ahorrando mucha energía y requiriendo menos mantenimiento (dispositivos del tipo instalar-olvidar). A todo hay que sumarle que son ecológicamente compatibles. Por todo ello estamos ante una tecnología con un gran futuro en cuanto a monitorización industrial y de edificaciones fundamentalmente.

Aplicaciones

Automatización de edificios, Hogares inteligentes, Medicina (control de pacientes), logística, entre otros.

PLC

Power-Line Communication (PLC) hace referencia a un sistema de transmisión de datos a través de cables por el cual discurre simultáneamente corriente alterna.

La principal ventaja de este método de transmisión de datos entre dispositivos radica en que si es necesario alimentarlos mediante corriente eléctrica no es necesaria la instalación de más cableado.

Existen dos modelos de funcionamiento, PLC de banda estrecha o de banda ancha. La banda estrecha tiene su uso en aplicaciones residenciales o tipo LAN, mientras que las soluciones de banda ancha permiten la transmisión a grandes distancias (pudiendo ser usado para proveer de acceso a internet).

Sin embargo, el gran problema de esta tecnología viene caracterizado por la naturaleza del trenzado de cable eléctrico que se encuentra sin blindar y sin giros, por lo tanto, termina comportándose como una antena, provocando interferencias y recibiéndolas de las emisiones de radio [66].

Aplicaciones

Todas aquellas aplicaciones en los cuales exista alimentación eléctrica y/o entornos hostiles de radiotransmisión.

Ethernet

Ethernet es una familia de tecnologías de red de transmisión por cable, ya sean de cobre, coaxial o fibra óptica. A día de hoy se considera la tecnología dominante en transmisión de datos a nivel mundial, aunque poco a poco comienza a desplazarla las tecnologías WIFI.

Las principales ventajas de esta familia son las altísimas velocidades de transmisión posibles y las largas distancias que es capaz de cubrir, todo ello siendo muy resistente a las interferencias (gracias al blindaje de los cableados o las propias características de la transmisión de ondas lumínicas).

Sin embargo, los principales puntos débiles de esta tecnología tales como la falta de movilidad y dificultad de instalación (necesario tendido de cableado) hacen que su aplicación en IoT quede limitado a aquellas aplicaciones que requieran un muy alto ancho de banda o la seguridad que proporciona el cableado físico [67].

Aplicaciones

Fundamentalmente como enlace entre nodos y con internet en localizaciones estáticas.

QR Codes

Un código QR *(del inglés Quick Response code, "código de respuesta rápida")* es un código de barras bidimensional cuadrada que puede almacenar los datos codificados. La mayoría del tiempo los datos es un enlace a un sitio web (URL).

Códigos QR fueron creados en 1994 por Denso Wave, subsidiaria japonesa en el Grupo Toyota. El uso de esta tecnología es ahora libre. El Código QR no es el único código de barras de dos dimensiones en el mercado, otro ejemplo es el código de matriz de datos.

En sus inicios lo códigos QR se utilizaron para registrar repuestos de automóviles e inventarios. Actualmente los Smartphone y otros dispositivos inteligentes decodifican estos códigos de manera sencilla y económica. Fundamentalmente se usan para escribir direcciones web donde permiten el ingreso más rápido a una página ya que los usuarios se libran de la tarea de ingresar las direcciones de manera manual. Existen entidades dedicadas a la elaboración y distribución de las etiquetas QR de acuerdo al entorno donde se aplican (industrial comercial, entre otros), para la mayoría de los casos una etiqueta sencilla, donde se garantice el adecuado contraste entre el fondo y los símbolos es más que suficiente para la lectura por parte de un dispositivo inteligente. Muchas páginas web ofrecen el servicio de codificación de manera gratuita, por lo que ese ha sido el método usado para la generación [68].

Aplicaciones

Se utiliza en Smartphone, en la medicina, comercio electrónico, posición GPS, entre otros.

Tecnología LAN/PAN

Estas tecnologías abarcan todas aquellas redes de área local o área personal, con un rango desde varios metros hasta centímetros.

Cabe resaltar que la mayoría de aplicaciones y dispositivos IoT están relacionadas con este tipo de redes por lo cual es necesario realizar un estudio más profundo de dichas tecnologías y así tener una visión más clara.

Wifi

Es posible considerar como Wifi a todos aquellos dispositivos inalámbricos que utilizan los estándares IEEE 802.11, o lo que es lo mismo, es una tecnología de intercambio de datos inalámbrica que sigue los estándares del IEEE.

Si bien es cierto que inicialmente los protocolos basados en IEEE 802.15.4 han sido los dominantes poco a poco los desarrolladores están reduciendo el consumo de los dispositivos Wifi de manera que puedan competir con tecnologías como Zigbee o 6LoPAN.

Una de las grandes ventajas que dispone Wifi frente a sus competidores con menos consumo es que disponen de compatibilidad nativa para redes IP, lo cual es muy importante para las redes IoT. Otra de las grandes ventajas es lo ampliamente extendido que está la tecnología en redes LAN, lo cual permite disponer de herramientas más avanzadas y una integración mucho más sencilla [69].

En el lado negativo es fácil entrever que el ser compatible de manera nativa con IP tiene un efecto nocivo en cuanto a la duración de la batería, ya que al contrario que con otras tecnologías es necesario realizar conexiones periódicas.

- **Estándar:** Basado en 802.11n
- **Frecuencia:** 2,4GHz y 5GHz
- **Alcance:** Aproximadamente 50m
- **Velocidad de transferencia:** hasta 600 Mbps, pero lo habitual es 150-200Mbps, en función del canal de frecuencia utilizado y del número de antenas (el standard 802.11-ac ofrece desde 500Mbps hasta 1Gbps)

Aplicaciones

Routers, SmarPhone, Tablets, laptops, entre otros.

Z-Wave

Z-Wave es un protocolo de comunicaciones diseñado específicamente para su uso en domótica del hogar o pequeños comercios. Esta tecnología está compuesta por un emisor de radio frecuencia de bajo consumo que puede ser encastrado en sistemas de iluminación, controles de acceso, etc.

Su esquema de funcionamiento es en red de malla siendo necesario tan solo dos dispositivos para comunicarse (un controlador y un dispositivo) pudiendo ir añadiéndose después más controladores o dispositivos como se deseen.

- **Estándar:** Z-Wave Alliance ZAD12837 / ITU-T G.9959
- **Frecuencia:** 900MHz (Banda ISM)
- **Alcance:** 30m
- **Velocidad de transferencia:** 9,6/40/100kbit/s

Sus principales ventajas son:

- Fácil de instalar.
- No requiere cableado.
- Requiere poca inversión inicial.
- Seguro y confiable (10 años en el mercado).
- 20 millones de productos en hogares del mundo.
- 9 de cada 10 compañías de seguridad lo usan.

Sus inconvenientes surgen directamente de sus premisas de diseño, está altamente adaptado al entorno de domótica del hogar, por lo tanto, sus campos de actuación quedan limitados como tecnología de uso general [70].

Aplicaciones

Domótica del hogar.

ZigBee

Esta tecnología hace uso de la capa física y de control de acceso al medio del estándar del IEEE 802.15.4, añadiendo cuatro componentes más, como son la capa de red, la de aplicación, los ZDOs (Zigbe Device Objects, responsable entre otras cosas del descubrimiento, seguridad y requerimientos de unión a la red) y por último de los objetos de aplicación definidos por los fabricantes que permiten la personalización y favorecen la integración.

Actualmente existen 3 especificaciones que sirven de base para ZigBee

- Especificación ZigBee: es el núcleo de la especificación como tal y define la versión ZigBee y ZigBee PRO (la más extendida). El objetivo de esta especificación es un sistema auto configurable, que sea capaz de auto-repararse, de bajo precio y muy bajo consumo energético, todo ello combinado con flexibilidad, movilidad y sencillez de uso.

- Especificación ZigBee IP: este estándar abierto es el primero para IPv6 que permite conectar completamente la red Malla a internet y está específicamente diseñado para dar soporte al estándar ZigBee Smart Energy ver.2 que está en desarrollo.

- Especificación RF4CE: esta especificación es una particularización de los casos de usos en los que no es necesario una red Mall completa, sino que es más bien para conectar dos dispositivos entre ellos, con lo que se consigue que el requerimiento de memoria sea mucho menor permitiendo con ello reducir aún más el coste.

Esta tecnología no ha hecho más que crecer desde su nacimiento hasta convertirse hoy en día en la tecnología de referencia para el estándar IEEE 802.15.4 [71].

- Estándar: ZigBee 3.0 basado en IEEE 802.15.4
- Frecuencia: 2.4GHz
- Alcance: 10-100m
- Velocidad de transferencia: 250kbps

Z-Wave y ZigBee son tecnologías de comunicación inalámbrica basadas en chip que permiten transmitir y recibir pequeñas instrucciones (señales de comando). Los chips Z-Wave y ZigBee se utilizan para crear sistemas inalámbricos que controlan funciones de iluminación, seguridad, acceso, sensores, alarmas y comunicación entre dispositivos residenciales o industriales. Los chips de ambas tecnologías son de muy bajo consumo de energía, por lo que pueden funcionar con base en pilas ordinarias en intervalos de tiempo que alcanzan el orden de años.

Las redes basadas en estas tecnologías son de topología de tipo malla (mesh), esto quiere decir que no dependen de un punto central de control (un servidor), ya que la plataforma de conectividad se establece a partir de dispositivos compatibles que se enlazan entre sí, como se muestra en la figura 26 [71].

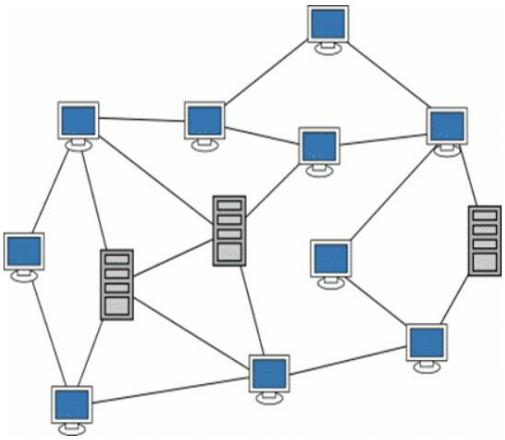


Figura 23 Diagrama de conexión una red tipo MESH [71]

	ZIGBEE	Z-WAVE
Tipo de estándar	Estándar abierto	Tecnología propietaria desarrollada por la empresa SigmaDesigns (que vende chips y software a las firmas que deseen diseñar productos compatibles con Z-Wave)
Respaldo de la Industria	Tecnología impulsada por la ZigBee Alliance (alianza industrial que incluye a firmas como Chipcom, Honeywell, Mitsubishi, Ember, Motorola, Samsung, Philips)	Estándar respaldado por la Z-Wave Alliance (grupo de empresas que se encarga de vigilar la compatibilidad entre productos, y que está liderado por las firmas Dayfoss, Intermatic, Leviton, UEI, Wayne Dalton y Zensys)
Capacidad de datos	Hasta 250 Kbps (en chips de primera generación)	40Kbps (en chips de segunda generación)
Capacidad en red	Soporta hasta 65,536 dispositivos	Soporta hasta 232 dispositivos. Es posible unir (puntear) redes
	2.4 GHz o 900 MHz en	868.42/900/ 916 /919.82

Frecuencias	26 canales	MHz en un canal
Patrón de propagación	Flooding	Routing
Mercados potenciales	Zonas comerciales, espacios residenciales y áreas industriales	Espacios residenciales

Tabla 5 ZigBee vs Z-Wave [72]

Aplicaciones:

Especializado en redes intra-edificaciones, por lo tanto, en general todas las aplicaciones de domótica e industriales de corto alcance.

Bluetooth

Bluetooth es una tecnología de comunicación inalámbrica entre dispositivos para intercambio de datos en el ámbito de las redes PAN. Originalmente se diseñó como una alternativa inalámbrica a la comunicación rs-232, sin embargo, hoy en día Bluetooth es mantenido por la Bluetooth Special Interest Group y está formado por más de 20.000 empresas.

En su primera versión esta tecnología no ofrecía suficientes características que la hicieran atractiva para IoT, sin embargo, con la aparición de un nuevo estándar denominado Bluetooth Low Energy la situación ha cambiado hasta el punto que algunos especialistas consideran que la creación de IoT tiene mucho que ver con esta tecnología [73].

Al igual que sucede con las tecnologías como ZigBee, el campo de aplicación concreto hace que su desarrollo en un futuro a corto plazo sea muy amplio, siendo a día de hoy uno de los referentes en cuanto a tecnologías en el mercado.

- Estándar: Bluetooth 4.2
- Frecuencia: 2,4GHz (ISM)
- Alcance: 50-150m (Smart/LE)
- Velocidad de transferencia: 1Mbps (Smart/LE)

Aplicaciones:

Sobre todo, Wearables[3] y sistemas con un número no muy alto de dispositivos.

[3] Hace referencia al conjunto de aparatos y dispositivos electrónicos que se incorporan en alguna parte de nuestro cuerpo interactuando de forma continua con el usuario.

ANT / ANT+

ANT es una tecnología de red wireless para sensores, multicast y de acceso abierto desarrollada por Dynastream Innovations (Canadá). Al igual que otras tecnologías está orientada especialmente al ULP (Ultra Low Power) de manera que los dispositivos pueden funcionar desde unos meses a años con la ayuda de una pequeña pila.

Este tipo de tecnología tiene corto alcance y soporta varias configuraciones de red, tales como estrella, malla o P2P, haciéndola muy práctica para su uso en redes PAN o LAN incluso (aumentando el rango mediante el uso de redes malla).

Existen dos versiones de este protocolo, ANT y ANT+ siendo la principal diferencia la compatibilidad total de dispositivos en la tecnología ANT+ mediante el uso de perfiles de uso.

Actualmente su uso está ampliamente extendido en el mundo de los Wearables y Gadgets de salud personal, sin embargo, no ha terminado de despegar como tecnología usada en redes sensoriales industriales [74].

Aplicaciones

Actualmente su uso está prácticamente limitado a dispositivos 1 a 1 y de corto alcance pese a que la tecnología está diseñada para redes de dispositivos M2M.

RFID

La tecnología RFID es un sistema inalámbrico de identificación por radiofrecuencia basado en el uso de campos magnéticos para transmisión de un identificador gracias a un lector. Esto permite acoplar a objetos (incluso animales) un chip que permite realizar un seguimiento, aunque no permite la comunicación en los dos sentidos.

Existen tres modos de transmisión de datos, el primero mediante la inducción de campos electromagnéticos cerca del emisor, el segundo modo mediante el uso de dispositivos con batería que les permita emitir su código (alcanzando incluso cientos de metros) y por último otros actúan como un transpondedor pasivo usando la energía que reciben del lector al intentar hacer un escaneado [75].

Aplicaciones

Inventario, Acceso presencial, peajes, ID de animales.

NFC

NFC es una tecnología inalámbrica de muy corto alcance con un concepto muy similar a la tecnología RFID, sin embargo, en este caso se pretende generar un campo magnético muy pequeño de manera que sea difícil interceptar.

Es necesario en esta tecnología que una parte actúe como iniciador generando un campo de radio-frecuencia que puede alimentar a la otra parte que actuará como receptor pasivo. La gran diferencia con un sistema RFID normal es que el código a emitir puede ser variable y se permite la comunicación entre dispositivos ya que ambos pueden estar alimentados por corriente eléctrica [76].

Estándar: ISO/IEC 18000-3
Frecuencia: 13.56MHz (ISM)
Alcance: 10cm
Velocidad de transferencia: 100–420kbps

Aplicaciones

Control de acceso, monederos inteligentes, teléfonos para pagos, etiquetas NFC.

Message Queue Telemetry Transport (MQTT)

Es un protocolo ligero usado para la comunicación máquina a máquina (M2M) en el Internet of Things ya que los clientes son pequeños y utiliza el ancho de banda de red de forma eficiente, facilitando ser utilizado en la mayoría de los dispositivos empotrados con pocos recursos. La cabecera de longitud fija tiene sólo 2 bytes de longitud y se minimizan los intercambios de protocolo para reducir el tráfico en la red. Se ejecuta sobre TCP/IP, que proporciona conectividad de red básica. No depende en modo alguno del contenido del mensaje.

El protocolo MQTT da soporte a la entrega asegurada y a transferencias 'dispara y olvida'. Es un protocolo de publicación/suscripción por lo que la entrega de mensajes es independiente de la aplicación. La entrega desacoplada libera a una aplicación de tener que estar conectada a un servidor y esperando mensajes. El modelo de interacción es como en el correo electrónico, pero optimizado para la programación de aplicaciones.

La entrega de mensajes puede ser de tres tipos: como máximo una vez, los mensajes se entregan en base a la carga de la red, se puede producir pérdida de mensajes; al menos una vez, se asegura que los mensajes llegan, pero se pueden producir duplicados; exactamente una vez, se asegura que los mensajes llegan

exactamente una sola vez. Además, dispone de una función que notifica a los suscriptores si se produce una desconexión de un cliente de un servidor MQTT.

La arquitectura de MQTT sigue una topología de estrella, con un nodo central que hace de servidor o “broker” con una capacidad de hasta 10.000 clientes. El broker es el encargado de gestionar la red y de transmitir los mensajes, para mantener activo el canal, los clientes mandan periódicamente un paquete (PINGREQ) y esperan la respuesta del bróker (PINGRESP). La comunicación puede ser cifrada entre otras muchas opciones.

La comunicación se basa en unos “topics” (temas), que el cliente que publica el mensaje crea y los nodos que deseen recibirlo deben suscribirse a él. La comunicación puede ser de uno a uno, o de uno a muchos. Un “topic” se representa mediante una cadena y tiene una estructura jerárquica. Cada jerarquía se separa con ‘/’. De esta forma un nodo puede suscribirse a un “topic” concreto o a varios. [77]

Aplicaciones

Redes de dispositivos Machine to Machine *(M2M)*

7.2. CLOUD AND FOG COMPUTING

¿Qué es la Nube?

La nube (The Cloud) es una abreviatura para describir la enorme red interconectada de servidores diseñados para entregar recursos informáticos sin un sentido de ubicación. En otras palabras, la nube concibe a los usuarios como una gigantesca masa que requiere de poder computacional para ejecutar todos los servicios que puedan ser ofrecidos a través de la web.

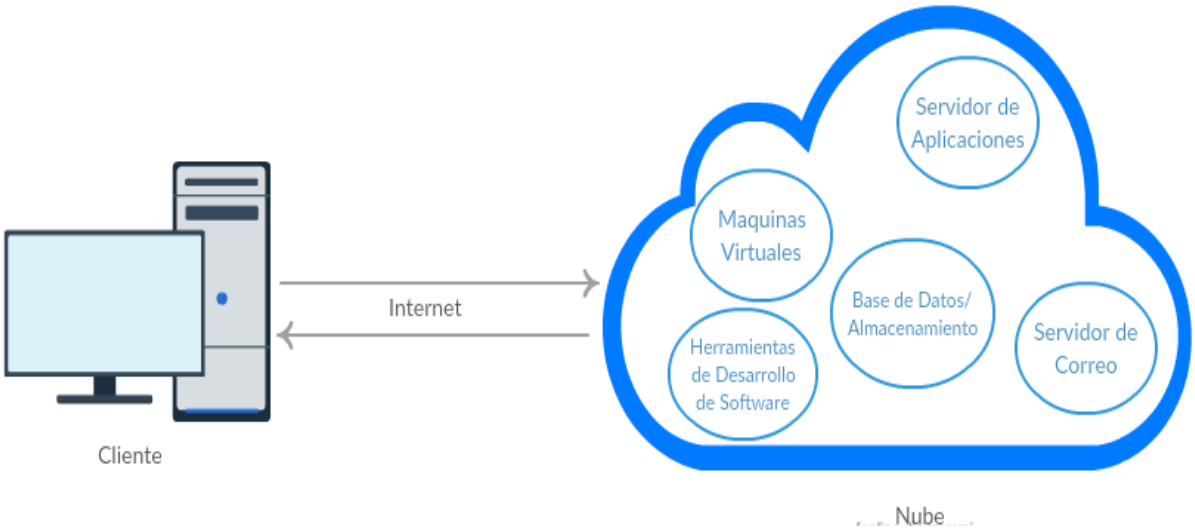


Figura 24 Servicios en la Nube [78]

La computación en la nube es considerada una colección de servicios proporcionados por diferentes proveedores. Los servicios en la nube eliminan la adquisición de tecnología y la sustituyen por productos que se administran en otros lugares y que sólo están activos cuando se necesitan.

La computación en nube encapsula una amplia gama de servicios empresariales y de consumo, utilizando recursos a través de Internet que se encuentran en algún otro lugar del mundo para propósitos específicos [78].

La interacción con un servicio en la nube normalmente se realiza a través de un navegador web o una interfaz de línea de comandos. Por lo general, no hay software para instalar, ni hay hardware para configurar.

Fog computing (Computación en la niebla)

Fog computing es considerada una extensión del **cloud computing.** El concepto alude a algo más simple de lo que parece: en lugar de alojar los datos en una nube centralizada, los datos se distribuyen a través de los llamados sistemas de niebla que operan en los “extremos” de la red [79].

En lugar de establecer canales de almacenamiento en la nube, los datos son procesados localmente en un dispositivo inteligente sin ser enviados a la nube.

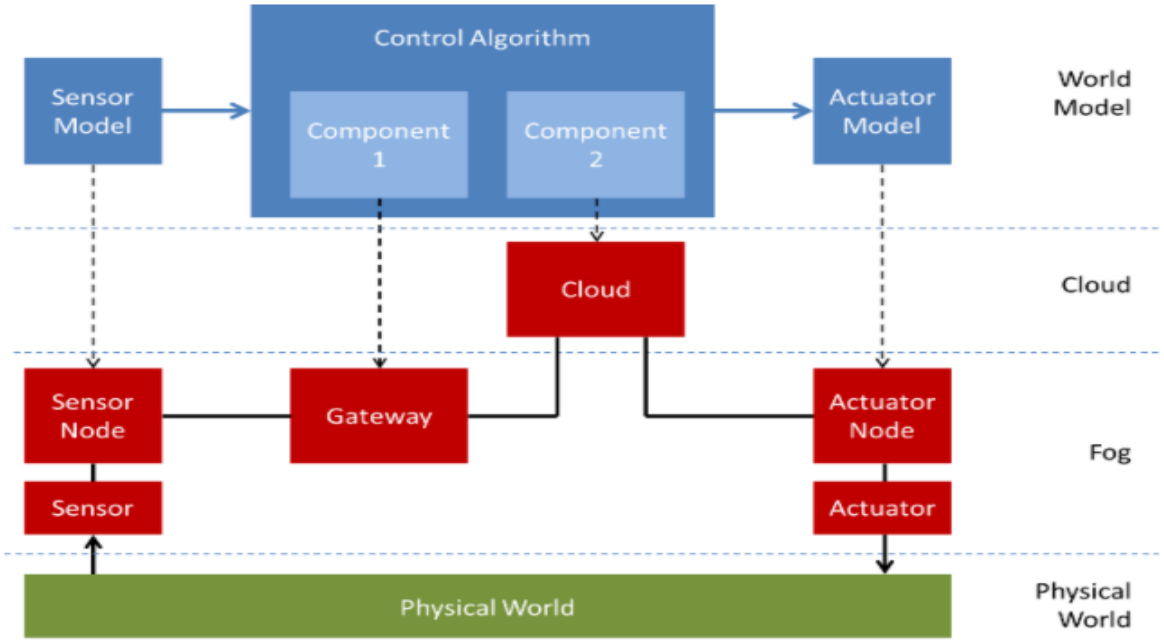


Figura 25 Representación de fog computing en un sistema IoT [80]

Según explica el experto Christopher Mims, autor de “El futuro de la tecnología está en la niebla, no en la nube”: «mientras la nube está “ahí arriba” en algún lugar del cielo, distante y remota y deliberadamente abstraída, la “niebla” está cerca del suelo, donde las cosas se concretan» [81].

A medida que el internet de las cosas se generalice la **computación en la niebla** irá ganando protagonismo. Se puede considerar este tipo de computación como un modo de proveer servicios de manera más inmediata.

7.3. BIG DATA

Big Data (Datos Grandes) son cualquier voluminosa cantidad de datos estructurados, semi-estructurados y no estructurados que tienen el potencial de ser extraídos para obtener información. Los datos se convierten en datos Big cuando es difícil procesar usando técnicas de análisis de datos tradicionales.

El éxito de la organización no sólo reside en lo bueno que hay en hacer su negocio, sino también, en lo bien que pueden analizar sus datos y obtener información sobre su empresa, sus competidores, etc. grandes datos pueden ayudarle a tomar la decisión correcta [82].

Figura 26. Big Data, de los datos a la sabiduría [Autores]

- **Características**

Volumen	Velocidad	Variedad	Veracidad	Validez	Volatilidad
Los datos grandes implican enormes volúmenes de datos generados por sensores, máquinas, medios sociales, comercio electrónico, dispositivos GPS, etc.	Implica la tasa a la que los datos se vierte, por ejemplo el caso de Facebook donde 3 millones de usuarios generan likes por día y alrededor de 450 millones de tweets son creados cada día por los usuarios.	Implica al tipo de formatos y se pueden clasificar en 3 tipos: • Estructurado: (RDBMS como Oracle, MySQL, Excel, Access) • Semi- Estructurado: (E-mails, Tweets, Archivos de registro, Opiniones de usuarios) • No Estructurados: (Fotos, Video, Archivos de audio).	Se refiere a los sesgos, el ruido y la anomalía en los datos. Si queremos una visión significativa de estos datos necesitamos limpiarlo inicialmente.	Se refiere a la adecuación y precisión de los datos ya que la validez de los datos es muy importante para tomar decisiones.	Se refiere a cuánto tiempo los datos son válidos ya que los datos que son válidos en este momento podrían no ser válidos sólo unos minutos o menos días después.

Tabla 6 Características de Big Data [82]

7.4. INTEGRACIÓN DE SISTEMAS DE SEGURIDAD ELECTRÓNICA IOT

Actualmente los dispositivos de seguridad electrónicos IoT funcionan de forma independientes o relacionados según el caso, más sin embargo carecen de una comunicación completa y de una plataforma para su gestión, esto hace que se pierda la autonomía y proactividad entre ellos, ya que necesitan una comunicación entre sí para la mejora de sus procesos.

Para esta necesidad se hace relevante la integración de los sistemas de seguridad electrónicos IoT y así lograr una efectiva comunicación y mejoramientos de sus procesos.

La palabra integrar conlleva a la definición de “contribuir, unirse o entrar a formar parte de un todo o conjunto”, por lo que se puede deducir que la aplicación de este concepto en el sector de seguridad es conjuntar y vincular diferentes sistemas autónomos para una buena comunicación y buen funcionamiento por medio de una plataforma central que permita tener el control y gestión de dichos sistemas.

Una plataforma que es aplicada a la integración de un sistema electrónico de seguridad, debe ser capaz de recibir y controlar la información, además debe generar señales de comunicación con otros dispositivos.

Los objetivos que se persiguen con la integración son:

- Relacionar diversos sistemas autónomos para optimizar los recursos disponibles.
- Centralizar las informaciones y comunicaciones generadas para facilitar la toma de decisiones.
- Mejorar la proactividad y funcionamientos de los sistemas.
- Incrementar la seguridad en la explotación del sistema: operaciones, procesos, procedimientos, actuaciones.
- Operación bajo una única interfaz.

Entre las posibilidades, más frecuentes de integración se necesita que la plataforma permite realizar el control simultáneo de:

- Los medios ópticos: facilitan la captación de imágenes para identificar personas, control de movimientos por el interior, acceso a zonas restringidas, etc.

- Sistemas de detección de intrusión: complementan las funciones de control de acceso especialmente durante las horas de reducida presencia en las instalaciones.

- Sistemas de detección y prevención de incendios, indispensable coordinación en casos de emergencia.

Notablemente se mejora la seguridad cuando se cuenta con un sistema de seguridad electrónico IoT integrado. Por lo que se tiene ventajas en: reducción en el tiempo de respuesta, precisión de las acciones según el tipo de evento, reducción de falsas alarmas, entre otros beneficios [83].

7.5. INTEGRACIÓN DE TECNOLOGÍAS IOT PARA LOS SISTEMAS DE SEGURIDAD ELECTRÓNICA (PROPUESTA).

7.5.1. Dispositivos

En esta sección se detallarán algunos de los principales dispositivos utilizados para realizar el diseño de un esquema de integración de tecnologías IoT de los sistemas de seguridad electrónica.

Cuando se habla de dispositivos, se relaciona cualquier tipo de objeto o cosa que se vaya a interconectar en una red de comunicación, con el objetivo de intercambiar información y garantizar el desempeño de una determinada aplicación.

Cada uno de estos componentes será capaz de realizar su identificación de manera única, podrá saber su ubicación y registros de ubicaciones anteriores, comunicar su estado a un servidor o al nodo de control para actualizar sus características y funcionamiento, y contextualizar su entorno y de esta manera aprovechar el máximo de sus recursos.

Características de un dispositivo IoT

Los dispositivos IoT están equipados con sensores, actuadores, procesadores y transceptores integrados. El Internet de las Cosas no es una sola tecnología; más bien es una aglomeración de varias tecnologías que trabajan en conjunto.

Los sensores y actuadores son dispositivos que ayudan a interactuar con el entorno físico. Los datos recogidos por los sensores tienen que ser almacenados y procesados inteligentemente para derivar inferencias útiles de la misma. Tenga en cuenta que definimos ampliamente el sensor de términos; Un teléfono móvil o incluso un horno de microondas puede contar como un sensor, siempre y cuando proporcione entradas sobre su estado actual (estado interno + entorno).

Un actuador es un dispositivo que se utiliza para efectuar un cambio en el entorno, como el controlador de temperatura de un acondicionador de aire [9].

A continuación, se listan los distintos dispositivos IoT tomados como referencia para la construcción de la propuesta.

Sensor de movimiento infrarrojo [84] 	*Sensor de movimiento infrarrojo inalámbrico basado en el protocolo de comunicación Zigbee, el rayo infrarrojo monitorea en tiempo real y el sensor envía inalámbricamente una alarma al centro de control la tarea asignada* • *Señales infrarrojas y monitoreo en tiempo real* • *Distancia de comunicación：100M (condiciones visuales)* • *Protocolo de comunicación：IEEE802.15.4 (ZigBee)*

Detector de Humo [85] 	*Puede evitar un incendio a través del monitoreo de la concentración de humo en tiempo real. Cuando la concentración de iones de humo está más allá del rango normal.* • *Monitoreo y registro de concentración de humo en tiempo real* • *Distancia de comunicación: 100 metros* • *Protocolo de comunicación: IEEE802.15.4 (ZigBee)*

Sensor de movimiento *[86]* 	*Detecta el movimiento y envía información en tiempo real, se basa en el protocolo inalámbrico Z-Wave* • *Protocolo inalámbrico: Z-Wave* • *Rango efectivo: 2x5 metros* • *Comandos Z-Wave*

Cámara Smart [87]	*Cámara Smart basada en tecnología inalámbrica, se desarrolla sobre el monitoreo y plataformas de almacenamiento en la nube*
	• *Sistema dinámico de dominio IP disponible* • *Sensor CMOS* • *WIFI 802.11b / g / n red inalámbrica* • *Dirección IP estática, dirección IP dinámica* • *Interfaz Ethernet 10Base -T / 100Bse - Tx* • *ISO / FCC / CE / RoHS Autenticación* • *Configuración del sistema: Android 4.0, visión IOS5.0 o versión posterior*

Alarma [88]	*La Alarma contiene un sistema GSM que al configurarlo permite enviar automáticamente un mensaje o realizar una llamada a los números determinados.*
	• *Envía automáticamente mensajes* • *Realiza llamada en tiempo real* • *Protocolo de comunicación: GSM*

Gateway Libelium [9] 	*El* Gateway Libelium está capacitado para conectar distintos dispositivos y plataformas.
	Procesador: 1GHz Quad Core Memoria RAM: 2GB DDR3 Disco duro: 16GB Fuente de poder: PoE (Power Over Ethernet) Tiempo de ejecución de los servicios: 60s Protocolo de red: ZigBee Tecnologías de conexión: Ethernet, WIFI, RF, Bluetooth, 4G, GPS Seguridad: autentificación WEP, WPA, WPA2, HTTPS

Detector de Gas y Combustible [89] 	El detector de gas y combustible se utiliza para monitorear y alertar eventuales fugas de gas en los hogares, oficinas y otros establecimientos. Supervisa la concentración de gas combustible en interiores, como el gas licuado y gas natural.
	Fuente de alimentación: AC 220V Distancia de comunicación: 100M Protocolo de comunicación: IEEE802.15.4 (ZigBee) Modo de detección: Inductiva Área de detección: 15㎡ (operación óptima)

7.5.2. Libelium

Libelium es una multinacional tecnológica española, fundada en 2006. Diseña y fabrica hardware y un kit completo de desarrollo de software (SDK) para redes de sensores inalámbricos para que integradores de sistemas, ingeniería y consultorías puedan ofrecer soluciones confiables de Internet de Cosas (IoT), M2M y Smart Cities con un tiempo mínimo de comercialización.

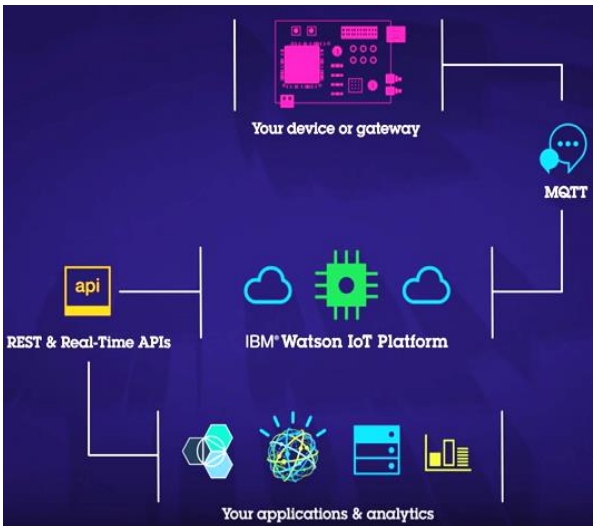
Se constituyó en noviembre de 2006 como Spin Off de la Universidad de Zaragoza tras detectar la necesidad de desarrollar tecnología capaz de monitorizar de manera inalámbrica cualquier tipo de parámetro ambiental [9].

7.5.3. Plataforma IBM Bluemix.

IBM Bluemix es un entorno de plataforma como servicio desarrollado por IBM. Soporta varios lenguajes de programación y servicios, así como la metodología de desarrollo DevOps de forma integrada para crear, ejecutar, desplegar y gestionar aplicaciones en la nube. Bluemix soporta Java, Node.js, Go, PHP, Python, Ruby Sinatra, Ruby on Rails, GeneXus y puede ser extendido a otros lenguajes tales como Scala. Los recursos de cloud pueden hacer posible reunir múltiples orígenes de datos, escalar sistemas e incorporar servicios cognitivos para redireccionar el valor del negocio de una forma rápida y económica [90].

Bluemix también ofrece implementaciones en la nube que se adaptan a las necesidades de los usuarios, desde una pequeña empresa que planea escalar o una gran empresa que requiere un aislamiento adicional, donde puede desarrollar y conectar en una nube sin fronteras sus servicios. IBM gestiona todas las instancias de servicio. Se recibirá una factura por sólo lo que se elija utilizar. Con el amplio conjunto de servicios y tiempos de ejecución en Bluemix, el desarrollador obtiene control y flexibilidad, y tiene acceso a diversas opciones de datos, desde la analítica predictiva hasta los grandes datos [91].

7.5.4. IoT IBM Watson



La plataforma IoT de IBM permite conectar sensores y dispositivos en la nube, también se pueden recolectar y brindar seguridad a los datos a partir del análisis y así obtener una visión en tiempo real para tomar decisiones oportunamente, también ayuda a construir y gestionar aplicaciones y soluciones IoT de forma rápida, segura y escalable [92].

IoT Bluemix puede ser conectado a su dispositivo IoT, un sensor, un Gateway y enviarlo a través de un protocolo de mensajería ligera como MQTT, ahora la plataforma administra sus dispositivos conectados al API de acceso para el análisis del mundo físico en tiempo real utilizando modelos predictivos para optimizar el servicio [93].

7.5.5. Comunicación

Modelo de comunicación Dispositivo – Gateway

Este es el modelo de comunicación más utilizado en Internet de las Cosas y se da cuando los dispositivos se conectan a Internet a través de un dispositivo llamado Gateway. Para ser más precisos, el Gateway está dotado de un software de aplicación que hace las veces de intermediario entre los dispositivos IoT y los servicios en la nube, haciendo la traducción entre protocolos [94].

Los dispositivos a utilizar se comunican a través de una red inalámbrica utilizando un protocolo de comunicación según la conexión empleada, dichos protocolo de comunicación son un conjunto de normas que permiten la comunicación entre dispositivos, entre ellos están:

Protocolo de comunicación: IEEE 802.11 (WIFI)
Protocolo de comunicación: IEEE 802.15.4 (ZEGBEE)
Protocolo de comunicación: (GSM) 2G.

Gateway – WEB

El Gateway utiliza algunos protocolos de comunicación para conectarse a la WEB, los cuales son:

Protocolo de comunicación: (GSM) 2G
Protocolo de comunicación: (UMTS) 3G
Protocolo de comunicación: (LTE) 4G
Protocolo de comunicación: (IEEE 802.3) ETHERNET

Gateway – Plataforma

El Gateway se comunica directamente a la plataforma por medio el protocolo de comunicación de M2M MQTT

A continuación, se presenta el siguiente diagrama ilustrando cada uno de los protocolos que utilizan los dispositivos para comunicarse entre ellos.

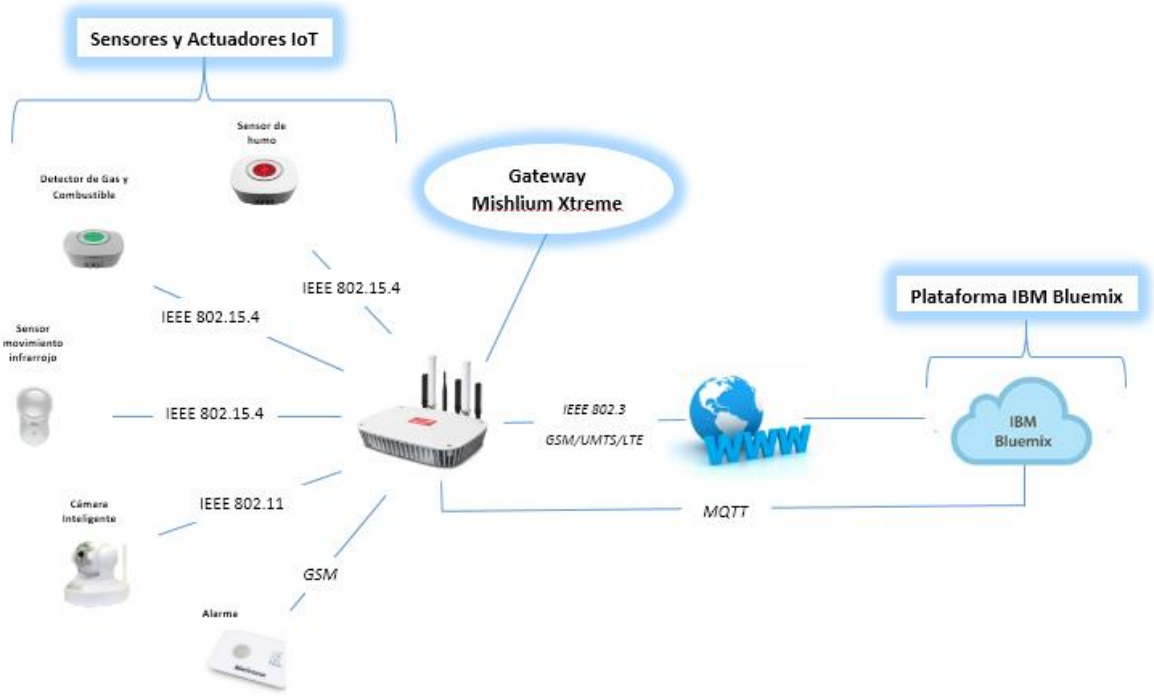


Figura 27 Comunicación entre dispositivos IoT [Autores]

7.5.6. Conectividad

Los objetos tienen la capacidad de interconectarse con los recursos de la internet e incluso entre sí para hacer uso de los datos, servicios y actualizar su estado; en esta medida son de gran relevancia las tecnologías inalámbricas como 2G, 3G, 4G, Wi-Fi, ZigBee y MQTT.

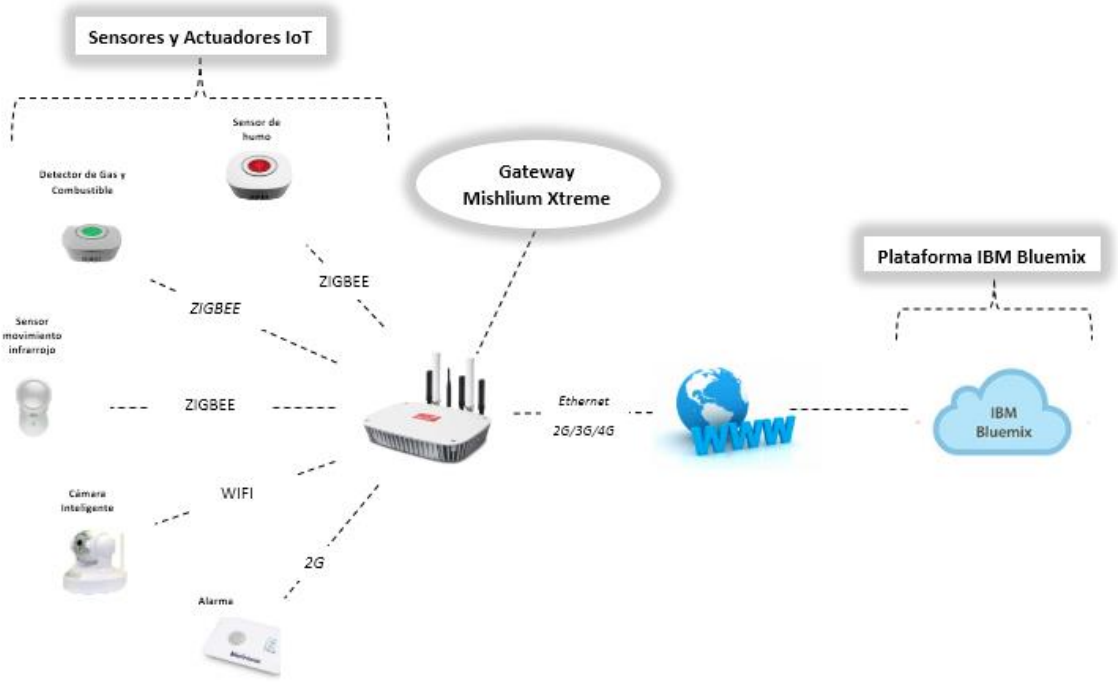


Figura 28 Conectividad entre dispositivos IoT [Autores]

7.5.7. Configuración Gateway [9]

Configuración de interfaces de red

Acceda a la configuración de las interfaces de red haciendo clic en el botón "Interfaces":

1. Configuración de Ethernet.

De forma predeterminada, Meshlium viene con la interfaz Ethernet activada para obtener dinámicamente la IP utilizando el servicio DHCP.

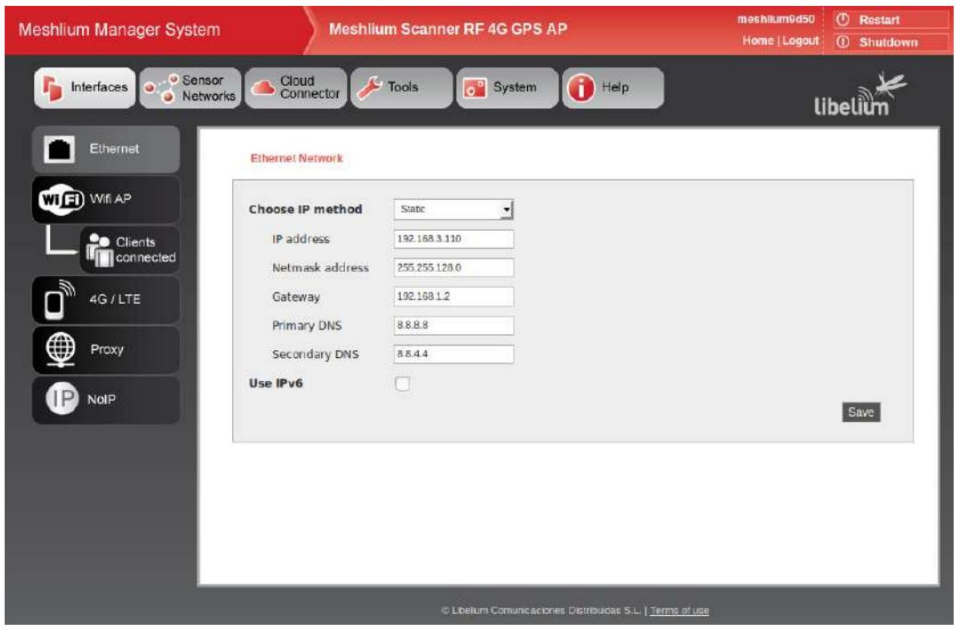


Figura 29 Configuración Ethernet

También se puede usar IPv6 (Internet Protocol versión 6) marcando la casilla "Use IPv6".

Figura 30 Configuración IPv6

2. Configuración del punto de acceso WiFi

Meshlium es un punto de acceso WiFi y puede proporcionar conectividad de red a través de WiFi. La característica más útil de la AP es proporcionar acceso a Manager System desde una tableta o portátil sin ninguna conexión física con Meshlium.

De forma predeterminada el AP tiene el ESSID "meshliumXXXX" donde XXXX son los últimos cuatro dígitos de Ethernet MAC. Esto permite identificar diferentes Meshliums instalados cerca.

Figura 31 Configuración Punto de acceso WIFI

2.1. Configuración

Hay tres secciones en la página de configuración: Red, Radio y Seguridad.

Red: aquí puede cambiar la IP del dispositivo en la red y la configuración DHCP. Aquí se puede configurar: dirección IP del AP, máscara de red de la dirección, intervalo DHCP.

Radio: estos son parámetros específicos de WiFi. Aquí se puede configurar: ESSID de la red, canal y protocolo de la red.

Seguridad: el AP WiFi puede protegerse con cifrado. WEP, WPA y WPA2 están disponibles.

3. Configuración 4G

Este complemento permite configurar los parámetros de la conexión del módem. Hay una lista con algunas configuraciones iniciales dependiendo el país y operador. Sin embargo, esta lista no se puede actualizar con la última configuración válida del proveedor de telefonía móvil. Se necesita solicitar a la compañía móvil la información necesaria para conectarse (APN, nombre de usuario, Contraseña).

4. Configuración de Proxy

Este complemento permite configurar un proxy HTTP para algunas características de Meshlium. Aquí se puede configurar el proxy la dirección, el puerto y las credenciales.

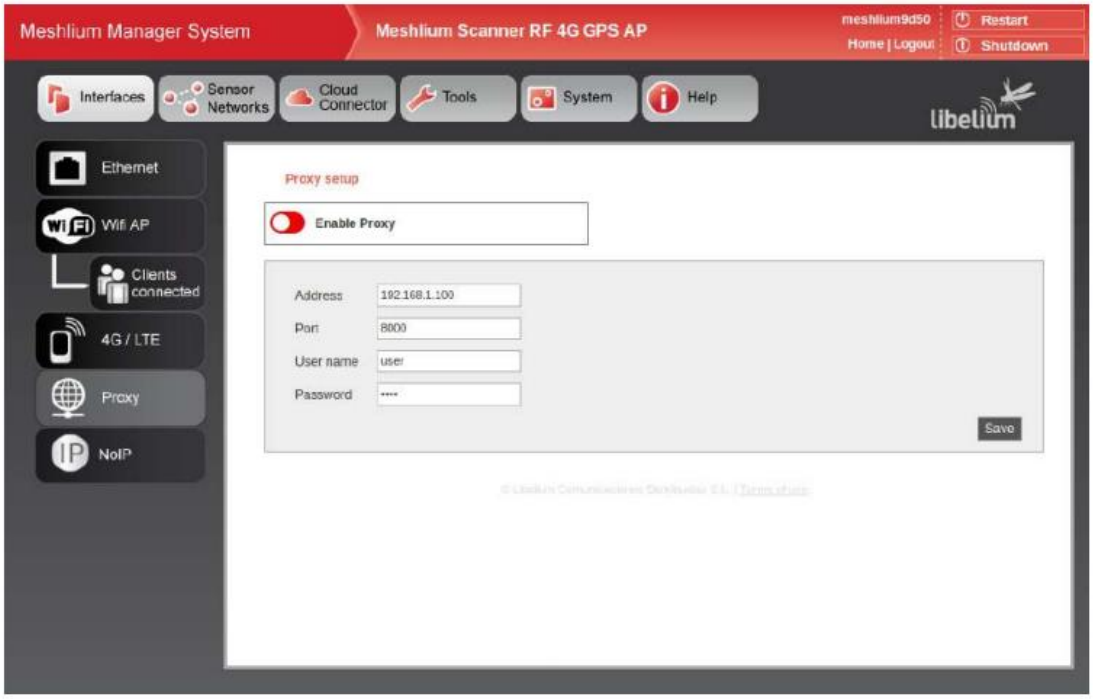


Figura 32 Configuración Proxy

Sensores de redes inalámbricas

Meshlium y Sensores

Una de las principales aplicaciones de Meshlium es ser una puerta de enlace para Wireless Sensor Networks. Estos son los sensores que pueden trabajar.

En la página principal de la pestaña "Redes de sensores" se mostrarán los dispositivos del sistema que muestran los últimos mensajes recibidos datos.

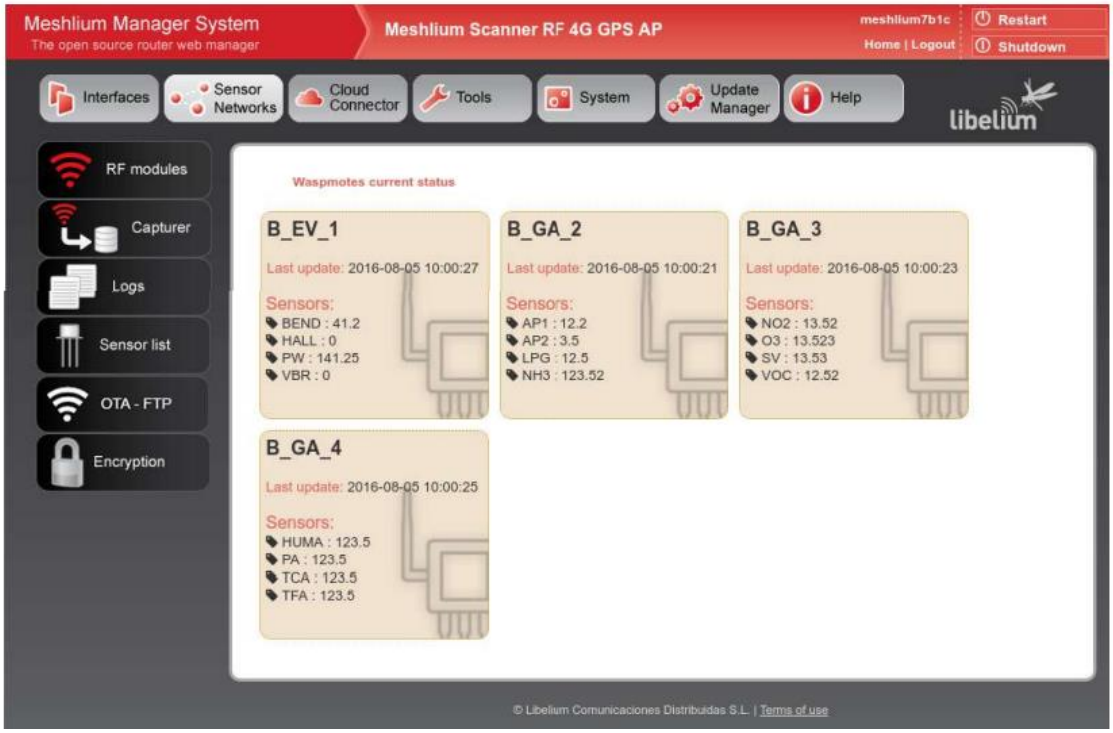


Figura 33 Página principal redes de sensores

Recepción y almacenamiento de datos

Recepción a través de comunicaciones RF

Meshlium puede equipar tres módulos RF diferentes: XBee-PRO 802.15.4 (2.4 GHz), XBee 868LP (868 MHz) y XBeePRO 900HP (900 MHz).

Configuración de cifrado

Gestión de claves de capa de enlace (AES-128). Esta característica es proporcionada por los módulos XBee.

La encriptación es esta capa proporcionada a través del algoritmo AES 128b. Específicamente a través del tipo AES-CTR. En este caso el campo Frame Counter tiene un ID único y cifra toda la información contenida en el campo Payload que es el lugar en el marco de capa de enlace donde se almacenan los datos a enviar. La forma en que las bibliotecas han sido desarrollado para la programación de módulos significa que la activación de cifrado es tan simple como ejecutar la inicialización función y darle una clave para usar en el cifrado.

```
{
xbee.encryptionMode(1);
xbee.setLinkKey(key);
}
```

En el sistema Administrador, en la sección de red de sensores, los usuarios pueden cifrar mensajes en la capa de enlace. Puede lograrse mediante Ajuste de los parámetros:

• Modo encriptado: true / false (por defecto false)
• Clave de cifrado: Debe tener 16 caracteres Consulte la sección

"Configuración del módulo XBee" para obtener más detalles sobre cómo configurar el cifrado.

Receptor 4G / WiFi / Ethernet (HTTP)

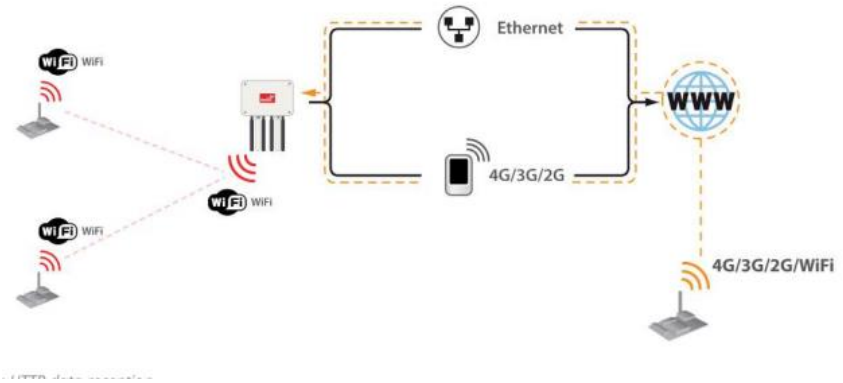


Figura 34 Esquema de sensor Gateway

Meshlium acepta las solicitudes POST y GET en cualquiera de sus interfaces para que los sensores puedan enviar marcos, a través de módulos GPRS, 3G, 4G o WiFi, por medio de solicitudes HTTP.

Meshlium, a través de peticiones HTTP es capaz de:

- Recibir fotogramas desde 4G / 3G / GPRS / GSM, WiFi o Ethernet a través de HTTP.
- Analizar estos marcos.
- Almacenar los datos en la base de datos local.
- Sincronizar la base de datos local con una base de datos externa.

Las tramas recibidas por este método se almacenan de la misma manera que las tramas RF y se procesan de forma idéntica en sincronización.

No se necesita ninguna configuración de ningún tipo para usar HTTP. Si se necesita HTTPS, se necesitaría la configuración del certificado en muchos casos (el certificado auto-firmado se incluye con Meshlium).

Al igual que en el caso de recepción de módulos RF, el usuario puede añadir sus propios sensores.

7.5.8. **Configuración de la Plataforma** [95]

Para la crear la plataforma Bluemix de IoT en el catálogo de servicio es necesario llenar el formulario encontrado la ventana principal.

Plantilla de aplicación

Buscar IoT plataforma en el Catálogo de servicios la opción plan de precios y luego pulsa en el botón “Crear”. Bluemix creará una instancia de la plataforma de IoT

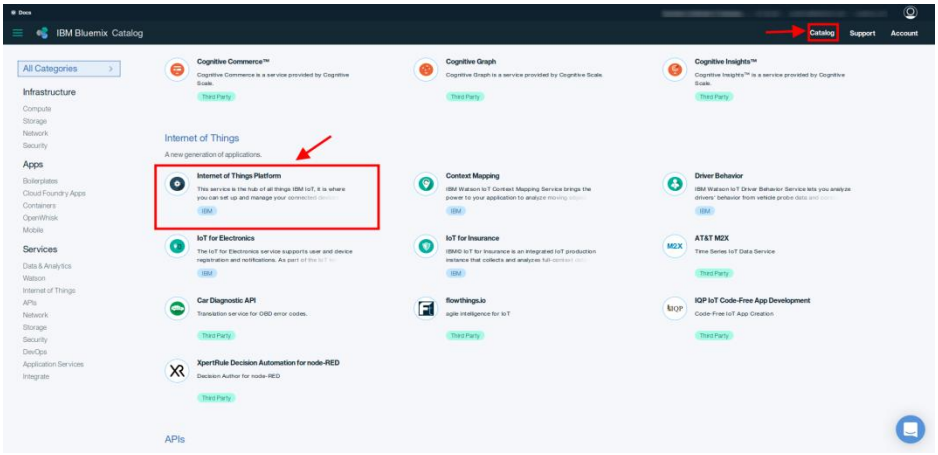


Figura 35 Plataforma Bluemix

En el catálogo de servicio de la plataforma IoT, seleccionar el plan de precios y presionar crear, y Bluemix creará una instancia de la plataforma de la IoT. En la cual se podrá ver un tablero de instrumentos. En la cabecera se encuentra el ***ID Organización*** necesario para la configurar de MeshLium.

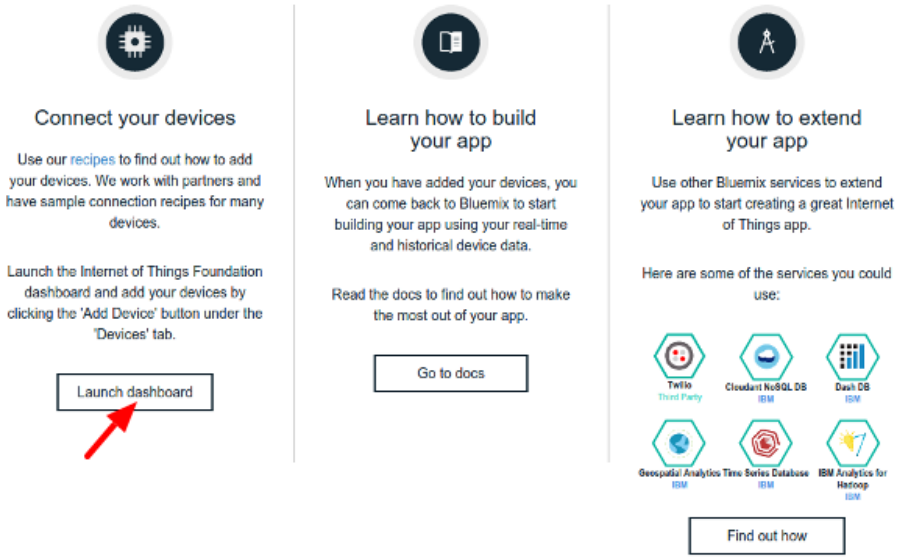


Figura 36 Catalogo de servicio plataforma Bluemix

Crear un acceso API

En este paso se genera la clave. La clave de API se utiliza sólo para la vinculación del Gateway a la Plataforma Watson. Una vez vinculación se haga no es necesario más dicha clave. MeshLium se ejecuta en modo de puerta de enlace y se crearán dos tipos de dispositivo (MESHLIUM_DEV y MESHLIUM_GW), cada MeshLium y cada dispositivo se asignarán con una identidad única.

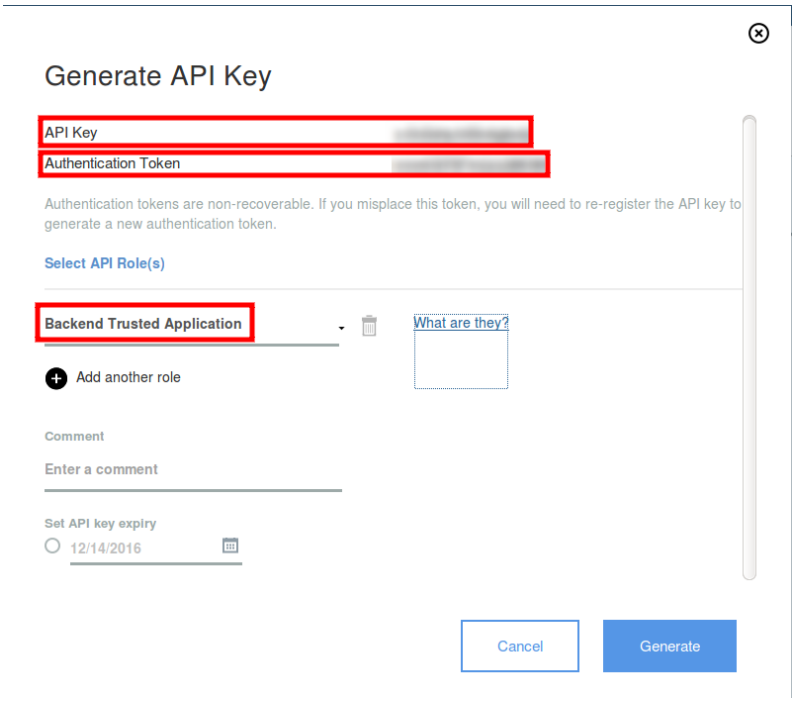


Figura 37 Generador de clave API

Conexión a la Nube

El objetivo de este apartado es introducir al usuario en la funcionalidad de Meshlium Cloud Connector. Esta sección Le ayudará a conectar su Meshlium a una plataforma de nube de terceros. Sólo se pueden enviar datos de los sensores a los servicios en la nube.

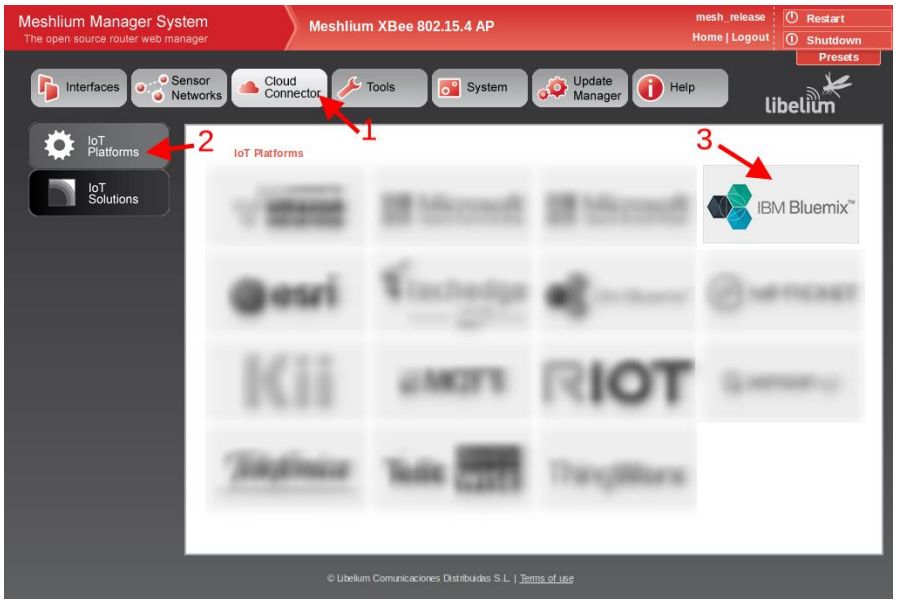


Figura 38 Página principal IoT Plataforma

1. Iniciar sesión en el sistema de administración de MeshLium y llenar los datos correspondientes.

   - **Organización:** es el ID de organización del tablero de instrumentos.
   - **Usuario de la API:** es la clave de la API generada.
   - **Contraseña de la API:** la autorización de emergencia generada.
   - **Identificación del acontecimiento:** campo que se utiliza para configurar el evento en el que desea enviar la información, si no se sabe qué escribir en este campo, se puede utilizar como valor de Eid.
   - **Intervalo:** campo utilizado para retrasar la comunicación después de enviar todos los mensajes.

2. Antes de iniciar la sincronización, es muy importante comprobar el nombre de host de todos los Meshliums y el ID de todas las sensores que tiene en su sistema. Deben ser diferente con el fin de identificar toda la información en el lado de la nube. Si algún dispositivo presenta la misma identificación, la información será mezclado, siendo inconsistente.

Comprobación de los resultados en Bluemix

En el menú de dispositivos se muestran todos los tipos de dispositivos conectados y los mensajes que se reciben.

En los tipos de dispositivo, se crearán dos tipos, MESHLIUM_DEV (que representa sensores) y MESHLIUM_GW (que representa MeshLium)

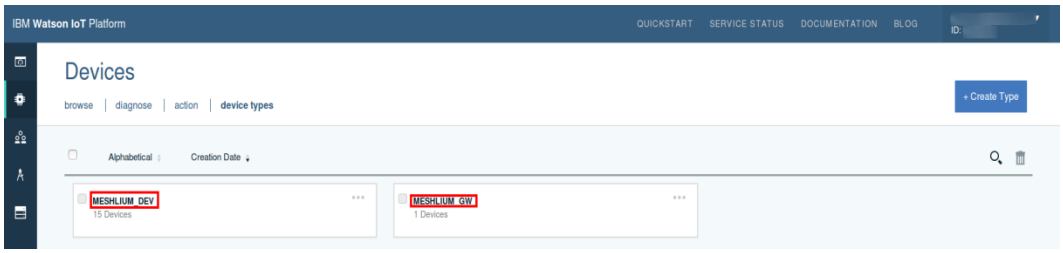


Figura 39 MESHLIUM_DEV y MESHLIUM_GW

En la ficha Dispositivos, se puede ver la lista de dispositivos, cada uno con su ID único. El ID de la Gateway se inicia con GW.

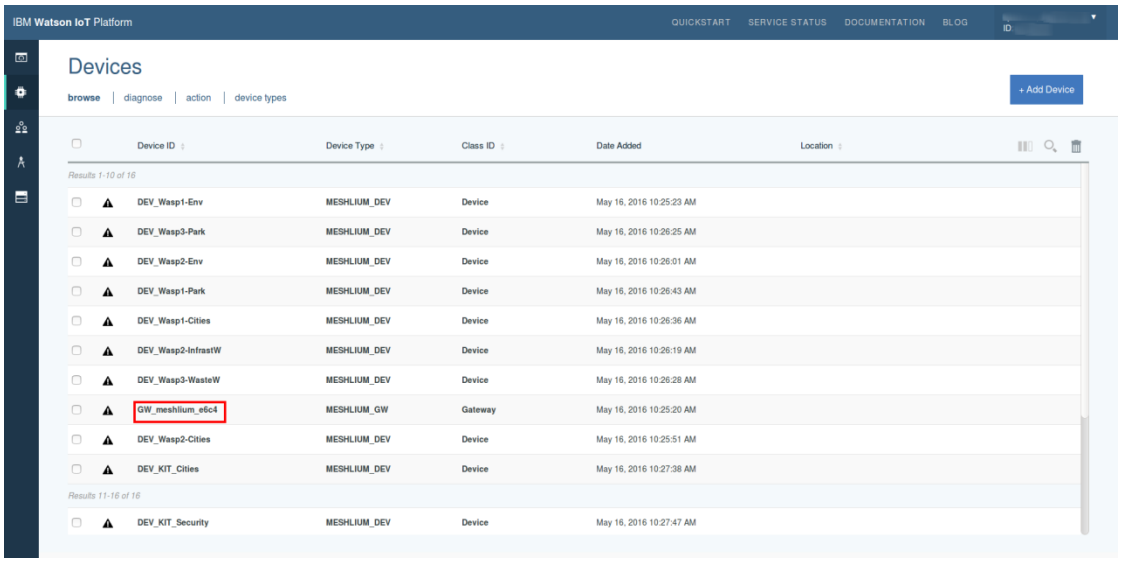


Figura 40 Lista de sensores conectados

Si se da clic en el dispositivo, mostrará los mensajes que llegan con el nombre del evento en la parte superior de la pantalla como lista, y la información para cada mensaje en la parte inferior de la pantalla. Como lo muestra la siguiente figura.

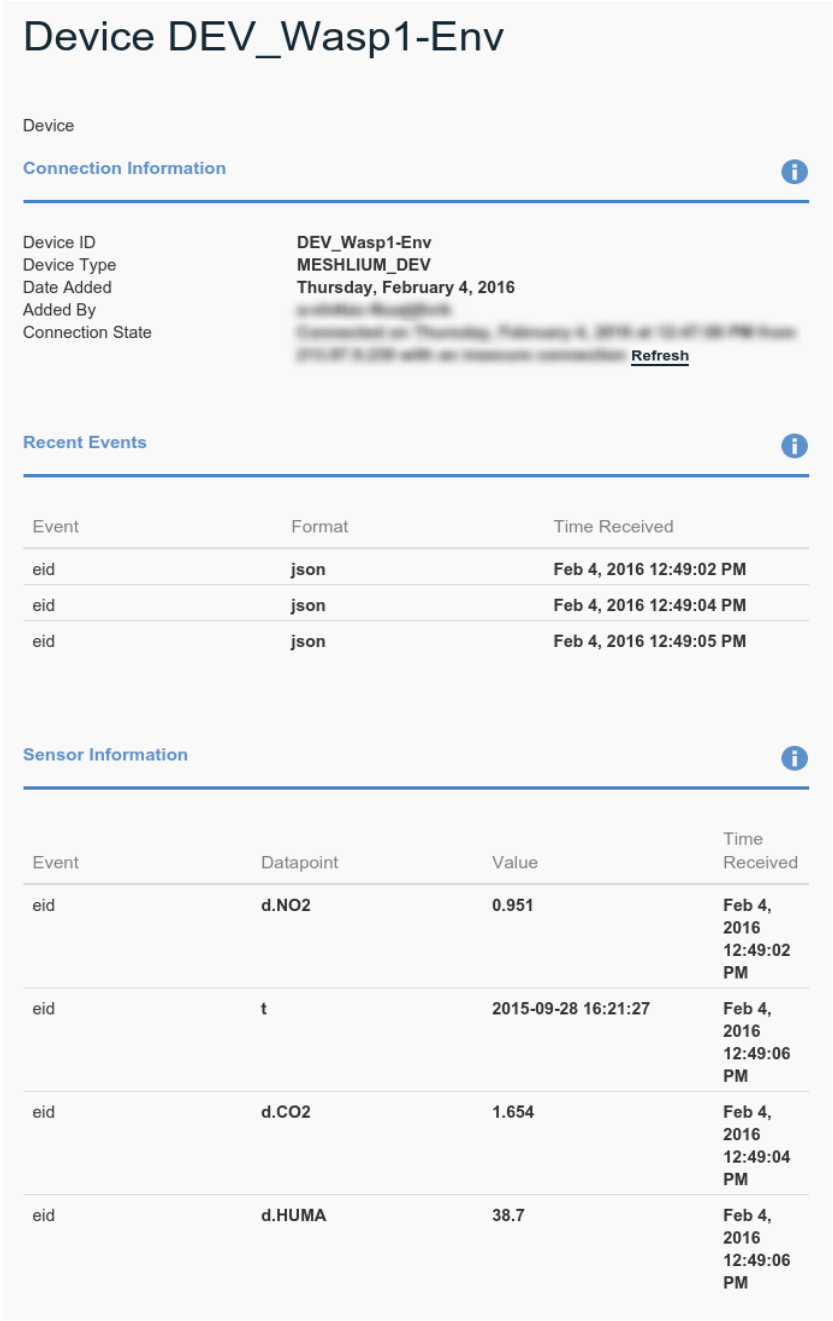


Figura 41 detalles de mensaje de sensores

Aplicación IBM Bluemix [96]

A continuación, se detallan las herramientas de software necesarias para el desarrollo de aplicaciones en IBM Bluemix que servirán para administrar y gestionar los sensores y actuadores a través de una app móvil:

Lo que necesitará para crear estas aplicaciones de IoT

- Una cuenta de IBM Bluemix®. (La plataforma suministra una prueba gratuita de 30 días)
- Un teléfono inteligente (Android o iOS).
- Para un Smartphone iOS, una cuenta de iTunes para instalar la aplicación IoT desarrollada.
- Una cuenta de twitter para ser notificada por un tweet (opcional).
- Una cuenta de correo electrónico con capacidades de retransmisión SMTP[4] para ser notificada por un mensaje de correo electrónico (opcional).

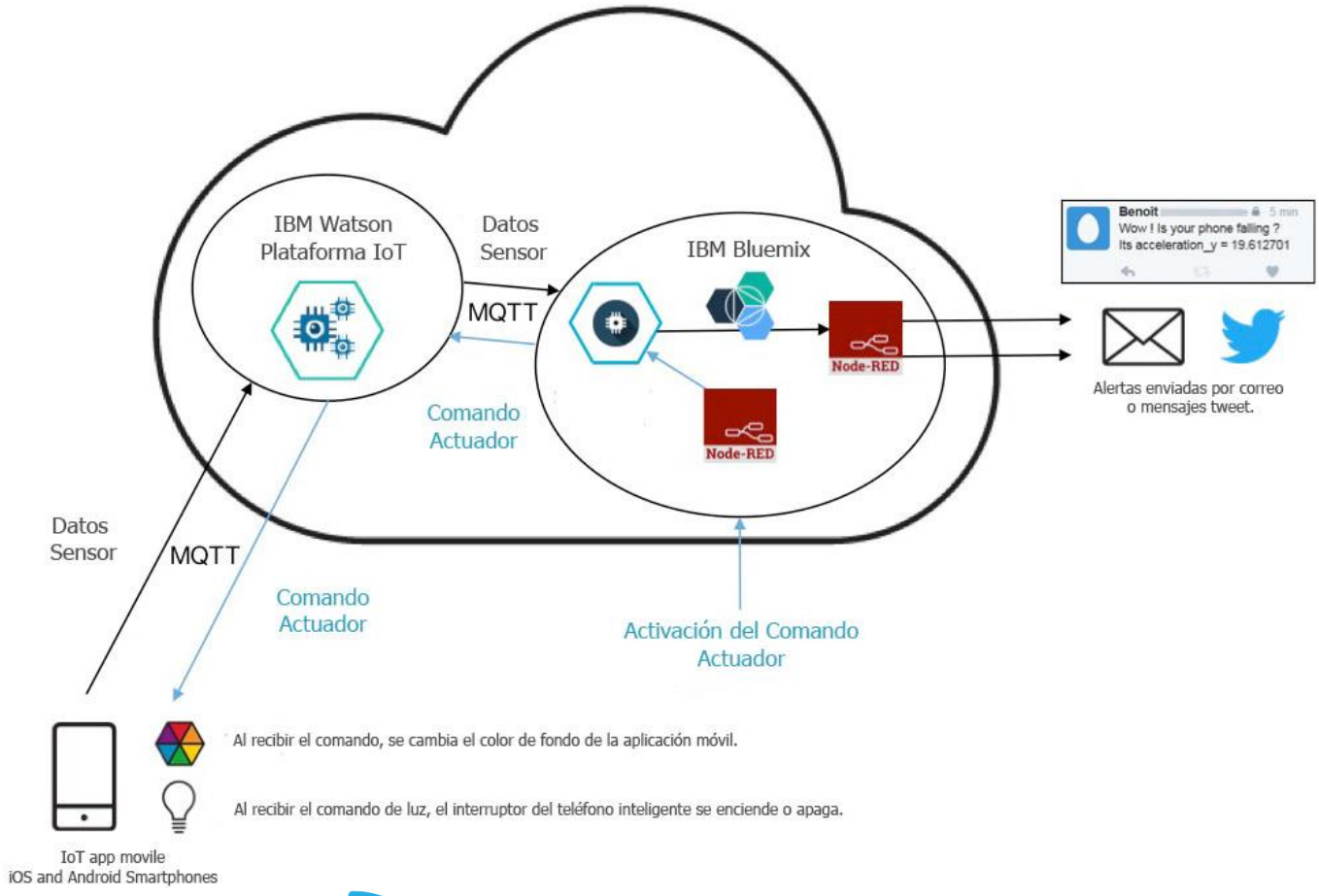
Antes de comenzar, revise la siguiente información:

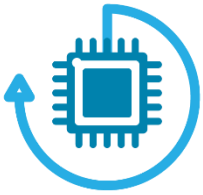
- Familiaridad con la plataforma IBM Bluemix y revisión documental
- Familiaridad con Node-RED; Necesita entender cómo usar nodos en Node-RED y cómo procesa un mensaje en Node-RED. Node-RED es una interfaz para JavaScript, por lo que también necesitas algo de experiencia con JavaScript.

[4] Simple Mail Transfer Protocol (SMTP) es un estándar de Internet para la transmisión de correo electrónico.

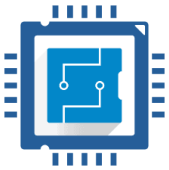
Arquitectura de aplicaciones IoT con IBM Bluemix.

La vista de alto nivel de la arquitectura para el desarrollo de aplicaciones IoT con IBM Bluemix se muestra en la siguiente figura:





Una aplicación de actuador IoT envía comandos sencillos a su teléfono inteligente.



Una aplicación de sensor lee y recibe valores tomados por los dispositivos IoT.

Figura 42 Arquitectura de aplicaciones IoT con IBM Bluemix [96]

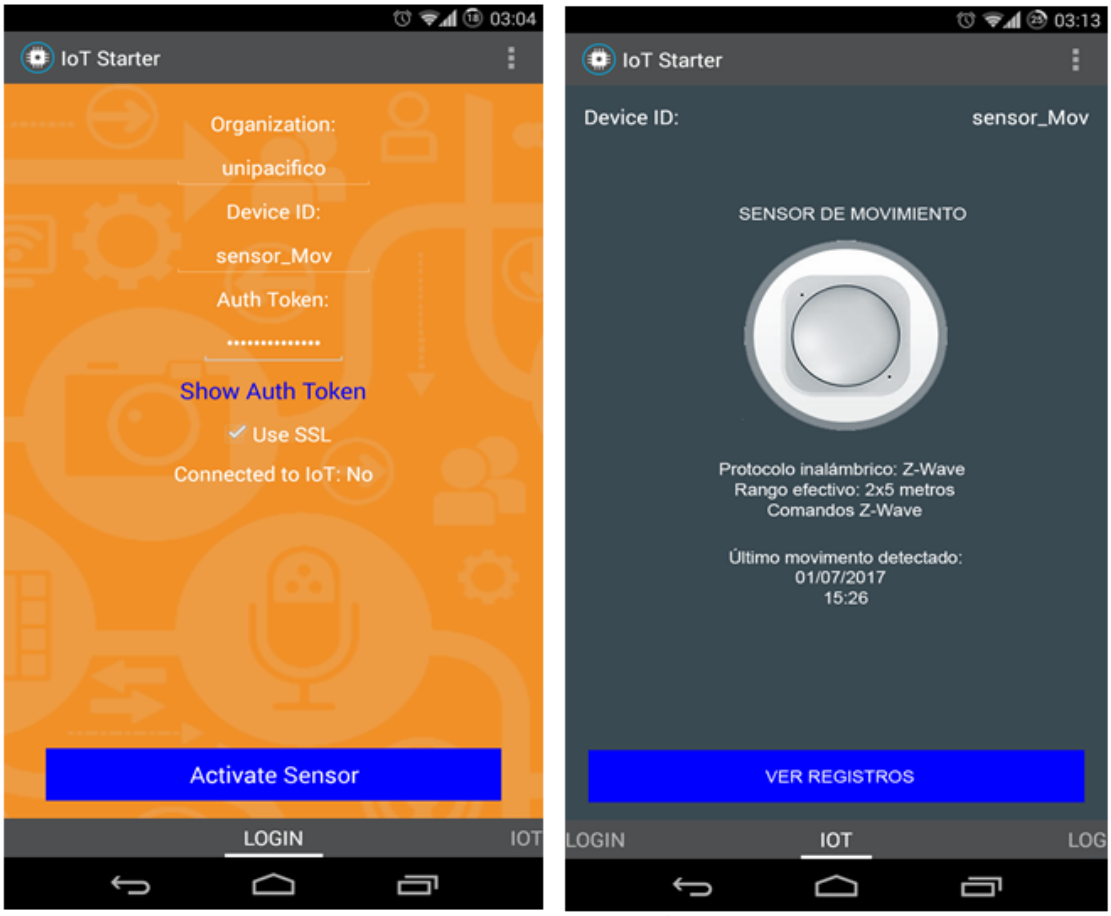


Figura 43 Interfaz de aplicación IoT, control de sensor de movimiento [96]

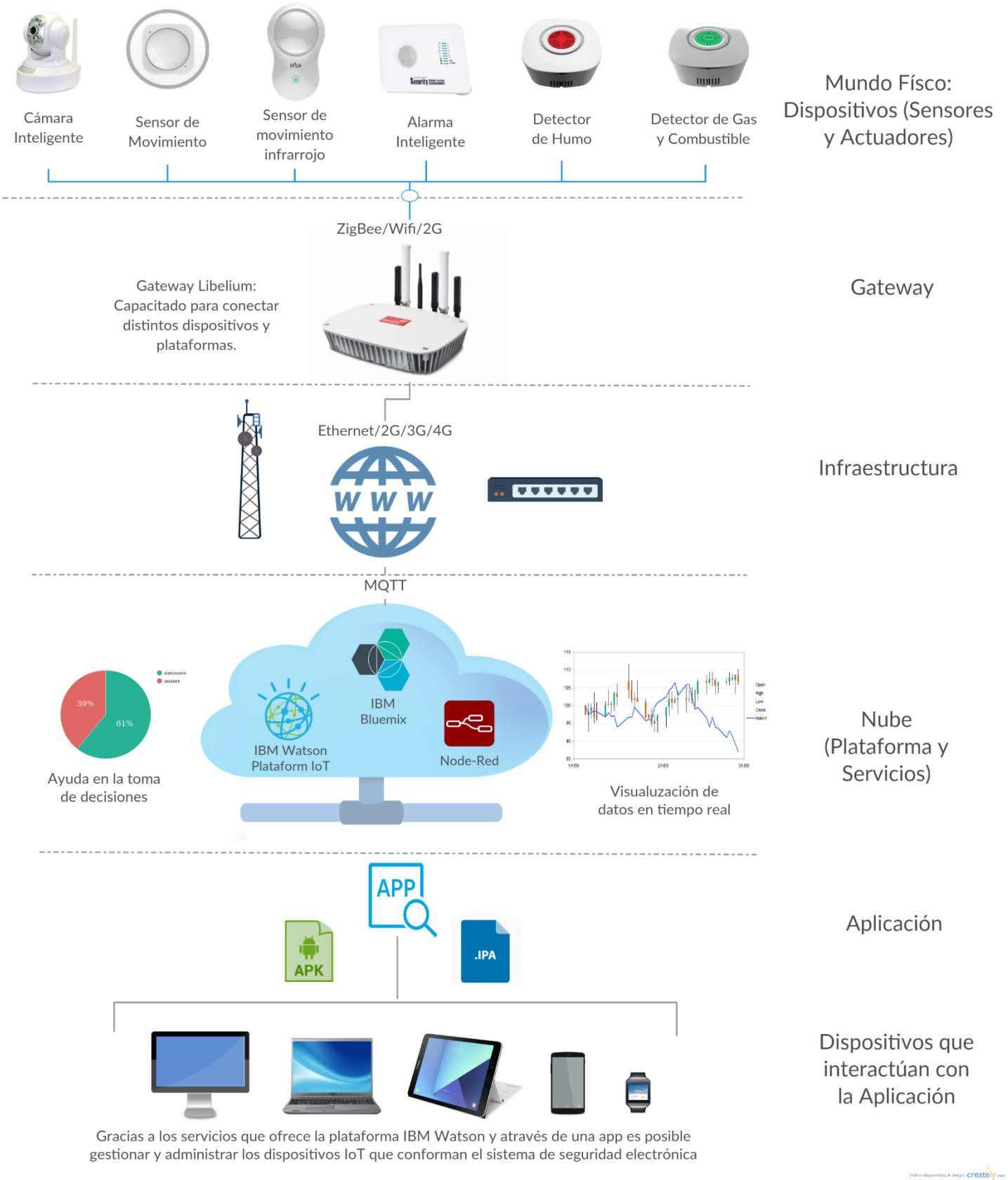


Figura 44. Esquema de Integración de dispositivos y tecnologías IoT.

8. CAPÍTULO 3. IOT UNA GRAN OPORTUNIDAD PARA LAS EMPRESAS

Para las empresas, el internet de las cosas puede representar nuevas oportunidades para conectarse con sus clientes y socios, así como reunir, almacenar y analizar grandes volúmenes de datos. La gama de posibilidades que IoT ofrece va en aumento y ahora las empresas de todo el mundo comienzan a andar los caminos destinados a aprovecharlo. Su impacto, sin duda, revolucionará la manera en que las empresas están haciendo negocio y elevará la productividad y eficiencia, similar a lo que sucedió con la llegada de las computadoras [97].

Para entender mejor la demanda corporativa de solución IoT, Zebra Technologies[4] realizó un estudio global de 646 empresas para identificar las percepciones corporativas de este término, los plazos para la implementación de soluciones IoT y sus beneficios. Esta encuesta mostró que muchas empresas tienen una percepción positiva de las soluciones IoT.

En general, el 71% de las empresas encuestadas tiene una percepción extremadamente positiva o positiva del término "Internet de las Cosas". La percepción de este término es aún más fuerte en Asia Pacífico, con un 96% de las empresas encuestadas en esta región, tienen una percepción positiva o extremadamente positiva del término. Es importante reconocer que no existe una definición estándar de "Internet de las Cosas", sin embargo, el 85% de los encuestados están totalmente de acuerdo con la siguiente definición de IoT:

"Dispositivos inteligentes interconectados que las empresas usan para obtener mayor visibilidad en la identificación, localización y condición de productos, activos, transacciones o personas para impulsar decisiones empresariales más eficaces y oportunas o para mejorar las interacciones con los clientes".

[4] Empresa tecnológica dedicada al a fabricación de impresoras de etiquetas de código de barra y codificadora RFID. Página oficial: <https://www.zebra.com/la/es.html>

La percepción del término Internet of Things en una escala de categorización de 1 a 5, siendo 1 Extremadamente negativo y 5 extremadamente positivo dio como resultado que un 25% lo considera extremadamente positivo (categoría 5), un 46% lo contempla en categoría 4, el 21% en categoría 3, el 6% en categoría 2 y el 2% en categoría 1 (Extremadamente negativo). Ver gráfico 4.

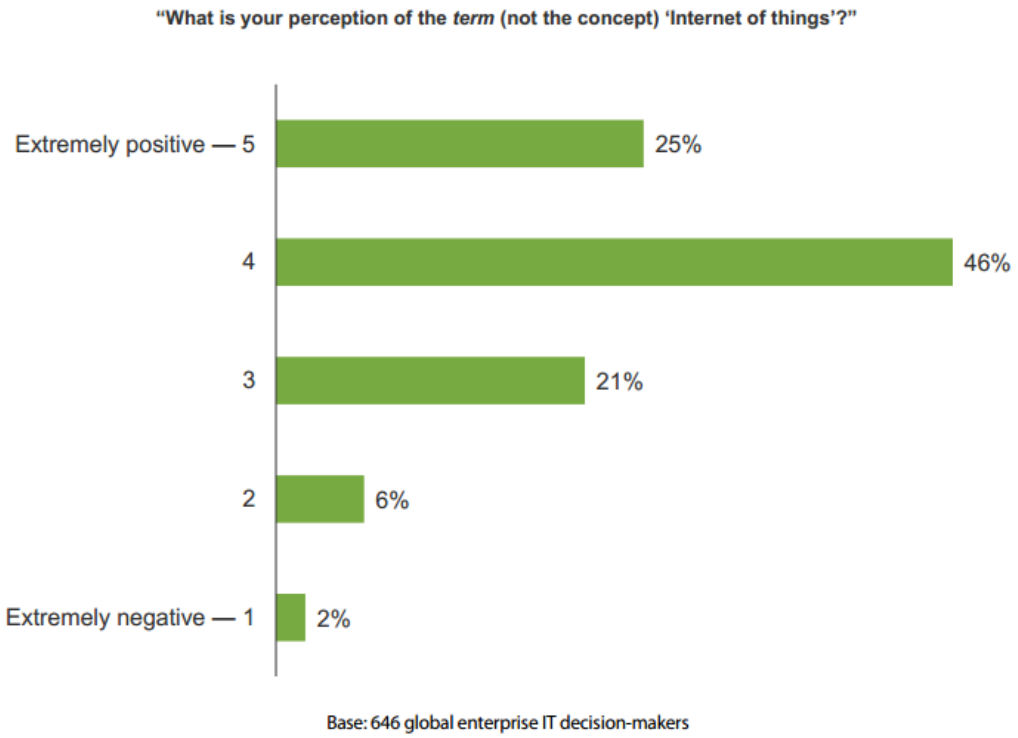


Gráfico 4. Internet de las Cosas Aplicación y Adopción entre las Empresas y las PYMES [98].

Entre las principales tecnologías que traen Soluciones IoT de gran valor para las compañías se encuentran el código de barras y la localización en tiempo real de la carga con un 35% dejándolas en categoría 5 (muy importante), seguido del Wi-Fi con un 34%, la computación móvil con un 27%, GPS Tracking 31% y sensores de seguridad con un 26%, entre otros. Ver gráfico 5 para más detalles de otras tecnologías.

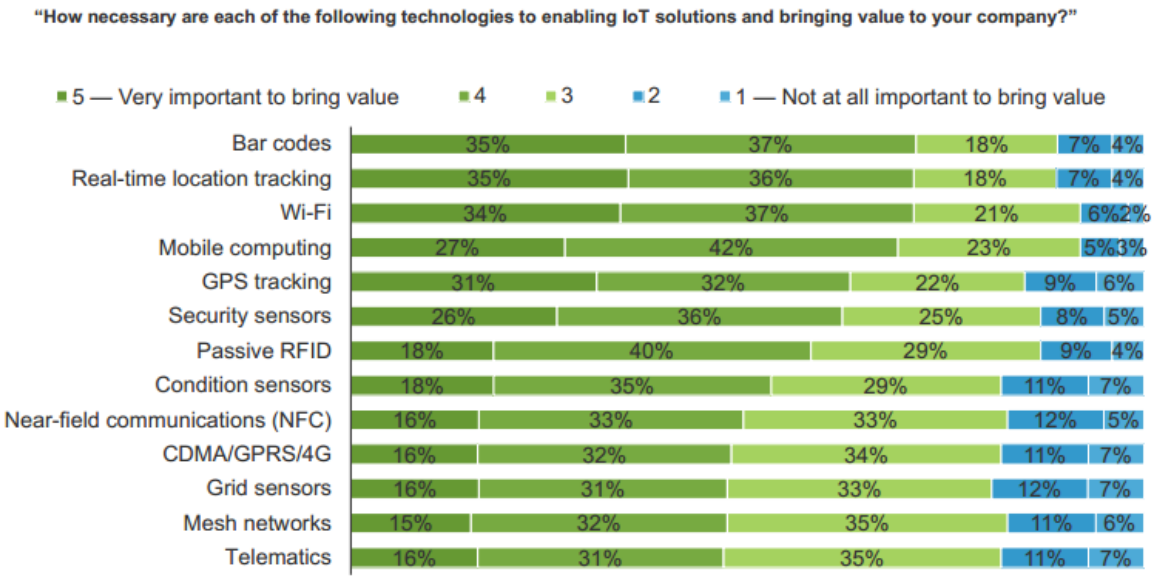


Gráfico 5. Una gran variedad de tecnologías y dispositivos permiten soluciones de Internet de las cosas [98].

Con respecto a los beneficios que pueden obtenerse con la implementación de soluciones IoT para las regiones de Asia, América Latina, Norte América y Europa se obtuvieron los siguientes resultados (ver gráfico 6):

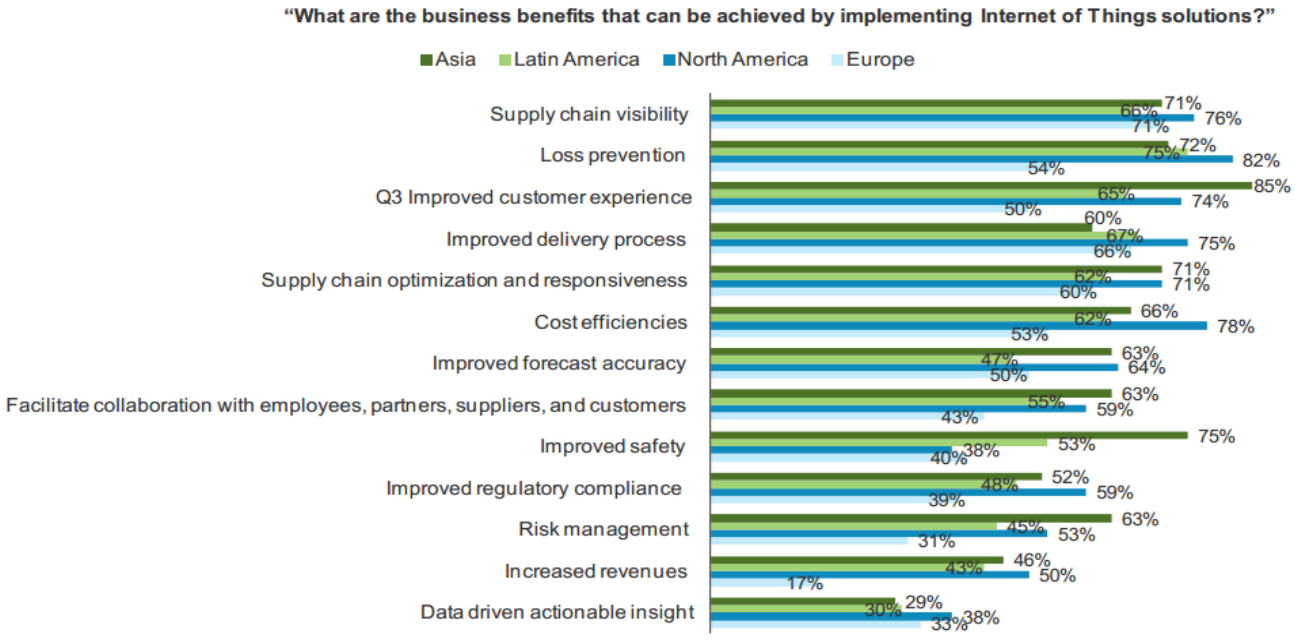


Gráfico 6. Los beneficios obtenidos de la implementación de Internet de las cosas, las soluciones varían según la geografía [98].

Del total de las empresas encuestadas el 23% se encuentra ya utilizando soluciones o aplicaciones IoT el 29% están planeando adoptarlas lo que representa un interés del 30% sobre el total de encuestados. Para el caso de las SMB (Small and Medium Business) en español (Pequeñas y medianas empresas PYMES) un 14% se encuentra utilizando las soluciones o aplicaciones y el 26% están planeando adoptarlas lo que representa un interés del 33% sobre el total de encuestados. Ver gráfico 7. En el mismo contexto se presenta los planes para adoptar soluciones o aplicaciones IoT denotando el interés por regiones siendo China e India los principales interesados en este aspecto, para más detalles ver gráfico 8.

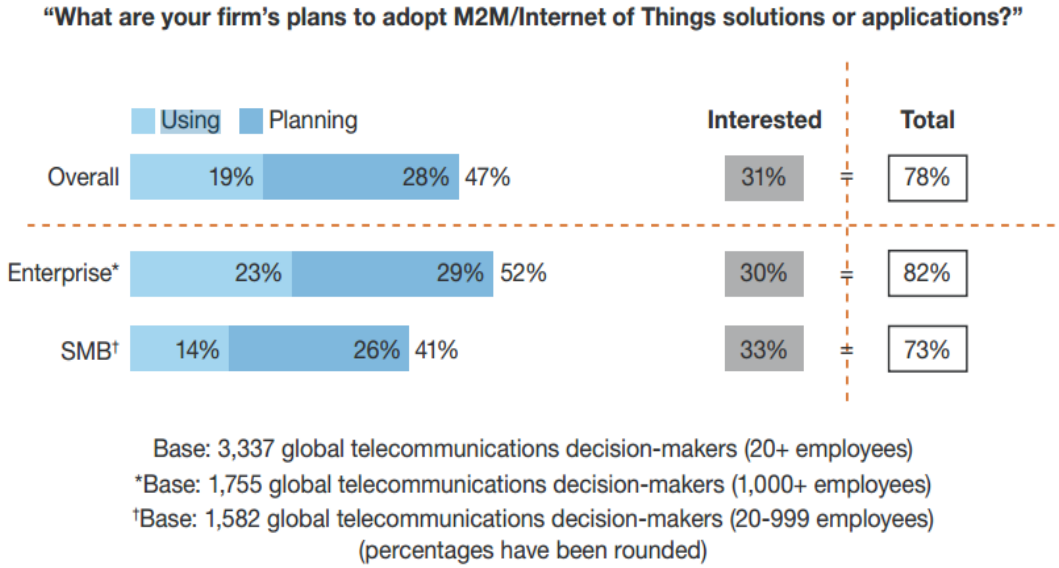


Gráfico 7. Planes de las empresas para adoptar Soluciones o Aplicaciones basadas en M2M/ IoT. [99]

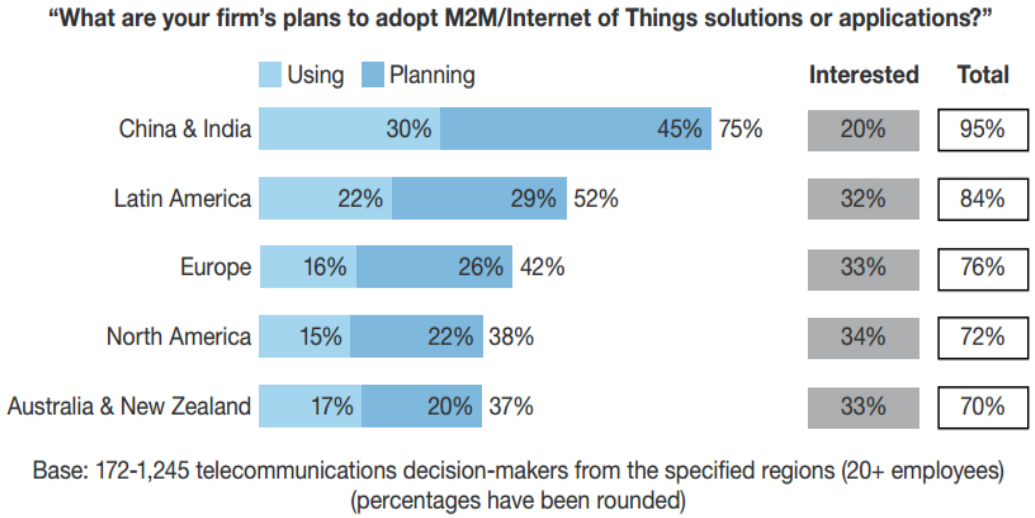


Gráfico 8. Diferencias geográficas en el despliegue de aplicaciones IoT [99].

8.1. OPORTUNIDADES DE IOT PARA LAS EMPRESAS EN COLOMBIA

De acuerdo con el estudio del impacto técnico y económico de la transición de internet al internet de las cosas para el caso colombiano elaborado por el Ingeniero en telecomunicaciones Luis Carlos García de la Universidad Nacional de Colombia, se evidencia que en el país hay muchas oportunidades de investigación y negocios aplicados al Internet de las Cosas, por lo que generar aplicaciones para dispositivos móviles se hace un campo interesante por explorar a nivel comercial, además de la creación y diseño de dispositivos terminales con sensores integrados, en la parte de investigación, la implementación de redes de nodos de sensores con aspectos de seguridad, de robustez del sistema, transmisión de datos entre otros harán posible mejorar la calidad de vida y ayudará a mitigar el impacto ambiental en Colombia [100].

Figura 45. Como las empresas se preparan para la Innovación [101]

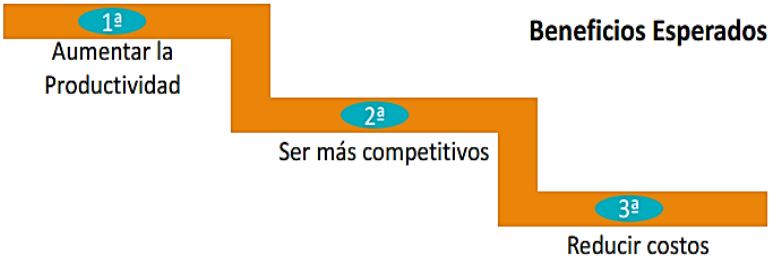
Por otra parte, la penetración de Smartphones en Colombia, es una oportunidad de modernizar a una amplia base de la población. El Gobierno se halla empeñado en el desarrollo de las personas y las empresas tanto en movilidad como en IoT.

La necesidad de mejorar la infraestructura y disminuir los costos son las principales tareas para desarrollar índices de adopción más competitivos. Existen conocidos apoyos a la Innovación, pero aún se necesita trabajar en comunicar los beneficios a las empresas y ciudadanía para justificarlos como prioridad en el negocio [101].

Familiaridad con IoT	
Muy Familiarizado	26,7%
Moderadamente familiarizado	40,8%
Poco familiarizado	18,3%
No familiarizado	14,2%

Planes para desplegar sensores, sistemas, productos para recolectar datos	
Solución ya instalada	10%
Planea lanzarlo en 12-24 meses	10%
No ha considerado una estrategia	15%
No tiene planes	45%

Principales fines del Ecosistema de IoT	
Automatización de producción	1ª
Dejar la oficina más conectada	2ª
Mayor rapidez y mejor recolección de datos	3ª



Principales Inhibidores

Inhibidores	
Costos iniciales	1ª
Otras prioridades de negocio	2ª
Seguranza y privacidad	3ª

Figura 46. ¿Cómo IoT es adoptado en las Empresas de Colombia? [101]

8.2. Infraestructura

Las proyecciones sobre el Internet del Futuro están dadas para el desarrollo sobre redes basadas en IP este es el caso de las redes de próxima generación que se están desplegando a nivel mundial para la mejor utilización de los recursos físicos de una red realizando la prestación de múltiples servicios a partir de solo un núcleo de red, para esto una exigencia global es trabajar sobre tecnologías de transmisión de datos cada vez más veloces como lo son la fibra óptica en el caso de la comunicación alámbrica y LTE para la comunicación inalámbrica, tecnologías en las que se alcanzan velocidades de Banda Ancha que en el caso de la información que se transmitirá en las redes para Internet de las Cosas es suficiente, por esta razón los diferentes países que están en la puesta en marcha de redes de próxima generación en aspectos de infraestructura tendrán la posibilidad de generar una gran variedad de servicios en temas del IoT [100].

En el caso de Colombia en el año 2010 se llevó a cabo un ambicioso proyecto por parte del gobierno colombiano, encabezado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), llamado “Proyecto Nacional de Fibra Óptica”, el cual busca la conexión de un alto porcentaje de municipios del país a Internet a través de un cable de fibra óptica que se tiende a través de los diferentes departamentos del país, al 2010 se tenían 200 municipios con conexión a Internet, en el 2013 este número alcanzo los 777 municipios conectados y para el 2014 llego a 1078 municipios dando cobertura al 96% de las poblaciones de Colombia [102]. El reto del MinTIC es alcanzar los 27 millones de conexiones a internet en 2018 [103].

8.2.1. Conexiones Banda Ancha y demás Conexiones

Al finalizar el cuarto trimestre del 2016, el número total de conexiones a Internet de Banda Ancha* alcanzó los 15.306.066 accesos en el país, mientras las demás conexiones a Internet (conexiones con velocidad efectiva de bajada – Downstream <1.024 Kbps + Móvil 2G) suman 546.925, para un agregado nacional de 15.852.991 conexiones a Internet. *Ver Gráfico 9.*

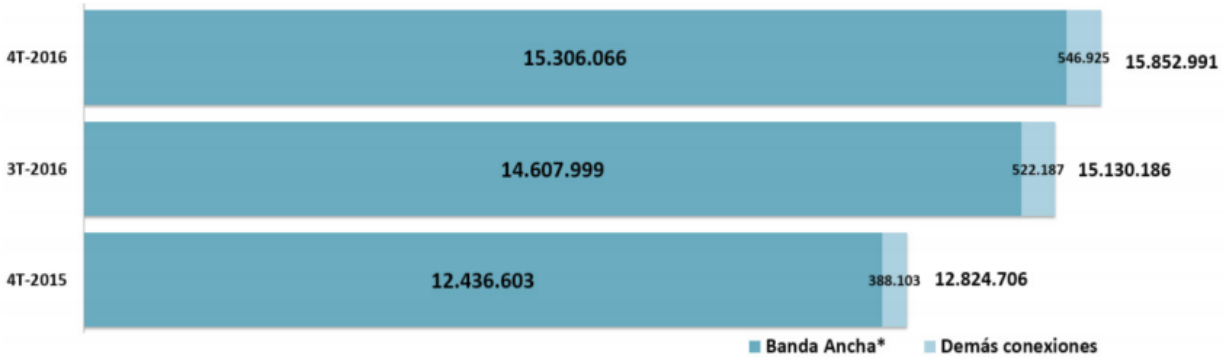


Gráfico 9. Conexiones Banda Ancha y demás Conexiones. [104].

Al término del cuarto trimestre del 2016, el número de conexiones a Internet de Banda Ancha* presentó un incremento del 4,8% con relación al tercer trimestre del 2016, y un crecimiento del 23,1% con referencia al cuarto trimestre del 2015. *Ver Gráfico 10.*

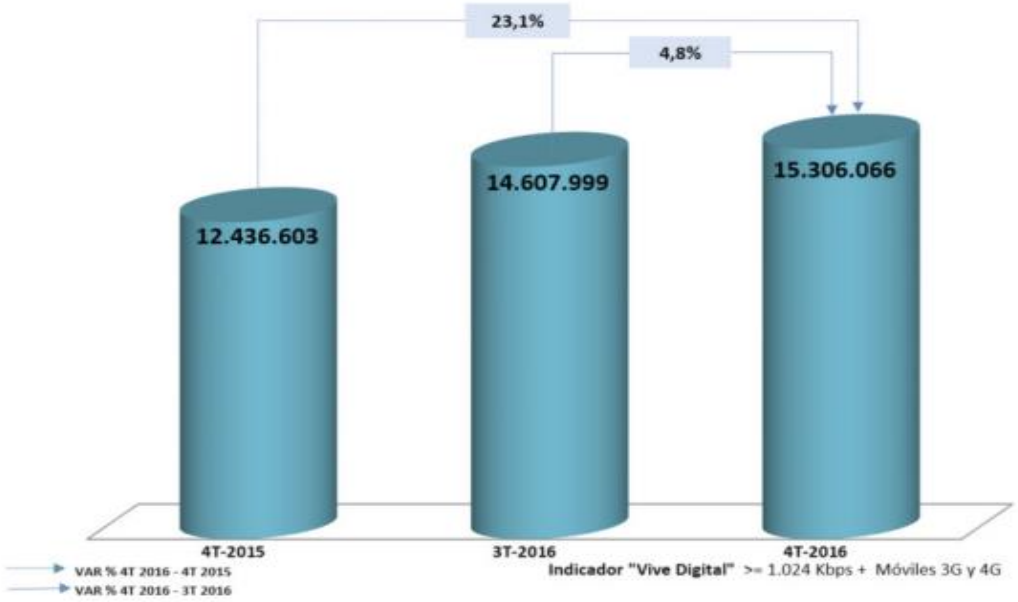


Gráfico 10. Variación % y conexiones a internet de banda ancha [105].

Al finalizar el cuarto trimestre del 2016, las conexiones a Internet de Banda Ancha se componían principalmente por accesos móviles a Internet con un total de 9.414.186, los cuales se discriminan en aquellas reportadas sobre redes de cuarta generación 4G, con un total de 4.886.391 conexiones, los cuales aumentaron su participación del 29,36% (3T-2016) al 31,92% en el cuarto trimestre. Los accesos a redes de tercera generación 3G móvil alcanzaron un total de 4.527.795 conexiones y una participación del 29,58%, disminuyendo esta última cifra 1,08 puntos porcentuales en relación al tercer trimestre del 2016. Por su parte, las conexiones a Internet fijo dedicado alcanzaron un total de 5.891.880 accesos y una participación del 38,49%.

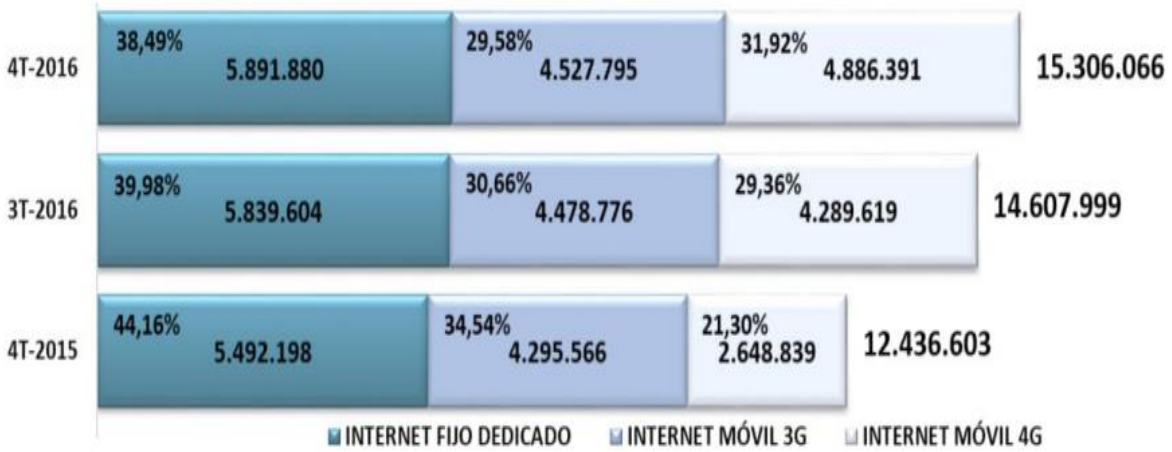


Gráfico 11. Conexiones de internet banda ancha, participación por tipo de acceso [104].

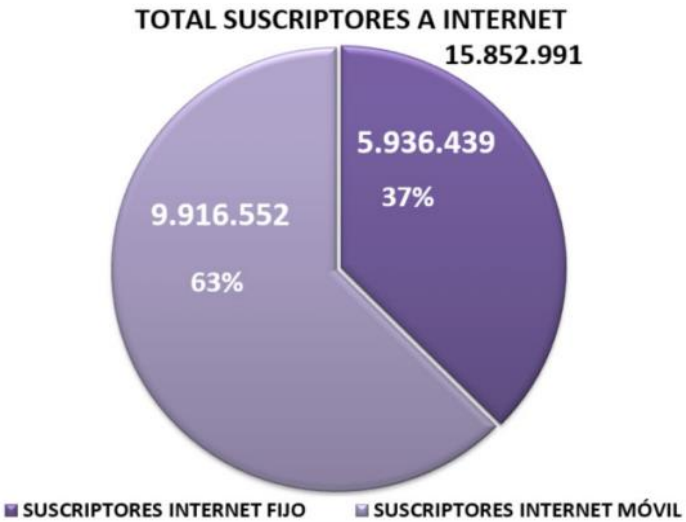


Gráfico 12. Suscriptores a internet fijo dedicado y móvil, y participación por tipo de acceso (4t-2016) [104].

Al cierre del cuarto trimestre del 2016, el número total de suscriptores a Internet estaba compuesto principalmente por accesos móviles a Internet con 9.916.552 suscripciones y una participación del 63%; mientras que los suscritores fijos a Internet alcanzaron los 5.936.439 y una participación del 37%.

Para el cuarto trimestre del 2016, la variación porcentual de suscriptores a Internet fijo fue del 6,9% respecto al cuarto trimestre del 2015, representado en una variación absoluta de 384.879 suscriptores. Por su parte, los suscriptores a Internet Móvil presentaron una variación porcentual del 36,3% respecto al cuarto trimestre del 2015.

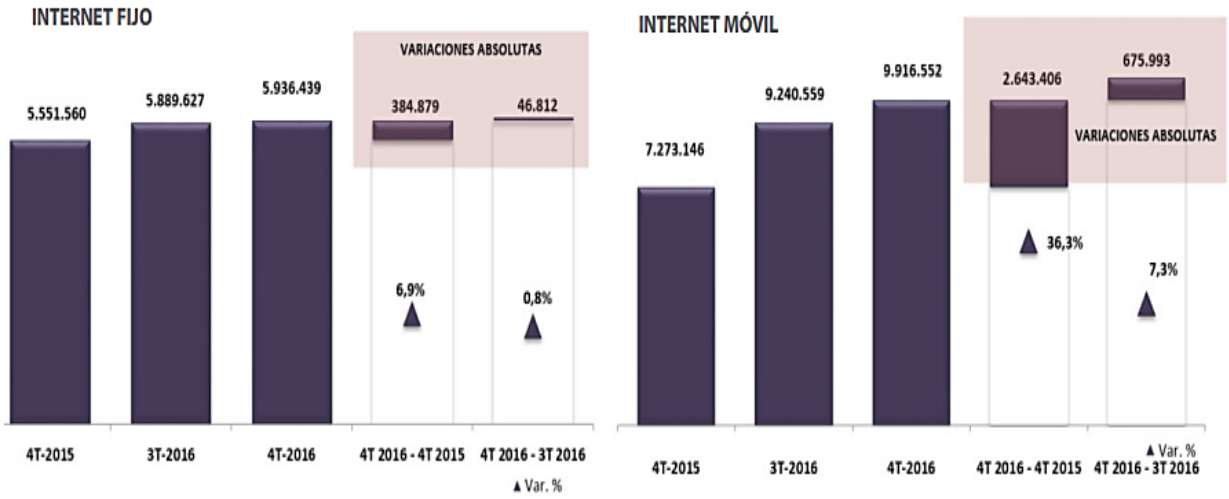


Gráfico 13. Variación porcentual suscriptores a internet fijo dedicado y móvil. [104]

Al finalizar el cuarto trimestre del 2016, el mayor índice de penetración de Internet fijo a nivel departamental, contando el Distrito Capital, lo lideró Bogotá.

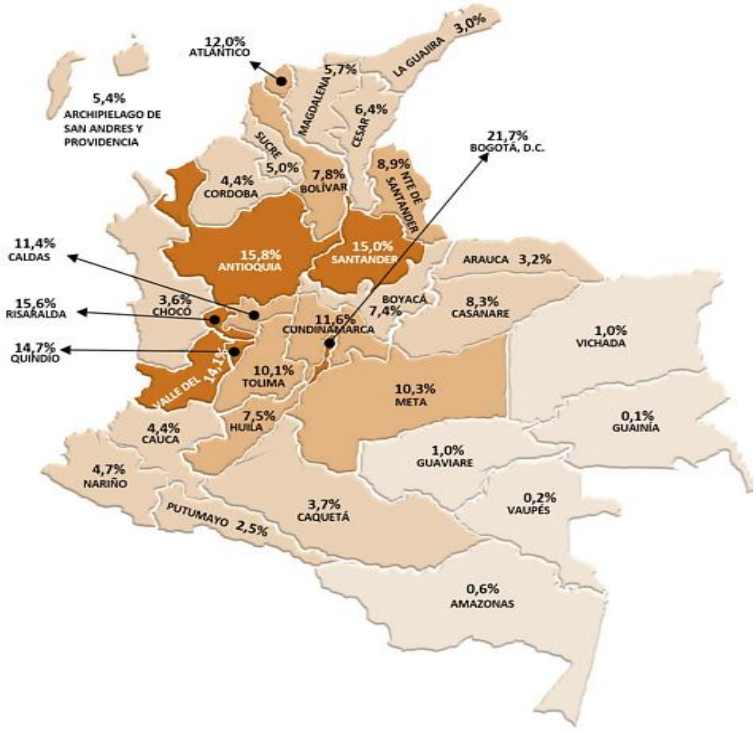


Figura 47. Índice de penetración de internet fijo dedicado por departamentos y distrito capital (4t-2016) [105].

8.2.2. Participación de los principales operadores móviles en Colombia

En el año 2014 de acuerdo con el reporte de Industria del sector TIC el operador de telefonía CLARO tuvo una participación total en servicios de TV satelital, internet fijo y móvil, telefonía fija y móvil y suscripciones del 54,09%, muy por encima del operador MOVISTAR que tuvo una participación total del 20,04%, seguido de UNE con un 11,69% , TIGO con un 4,53%, ETB con 2,07%, DIRECT TV con 1% , entre otros operadores de servicios que sumaron entre ellos una participación total del 6,22%. *Ver Tabla 7.*

Operador / Servicio	TV suscripción y satelital	Internet Fijo	Telefonía Fija	Internet Móvil-Demanda	Internet Móvil-Suscripción	Telefonía Móvil	TOTAL
Claro	43.62%	33.33%	21.25%	76.50%	41.00%	53.81%	54.09%
movistar	7.95%	19.06%	20.07%	12.62%	35.01%	23.21%	20.40%
une	21.24%	24.88%	21.30%	0.09%	4.87%	0.70%	11.69%
tigo	0.00%	0.00%	0.00%	6.89%	17.91%	16.54%	4.53%
eTb	0.35%	11.15%	19.84%	0.01%	0.52%	0.04%	2.07%
DIRECTV	20.13%	0.13%	0.00%	0.00%	0.00%	0.00%	1.00%
OTROS	6.72%	11.43%	17.53%	3.89%	0.69%	5.70%	6.22%

Tabla 7. Participación de los proveedores en los servicios TIC por número de usuarios 2014 (%) [105].

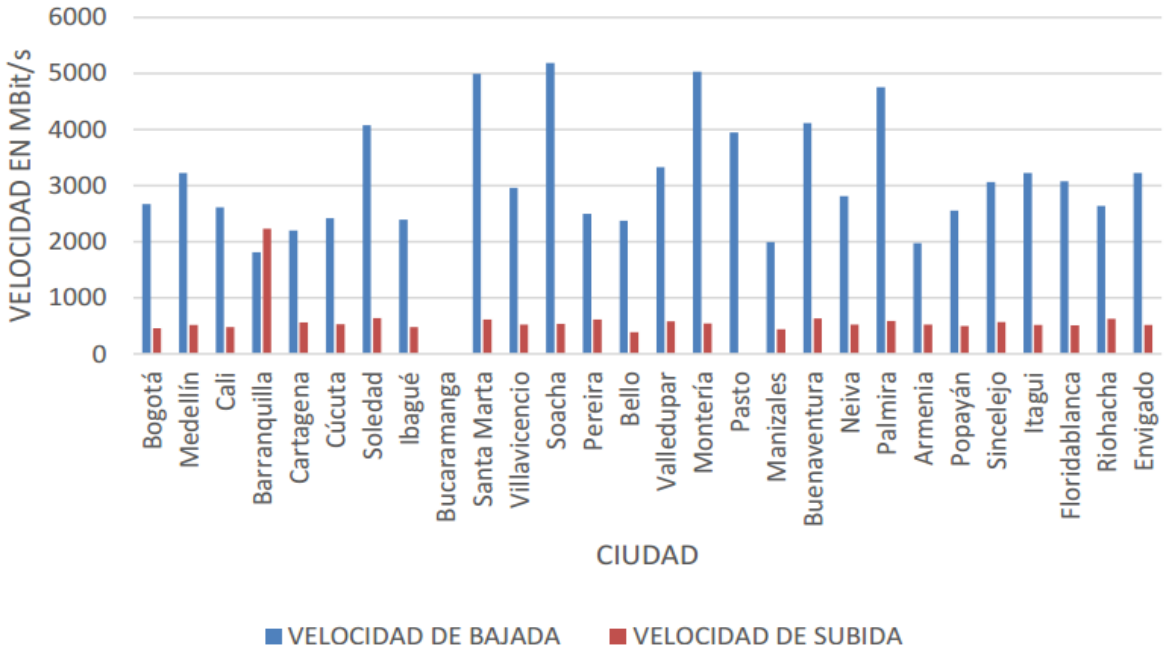


Gráfico 14. Velocidad de la red de datos de CLARO en municipios con más de 200.000 habitantes [100]

:

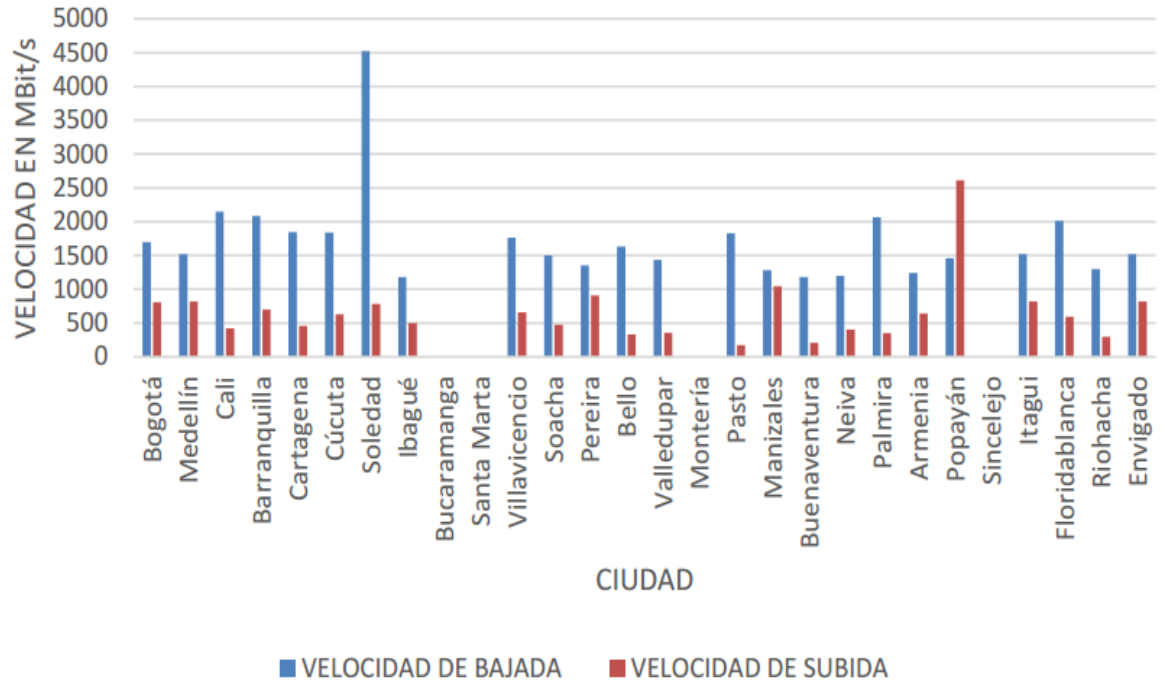


Gráfico 15. Velocidad de la red de datos de MOVISTAR en municipios con más de 200.000 habitantes [100].

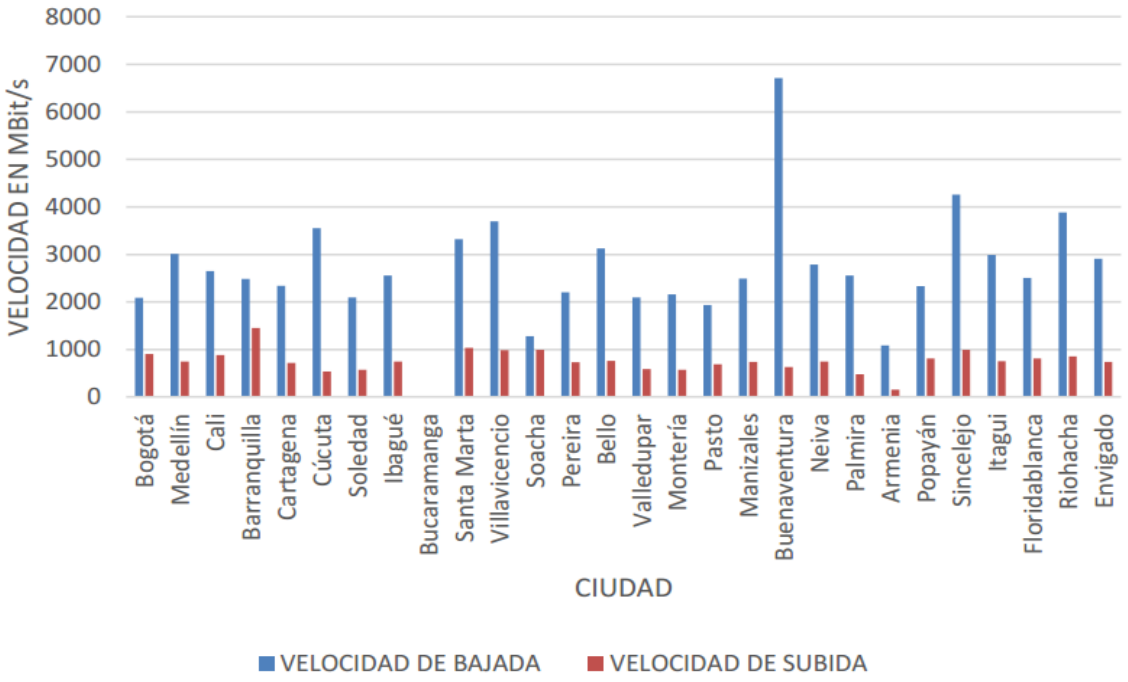


Gráfico 16. Velocidad de la red de datos de TIGO en municipios con más de 200.000 habitantes [100].

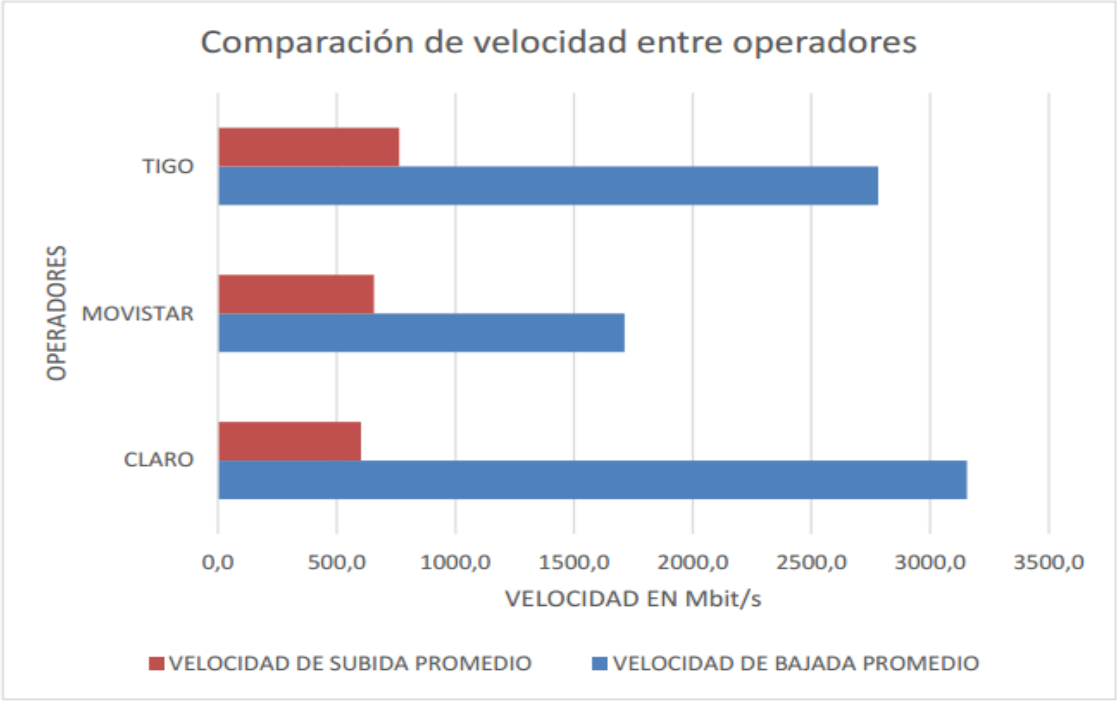


Gráfico 17. Comparación de Velocidad entre operadores [100].

A partir de estas velocidades se puede afirmar que para las primeras fases del Internet de las Cosas donde las aplicaciones no tendrán un grado alto de complejidad la red móvil de Colombia podrá soportar el IoT pero que como todo sistema este deberá ir mejorando para prestar mayores facilidades y aplicaciones cada vez más robustas, también es importante mencionar que a pesar que son conexiones móviles, se están obteniendo velocidades superior a 1.024kbps valores comprendidos para Banda Ancha en el país.

En el caso de Buenaventura se observa que la velocidad en conexiones móviles es mucho mayor en bajada que en subida en donde se evidencia que la red de servicios de red móvil de Claro y Tigo sobresalen con valores superiores a las 4000 MBit/s, velocidad aceptable para adoptar IoT en sus etapas iniciales. Ver gráficos 14 y 16.

De acuerdo con el informe del cuarto trimestre del 2016 del MinTIC [105] el número de suscriptores con acceso a internet para el municipio de Buenaventura fue de 17.762 para el cuarto trimestre del 2015, 20.345 para el tercer trimestre del 2016 y de 19.836 para el cuarto trimestre del 2016.

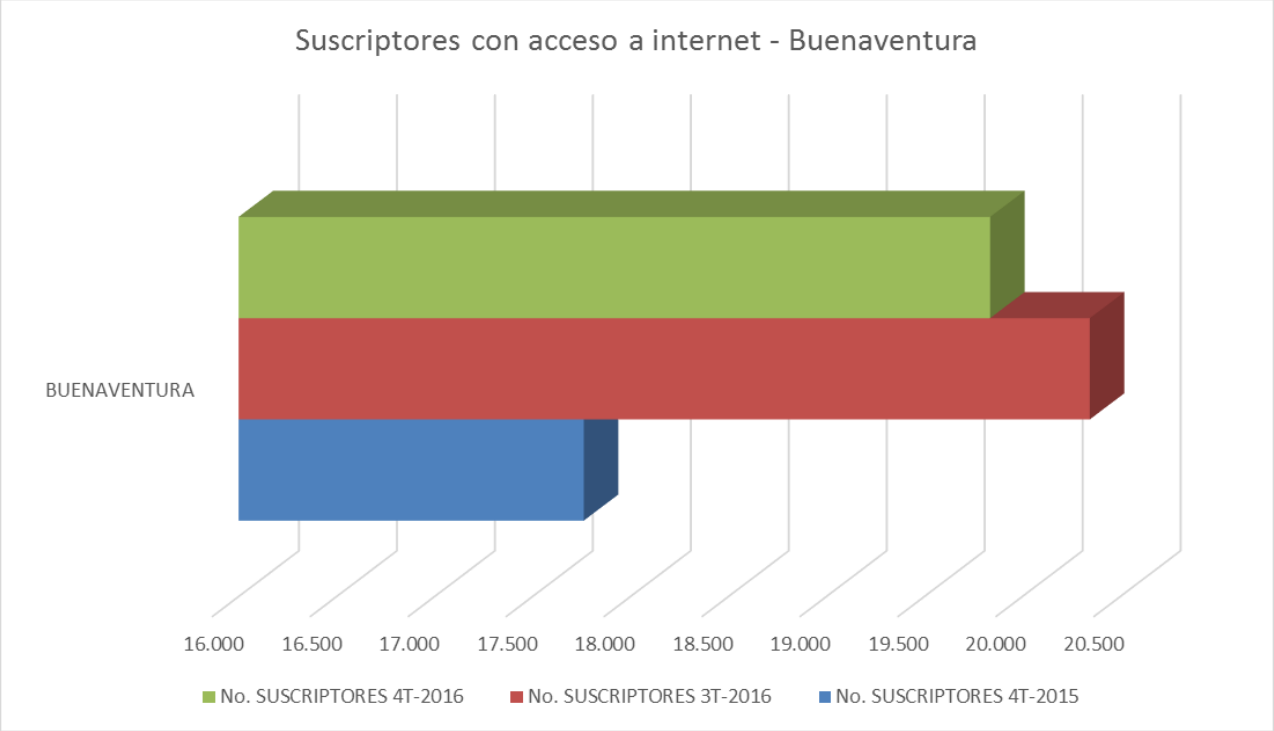
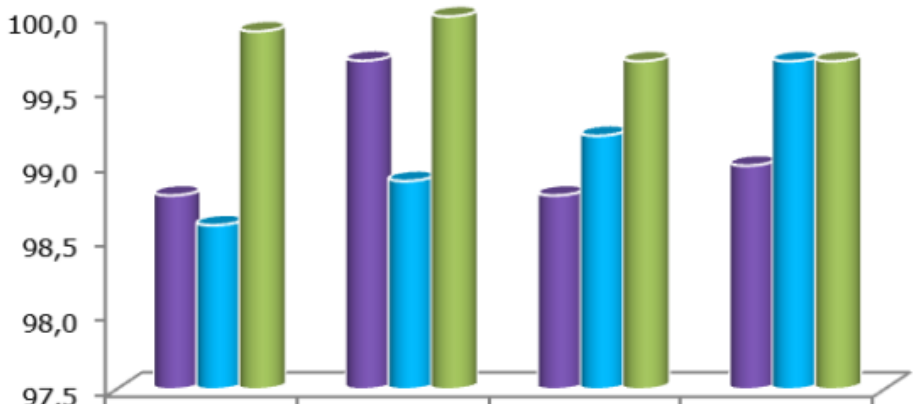


Gráfico 18 Suscriptores con acceso a internet en Buenaventura. [105]

8.2.3. Uso de TIC por Empresas

El porcentaje de empresas que utilizan Internet permite observar la masificación e importancia para el desarrollo de las labores en cada uno de los sectores. De acuerdo con la información en el año 2013, las empresas de los tres sectores (Industria, comercio y servicios) se encontraban por encima del 99% de utilización de Internet. Entre 2012 y 2013 no se presentó una variación significativa en este indicador puesto que se encuentra muy cercano al 100%, lo que significa que en todos los sectores las herramientas disponibles en Internet son de vital importancia.



	2010	2011	2012	2013
Sector Industria	98,8	99,7	98,8	99
Sector Comercio	98,6	98,9	99,2	99,7
Sector Servicios	99,9	100,0	99,7	99,7

Gráfico 19. Porcentaje de empresas que utilizan Internet [105].

8.2.4. Proyecto Nacional de Fibra Óptica (2010 – 2014) [103]

El Gobierno Nacional de Colombia busca ampliar la infraestructura actual de redes de fibra óptica existentes, a través del despliegue de redes terrestres y la ampliación de la infraestructura de transporte y acceso, especialmente en zonas de difícil acceso y con poblaciones vulnerables. La operación de dicha red se hará durante 15 años, para facilitar el acceso a la autopista de la información, y por consiguiente, multiplicar el número de conexiones a Internet.

Beneficiarios

Los potenciales beneficiarios son aproximadamente 3.725.000 habitantes, residentes en las cabeceras municipales de los 753 municipios a conectar, así como dos mil instituciones públicas que contarán con servicio gratuito de conectividad a Internet en banda ancha por cinco años.

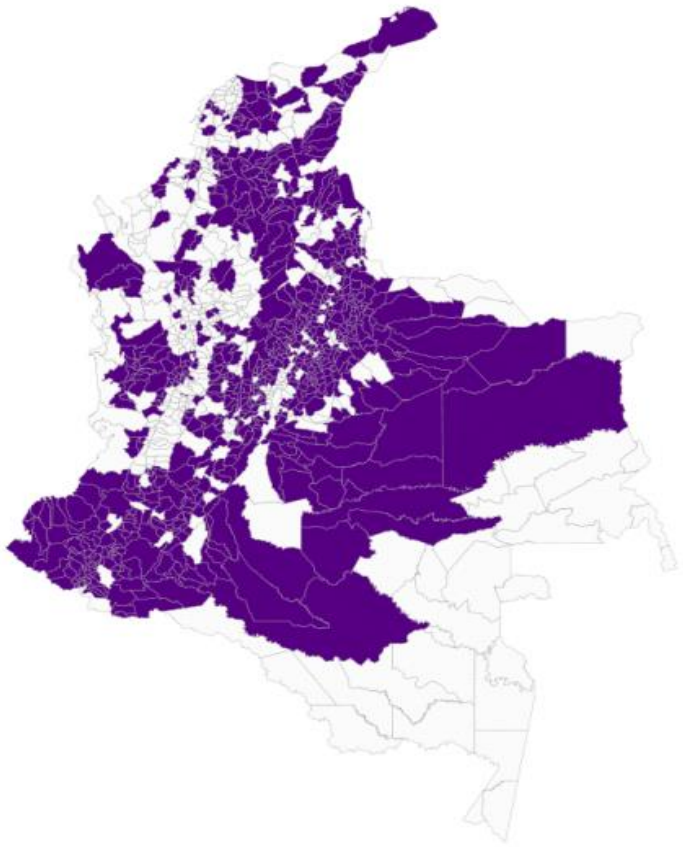


Figura 48 Distribución de municipios a conectar

8.3. PROPUESTAS PRESENTES EN COLOMBIA EN CUANTO A LOS SISTEMAS DE SEGURIDAD ELECTRÓNICA IOT – CASO SOLUTEK. [106]

La importante compañía Solutek está implementando Internet de las cosas (IoT) para seguridad y protección en Colombia. Gracias al sistema centralizado de captura de información de IoT se pueden establecer parámetros de alerta y seguridad que ayudan a tomar decisiones en tiempo real, e inclusive ayudar a prevenir futuros accidentes, o incidentes criminales que puedan presentarse en cualquier circunstancia de la vida diaria.

La solución de internet de las cosas de Solutek en Colombia consiste en una robusta solución de ingeniería, en donde los más expertos profesionales de tecnología convergen para realizar una integración de hardware y software dependiendo de las necesidades y requerimientos de los clientes que tengan en un momento determinado.

El objetivo de contar con una solución de Internet de las cosas (IoT) de Solutek, es permitirle al cliente contar con una solución escalable en el tiempo, y un respaldo en las verticales más importantes de infraestructura y tecnología, como lo son el desarrollo de software, creación de hardware, venta y distribución de hardware y software más importante del mercado, y un grupo de talento humano inigualable para la implementación de la tecnología en pro de la eficiencia tecnológica de las empresas.

En Solutek Internet de las cosas (IoT) proveer soluciones de:

- Software de Videovigilancia: Optimice costos, rendimiento y capacidad mediante soluciones de video vigilancia de alta calidad.

- Plataformas para la seguridad de sus activos: Mejore la disponibilidad, la escalabilidad y la eficiencia empresarial con plataformas modulares basadas en soluciones.

- Cámaras IP: Rendimiento superior en una amplia variedad de entornos con cámaras digitales profesionales de alta resolución.

- Control de acceso: Implemente control de acceso electrónico a través de la red IP mediante una solución integral con componentes de hardware y software.

- Respuesta a incidentes: Proporcione rápidamente información valiosa a las personas que la necesitan en situaciones de emergencia en las que cada segundo vale.

9. CONCLUSIONES

- El conocimiento del contexto de IoT, sus campos de aplicación y el ecosistema de integración entre dispositivos permite entender como los dispositivos IoT se comunican entre sí de manera proactiva para brindar soluciones efectivas que contribuyen a mejorar la calidad de vida y hacerla mucho más práctica y fácil.

- Gracias a la identificación de las tecnologías IoT y los protocolos de comunicación, se logró conocer cuáles son los dispositivos inteligentes que cuentan con la compatibilidad requerida para ser utilizados en los sistemas de seguridad electrónica IoT.

- El Gateway Xtreme Meshillium y los sensores IoT fabricados por la multinacional tecnológica Libelium sirvieron como referente técnico para la construcción de la propuesta por la compatibilidad, calidad y robustez de sus elementos tecnológicos.

- La plataforma IBM Bluemix además de permitir la integración con la nube para ver en tiempo real el comportamiento de los datos y la información procesada y ser compatible con el Gateway de Libelium cuenta con un entorno de desarrollo de aplicaciones IoT para sistemas operativos Android e iOS.

- La importancia de implementar sistemas de seguridad electrónica IoT radica en la necesidad de brindar soluciones inteligentes, confiables, efectivas y robustas para cada uno de los procesos y actividades de las empresas.

- Se evidencia que las muchas empresas a nivel mundial están preparadas para implementar soluciones IoT o planear proyectos a futuro, aunque existen variables tales como el costo de la implementación, dispositivos e infraestructura.

- Las limitaciones tecnológicas están retrocediendo exponencialmente. Cuando billones de cosas están conectados, hablando y aprendiendo, la única limitación dejada será nuestra propia imaginación.

10. RECOMENDACIONES

- Se requiere que los sistemas de seguridad electrónica IoT actuales sean completamente proactivos, ya que aún requieren de algún tipo de intervención humana ya sea para su funcionamiento, monitorización, almacenamiento y/o procesamiento de datos recolectados.

- Para dar soporte a los posibles miles de millones de dispositivos IoT, se necesita una infraestructura inalámbrica que no solo sea escalable en términos de su capacidad, sino que además pueda manejar de manera óptima las diferentes necesidades de servicio de diversas verticales de IoT.

- Las grandes compañías tecnológicas deben fabricar dispositivos IoT que sean compatibles entre sí y hablen el mismo idioma.

- Mejorar la infraestructura de red en Colombia para lograr que IoT pueda trabajar en óptimas condiciones.

- Mayor inversión en investigación para el tema de IoT

11. BIBLIOGRAFÍA

[1] DAVE EVANS, Internet de las cosas: Cómo la próxima evolución de Internet lo cambia todo, abril de 2011, Informe técnico. Cisco Internet Business Solutions Group (IBSG) disponible en: <http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf> [citado el 10 de septiembre de 2016].

[2] CISCO. Internet de las Cosas. [en línea] <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf> [citado el 15 de enero de 2017].

[3] HINDAWI PUBLISHING, Corporation. Internet of Things: Architectures, Protocols, and Applications. New Delhi: Academic Editor: Rajesh Khanna, 2017. 25 p.

[4] DZONE, Research. Guide to Internet of Things. New York: Editor: Rick Ross, 2016. 36 p.

[5] POSTSCAPES. Internet of Things (IoT) History [en linea]. <https://www.postscapes.com/internet-of-things-history/> [citado en 4 agosto de 2016].

[6] SORAYAPANIAGUA. El gran reto de IoT es el idioma de los dispositivos. [en línea]. <http://www.sorayapaniagua.com/2015/01/12/el-gran-reto-de-iot-es-el-idioma-de-los-dispositivos/> [citado en 4 agosto de 2016].

[7] IOT TECHNOLOGY SOLUTIONS. What is the Internet of Things (IoT)? [en línea]. <http://www.iottechnology.com/what-is-the-internet-of-things/> [citado en 4 agosto de 2016].

[8] DIGIKEY. IoT e inteligencia de las cosas de Analog Devices. [en línea] <https://www.digikey.com/es/product-highlight/a/analog-devices/iot> [citado en 16 febrero de 2017].

[9] LIBELIUM. Meshlium Xtreme Technical Guide. [en línea] <http://www.libelium.com/downloads/documentation/meshlium_technical_guide.pdf> [citado en 16 febrero de 2017]

[10] AXIS, Communications. Hardening Guide [en línea] <https://www.axis.com/files/sales/AXIS_Hardening_Guide_1488265_en_1510.pdf> [citado en 2 febrero de 2017].

[11] SILICON LABS. The Evolution of Wireless Sensor Networks. [en línea]. <http://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf> [citado en 15 marzo 2017].

[12] INTERNATIONAL ELECTROTECHNICAL COMMISSION. Internet of Things: Wireless Sensor Networks. [en línea]. <http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf> [citado en 15 marzo 2017].

[13] USC VITERBI SCHOOL OF ENGINEERING. An Introduction to Wireless Sensor Networks. [en línea]. <http://ceng.usc.edu/~bkrishna/research/talks/WSN_Tutorial_Krishnamachari_ICISIP05.pdf> [citado en 15 marzo 2017].

[14] UNIVERSIDAD VERACRUZADA. Introducción a los Sistemas de Información. [en línea]. <https://www.uv.mx/personal/artulopez/files/2012/08/FundamentosSistemasInformacion.pdf> [citado en 30 marzo 2017].

[15] ICO. Las definiciones clave de la Ley de Protección de Datos. [en línea]. <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/> [citado en 30 marzo 2017].

[16] JEREZ LUGO, Carlos Augusto. Seguridad para lograr Confiabilidad y Calidad de los Servicios Digitales en Internet: Cholula, Ciudad de México 2004, 105 h. Trabajo de grado (Ingeniería de Sistemas). Universidad Las Américas Pueblas. Faculta de Ingeniería, Departamento de Ingeniería de Sistemas Computacionales. Disponible en <http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/>

[17] ASIR2. Autentificación [en línea] <http://asir2-luisvives.blogspot.com.co/2013/01/fiabilidad-confidencialidad-integridad.html> [citado en 3 mayo de 2017].

[18] UNIVERSIDAD DE TARAPACÁ. Sensores y transistores [en línea] <http://www.eudim.uta.cl/files/5813/2069/8949/fm_Ch03_mfuentesm.pdf> [citado en 3 mayo de 2017].

[19] COLEGIO DISTRITAL NACIONES UNIDAS. Introducción a los sistemas automatizados: Actuadores. [en línea] <http://www.colegionacionesunidasied.com/pdf/competencias/actuadores.pdf> [citado en 3 mayo de 2017].

[20] UNIVERSIDAD DE LA REPUBLICA DE URUGUAY. Instrumentación. [en línea]. <https://www.fing.edu.uy/iq/cursos/dcp/teorico/Instrumentacion_12b.pdf> [citado en 3 mayo de 2017].

[21] GABRIEL CEVALLOS. Seguridad electrónica [en línea]. <https://sites.google.com/site/seguridadelectronicagcm/> [citado en 05 marzo de 2017].

[22] ISEC. Control de acceso: qué es y para qué sirve. [en línea] <http://www.isec.com.co/control-de-acceso-que-es-y-para-que-sirve/> citado en 05 marzo de 2017].

[23] SIGNIFICADOS. Que es CCTV. [en línea] <https://www.significados.com/cctv/> [citado en 05 marzo de 2017].

[24] VOLTIMUM. Sensores de movimiento. [en línea] <https://www.voltimum.es/articulos-tecnicos/sensores-movimiento> [citado en 05 marzo de 2017].

[25] WIKIPEDIA. Sistemas de alarma. [en línea] <https://es.wikipedia.org/wiki/Sistema_de_alarma> [citado en 05 marzo de 2017].

[26] TODOREDES. Gateway (puerta de enlace). [en línea] <https://todo-redes.com/equipos-de-redes/gateway-puerta-de-enlace> [citado en 05 marzo de 2017].

[27] WIKIPEDIA. Detector de gas. [en línea] <https://es.wikipedia.org/wiki/Detector_de_gas > [citado en 05 marzo de 2017].

[28] INTEREMPRESAS. Lectores de reconocimiento biométrico: seguridad y control de acceso [en línea] <http://www.interempresas.net/Seguridad/Articulos/50527-Lectores-de-reconocimiento-biometrico-seguridad-y-control-de-acceso.html> [citado en 05 marzo de 2017].

[29] PALACIOS TOLÓN, Álvaro. Diseño de Solución Interoperable para Aplicaciones M2M, Madrid 2013, 121 h. Trabajo de grado (Ingeniería de Electrónica y Telecomunicación). Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Departamento DIAC. Disponible en <http://oa.upm.es/22160/1/PFC_ALVARO_PALACIOS_TOLON.pdf>

[30] CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991. Actualizada con los Actos Legislativos a 2015. Edición especial preparada por la Corte Constitucional.

[31] CONGRESO DE COLOMBIA. GENERAL DE LAS TICS. Ley No.1341 Bogotá, Colombia; 30 junio del 2009.

[32] CONGRESO DE COLOMBIA. DELITOS INFORMÁTICOS. Ley No. 1273. Bogotá, Colombia; 05 enero del 2009.

[33] CONGRESO DE COLOMBIA. PROTECCIÓN DE DATOS. Ley No. 1581 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Bogotá, Colombia.

[34] ITU. The Internet of Things-Executive Summary [en línea]. <www.itu.int/osg/spu/publications/internetofthings> [citado en 05 marzo de 2017].

[35] CISCO ISBG. The Internet of Things. [en línea] <https://gigaom.com/2011/07/17/the-internet-of-things-infographic/> [citado en 08 febrero 2017].

[36] GOOGLE TRENDS. Internet of Things. [en línea]. <https://trends.google.com/trends/explore?date=all&q=Internet%20of%20Things> [citado en 08 febrero 2017].

[37] SEMANTIC SCHOLAR. Internet Clean-Slate Design: What and Why? [en línea]. <https://pdfs.semanticscholar.org/700b/a413874b914557742ab688cf4c7a445e7c47.pdf> [citado en 08 febrero 2017].

[38] BI INTELLIGENCE. The Internet of Things: Examining How the IoT Will Affect the World [en línea]. <http://read.bi/iot2015> [citado en 08 febrero 2017].

[39] HINDAWI. Internet of Things: Architectures, Protocols, and Applications. [en línea]. <https://www.hindawi.com/journals/jece/2017/9324035/> [citado en 08 febrero 2017].

[40] GOOGLE CLOUD PLATFORM. Overview of Internet of Things [en línea] <https://cloud.google.com/solutions/iot-overview> [citado en 10 enero 2017].

[41] G. H. Bo Yan, «Application of RFID and Internet of Things in Monitoring and Anticounterfeiting for products» IEEE, 2008.

[42] D. Saint-Exupery, «Internet of Things: Strategic Research Roadmap, » 2009

[43] N. W. Lu Tan, «Future Internet: The Internet of Things, » IEEE, 2010.

[44] Unión Internacion de Telecomunicaciones UIT, «Ubiquitous Network Societies and their impact on the telecommunication industry, » 2005.

[45] B. Y. Miao Yun, «Research on the Architecture and Key Technology of Internet of Things (loT) Applied on Smart Grid, » IEEE, 2010.

[46] IOT. Ejemplos IoT [en línea] <https://i1.wp.com/ignaciocm.com/wp-content/uploads/2014/10/Un-experimento-con-Pinterest-y-el-SEO-Pirata.jpg?resize=516%2C698> [citado en 11 enero 2017].

[47] KW FOUNDATION. Internet de las Cosas en las Empresas. [en línea]. <http://tngconsultores.com > [citado en 11 enero 2017].

[48] TEJERO LÓPEZ, Alberto. Seguridad en el Internet de las Cosas: Retos y oportunidades detectadas. Madrid 2014. Informe Técnico. Universidad Politécnica de Madrid. Área de Innovación, Comercialización y Creación de Empresas Centro de Apoyo a la Innovación Tecnológica (CAIT), Disponible en: <http://www.upm.es>

[49] IEEE EXPLORE. A decentralized approach for security and privacy challenges in the Internet of Things. [en línea]. <http://ieeexplore.ieee.org/document/6803122/> [citado en 11 enero 2017].

[50] GARTNER. Gartner Says Over 20 Percent of Enterprises Will Have Digital Security Services Devoted to Protecting Business Initiatives Using the Internet of Things by End of 2017. [en línea]. <http://www.gartner.com/newsroom/id/2844317> [citado en 11 enero 2017].

[51] EUROPEAN COMMISION. IoT Privacy, Data Protection, Information Security. [en línea]. <https://www.europa.eu> [citado en 15 febrero de 2017].

[52] SHODAN. Motor de búsqueda. [en línea]. <https://www.shodan.io/> [citado en 15 febrero de 2017].

[53] SHODAN. Motor de búsqueda: Cámara de seguridad. [en línea]. <http://107.218.37.152/ViewerFrame?Mode=Motion&Language=0> [citado en 15 febrero de 2017].

[54] POSTSCAPES. IOT TECHNOLOGY. [en línea]. <https://www.postscapes.com/internet-of-things-technologies/> [citado en 17 de febrero de 2017].

[55] I-SCOOP. CONNECTIVITY AND NETWORKS FOR THE INTERNET OF THINGS DATA DELUGE. [en línea]. <https://www.i-scoop.eu/internet-of-things-guide/connectivity-networks-fog-computing-internet-of-things/> [citado en 18 de febrero de 2017].

[56] ADECOM. LA EVOLUCIÓN DE LA TELEFONÍA MOVIL. [en línea]. <http://www.adecom.biz/pdf/pdf_agosto2005/La%20evolucion%20de%20la%20telefonia%20movil.pdf> [citado en 19 febrero de 2016].

[57] ROHDE&SCHWARZ. UMTS Long Term Evolution (LTE) – Technology Introduction, junio 2012, disponible en: <http://cdn.rohdeschwarz.com/pws/dl_downloads/dl_application/application_notes/1ma111/1MA111_4E_LTE_technology_introduction.pdf> [citado el 15 de noviembre de 2016]

[58] 4G AMERICAS, Recomendaciones sobre el espectro para 5G, agosto de 2015, disponible en: <http://www.5gamericas.org/files/8914/3930/9333/4G_Americas_5G_Spectrum_Recommendations_White_Paper_-_Spanish.pdf> [citado el 15 de febrero 2017].

[59] GSM INTELLIGENTE. UNDERSTANDING 5G: PERSPECTIVES ON FUTURE TECHNOLOGICAL ADVANCEMENTS IN MOBILE. [en línea]. <https://www.gsmaintelligence.com/research/?file=141208-5g.pdf&download> [citado el 15 de febrero 2017].

[60] CASANOVA MATERA, Leonardo. Sistema de Posicionamiento Global (G.P.S.). En: Topografía Plana. Venezuela: Merida, 2002. p. 232-243.

[61] WEIGTHLESS TM. SPECTRUM FOR WEIGHTLESS. Mayo 2014. Disponible en <http://www.weightless.org/about/spectrum-for-weightless> [citado el 25 de junio de 2016].

[62] WIMAX FORUM. WiMAX Forum Withe papers. Febrero 2012. Disponible en <http://resources.wimaxforum.org/resources/documents/marketing/whitepaper> [citado el 25 de junio 2016].

[63] DASH7 ALLIANCE. DAsh7 Alliance, Why Dash7? Octubre 2014. <http://www.dash7-alliance.org/?page_id=18> [citado el 25 de Junio de 2016].

[64] EnOcean. (2014). EnOcean Green Smart Wireless, Technology. Junio 2014. Disponible en <https://www.enocean.com/en/technology/> [citado el 27de junio 2016].

[65] MICRO AUTOMACIÓN. CONTROLADOR LÓGICO PROGRAMABLE. [en línea]. <http://www.microautomacion.com/capacitacion/Manual061ControladorLgicoProgramablePLC.pdf> [citado el 27de junio 2016].

[66] UNIVERSIDAD TECNOLÓGICA DE PEREIRA. ETHERNET. [en línea]. <http://blog.utp.edu.co/ee973/files/2012/04/capitulo09-ethernet.pdf> [citado el 27de junio 2016].

[67] DIPUTACIÓN DE CÁLIZ. CÓDIGOS QR. [en línea]. <http://www.dipucadiz.es/export/sites/default/galeria_de_ficheros/sociedad_de_la_informacion/destacados/Manual.CodigosQR.pdf> [citado el 27de junio 2016].

[68] SERBULENT TOZLU, M. S. IEEE Communications Magazine. Wi-Fi Sensors for Internet of Things: A Practical Approach. Junio 2012. Disponible en <https://clarinet.u-strasbg.fr/~gallais/uploads/ESIROI/wifi-sensors-iot.pdf> [citado el 27 de junio 2016].

[69] Z-WAVE. About Z-Wave, what is Z-Wave home control? Disponible en <http://www.z-wave.com/what_is_z-wave> [citado el 27 de junio 2016].

[70] ZigBee Alliance. (2012). ZigBee Specifications. Disponible en <http://www.zigbee.org/Specifications.aspx> [citado el 28 de junio 2016].

[71] MARTÍNEZ VARGAS, Daniel Eduardo. Sistema de domótica para control y supervisión de una habitación de manera remota, Bogotá, 2015, 66 h. Trabajo de grado (Ingeniero Electrónico). Pontificia Universidad Javeriana. Facultad de Ingeniería. Departamento de Ingeniería Electrónica. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20141107MarioRodriguezCerezo.pdf

[72] ATHOW, D. TechRadar.pro: How Bluetooth Smart is shaping the internet of things. Octubre 2014. Disponible en <http://www.techradar.com/news/world-of-tech/futuretech/how-bluetooth-smart-is-shaping-the-internet-of-things-1253196/1#articleContent> [citado el 28 de junio 2016].

[73] ANT+. ANT / ANT+ Defined. Marzo 2014. Disponible en <http://www.thisisant.com/developer/ant-plus/ant-antplus-defined/> [citado el 28 de junio 2016].

[74] MADRIOD. Tecnología de Identificación por Radiofrecuencia. [en línea]. <http://www.madrimasd.org/uploads/informacionidi/biblioteca/publicacion/doc/VT/_VT13_RFID.pdf> [citado el 28 de junio 2016].

[75] REVISTA ESPAÑOLA DE ELECTRÓNICA S.L. Redes fundamentales para IoT. [en línea]. <http://redeweb.com/articulos/articulo.php?id=1423&categoria=software> [citado en 4 de diciembre 2016].

[76] DIGITAL DIMENSION. MQTT: Un protocolo específico para el Internet de las Cosas. [en línea]. <http://www.digitaldimension.solutions/es/blog-es/opinion-de-expertos/2015/02/mqtt-un-protocolo-especifico-para-el-internet-de-las-cosas/> [citado en 4 de diciembre 2016].

[77] DZONE. Understanding Cloud Computing. [en línea]. <https://dzone.com/refcardz/getting-started-cloud> [citado en 4 de marzo 2017].

[78] NUBIT. ¿Sabes lo que es fog computing o computación en la niebla? [en línea]. <http://www.nubit.es/sabes-lo-que-es-fog-computing/> [citado en 4 de marzo 2017].

[79] <https://www.linkedin.com/pulse/cloud-computing-fog-haze-oliver-meili> [citado en 4 de marzo 2017].

[80] WSJ. Opinión: El futuro de la tecnología está en 'la niebla', no en 'la nube'. [en línea]. <https://www.wsj.com/articles/opinion-el-futuro-de-la-tecnologia-esta-en-la-niebla-no-en-la-nube-1401232160> [citado en 4 de marzo 2017].

[81] PRESAD, Lakshni. Big Data Analytics. Chennai: Notion Press, 2016. 170 p. (Chennai; no. 600 031) ISBN 978-1-946390-72-1.

[82] ACADEMIA. Integración de sistemas de seguridad electrónica. [en línea]. <https://www.academia.edu/11346204/Integraci%C3%B3n_de_sistemas_de_seguridad_electr%C3%B3nica_mailxmail_Cursos_para_compartir_lo_que_sabes> [citado en 4 de marzo 2017].

[83] SEED SMART IOT. Sensor de Movimiento Infrarrojo. [en línea]. <http://www.smart-iot.cl/sensor-de-movimiento> [citado en 5 de junio 2016].

[84] SEED SMART IOT. Detector de Humo. [en línea]. <http://www.smart-iot.cl/detector-de-humo> [citado en 5 de junio 2016].

[85] AEOTEC. Sensor de Movimiento. [en línea]. <http://aeotec.com/z-wave-sensor> [citado en 5 de junio 2016].

[86] SEED SMART IOT. Camera Smart. [en línea]. <http://www.smart-iot.cl/camara-smart> [citado en 5 de junio 2016].

[87] SEED SMART IOT. Alarma GSM. [en línea]. <http://www.smart-iot.cl/alarma-gsm> [citado en 5 de junio 2016].

[88] SEED SMART IOT. Detector de Gas y Combustible. [en línea]. <http://www.smart-iot.cl/detector-de-gas-y-combustible> [citado en 5 de junio 2016].

[89] WIKIPEDIA. IBM Bluemix. [en línea]. <https://es.wikipedia.org/wiki/Bluemix> [citado en15 de enero 2017].

[90] IBM REDBOOKS. IBM Bluemix: The Cloud Platform for Creating and Delivering Applications. [en linea]. <http://www.redbooks.ibm.com/redpapers/pdfs/redp5242.pdf> [citado en15 de enero 2017].

[91] IBM. Watson Internet of Things. [en línea]. <https://www.youtube.com/watch?v=o0kc1Xe6ltQ> [citado en15 de enero 2017].

[92] IBM. Watson Internet of Things. [en línea]. < https://www.ibm.com/internet-of-things/> [citado en15 de enero 2017].

[93] ERMESH - INGENIERIA Y DISEÑO DE IOT. Modelos de comunicación para Internet de las Cosas. [en línea]. <http://www.ermesh.com/modelos-de-comunicacion-para-internet-de-las-cosas/#more-581> [citado en15 de enero 2017].

[94] IBM. Meshlium to Watson IoT Platform Configuration Guide [en línea] <https://developer.ibm.com/recipes/tutorials/bluemix-configuration-guide-for-meshlium/> [Citado en 16 enero 2017]

[95] IBM. APPS BUEMIX [en línea] <https://www.ibm.com/developerworks/library/iot-smartphone-sensor-actuator-bluemix-apps-trs/index.htmlv> [citado en16 de enero 2017].

[96] SG BUZZ. El Impacto Real del IoT en las Empresas. [en línea]. <https://sg.com.mx/revista/51/el-impacto-real-del-iot-las-empresas#.WVB_kus1_IV> [citado en 20 marzo de 2017]

[97] ZEBRA. A Forrester Consulting Thought Leadership Paper Commissioned by Zebra Technologies: Building Value from Visibility. [en línea].

<https://www.zebra.com/content/dam/zebra/white-papers/en-us/zebra-iot-report-en-us.pdf> [citado en 15 marzo de 2017].

[98] FORRESTER. The Internet of Things Heat Map, 2016: Where IoT Will Have the Biggest Impact on Digital Business. [en línea]. <https://www.cloudera.com/content/dam/www/static/documents/analyst-reports/forrester-the-iot-heat-map.pdf> [citado en 15 marzo de 2017].

[99] LUIS GARCIA, Luis Carlos. Estudio del Impacto Técnico y Económico de la Transición de Internet al Internet de las Cosas (IoT) para el Caso Colombiano. Bogotá, 2014, 111 h. Trabajo de grado (Magister en Ingenieria de Telecomunicaciones). Universidad Nacional. Faculta de Ingeniería. Departamento de Ingeniería de Sistemas e Industrial. Disponible en. <http://www.bdigital.unal.edu.co>

[100] IDC ANALYZE THE FUTURE. Índice de Innovación de la Sociedad (QuISI) Ene 2016. [en línea]. <http://www.idclatin.com/QuISI/web/descargas/IDC-Qualcomm-QuISI-20151217-MEXICO.pdf> [citado en 15 de marzo de 2017].

[101] MINITIC. Vive Digital: Informe Rendición de Cuenta 2014. [en línea]. <http://www.mintic.gov.co/portal/604/articles-4323_recurso_1.pdf> [citado en 15 de marzo de 2017].

[102] SAAVEDRA CRESPO, Mónica Andrea. Aumenta la cobertura de internet en Colombia. En: Mundo.com [en línea]. (2016). <http://www.elmundo.com/portal/noticias/economia/aumenta_la_cobertura__de_internet_en_colombia.php#.WVE5zOs1_IW > [citado en 16 de marzo de 2017].

[103] MINTIC. Boletín Trimestral de las TIC. [en línea]. <http://colombiatic.mintic.gov.co > [citado en 16 de marzo de 2017].

[104] MINISTERIO INDUSTRIA Y COMERCIO. Estudios Económicos Sectoriales: Estudio del Servicio de Internet en Colombia. [en línea]. <http://www.sic.gov.co/sites/default/files/files/Estudio_del_Servicio_de_Internet_en_Colombia.pdf> [citado en 16 de marzo de 2017].

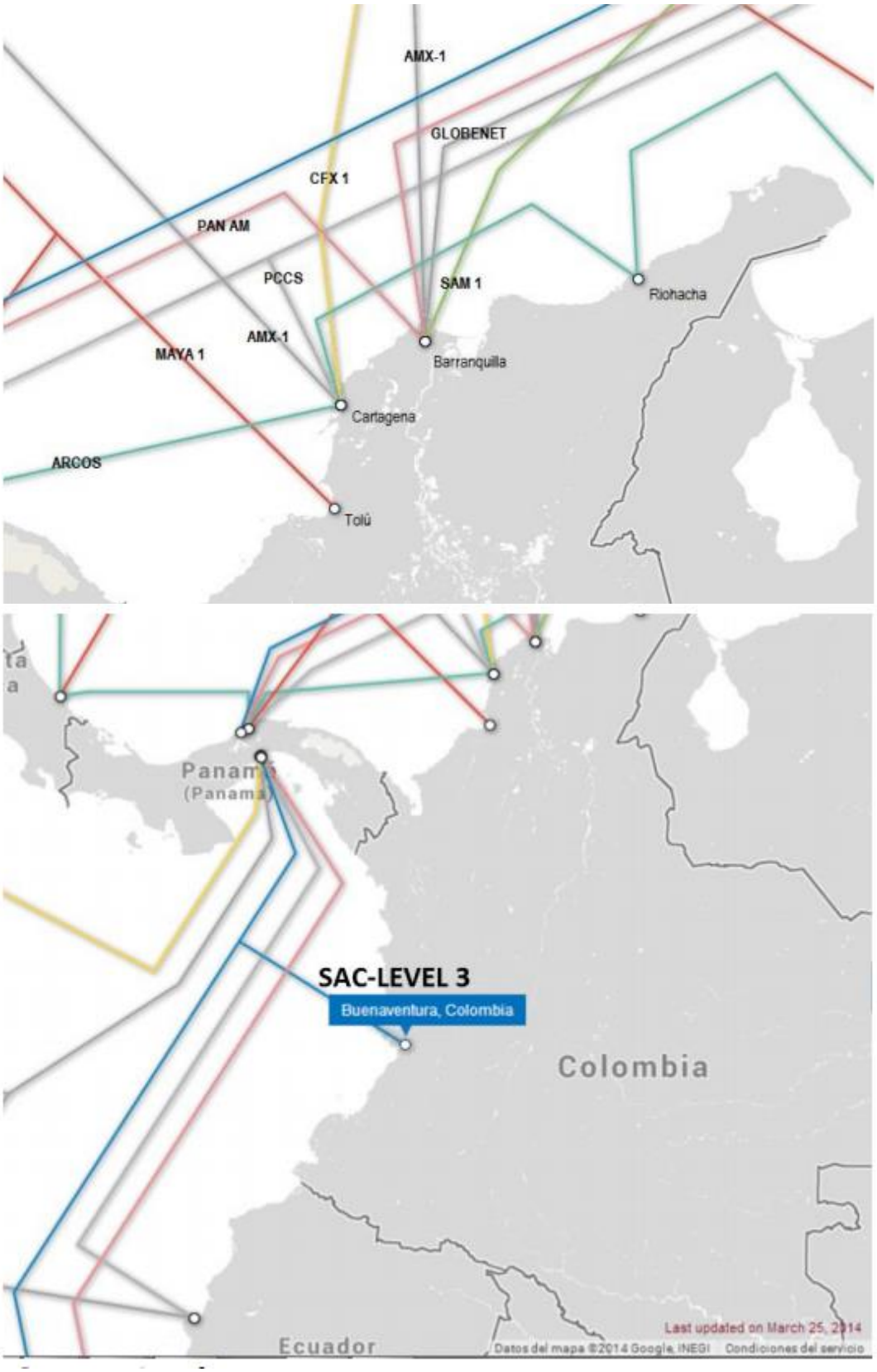
[105] MINTIC. REPORTE TRIMESTRAL DE LAS TIC: TABLAS. [en línea] <http://colombiatic.mintic.gov.co/602/articles-51235_archivo_xls.xlsx> [citado en 16 de marzo de 2017].

[106] SOLUTEK. INTERNET DE LAS COSAS (IOT) PARA SEGURIDAD Y PROTECCIÓN COLOMBIA. [en línea] <http://internetcolombia.com.co/service/internet-las-cosas-iot-seguridad-proteccion-colombia/> [citado en 30 de mayo de 2017].

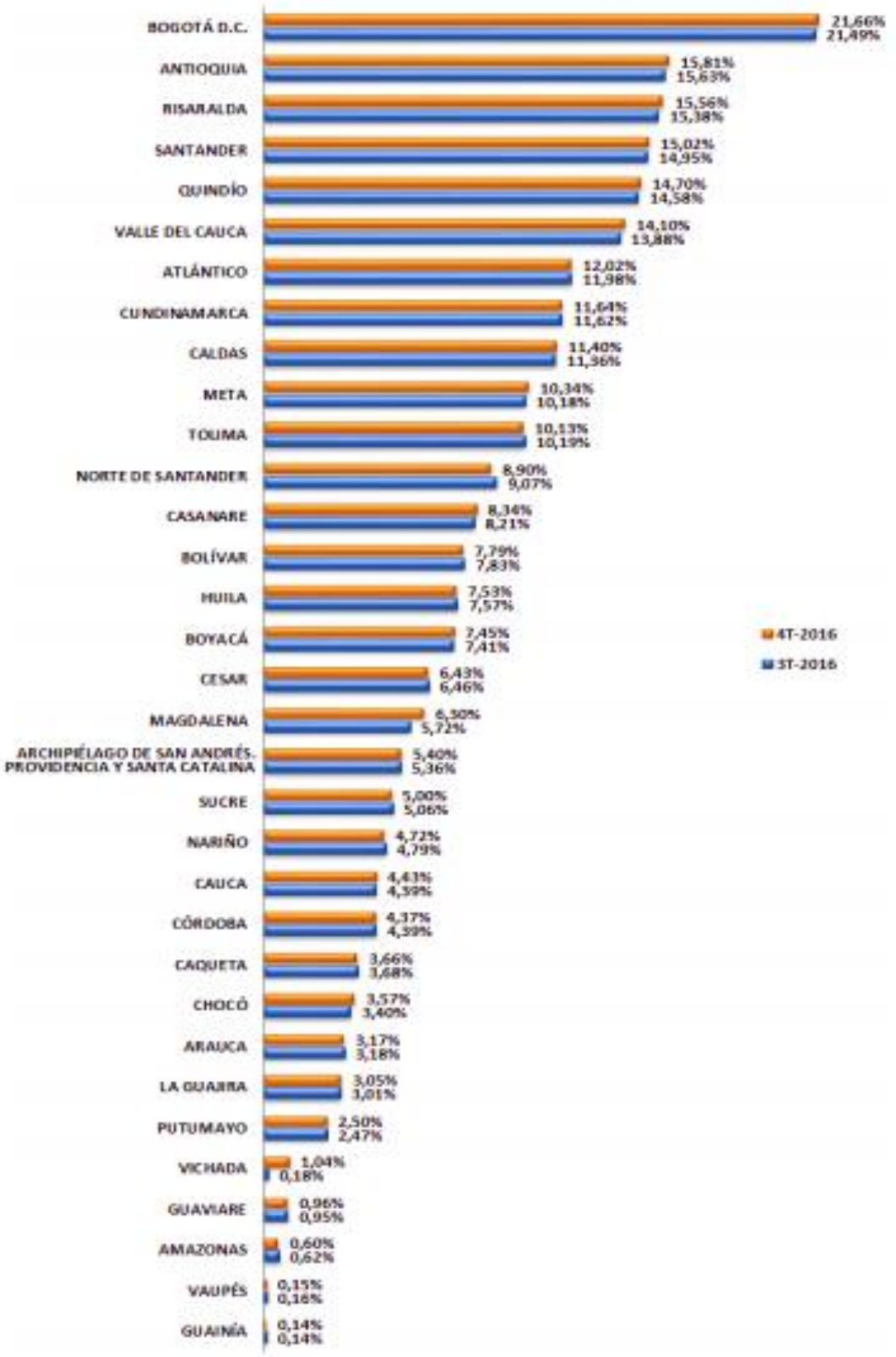
12. ANEXOS

Item	Cantidad	Valor Unidad	Descripción	Total
1	4	$ 1.500	Marcador	$ 6.000
2	4	$ 800	Esfero	$ 3.200
3	2	$ 500	Lápiz	$ 1.000
4	2	$ 11.000	Papel (Resma)	$ 22.000
5	3	$ 10.000	Tinta (Recarga)	$ 30.000
6	150	$ 200	Minutos	$ 30.000
7	3	$ 150.000	Internet (Meses)	$ 450.000
8	__	$ 200.000	Transporte	$ 200.000
9	__	$ 100.000	Alimentación	$ 100.000
10	__	$ 47.400	Imprevistos	$ 47.400
			TOTAL	**$ 889.600**

Anexo 1 Gastos en la elaboración de la propuesta

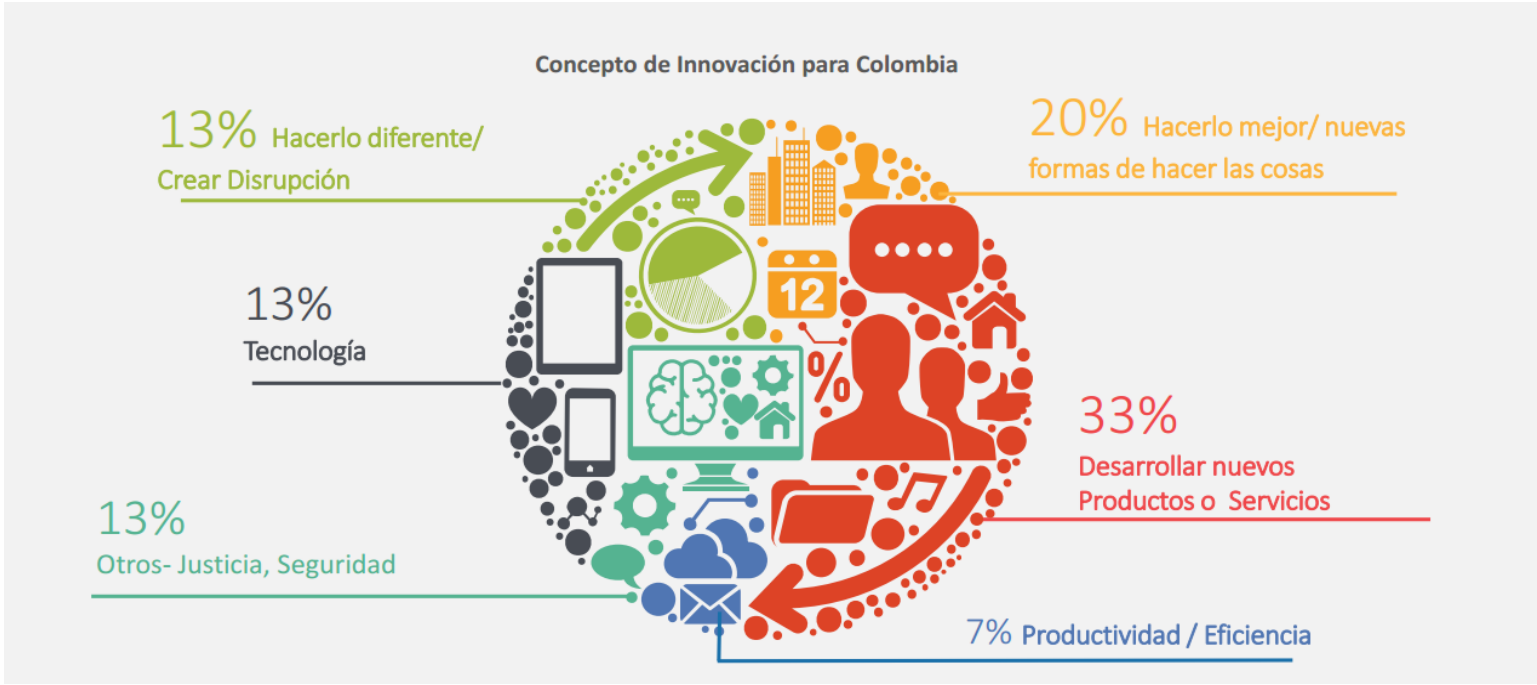


Anexo 2 Cables submarinos Fibra Óptica GlobeNet, AMX-1 SAC-LEVEL 3 y Pacific Caribbean Cable System –PCCS



Anexo 3. Ranking de Penetración por Departamento IV Trimestre de 2016 y III Trimestre de 2016 Suscriptores Internet Dedicado

Anexo 4. Proyectos de Innovación Tecnológica



Anexo 5. Concepto de Innovación para Colombia