ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

Internet del Futuro – Estudio de tecnologías IoT

Future Internet - Survey of IoT technologies

Leonardo González, Osiris Sofía, Daniel Laguía, Esteban Gesto, Karim Hallar
lgonzalez@uarg.unpa.edu.ar, osofia@uarg.unpa.edu.ar, dlaguia@uarg.unpa.edu.ar, egesto@uarg.unpa.edu.ar, khallar@uarg.unpa.edu.ar
Unidad Académica Río Gallegos - Universidad Nacional de la Patagonia Austral
Avda. Gregores y Piloto Lero Rivera - Río Gallegos - Santa Cruz – Argentina

Recibido: 02/06/2020. Aceptado: 17/11/2020

RESUMEN

Este trabajo proporciona una visión general del paradigma Internet de las Cosas (IoT) apuntando a las aplicaciones, arquitecturas, protocolos, tecnologías, y problemas pendientes y oportunidades para la investigación, tal como puede encontrarse en literatura reciente. El trabajo comienza proveyendo marcos históricos y conceptuales breves. A continuación, se profundiza en temas teóricos como las soluciones verticales, arquitecturas propuestas, protocolos específicos y tecnologías comerciales. También se revisan problemas concernientes al marco legal, todavía por desarrollarse. El postulado básico de IoT es la colaboración entre sensores inteligentes para realizar tareas innovadoras sin intervención humana. Sin embargo, avances recientes indican que serán posibles aplicaciones más potentes combinando IoT con cierto grado de inteligencia, previamente reservado a la nube. El objetivo principal de este informe es proporcionar un marco de trabajo inicial que permita a los investigadores iniciarse rápidamente en la materia, y al mismo tiempo, enfatizar la importancia de la identificación y desarrollo de aplicaciones. El trabajo concluye recomendando especial atención al modelado de sistemas IoT, a los protocolos de aplicación de tiempo real, y a la computación *fog*.

Palabras clave: IoT; Cloud; Fog; Edge.

ABSTRACT

This paper provides an overview of the Internet of Things (IoT) paradigm focusing attention on applications, architectures, protocols, enabling technologies, and open issues and research opportunities, as reported in recent literature. This work starts by providing very brief historical and conceptual frameworks. Then, a more thorough examination of theoretical subjects is given by delving deeper on common vertical solutions, proposed architectures, protocols and available commercial technologies. A brief review of issues about the yet-to-be-developed legal framework is also provided. The basic postulate of IoT is the collaboration of smart sensors to perform innovative use cases without human intervention. However, recent developments suggest that more powerful applications will be possible by combining the basic IoT core with some degree of intelligence previously restricted to the cloud. The main objective of this report is to provide an initial framework to allow researchers to quickly come up to the subject, as well as stressing the importance of applications identification and development. We conclude by recommending special attention to IoT systems modeling, real time enabled application protocols, and fog computing.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

Keywords: IoT; Cloud; Fog; Edge

INTRODUCCION

Este trabajo se realiza motivado por la incesante actividad observada en la adopción del paradigma conocido como «Internet de las Cosas» (IoT) por parte de los agentes que operan en las Tecnologías de la Información y la Comunicación. La aplicación y empleo de este modelo, que comenzó a adquirir mucha fuerza en la primera década del siglo XXI, se muestra imparable al finalizar el segundo decenio. Esta primera exploración, realizada en el marco del proyecto de investigación «Internet del futuro: aplicaciones de IoT en la Patagonia Austral» (PI 29/A425-1) comprende el relevamiento, y análisis de 58 artículos y páginas web, publicados desde la década de 1990 en adelante.

El objetivo general de este informe consiste en adquirir y dejar asentada una visión general del estado actual del conocimiento en el dominio IoT. Un segundo objetivo, no menos importante que el anterior, y que deberá perseguirse en nuestros futuros trabajos, es la identificación, investigación y desarrollo de soluciones verticales de negocio aplicables al contexto y particularidades de la Patagonia Austral.

La contribución de este trabajo consiste en el establecimiento de un mapa preliminar (y necesariamente incompleto) para el abordaje al estudio en mayor profundidad de los diversos temas, cuestiones y desafíos que se plantean dentro del paradigma IoT.

El método de investigación comprende la obtención, el relevamiento, análisis de literatura científica principalmente en idioma inglés, publicada por fuentes científicas reconocidas, fundamentalmente de acceso libre. Se ha hecho énfasis en el análisis de trabajos publicados durante los últimos cinco años. Esta investigación se relaciona con otros trabajos complementarios correspondientes a proyectos en curso en la Universidad Nacional de la Patagonia Austral (Unidad Académica Caleta Olivia), como (Villagra et al., 2018) y (Villagra et al., 2019).

Este trabajo proporciona una visión general del estado del arte del universo IoT y ha identificado algunas aplicaciones posiblemente viables en el contexto y particularidades de la Patagonia Austral.

El documento se estructura en cuatro capítulos y un Anexo. El Capítulo 1 IoT presenta el paradigma Internet de las Cosas desde los marcos de referencia históricos, conceptuales, teóricos y legales. El marco histórico hace un breve repaso de los hitos que jalonan la evolución de este moderno paradigma. El marco conceptual introduce una noción elemental de la Internet de las Cosas propiamente dicha. El marco teórico abarca los aspectos referentes a Aplicaciones, Arquitecturas y Protocolos. A continuación, se ofrece una breve revisión de las tecnologías más comúnmente utilizadas en la industria, así como una breve revisión del *middleware*, que recurre a la abstracción para facilitar la creación de aplicaciones. Posteriormente se hace referencia a los problemas que permanecen abiertos y oportunidades para la investigación. El marco legal nos introduce en la problemática de la contienda entre regulación e innovación. En este capítulo también se explican los materiales y métodos utilizados para realizar el trabajo, los resultados obtenidos y una discusión sobre los resultados. En los Capítulos 2, 3 y 4 se presentan las conclusiones del trabajo, recomendaciones y agradecimientos.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

INTERNET DE LAS COSAS - IOT

1.1 Marco de referencia

Se incluye a continuación el marco histórico, conceptual y teórico de la tecnología IoT.

1.1.1. Marco histórico

La noción de una red de dispositivos inteligentes interconectados se remonta, probablemente, hasta el año 1982, cuando en la Universidad de Carnegie Mellon se modificó una máquina expendedora de Coca Cola para que pudiese informar acerca de sus existencias así como de la temperatura de las bebidas recientemente cargadas (Teicher, 2018), (CMU Computer Science Department, 2005). El concepto de computación ubicua (*ubiquitous computing*) introducido en 1991 por Mark Weiser en "*The Computer of the 21st Century"* (Weiser, 1991) prefiguró la revolución que la IoT produciría en años posteriores. En su conocido artículo, Weiser planteó que en años venideros una multitud de dispositivos programables interconectados invadiría el hábitat humano haciéndose omnipresente a tal punto que se haría "invisible" al usuario; para atender a las demandas no se requeriría ya de una revolución en la inteligencia artificial, sino sólo de pequeñas computadoras embebidas en el entorno habitual de los usuarios.

El término "*The Internet of the Things"* fue acuñado por Kevin Ashton en 1999 (Procter & Gamble) al conectar la idea de utilizar etiquetas de identificación RFID dentro de las cadenas de suministro con la entonces novedosa tecnología de Internet (Ashton, 2009). Ashton cofundó Auto-ID Center, en MIT y ayudó a crear un estándar global para los dispositivos RFID y otros sensores. (Cohen & Gershenfeld, 1999) mencionaron por primera vez los principios de la IoT.

(Gershenfeld, Krikorian, & Cohen, 2004), desarrollaron Internet-0 (I0), una capa física de baja velocidad diseñada para asignar direcciones IP a cualquier objeto, estableciendo un conjunto de siete principios para el diseño de dispositivos.

En 2005, la Unión Internacional de Telecomunicaciones publicó su primer informe sobre el tema "Internet de las Cosas" (ITU, 2005). El documento proporciona una visión amplia de las redes y tecnologías subyacentes, el potencial de mercado y sus factores limitantes, las implicaciones para la sociedad, privacidad, los aspectos éticos, el problema de la estandarización, las oportunidades para el mundo en desarrollo, y un resumen de las interacciones clave dentro del nuevo ecosistema durante los siguientes 15 años.

IoT fue incluida en un informe, preparado por el Concejo Nacional de Inteligencia de los EE.UU. , como una de las 6 tecnologías disruptivas con impacto potencial en los intereses de esa nación hacia el año 2025 (NIC, 2008), (Madakam, Ramaswamy, & Tripathi, 2015). Entre otras cosas, el informe advertía sobre el surgimiento de riesgos potenciales al abrirse la posibilidad de controlar, localizar y monitorizar hasta los objetos más insignificantes; sugirió entonces que la fusión de datos recolectados masivamente podría socavar la cohesión social por su incompatibilidad con las garantías de privacidad proporcionadas por la Constitución.

Por su parte, en China, el Primer Ministro Wen Jiabao reconoció a la IoT como una industria clave para ese país y lanzó planes para realizar grandes inversiones en Internet de las Cosas (Madakam et al., 2015). En 2011 se realizó el lanzamiento público del protocolo IPv6 que proporciona ~ 6,7 x 10^{17} direcciones diferentes, haciendo así a la IoT una tecnología viable.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

En octubre de 2013, se inauguró la feria "Internet of Things World Forum" (IoTWF) en Barcelona (Groteck, 2015), un evento a nivel mundial en el que participan líderes de opinión, directivos de negocio y profesionales de distintos sectores, Administraciones e instituciones académicas. CISCO Visual Networking Index predijo que más de la mitad del tráfico de Internet será generado por dispositivos que no serán PCs en 2020.

IoT Analytics estimó que a finales de 2019 había alrededor de 9.500 millones de dispositivos IoT conectados, un número substancialmente mayor que el pronosticado, siendo los mayores impulsores de este fenómeno una explosión en la utilización de dispositivos de consumo (principalmente para *Smart Home*), una mayor cantidad de conexiones celulares (IoT/M2M) que la prevista y un crecimiento particularmente fuerte en el número de conexiones de dispositivos en China (Lueth, 2019).

De acuerdo a esta misma fuente, durante 2019 se produjeron varios hitos interesantes, como el anuncio por parte de varias compañías (Eutelsat, Astrocast, Myriota, etc.) del lanzamiento de constelaciones de nanosatélites para desplegar redes *ubicuas* que servirán al mercado IoT, el lanzamiento y consolidación de varias plataformas de contenedores por parte de las grandes compañías globales (Google, Cisco, VMWare, etc.) o el fallo de seguridad del sistema de cámaras Ring de Amazon.

(Dervan, 2019) lista diez de las Conferencias sobre temática IoT de mayor influencia a nivel global. En nuestro país (CABA) se celebra IoT Day desde hace tres años. Este evento reúne a los actores que desarrollan IoT y proporciona espacios para establecer contactos y redes de trabajo.

1.1.2. Marco conceptual

Internet de los Cosas (IoT), o *Internet de los Objetos* es "la infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras" (ITU, 2005). Una definición alternativa la describe como una red de dispositivos físicos, vehículos, accesorios domésticos y otros artículos o dispositivos que tienen electrónica, software, sensores, actuadores y conectividad embebida, que les permite a dichos objetos conectarse e intercambiar datos. La definición de IoT se ha expandido desde su foco inicial Máquina-a-Máquina (M2M), para incluir dispositivos embebidos, robots, computadoras de automóviles, drones, *wearables*, etc., (ITU, 2005), (Brown, 2016b), (Brown, 2016a). (Brown, 2016a) permite imaginar el panorama diverso de la escena IoT en la actualidad.

Los objetos del ecosistema IoT pueden ser tanto objetos físicos como virtuales, identificables y con capacidad para integrarse en redes de comunicaciones. Mientras los objetos físicos se pueden conectar, detectar y accionar, los objetos virtuales sólo existen en el mundo de la información pudiéndose almacenar, procesar y 'ser accedidos' (ITU, 2005). Los objetos IoT recolectan datos y los difunden automáticamente hacia otros objetos. Año a año empresas, desarrolladores e investigadores idean e implementan nuevas aplicaciones y enlaces entre objetos antes impensados.

La mayor fortaleza del concepto de la IoT proviene del impacto que tiene y tendrá en los próximos años en la vida diaria y el comportamiento de los usuarios. En el contexto de los usuarios privados el paradigma está teniendo un protagonismo singular en escenarios tales como la domótica, *e-health*, asistencia doméstica, aprendizaje mejorado, etc. Desde la

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

perspectiva de los negocios tendrá un gran impacto en campos como la automatización y fabricación industrial, logística, gestión de negocios y procesos, transporte inteligente de personas y mercancías, etc. (ITU, 2005).

1.1.3. Marco teórico

Por tratarse de una tecnología en franco crecimiento, existen otros trabajos que abordan el estudio del estado del arte. Entre ellos es importante destacar a (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015), (Hejazi, Rajab, Cinkler, & Lengyel, 2018), y (Hu, Dhelim, Ning, & Qiu, 2017). Sin embargo, su despliegue vertiginoso requiere una revisión permanente del estado del arte de esta tecnología.

1.1.3.1 Aplicaciones

A grandes rasgos, las aplicaciones mencionadas en la bibliografía consultada se pueden agrupar en las siguientes categorías: (1) Smart Cities, (2) IoT Industrial (IIoT), (3) Entorno Inteligente, (4) Otros: Personal y Social, Futurista. La Tabla 1 muestra algunas de las aplicaciones más típicas:

Smart Cities	IoT Industrial	Entorno inteligente (hogar/oficinas/…)	Otros
Smart Grid	Agricultura Inteligente	Energía hogar	Personal y Social: *wearables* ("ponibles") deportivos, redes sociales, objetos perdidos
Transporte Inteligente y Logística	Invernaderos	Consumo agua	"Futuristas": taxis autónomos, reparto mediante vehículos autónomos, etc.
Iluminación Inteligente	Hidroponía	Ambiente (Temperatura, iluminación, O_2, CO_2)	Seguimiento de animales silvestres
Consumo Inteligente de Agua	Acuaponía	Seguridad (controles de acceso, cámaras)	
Gestión de residuos	Seguimiento de ganado	Apertura de accesos	
Monitoreo ambiental	Trazabilidad de alimentos	Riego	
Salud Inteligente	Trazabilidad de productos	Electrodomésticos	
Monitoreo de Integridad estructural de edificios			

Tabla 1. Soluciones verticales de negocio que utilizan IoT

A continuación, se describen brevemente algunas de las soluciones verticales anteriormente vistas.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

1.1.3.1.1 Smart Cities

Smart Cities es un concepto amplio que abarca varios campos de aplicación como Smart Grid, Transporte Inteligente (*Smart Transportation*), Iluminación inteligente, Gestión de residuos, Monitoreo ambiental, Salud inteligente y Salud (o Integridad) estructural de edificios. La ciudad de Padua es un ejemplo de implementación de Smart City, en la que se puede acceder a datos abiertos y soluciones TIC para aprovechar los recursos públicos de la mejor manera (Lin et al., 2017), (Villagra et al., 2018) y (Villagra A et al., 2019), (Sarker & Pe, 2019). Daremos algunos ejemplos:

Smart Grid: Estas aplicaciones buscan reemplazar a las redes de energía tradicionales apuntando a conseguir servicios más eficientes. Los escenarios contemplan la generación distribuida y la utilización de coches eléctricos. Con ello se buscan mejoras en el almacenamiento, la reducción de CO_2, y la interacción entre usuarios y proveedores de energía. Ello requiere el despliegue de medidores inteligentes conectados entre sí, el procesamiento de datos masivos y optimización de recursos. Esta aplicación plantea determinados problemas de seguridad, entre otros, el robo de medidores, la vulneración de los nodos de la infraestructura *fog* y la potencial disrupción del funcionamiento de la red (Lin et al., 2017).

Transporte Inteligente y Logística: Estas aplicaciones buscan hacer eficiente y seguro el transporte de personas y mercancías. Los escenarios contemplan un gran número de vehículos que se conectan entre sí, permitiendo percibir el tráfico y programarlo, en base a datos masivos obtenidos desde los propios vehículos. Para ello, cada vehículo dispondría de unidades de control y capacidad de comunicación vehículo-a-vehículo y vehículo-a-infraestructura. Este campo de aplicación plantea ciertos problemas de seguridad, tales como intrusión en las unidades de control, en los nodos *fog* de la infraestructura y la consecuente potencial disrupción de los servicios de transporte y riesgo para las personas (Lin et al., 2017).

Salud Inteligente: Comprende aplicaciones para el seguimiento, identificación/autenticación, recolección de datos, y ‘sensorización' de parámetros biomédicos (ITU, 2005), y monitorización de la salud.

Monitorización de Integridad Estructural: Las aplicaciones de Monitoreo de “Salud” Estructural (SHM, por sus siglas en inglés) tienen la misión de reunir información para detectar, localizar y cuantificar tempranamente vulnerabilidades tales como fatiga, degradación de condiciones de frontera, etc., con el objeto de mejorar la resistencia o fortaleza de infraestructuras criticas (CI) frente acciones terroristas, desastres naturales, etc. Las siguientes se consideran generalmente como infraestructuras críticas: Alimentación y Agricultura, Base industrial de la Defensa, Comunicaciones, Energía, Fábricas Críticas, Instalaciones Comerciales, Instalaciones del Gobierno, Instalaciones Químicas, Reactores, Materiales y Desechos Nucleares, Represas, Servicios de Emergencia, Servicios Financieros, Salud y Salud Pública, Sistemas de Distribución de Agua y Aguas Residuales, Sistemas de Transporte, Tecnologías de la Información. Así, el campo de posibilidades de aplicación es muy amplio.

1.1.3.1.2 IoT Industrial y Procesos Productivos en general

Invernaderos: Los invernaderos constituyen un sistema de cultivo industrial, ampliamente extendido. El paradigma IoT se adecua muy bien a esta aplicación debido a que las tecnologías asequibles y los bajos costos implicados en el establecimiento de la infraestructura necesaria son compatibles con el perfil del público objetivo (medianos y

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

pequeños productores, cooperativas, etc.) (González et al., 2019). (Guirado-Clavijo, Sanchez-Molina, Wang, & Bienvenido, 2018) desarrolló un modelo conceptual de base de datos para un Sistema de Información de Agricultura (AIS) al que se pueden generalizar los actuales sistemas informatizados. El modelo considera un máximo de 84 mediciones, recogiéndose datos climáticos, consignas de control, acciones de control, características del cultivo y su crecimiento, etc. La información se recolecta automáticamente desde sensores instalados en el invernadero. El proceso productivo completo comprende siete pasos: (1) venta de semillas desde el almacén hasta el agricultor; (2) entrega de las semillas desde el semillero hasta el vivero del agricultor; (3) crecimiento del cultivo y, en caso que el fruto alcance la madurez, cosecha y entrega a la cooperativa o cliente; (4) recepción de la producción de los invernaderos, clasificación y embalaje por parte de la cooperativa/cliente; (5) recolección de uno o más y transporte de los ítems vendidos; (6) recepción de los lotes en los destinos y distribución de los minoristas por parte de los mayoristas; (7) venta directa de los productos al cliente final. El modelo de datos propuesto es muy interesante ya que permite dar trazabilidad a productos específicos (o lotes) para identificar el origen de cualquier problema detectado, ya sea en el estadio de producción (3), en los posteriores (4-7) y en los previos (1-2). Este sistema permite detectar los siguientes tipos de problemas: (a) problemas en los transportes, que pueden afectar lotes de diferentes productores, pero no toda la producción, y (b) problemas con los lotes de semillas que afecten a varios productores.

Hidroponía: Desde la experiencia de este grupo de investigación, se ha encontrado que los procesos de monitorización y control de cultivos hidropónicos para entornos extremos (INTA, 2019), son dos tipos de aplicaciones que claramente se pueden llevar a cabo usando el paradigma IoT.

Acuaponía: La acuaponía es un sistema de producción sostenible que combina la acuicultura tradicional con lo hidroponía. La acuaponía de doble circulación es un proceso productivo complejo que requiere hacer recircular los componentes acuapónicos e hidropónicos en un ciclo cerrado. Los peces producen efluentes ricos en nutrientes que luego se utilizan para fertilizar las plantas. Los desperdicios de los peces se descomponen usando bacterias para formar nutrientes, que finalmente son empleados por las plantas para crecer dentro del componente hidropónico. De esta forma, (1) la remoción del nutriente mejora la calidad del agua de los peces, y además reduce el consumo de este recurso, acotando la cantidad de efluentes del sistema de producción; (2) el agua evaporada en la sección hidropónica se recupera mediante sistemas enfriadores y se reintegra a los tanques de los peces. En este contexto se requiere una infraestructura tecnológica informática muy flexible para obtener una producción costo-eficiente. (Karimanzira & Rauschenbach, 2019) proponen mejoras en las siguientes capas de la llamada *pirámide de automatización* en un sistema de producción automatizada tradicional: (a) En la Capa SCADA (Supervisory and Control Data Acquisition): Analíticas basadas en IoT y en la nube, dando carácter de tiempo real y proporcionando análisis de datos históricos como insumos de analítica predictiva y decisiones informadas; (b) En la capa ERP (Enterprise Resource Planning): IoT puede facilitar la adquisición del conocimiento profundo (*insights*) acerca de las causas primarias y sustento para realizar acciones futuras; agilidad de tiempo real, flexibilidad y predictibilidad; gran parte de los procesos se pueden automatizar; (c) En la capa MES (Manufacturing Execution Systems): IoT basado en la nube puede contribuir con la federación de datos, analíticas y aprendizaje automático.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

1.1.3.1.3 Entorno Inteligente

Se refiere a los entornos: hogar, oficina, planta, y medioambiente. Incluyen aplicaciones para hogares/oficinas confortables, y museos y gimnasios inteligentes, plantas industriales, y automatización del hogar (ITU, 2005). Por ejemplo, *Smart Home* o la Casa Inteligente, se refiere a sistemas diseñados para realizar determinadas tareas anteriormente efectuadas por seres humanos, como la gestión energética, seguridad, bienestar y comunicación. A esta disciplina se la suele llamar *domótica*. Son objetos de la domótica el control de la iluminación, de la energía, de la temperatura, monitorización de gases (como CO2 u oxígeno), seguridad, apertura de portones y persianas, riego, electrodomésticos, etc.

1.1.3.1.4 Otros

Otros ejemplos de aplicaciones identificadas en (ITU, 2005) son:

Personal y Social: Incluye redes sociales, aplicaciones para consultas históricas, Pérdidas y Robos.

Futurista: Incluye aplicaciones como taxis robot, modelo de información de ciudad, y salas de juegos mejoradas.

1.1.3.2 Arquitecturas

El paradigma IoT es tan amplio y cubre tantos aspectos que no existe una visión unificada acerca de cuál debería ser su modelo arquitectónico, o si existe un modelo que sea el más adecuado. En las siguientes subsecciones se muestran algunas de las propuestas que han surgido a lo largo de los años.

1.1.3.2.1 Modelos arquitecturales clásicos

(Gershenfeld et al., 2004), desarrollaron Internet-0 (I0), una capa física de baja velocidad diseñada para asignar direcciones IP a cualquier objeto. Los autores utilizaron un conjunto de siete principios para diseñar sus dispositivos, a saber: (1) Todo dispositivo debería utilizar el protocolo IP; (2) Todos los protocolos de comunicaciones se implementarían conjuntamente (no separadamente); (3) Dos dispositivos podrían comunicarse entre sí sin necesidad de un tercero; (4) Cada dispositivo sería responsable de mantener su propia identidad; (5) Se utilizarían “bits grandes” (equivalente a bajo *bitrate*); (6); Los datos se representarían uniformemente en cualquier medio de comunicación utilizado; (7) Se utilizarían estándares abiertos.

En general, las arquitecturas más conocidas obedecen a modelos organizados en capas. Existen diversas propuestas (Madakam et al., 2015). El modelo de referencia propuesto por ITU-T (Comunicaciones, 2012) se asemeja mucho al modelo de interconexión ISO-OSI (Madakam et al., 2015) y contempla las capas indicadas en la Tabla 2:

Capas
Capacidades de Seguridad
Capacidades de Gestión
de Apoyo y Servicio a Aplicaciones
de Red
de Dispositivo

Tabla 2. Modelo de referencia ITU-T

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

El modelo propuesto por Qian Xiaocong y Zhang Jidong (2012) se compone de tres capas: (1) la capa de percepción (sirve para reconocer y recolectar información de los objetos), (2) la capa de transporte (fibra óptica, redes de telefonía móvil y fijas, redes de radiodifusión, redes de datos IP) y (3) la capa de aplicación (que incluye numerosas aplicaciones, como, por ejemplo: protección del medioambiente, *e-health*, etc.) (Madakam et al., 2015).

(Bassi et al., 2013) dedica el capítulo 7 a explicar el Modelo de Arquitectural de Referencia IoT (IoT ARM). El IoT ARM se compone de varios submodelos IoT interconectados (Modelos de Dominio, Información, Funcional, Comunicaciones y finalmente de Confianza Digital, Seguridad y Privacidad). Estos modelos se describen mediante el lenguaje UML. El Modelo de Dominio IoT es el modelo fundamental que describe las abstracciones principales, las responsabilidades y sus relaciones. El modelo de dominio expuesto se basa en el utilizado en el IoT-A Project (Meyer, Sperner, MAgerkurth, Debortoli, & Thoma, 2012). Los autores introducen el concepto de Entidad Aumentada, como la composición de una Entidad Física y una Entidad Virtual. La Entidad Aumentada es lo que se conoce como "Cosa" o "Thing" (siendo la Entidades Virtuales abstracciones sincronizadas de las Entidades Físicas).

Dado el problema de la privacidad de los usuarios y la protección de datos, se requieren arquitecturas seguras de varios niveles. Se han propuesto arquitecturas de tres, cuatro, cinco y seis capas. La Tabla 3 muestra la arquitectura de seis capas propuesta en (Farooq, Waseem, Mazhar, Khairi, & Kamal, 2015).

	Capa	Función
6	De Negocio	Maneja las aplicaciones y servicios de IoT, generando diferentes modelos de negocio
5	De aplicación	Incluye multitud de aplicaciones como casas inteligentes, transporte inteligente, etc.
4	De *Middleware*	Procesa los datos recibidos de los sensores, e incluye tecnologías como Cloud Computing
3	De Red	Transmisión de la información utilizando diferentes tecnologías (WiFi, Bluetooth, ZigBee, GSM, etc., mediante protocolos como IPv4, IPv6, etc.)
2	De Percepción	Sensor/es del objeto que reúnen información
1	De Codificación	Identificación unívoca del objeto

Tabla 3. Modelo de 6 capas

En (Lin et al., 2017) se refieren a dos tipos de arquitecturas: la arquitectura de tres capas ya mencionada (capa de Percepción, de Red, y de Aplicación) y el modelo basado en SoA (*Service oriented Architecture*). En este enfoque, el modelo se basa en componentes o unidades funcionales denominadas "servicios". Los servicios están coordinados y se promueve la fuerte reutilización de hardware y software. El modelo basado en SoA dispone asimismo de cuatro capas, las tres capas 'clásicas' (percepción, red y aplicación) más una cuarta interpuesta entre las capas de red y de aplicación, la capa de servicios. Ésta última se responsabiliza por el descubrimiento de los servicios, la composición de los servicios, su gestión y las interfaces de los mismos.

La arquitectura de numerosos sistemas IoT de análisis de datos actuales constan de: (1) los dispositivos inteligentes (las 'cosas') que residen en la frontera de la red y recolectan datos (*wearables*, sensores de temperatura inalámbricos, monitores cardíacos, etc.; (2) la nube

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

(*cloud*), en la que se agregan y analizan datos provenientes de diversas fuentes en tiempo real, generalmente en una plataforma analítica (que reúne, procesa, almacena datos de dispositivos dispersos y tiene la capacidad de analizar y realizar acciones basadas en los datos entrantes); (3) algoritmos de la aplicación IoT, mediante los cuales el ingeniero o el analista científico de datos buscan obtener conocimiento e *insights* realizando análisis históricos de los datos. (En este escenario los datos se extraen de la plataforma hacia un entorno software de escritorio en el que el analista crea prototipos de los algoritmos que eventualmente se ejecutarán en la nube o en los mismos dispositivos.)

1.1.3.2.2 Avances recientes

A medida que el hardware de los dispositivos, el *software*, el *middleware* y los marcos de trabajo para IoT se hacen más potentes, la capacidad de procesamiento, de almacenamiento y la inteligencia han comenzado a migrar desde la nube hacia el borde de la red, es decir hacia los nodos terminales. Esto permite mejorar las latencias, el ancho de banda utilizado y otros aspectos como la *localidad*. Aunque esto de algún modo contradice la idea de que los dispositivos IoT están por definición limitados en recursos, muchos de los últimos trabajos relacionados con el paradigma IoT se enfocan en la computación *fog* y la computación *Edge* (a veces traducidos al español como "computación en la niebla" y "computación de borde", respectivamente).

La *computación fog* es un paradigma que permite adaptar los requisitos de aplicaciones de diferentes tamaños, usando múltiples capas de infraestructura computacional combinando recursos del borde de la red y de la nube. Este modelo introduce una jerarquía de la capacidad de cómputo entre los dispositivos de borde y la nube (p. ej.: nodos *fog*, *cloudlets* o micro *data centers*). La infraestructura *fog* permite el funcionamiento de soluciones con distintos requerimientos de calidad de servicio, porque las aplicaciones pueden funcionar en el nivel jerárquico que provee la capacidad adecuada de procesamiento, cumpliendo al mismo tiempo con las metas de latencia. Por otra parte, reduce el ancho de banda agregado en el camino entre la nube y el borde. (L. Bittencourt et al., 2018). Dos conceptos importantes en el ámbito de la computación *fog* son las nociones de Orquestación y Federación. En primer lugar, las funciones de Orquestación comprenden el manejo dinámico de los recursos, considerando los requisitos de las aplicaciones y las cargas de trabajo. Los recursos de la computación *fog* comprenden: sensores básicos, componentes CPU, de memoria, máquinas virtuales, funciones de red virtuales, redes, servicios de aplicaciones y microservicios. El rol de la orquestación es garantizar el funcionamiento apropiado de todos esos recursos en el marco de la seguridad y el rendimiento requerido por las aplicaciones. En segundo lugar, una Federación es un contexto de seguridad y colaboración en la que los partícipes de diferentes organizaciones y dominios administrativos pueden definir, acordar y hacer cumplir conjuntamente el descubrimiento de recursos conjuntos y la política de accesos a los mismos. (L. Bittencourt et al., 2018).

La *computación Edge* es un paradigma computacional que extiende los servicios de la nube a los dispositivos que están en el borde o frontera de la red. Comprende todas las tecnologías que permiten realizar el procesamiento y almacenamiento directamente en los dispositivos del borde, es decir, la acción ocurre cerca de los dispositivos terminales. Los nodos del borde pueden ser sensores, teléfonos inteligentes, vehículos inteligentes e incluso servidores de borde (Hu et al., 2017). Algunos autores no distinguen entre *Edge* y *Fog*; no obstante, se pueden identificar algunas diferencias en lo relativo a la cercanía a los dispositivos (*Fog* no se ubica en los dispositivos, mientras que *Edge son* los dispositivos), recursos (*Edge* es más limitado en potencia computacional y almacenamiento), etc. Por otra parte, ambos modelos

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

tienen muchas similitudes, como la arquitectura descentralizada y distribuida, la latencia reducida en comparación con la computación en la nube, el bajo costo del ancho de banda, el soporte a la movilidad, y la elevada escalabilidad (Hu et al., 2017).

(Mocnej, Seah, Pekar, & Zolotova, 2018) identificó un conjunto de cinco características deseables en toda plataforma IoT descentralizada, y propuso una arquitectura de este tipo eficiente en recursos. Las características identificadas son: (1) plataforma multi-red, que permita la comunicación con dispositivos heterogéneos ocultando las tecnologías de red subyacentes; (2) la implementación escalable e interoperable, no invasiva y lista para integrar nuevas aplicaciones reaccionando a tiempo; (3) bajo consumo: soporte de mecanismos como comunicaciones M2M dirigidas por eventos y otras técnicas de optimización de recursos; (4) gestión intuitiva de datos y dispositivos tanto centralizada como individual y automatizada; (5) presencia de inteligencia artificial (AI) en el "Edge", moviendo parte de los servicios que actualmente proporciona la nube hacia el borde (pudiendo implementarse en un gateway sin limitación de recursos). En el trabajo se propone la utilización de las métricas indicadas en la Tabla 4:

Métrica	Atributos
Calidad del Dispositivo (QoD)	Estado de la batería, precisión, *throughput*, etc.
Calidad del Servicio (QoS)	Ancho de banda, retardo, *jitter*, y pérdida de paquetes
Calidad de la Información (QoI)	Exactitud, precisión y *freshness* (frescura)
Valor de la Información (VoI)	Relevancia, integridad, *timeliness* (la cualidad de que la información sea oportuna) y *entendibilidad*

Tabla 4. Métricas de calidad propuestas por (Mocnej et al., 2018)

La arquitectura descentralizada propuesta consiste en los tres bloques funcionales indicados en la Figura 1:

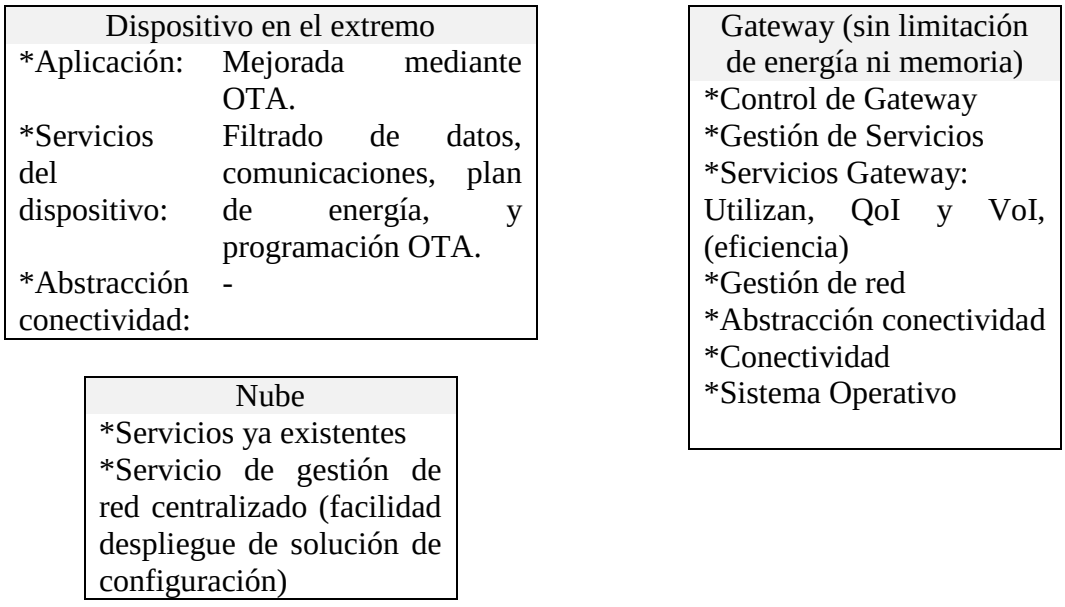

Figura 1. Arquitectura descentralizada propuesta por (Mocnej et al., 2018)

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

(L. Bittencourt et al., 2018) revisa los principales aspectos y desafíos que hacen a las tecnologías de la computación *fog* y *cloud* apropiadas para todo tipo de aplicaciones potenciadas por el paradigma IoT. Estudia las infraestructuras de procesamiento, protocolos e infraestructura para 5G, aplicaciones tales como *smart cities*, computación urbana, industria 4.0, y gestión de la complejidad de ecosistemas IoT-*fog-cloud* (servicios, asignación de recursos y optimización, consumo de energía, gestión de datos y localidad, federación de dispositivos y confianza, y modelos de negocios y servicios). Con respecto a la jerarquía, se señala que en las infraestructuras IoT-Fog-Cloud, los datos atraviesan más de un nivel del *fog* y que la decisión acerca de cómo conectarse a los distintos nodos dependen del escenario tecnológico: por ejemplo, mientras los nodos *fog* dentro de un proceso de manufactura se conectan generalmente por cable, es más probable que un nodo *fog* que sólo envía datos crudos lo haga en forma inalámbrica. Además, las conexiones del tipo inalámbrico permiten comunicar en modo *fog-fog* o *fog-cloud*, dependiendo de la infraestructura disponible.

Las tecnologías inalámbricas candidatas son 3G, 4G, 5G. En particular, las redes 5G permiten orquestar los recursos de la red para ofrecer servicios de banda ancha móvil mejorada (eMBB), comunicaciones de baja latencia ultra-fiable (URLL), y comunicaciones masivas de máquinas (mMTC). De esta forma, un operador 5G podrá 'rebanar' la red, proporcionando a cada porción los recursos necesarios para distintas necesidades en términos de latencia, fiabilidad, *throughput*, escalabilidad y apoyo a la movilidad. Cada rebanada es similar a red virtual cuyos recursos son aprovisionados para un servicio o clase de servicio, completamente aislado de otras porciones que comparten la misma infraestructura. Como resultado las redes se vuelven más flexibles, fiables, escalables y seguras. Mediante esta tecnología una red puede reconfigurar las rebanadas de recursos en cuestión de segundos para responder a necesidades inesperadas, tales como tumultos o emergencias (Aunque también permite establecer contratos a largo plazo, p. ej. con compañas eléctricas y otras *Utilities* que empleen, sensores, controles y otros dispositivos IoT. Se dispondrá entonces de la capacidad de reunir y procesar enormes cantidades de datos, originados en servicios IoT de diferente índole, encaminados a través de la infraestructura *fog*. Aunque los dispositivos *Edge* estén limitados en recursos, la combinación de las capacidades de computación de *fog* y *cloud* aligera considerablemente esas restricciones.

(Mendoza, Ordóñez, Ordóñez, & Jurado, 2017) presenta una arquitectura para soluciones basadas en microcontroladores. Describe los componentes de la arquitectura del software y su interacción, poniendo el foco en los requisitos funcionales y atributos de calidad tales como la escalabilidad, mantenibilidad y la seguridad. La arquitectura propuesta permite el desarrollo de aplicaciones, sin un dominio en particular, modulares y configurables, centrándose en el diseño y las especificaciones del Sistema. La evaluación de la arquitectura se realiza mediante el diseño de un sistema *fog computing* para un sistema de recolección de agua. Los requisitos funcionales del sistema contemplaron: (1) la captura de datos de sensores analógicos y/o digitales; (2) la normalización de los datos obtenidos mediante algoritmos estándares; (3) la capacidad de cambiar el status del sistema (ON/OFF) a voluntad; (4) la capacidad de conexión a Internet mediante las tecnologías Ethernet, WiFi, GSM y GPRS; (5) la capacidad para compartir datos a sistemas remotos mediante protocolos HTTP, REST, CoAP y MQTT; y (6) la necesidad de una interfaz de configuración (móvil o web). La arquitectura del software se basa en un patrón MVC-C (Model, View, Controller + Communications) en la que se identifican las capas indicadas en la Tabla 5:

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

Capa	Función
Capa “Interfaz”	Permite la comunicación con el mundo exterior (serial o UDP/TCP)
Capa “Controller”	Interactúa con las rutinas firmware de bajo nivel del micro controlador para acceder a los datos (sensores y actuadores), a través de la capa de abstracción del sistema.
Capa “Modelo”	Controladores de dominio (sensores/actuadores, rutinas web, de servidor y de cliente).
Capa de abstracción del sistema	Funciones de bajo nivel sobre el *kernel*, las comunicaciones, y las entradas y salidas.

Tabla 5. Modelo MVC-C

La evaluación de la arquitectura se realizó mediante el método ATAM (Architecture Tradeoff Analysis Method) que permite caracterizar varios atributos tales como el rendimiento, la modificabilidad, la disponibilidad y la seguridad).

(Sarker & Pe, 2019), propuso una arquitectura genérica para integrar las capacidades de computación Edge en aplicaciones IoT con un rendimiento mejorado usando la tecnología LoRa.

1.1.3.3 Protocolos

En este apartado se proporciona una breve descripción de los protocolos que se han desarrollado (o reutilizado) para ser utilizados en IoT. Estos protocolos presentan particularidades que los hacen eficientes para el tipo de aplicaciones típicas de este paradigma. Los protocolos que se describirán se concentran en los niveles de Capa de Aplicación (MQTT, AMQP, XMPP, CoAP y DDS), y de Capa de Red (RPL y 6LoWPAN, que realmente es un protocolo de adaptación entre capas). Otros protocolos se describen en el apartado 1.2-Tecnologías utilizadas.

La Figura 2 muestra la pila de protocolos en una estructura de capas asimilable a la del modelo OSI.

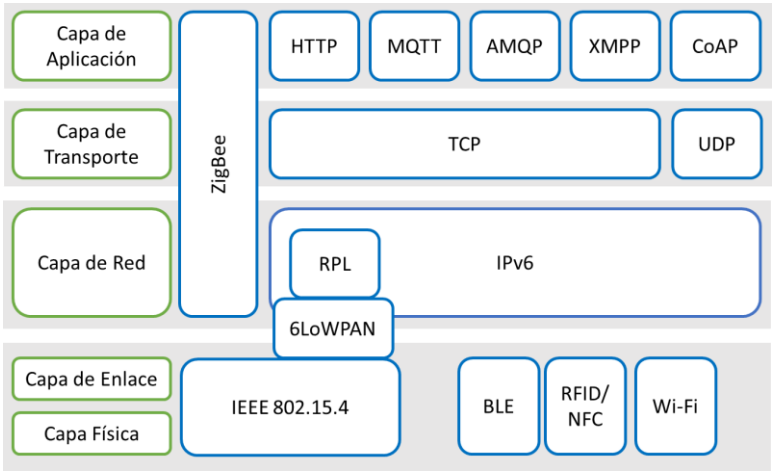

Figura 2. Pila de protocolos para IoT

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

1.1.3.3.1 Protocolos de Capa de Aplicación

Los protocolos de capa de aplicación se orientan a la comunicación proceso-a-proceso. Ejemplos típicos de la Internet clásica son HTTP, FTP, SMTP, Telnet, etc. A continuación, se describen protocolos específicos de IoT.

1.1.3.3.1.1 MQTT

Message Queue Telemetry Transport (Transporte de Telemetría en Cola de Mensajes) es un protocolo de mensajería que se utiliza para recolectar datos provenientes de sensores remotos y transmitirlos hacia los servidores usando el mecanismo de publicación y suscripción (P&S). Siendo un protocolo ligero funciona en redes con un pequeño ancho de banda y una elevada latencia. Juega un papel importante en IoT porque permite comunicar sensores y actuadores con los servidores (Lin et al., 2017). Utiliza los servicios del protocolo TCP. (Aziz, 2016) presentó un modelo formal del protocolo MQTT ver3 basado en álgebra de procesos con pasaje de mensajes, señalando las ambigüedades en la especificación original del protocolo. Realizó un análisis estático del modelo formal y sugirió una mejora en el tercer nivel de QoS del protocolo. También sugirió usar criptografía ligera para la autenticación de pequeños dispositivos y realizó una modificación simple a QoS = 2 que elimina la vulnerabilidad de mensajes del tipo *publish* duplicados. (Fysarakis et al., 2016) evaluó los protocolos DPWS, COAP y MQTT en el contexto del diseño de una aplicación que requiere varias interacciones *machine-to-machine* (M2M) concluyendo que COAP y DPWS aventajan a MQTT dado que este último solo soporta interacciones asíncronas enrutadas a través de un *broker*, lo que conduce a un modelo de comunicación con demasiadas interacciones. (Hasan & Mohammed, 2018) evaluó el protocolo MQTT (en la plataforma OMnet++, framework INET) para utilizarse en entornos industriales, observando que el *throughput* obtenido por el suscriptor, con respecto al número de sensores, se incrementa constantemente hasta los primeros 40 sensores y luego disminuye debido al gran rango de parámetros distribuidos sobre toda la red.

1.1.3.3.1.2 AMQP

El Protocolo de Colas de Mensajes Avanzado (AMQP, Advanced Message Queuing Protocol) es un protocolo de encolamiento de mensajes estándar y abierto que proporciona los siguientes servicios de mensajes: encolamiento, enrutamiento, seguridad y fiabilidad. Se puede considerar un protocolo de *middleware* orientado a mensajes. Utilizando este protocolo los clientes consiguen estabilidad en las comunicaciones con los middlewares de mensajes incluso si estos middlewares han sido codificados mediante diferentes lenguajes. AMQP implementa diferentes modos de comunicación de mensajes, a saber: almacenamiento y reenvío (S&F), publicación y suscripción (P&S), distribución de mensajes, encolamiento de mensajes, enrutamiento basado en contextos y enrutamiento punto a punto (Lin et al., 2017). Utiliza los servicios del protocolo TCP.

1.1.3.3.1.3 XMPP

El Protocolo de Mensajes y Presencia Extensible (eXtensible Messaging and Presence Protocol, XMPP) es un protocolo de mensajes instantáneos basado en XML. Hereda las características de XML, tales como la escalabilidad, capacidad de direccionamiento y seguridad. Se puede utilizar para el chateo multi partes, *streaming* de voz y de video, y telepresencia. XMPP incluye tres roles: (1) el cliente, (2) el servidor y (3) el gateway. El protocolo soporta la comunicación bidireccional entre dos de las partes de estos tres roles. El servidor puede tener la funcionalidad de la gestión del enlace y el enrutamiento de los mensajes. El gateway se utiliza para apoyar una comunicación estable entre sistemas heterogéneos. El cliente se puede conectar al servidor utilizando la pila TCP/IP y transmitir contexto basándose en el protocolo *streaming XML*. De esta forma, XMPP se puede utilizar

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

en IoT para permitir la comunicación objeto a objeto mediante mensajes de texto basados en XML. (Lin et al., 2017)

1.1.3.3.1.4 CoAP

El Protocolo de Aplicación Restringido (Constrained Applicaction Protocol, CoAP) es un protocolo de mensajes que se basa en la arquitectura REST (REpresentational State Transfer). Como la mayor parte de los dispositivos IoT están limitados en recursos (computacionales y de almacenamiento), HTTP no es útil para ellos debido a su complejidad. CoAP modifica algunas de las funciones de HTTP para satisfacer los requisitos de IoT. Se puede decir que CoAP es el protocolo de capa de aplicación en la pila de protocolos 6LoWPAN. Mediante este protocolo los dispositivos con escasos recursos consiguen, sin embargo, realizar interacciones del tipo RESTful. CoAP soporta las comunicaciones de grupo y notificaciones *push*, pero no soporta *broadcasting*. CoAP proporciona las siguientes prestaciones importantes: (1) observación de recursos, (2) transporte de recursos en bloque, (3) descubrimiento de recursos, (4) interacción con HTTP y (e) seguridad. CoAP se implementa sobre los servicios UDP (Lin et al., 2017). (Misic, Ali, & Misic, 2018) estudió diferentes arquitecturas con caché de datos (proxy), para conectar dominios IoT a la Internet usando el protocolo CoAP. El estudio apuntó a la creación de arquitecturas jerárquicas escalables y se investigaron varios problemas de diseño con respecto a la transmisión de datos, el retardo de ida y vuelta, y el consumo energético. Se investigaron tres modos de comunicación en el dominio IoT: (a) POST/GET, (b) GET multicast y (c) observación/GET. Los resultados mostraron que el proxy basando en multicast es el que exhibe el mejor rendimiento, seguido por el basado en observación/GET y finalmente en POST/GET.

1.1.3.3.1.5 DDS

El Servicio de Distribución de Datos (Distribution Service, DDS) fue desarrollado por el Object Management Group (OMG). La característica más importante de este protocolo, centrado en los datos, es que permite la comunicación eficiente en modo dispositivo-a-dispositivo. El protocolo es del tipo publicación/suscripción (P&S), sin *broker* (*brokerless*), que lo hace muy adecuado para aplicaciones de tiempo real en dispositivos IoT de recursos limitados. Otras muy interesantes características del protocolo son que: (1) admite el *multicasting*, (2) puede conseguir una elevada calidad de servicio (QoS), (3) elevada fiabilidad, (4) elevada escalabilidad. (Lin et al., 2017). El protocolo se usa con éxito en aplicaciones IoT industriales (IIoT) ("IIoT Standards | Object Management Group," n.d.).

1.1.3.3.1.6 Combinaciones de protocolos

(Fysarakis et al., 2016), plantea que la falta de inter operatividad entre las soluciones representa un obstáculo significativo para la era de la computación urbana sobre IoT. El estado actual es el de una variedad de dispositivos incompatibles y segregados, cuyas restricciones de recursos, su heterogeneidad de hardware, redes y tecnologías solo empeoran las cosas. Identificó tres protocolos estandarizados prometedores y los evaluó en el contexto del diseño de una aplicación que requiere varias interacciones *machine-to-machine* (M2M): DPWS, CoAP, y MQTT. Finalmente propuso considerar una solución que combine uno o más protocolos, delegando a cada uno la tarea para la que es más apropiado, por ejemplo: (1) CoAP podría usarse para las interacciones ligeras del tipo M2M, (2) MQTT para comunicaciones en dominios cruzados y (3) DPWS, basado en SOA, podría emplearse en interacciones *machine-to-human* (M2H).

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

1.1.3.3.2 Protocolos de Capa de Red

La capa de red es el nivel que provee conectividad y selección de ruta entre dos sistemas que pueden estar en redes geográfica y tecnológicamente distintas. Protocolos típicos en la Internet clásica son IP, IPX y RIP. A continuación, se describen protocolos específicos de IoT.

1.1.3.3.2.1 RPL

RPL es el protocolo de enrutamiento para dispositivos de baja potencia y redes con pérdidas (LLN) desarrollado por IETF y estandarizado en la recomendación RFC6550 en 2012 (Kelsey, 2015). IETF desarrolló el protocolo 6LoWPAN (IPv6 para redes de área personal inalámbricas con dispositivos de baja potencia) como capa de adaptación para permitir a los nodos sensores implementar la pila de protocolos IP y ser así accesibles por otros dispositivos de la red. RPL es un protocolo basado en vectores de distancia que opera sobre el protocolo IEEE 802.15.4 (capa física y de enlace del modelo OSI) con la ayuda de la capa de adaptación 6LoWPAN. El protocolo permite crear, en forma dinámica, una topología de árbol multi saltos (DAG o grafo acíclico dirigido) en la que cada nodo de la red envía datos a su nodo padre hasta que los mensajes alcanzan la raíz o nodo gateway. De la misma forma el nodo raíz envía mensajes *unicast* a nodos específicos de la red auto conformada. RPL proporciona un marco de comunicaciones bidireccional, robusto, fiable, flexible y escalable. Las características principales de RPL son la jerarquía eficiente, la utilización de temporizadores para reducir el uso de mensajes de control, y la utilización de funciones objetivo que alojan las métricas con las que los nodos pueden seleccionar el mejor padre (Kharrufa, Al-Kashoash, & Kemp, 2019). Por otra parte, (Iova, Picco, Istomin, & Kiraly, 2016) analizó el grado de satisfacción de las expectativas del protocolo RPL años después del establecimiento del estándar (2012) identificando algunos problemas correspondientes a aspectos incluidos en los requerimientos originales, referidos fundamentalmente a baja confiabilidad y robustez.

1.1.3.3.2.2 6LoWPAN

El protocolo 6LoWPAN se diseñó para combinar IPv6 con las redes LoPWAN (Low Power Wireless Personal Area Network), es decir para dispositivos de bajo costo conectados por medios inalámbricos. Sus características lo hacen ideal para redes IoT compuestas de muchos dispositivos. Presenta un gran número de ventajas frente a otros protocolos, tales como: (1) el tamaño reducido de los paquetes, (2) el pequeño ancho de banda requerido, (3) el bajo consumo requerido, (4) la elevada conectividad, (5) la compatibilidad con arquitecturas heredadas y (6) la auto organización *ad-hoc*. (Lin et al., 2017). Sus funcionalidades se mapean entre las Capas Física y de Enlace de Datos, y la Capa de Red del modelo OSI.

1.2 Tecnologías utilizadas

A continuación, se describen algunas de las tecnologías de mayor relevancia comercial ordenadas según la arquitectura más ‘clásica’, la de tres capas. También se proporciona un apartado dedicado al *middleware*.

1.2.1. De la Capa Perceptiva

Identificación por Radio Frecuencia (RFID): Es la primera tecnología de sensores que se asoció al paradigma IoT. Consiste de un sistema que proporciona la identidad de un objeto o persona en forma inalámbrica. Se compone de una etiqueta, un lector, una antena, un controlador de acceso, software y un servidor (Madakam et al., 2015) . La etiqueta se une al objeto requerido y le proporciona su identidad. El lector obtiene la identificación del objeto haciendo la consulta a la etiqueta (Lin et al., 2017). La tecnología RFID se utiliza en

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

aplicaciones como distribución, rastreo de mercancías y personas, monitorización de pacientes y aplicaciones militares (Madakam et al., 2015). Las ventajas de RFID son: escaneo rápido, durabilidad, reusabilidad, almacenamiento masivo, lectura sin contacto, seguridad, pequeño tamaño, bajo costo, etc. (Lin et al., 2017).

Códigos de Barras: permite codificar letras y números utilizando una combinación de barras y espacios de diversa longitud. Para leer el código se utiliza un lector de código de barras que hace un barrido con un haz laser. Los códigos QR (Quick Response) son códigos de barras matriciales que comenzaron a usarse en la industria automotriz japonesa y posteriormente se hicieron populares en otros ámbitos por su velocidad de lectura y capacidad de almacenamiento (Madakam et al., 2015). Los códigos de barra lineales se denominan 1-D, mientras que los matriciales se denominan 2-D (Lin et al., 2017).

Redes de Sensores inalámbricos (WSN): Constituyen una tipología de redes, formadas por dispositivos autónomos distribuidos geográficamente que utilizan sensores para monitorizar condiciones ambientales en forma cooperativa (p. ej.: temperatura, polución ambiental, presión). Se conforman mediante cientos o miles de 'motas'(*motes*) que se transfieren los datos de una en una, directamente. Se utilizan en áreas como seguridad interior, defensa, salud, monitorización de agricultura, detección de incendios forestales, de inundaciones, etc. (Madakam et al., 2015). Estas redes frecuentemente son auto-organizadas y forman estructuras altamente robustas. Las redes WSN presentan numerosas ventajas: escalabilidad, reconfiguración dinámica, fiabilidad, pequeño tamaño, bajo costo, bajo consumo, etc. (Lin et al., 2017).

Actuadores: Son dispositivos que convierten la energía en movimiento, lineal, rotatorio u oscilatorio. Los actuadores son indispensables en el control industrial; generalmente son de los siguientes tres tipos: eléctricos, hidráulicos, y neumáticos. Los actuadores eléctricos (p. ej. motores *stepper* y válvulas solenoides) son, de lejos, los tipos más utilizados en IoT (Madakam et al., 2015).

1.2.2. De la Capa "de Red"

Las siguientes tecnologías se refieren a la "capa de red" tal y como se entiende en el apartado "Arquitecturas", y en general no necesariamente a la capa de red del modelo OSI de ISO.

LoRaWAN: LoRa (Long Range) es una tecnología de comunicaciones inalámbricas de capa física propietaria que opera en espectro sin licencia ISM. El resto de la pila de protocolos, conocida como LoRaWAN, es abierta, y su desarrollo lo lleva a cabo la LoRa Alliance (IBM, Actility, Semtech, Microchip, etc.). LoRa se caracteriza por el bajo bitrate (0.3 a 50 kbps), que le permite conseguir alcances de hasta 15 km en entorno suburbano. Las ventajas de LoRaWAN son: capacidad de negociar alcance por tasa de datos, y cubrir grandes distancias con menor cantidad de *gateways* que con las redes celulares (Houimli et al., 2016). (Sarker & Pe, 2019), explora oportunidades de mejoras y algunas consideraciones especiales, haciendo hincapié en el colapso de los sistemas LoRA al crecer el número de nodos.

SigFox: es una tecnología de comunicaciones inalámbricas propietaria de banda ultra estrecha (y tasa de señalización, unas 100-1000 veces menor que las de otras tecnologías IoT). Brinda una solución única de conectividad celular a nivel global, desde los dispositivos de los clientes hasta sus aplicaciones de software. Los dispositivos SigFox están diseñados para escenarios tales como agricultura y medio ambiente, industria automotriz, edificios, y electrónica de consumo. Las ventajas de SigFox son: comunicaciones de largo alcance (hasta

10 km en entorno urbano y 30-35 km en entorno rural), manejo de millones de dispositivos con un único *gateway* (Mehboob, Zaib, & Usama, 2016). SigFox implementa toda la pila del protocolo de comunicaciones, que se mapea con las capas del modelo OSI de la forma indicada en la Tabla 6:

Capa	SigFox	ISO-OSI
4	Application Layer	Aplicación Presentación Sesión
3	Frame Layer	Transporte Red
2	MAC Layer	Enlace de Datos
1	PHY Layer	Física

Tabla 6. Mapeo de capas SigFox en OSI

Comunicación por Campo Cercano (NFC): Es una tecnología inalámbrica de ultra corto alcance (típicamente 4cm como máximo) que se utiliza para hacer transacciones e intercambios de contenido digital con un simple toque entre dos dispositivos (p. ej.: teléfonos móviles), (Madakam et al., 2015). Se mapea sobre la Capa Física y de Enlace de Datos OSI.

Bluetooth: (Madakam et al., 2015) Es una tecnología inalámbrica de corto alcance (10-100m) y ancho de banda moderado (1 Mbps) basada en el estándar IEEE 802.15.1 y apoyada por más de 1000 compañías de primer nivel. Se usa extensivamente para intercambiar datos entre notebooks, *tablets*, cámaras e impresoras. Se mapea sobre la Capa Física y de Enlace de Datos OSI. Blootooth LE (Low Energy) se está posicionando como el estándar clave para dar soporte a la nueva ola de dispositivos "ponibles" (*wearable devices*) que llegan incesantemente al mercado.

IEEE 802.15.4: es un protocolo de capa física y capa de acceso al medio MAC, basado en el modelo OSI, para redes de área personal (WPANs) de bajo consumo, bajo costo y baja velocidad. Trabaja en las bandas de 868/915M y 2.4 GHz con tasas binarias de hasta 250 Kb/s (Lin et al., 2017). Se mapea sobre la Capa Física y de Enlace de Datos OSI.

Wireless Fidelity (Wi-Fi): la tecnología inalámbrica Wi-Fi se ha impuesto al punto de transformarse en una *commodity* en hogares, oficinas, edificios públicos de todo tipo e incluso en ciudades enteras. Wi-Fi encarna el paradigma de la ubicuidad imaginado en (Weiser, 1991). Actualmente, casi todo *gadget* dispone de recursos radio conformes a estándares como IEEE 802.11a/b/g/n. (Madakam et al., 2015). Se mapea sobre la Capa Física y de Enlace de Datos OSI.

6LoWPAN: La sigla LoWPAN designa a las redes personales inalámbricas de baja potencia (Low Power Wireless Personal Area Networks). 6LoWPAN implementa, como mejora, el protocolo IPv6. Los paquetes IPv6 se pueden transmitir por ejemplo sobre redes IEEE 802.15.4. Presentan ventajas como elevada conectividad, compatibilidad con arquitecturas heredadas, bajo consumo, auto-organización ad-hoc, etc. (Lin et al., 2017). Sus funcionalidades se mapean entre las Capas Física y de Enlace de Datos, y la Capa de Red del modelo OSI.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

Internet Protocol v6 (IPv6): Creado en los años ’70, el protocolo de nivel de red IP es indiscutiblemente el componente indispensable sobre el que se sustenta IoT. En su versión IPv6 posibilita el direccionamiento de hasta 2^{128} dispositivos diferentes (Madakam et al., 2015). Se mapea sobre la Capa de Red OSI.

ZigBee: Creada por ZigBee Alliance en 2001 y basada en el estándar IEEE 802.15.4, es una tecnología de red inalámbrica de corto alcance (100 m) y bajo consumo que permite la configuración de redes en topologías estrella, árbol de *clusters* y malla. Se utiliza extensivamente en automatización del hogar, agricultura, controles industriales, sistemas de energía, salud, etc. (Madakam et al., 2015). Las ventajas de las redes ZigBee incluyen el bajo consumo, bajo costo, baja complejidad, fiabilidad y seguridad (Lin et al., 2017). ZigBee implementa funcionalidades de las Capas de Red, Transporte y Aplicación del modelo OSI.

Z-Wave: es una tecnología de comunicaciones inalámbricas propietaria de corto alcance (30-100m) en banda ISM. Promovida por Z-Wave Alliance, está diseñada para transmitir mensajes cortos desde una unidad de control hacia los dispositivos esclavos (Houimli et al., 2016) Sus ventajas son el bajo costo, el bajo consumo y la elevada fiabilidad. Todos los esclavos tienen capacidad de encaminamiento y soportan el encaminamiento dinámico (Lin et al., 2017). Esta tecnología, soportada por más de 300 fabricantes, se utiliza en dispositivos electrónicos del hogar, sistemas de entretenimiento, luces, termostatos, etc. (Houimli et al., 2016).

1.2.3. De la Capa de Servicios

Interfaces: Se requieren para asegurar el intercambio seguro de información entre dispositivos y aplicaciones, así como la gestión, la conexión, desconexión, comunicación y operación de los dispositivos. Se han desarrollado diferentes tecnologías de interfaz, efectivas, seguras y escalables, pero aún presentan considerables desafíos que deberán ser investigados (Lin et al., 2017).

Gestión de los Servicios: Permite descubrir los dispositivos y aplicaciones y programar servicios eficientes y fiables para satisfacer las solicitudes. Se puede ver un servicio como un comportamiento o una asociación de comportamientos necesarios para alcanzar un objetivo específico. En IoT algunos requisitos se pueden satisfacer mediante un único servicio, mientras que en otros se requiere la integración de varios servicios (Lin et al., 2017).

Gestión de Recursos y Compartición: consiste en compartir parte de los recursos de la red entre diversas aplicaciones para incrementar su utilización y reducir los costos. Asegurar que la información solicitada por diferentes aplicaciones se entregue a tiempo implica un desafío importante para IoT (Lin et al., 2017).

1.2.4. Middleware

El *middleware* es aquel software o servicio que proporciona a las aplicaciones una visión abstracta de las tecnologías IoT, permitiendo a los desarrolladores enfocarse en el desarrollo de aplicaciones sin considerar problemas de compatibilidad entre éstas y la infraestructura. (Lin et al., 2017) separa al *middleware* reconociendo las siguientes categorías: (1) middleware orientado a mensajes; (2) basado en web semántica; (3) de servicios basados en localización, y de vigilancia; (4) de comunicaciones; y (5) penetrante (*pervasive middleware*). Señala que la integración del middleware en IoT requiere resolver problemas de inter operatividad, escalabilidad, abstracción, interacción espontánea, infraestructura y multiplicidad.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

(Farahzadi, Shams, Rezazadeh, & Farahbakhsh, 2018) estudió diferentes tecnologías de middleware para Cloud of Things (CoT) desde tres aspectos diferentes: (1) desde el punto de vista de las principales características que debe poseer el middleware, (2) del estudio de varias tecnologías basadas en diferentes arquitecturas, dominio de servicios y aplicación, y (3) desde los desafíos y problemas del middleware. Como atributos del middleware, establece los siguientes: la flexibilidad; la transparencia de plataforma (de modo que el middleware pueda funcionar en varias plataformas, sin el conocimiento de los clientes y servidores; transparencia de red (los usuarios no son conscientes acerca de si los recursos son locales o remotos); la gestión de contexto, la inter operatividad, la reusabilidad, la portabilidad de plataforma, la mantenibilidad, la capacidad de descubrimiento de recursos, la gestión de la confianza, la adaptabilidad, la seguridad y privacidad y la convergencia de la conectividad. En este trabajo se estudiaron 20 middlwares, a saber: C-MOSDEN; Xively; ThingsWorx; Carriots, CHOReOS; Rimware; DropLock; ABC&S; OpenIoT; Aura; Capnet; Carisma; LinkSmart; GSN; COPAL; Gaia; UPnP; CoMiHoC; SOCAM; Virtus. De la comparación se extrajo una clasificación de las arquitecturas y características de los middlewares: (a) basados en componentes, (b) distribuidos, (c) basados en servicios; (d) basados en nodos, (e) centralizados, y (f) tipo cliente-servidor.

También se extrajo una división por el dominio de los servicios ofrecidos: (a) intercambio de información y almacenamiento (permite a los usuarios pasar las solicitudes al middleware para intercambiar con otros nodos o grabar la información en bases de datos); (b) middleware de gestión de datos y analíticas; (c) middleware de objetos (conocido como objeto-solicitud-broker); y (d) middleware de comunicación (sirve como base para otros dominios).

Como problemas a resolver menciona: (a) la necesidad de aplicar mecanismos para medir situaciones inesperadas en tiempo real y proporcionar servicios de cloud de acuerdo a la importancia de las solicitudes (b) la implementación apropiada del descubrimiento de recursos; (c) la seguridad de los usuarios y mejora de privacidad; (d) el soporte a varios protocolos de interface para el dominio *e-health* en lo que hace a posibles efectos adversos de las señales de comunicaciones dentro de cuerpo humano; (e) la necesidad de un middleware CoT ligero para dispositivos con recursos ultra restringidos; (f) establecer el lugar óptimo para hacer análisis en computación fog (¿hasta qué punto se puede llevar la tarea del análisis de datos entre la nube y el fog?); (g) la provisión de calidad de servicio; y (h) la necesidad de estandarización.

(Gaamel, Sheltami, Al-Roubaiey, & Shakshuki, 2017), investigó y evaluó tres middlewares sin bróker basados en DDS, en el contexto de redes inalámbricas de sensores (WSN) y redes inalámbricas de sensores y actuadores (WSAN). Para la comparación utilizó el simulador TOSSIM de TinyDDS. Los middlewares estudiados son: (1) DefTDDS (versión original de TinyDDS), (2) BLTDDS (Broker-Less TinyDDS), y (3) HyTDDS (Hybrid TinyDDS). Para comparar, varió diferentes parámetros tales como carga de tráfico y requisitos de entrega. Finalmente hizo recomendaciones aplicables a la utilización de cada implementación, concluyendo que, de acuerdo a los parámetros utilizados, BLTDDS es la mejor elección para aplicaciones de tiempo real, y que tanto BLTDDS como HyTDDS son apropiados para aplicaciones de tráfico elevado. Por otra parte, en entornos en los que la batería pueda constituir un problema recomienda utilizar HyTDDS en aplicaciones con tráfico elevado, y BLTDDS en aplicaciones de tráfico medio y bajo.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

1.3 Problemas abiertos y oportunidades de estudio

A continuación, se proporciona una lista de problemas pendientes de resolución que comportan oportunidades para el estudio, investigación y desarrollo:

1.3.1. Redes e Infraestructura

Escalabilidad: IoT demanda nuevas funciones y métodos para conseguir operar eficientemente tanto a pequeña como a gran escala, dado que trabaja en un entorno completamente abierto (Kamal, Mohammed, Sayed, & Ahmed, 2017).

Autoorganización: Los objetos IoT requieren establecer conexiones, organizarse y configurarse espontáneamente para adaptarse a sus entornos particulares, a diferencia de las computadoras personales (Kamal et al., 2017).

Descubrimiento Automático: Se requieren servicios apropiados para identificar automáticamente a los objetos IoT (Kamal et al., 2017).

Tolerancia a fallos: Dada la naturaleza dinámica y frecuentemente móvil de la IoT se requerirán niveles de redundancia en varios niveles y la capacidad de adaptación ante condiciones cambiantes (Kamal et al., 2017).

Comunicaciones inalámbricas: Los estándares WPAN como ZigBee están aún en desarrollo. Estos sistemas de comunicaciones son mucho más apropiados que GSM, UMTS, Wi-Fi y Bluetooth desde un punto de vista de consumo y economía del espectro radioeléctrico (Kamal et al., 2017).

Nombres de objetos: Se requieren Servidores de Nombres para mapear referencias a una descripción de un objeto específico y el identificador relacionado, y viceversa (Atzori, Iera, & Morabito, 2010).

Protocolos de transporte: Los mecanismos de establecimiento y control de congestión de los protocolos de transporte ‘clásicos’ son inútiles en los escenarios IoT, y además requieren excesivo *buffering* (Atzori et al., 2010).

Caracterización del tráfico y apoyo a: Los patrones de tráfico generados en escenarios IoT diferirán significativamente de los observados en la Internet, por lo que se deberán crear nuevos requisitos y esquemas de apoyo a la calidad de servicio (Atzori et al., 2010).

1.3.2. Estandarización

Estandarización e interoperabilidad: (Atzori et al., 2010) hacía notar que a pesar de todos los esfuerzos, aún no existe un marco de trabajo exhaustivo para la estandarización de IoT. Se requieren estándares comunes para facilitar la comunicación y cooperación entre objetos con diferentes capacidades de comunicación, disponibilidad de energía, requisitos de ancho de banda, y que manejan informaciones diferentes (Kamal et al., 2017). En la aplicación del concepto de federación en el *fog* y entornos IoT, (Bittencourt et al., 2018) indica que es necesario crear gestores de federación en escala, estandarizados para escenarios heterogéneos. En el campo de computación sin servidores, indica que la heterogeneidad de la infraestructura IoT-Fog-Cloud dificulta el despliegue de microservicios.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

Apoyo a la movilidad: (Atzori et al., 2010) reportaba la ausencia de propuestas para el apoyo a movilidad, en el que la escalabilidad y la adaptabilidad a tecnologías heterogéneas son cruciales. En referencia a la computación *fog* para IoT (Bittencourt et al., 2018) indicó la necesidad de crear mecanismos de gestión eficientes para redes cada vez más complejas y heterogéneas, particularmente LoRAWAN, SigFox y NB-IoT.

1.3.3. Modelado

El modelado acompaña cada una de las actividades del ciclo de vida de desarrollo de un producto. En la bibliografía se hallan referencias a: Lenguajes de modelado (Eterovic, Kaljic, Donko, Salihbegovic, & Ribic, 2015), Ingeniería de sistemas basada en modelos (Papke, 2017), y Especificación, análisis y verificación mediante métodos formales (Houimli, Kahloul, & Benaoun, 2017), (Latif, Afzaal, & Zafar, 2017), (Afzaal & Zafar, 2017), (Robles-Ramirez, Escamilla-Ambrosio, & Tryfonas, 2017).

(Robles-Ramirez et al., 2017) menciona las siguientes extensiones del lenguaje UML específicas para el modelado de IoT: IoT-A, SysML, UML4IoT, "IBM approach", y ThingML. No obstante, estas extensiones no dan soporte a la Seguridad, y por lo tanto propone una nueva extensión denominada IoTSec, que: es específica para IoT, modela problemas de seguridad de los sistemas, es una extensión visual de UML, y modela requisitos de seguridad.

(Eterovic et al., 2015) aborda el problema de desarrollar un lenguaje de modelado visual, basado en UML, suficientemente potente para el analista y al mismo tiempo cercano al usuario final, quien frecuentemente no posee formación técnica.

En (Papke, 2017) se utiliza la ingeniería de sistemas basada en modelos y marcos de trabajo de arquitectura empresarial para modelar y describir una "arquitectura ágil de sistemas" con el objeto de diseñar sistemas de seguridad. (Houimli et al., 2017) utiliza un autómata temporizado para el modelado formal del protocolo MQTT (*Message Queue Telemetry Transport*) y verificación del modelo estadístico utilizando una herramienta informática para evaluar su rendimiento.

En (Afzaal & Zafar, 2017) se modela un sistema de protección de fronteras basado en IoT (utilizando grafos, casos de uso y diagramas de secuencia) y a continuación se emplean métodos formales para especificar y analizar el sistema mediante el Lenguaje de Especificación Vienna Development Method (VDM-SL).

En (Latif et al., 2017) los autores modelan un sistema de alcantarillado para una ciudad inteligente utilizando teoría de grafos. El modelo se transforma luego en una representación formal utilizando el Lenguaje de Especificación Vienna Development Method (VDM-SL) y con la herramienta VDM-SL se verifica la corrección del mismo.

1.3.4. Software

Software complejo: Dado que los objetos IoT deben funcionar con mínimos recursos, es probable que se requiera una mayor 'infraestructura' software en las redes y servidores para darles apoyo (Kamal et al., 2017). (Bittencourt et al., 2018) señala que, en el tema de asignación de recursos y optimización en la asignación de los mismos, la naturaleza dinámica de los sistemas y su heterogeneidad requieren estrategias de *asignación de recursos multicriterio*. En referencia al consumo energético indica que se debería examinar en detalle la importancia relativa de los diferentes tipos de datos y si todos ellos se requieren al mismo

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

tiempo; el objetivo sería encontrar una solución óptima en el sentido de Pareto por medio de la asociación de estrategias de gestión que incluyan el correspondiente costo de consumo energético.

Volumen de datos: Algunos casos de uso de la IoT incluyen el fenómeno de *big data*: en estos escenarios se requiere reunir enormes cantidades de datos provenientes de redes de sensores, de logística, etc., y se requieren nuevos mecanismos operativos, así como tecnología de almacenamiento, procesamiento y gestión (Kamal et al., 2017).

1.3.5. Ciclo de vida de desarrollo

En la bibliografía se encuentran referencias a 1. Ingeniería de Sistemas basada en modelos (MBSE) (Mazzini, Favaro, & Baracchi, 2015) (Papke, 2017), y 2. Empleo de ciclos de vida iterativos e incrementales (Redmond & Zarli, 2018), (Mazzini et al., 2015). Los autores de (Mazzini et al., 2015) presentan "CHESS", una metodología de ingeniería de sistemas basada en modelos que se adapta a la implementación de sistemas y componentes IoT. La metodología proporciona mecanismos de preservación de propiedades no-funcionales tales como el tiempo real, la seguridad (de las personas), la seguridad y el rendimiento, y permite acometer: el modelado, el desarrollo, el análisis, la verificación, la operación y la gestión y monitorización de aplicaciones inteligentes heterogéneas de misión crítica en despliegues distribuidos y escalables de componentes IoT (concretamente los servicios de distribución de datos para Sistemas de Transporte Inteligentes).

En (L. F. Bittencourt et al., 2017) y (Papke, 2017) se utiliza la ingeniería de sistemas basada en modelos y marcos de trabajo de arquitectura empresarial (EAF) para diseñar sistemas de seguridad. En (Redmond & Zarli, 2018) se evalúa la problemática asociada al desarrollo de soluciones IoT para "entornos urbanos sustentables" empleando prácticas ágiles y se presenta el diseño de arquitecturas de sistemas automatizados distribuidos desde la perspectiva de grupos de trabajo auto-organizados.

1.3.6. Seguridad y Privacidad

Se requiere tratar aspectos conocidos de la Seguridad en la Internet (confidencialidad, autenticación, integridad, etc.) y otros tales como impedir que los objetos involucrados en transacciones de negocios sean vulnerables a personas malintencionadas (Kamal et al., 2017).

Confidencialidad: la confidencialidad permite asegurar que los datos estarán disponibles solamente para los usuarios autorizados y no pueden ser interferidos ni 'pinchados' por usuarios no autorizados. Para conseguir un elevado grado de confidencialidad se requerirá desarrollar técnicas mejoradas, incluyendo mecanismos de gestión de claves (Lin et al., 2017). El acceso no autorizado a etiquetas RFID que contengan datos de identificación es un problema importante en IoT. Los datos no sólo pueden ser leídos, sino que pueden modificarse o dañarse. Se han reportado amenazas tales como Virus RFID, Ataques de Canal Lateral, Ataques con teléfonos móviles, etc. (Farooq et al., 2015).

Identificación y Autenticación: La identificación asegura que tanto dispositivos como aplicaciones no autorizados no puedan conectarse a IoT. La autenticación asegura que los datos entregados en las redes son legítimos y los dispositivos y aplicaciones que los solicitan también lo son. Dado el enorme número de dispositivos IoT será crucial diseñar mecanismos de autenticación eficientes (Lin et al., 2017). (Atzori et al., 2010) reconocía la dificultad de los procesos de autenticación (que requieren infraestructuras específicas, no existentes en los escenarios IoT) y para empeorar las cosas, los objetos están restringidos en recursos. Esta

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

problemática propicia los ataques del tipo *man-in-the-middle.* En este tipo de ataque el atacante altera o intercepta los mensajes entre dos partes que se comunican (Farooq et al., 2015). Allí también se menciona un tipo de ataque a sensor denominado "ataque Sybil", en el que un nodo se atribuye múltiples identidades ganando gran influencia. En referencia a los modelos de confianza para *fog computing* y entornos IoT (Bittencourt et al., 2018) hace notar que la criptografía debería ser más ligera cuanto más cerca se encuentre del dispositivo terminal.

Integridad de los datos: La integridad asegura que los datos no puedan ser alterados en la red durante su entrega, proporcionando así datos exactos a los usuarios. Para conseguir niveles aceptables de integridad se requerirán mecanismos mejorados de securización de datos (esquemas de filtrados de datos falsos, etc.) (Lin et al., 2017). En (Farooq et al., 2015) se menciona un tipo de ataque a nodo sensor en el que los que el atacante extrae y altera los datos del nodo para convertirlo en un nodo controlado. En (Farooq et al., 2015) también se mencionan dos formas de ataque del tipo 'abuso de computación en cloud': (1) *Malicious Insider*: una persona interna accede y manipula la información del usuario. (2) Una persona malintencionada obtiene acceso no autorizado a la red y modifica o borra los datos. (Atzori et al., 2010) advertía que las longitudes de contraseña soportadas por las tecnologías IoT son, en la mayor parte de los casos, excesivamente cortas para proporcionar niveles de protección adecuados. (Bittencourt et al., 2018) indica que será primordial mejorar la seguridad para preservar la integridad de los sistemas IoT Industriales (IIoT).

Privacidad: La privacidad es el atributo que asegura que los datos sólo pueden ser controlados por su correspondiente usuario, y que ningún otro usuario puede acceder a ellos y procesarlos. La privacidad es uno de los principios importantes en IoT, dado el enorme número de dispositivos, servicios y personas que utilizan la red. (Lin et al., 2017). (Atzori et al., 2010) indicaba que con las técnicas disponibles resulta imposible controlar la difusión de información privada de las personas en el entorno IoT. En (Farooq et al., 2015) se menciona una forma de ataque del tipo 'abuso de computación en cloud' en el que el atacante sube software malicioso a un servidor para obtener acceso a otros dispositivos conectados.

Disponibilidad de datos: La disponibilidad de los datos asegura que los datos y dispositivos estarán disponibles para los usuarios y servicios autorizados cada vez que se soliciten. En IoT los servicios se solicitan generalmente en tiempo real; por ello la disponibilidad es un principio importante de la seguridad. La amenaza más común a la disponibilidad de datos la constituye los ataques de denegación de acceso (DoS). (Farooq et al., 2015) describe dos tipos de ataques a sensores: 1. Perturbación: obstruye la red interfiriendo con las frecuencias utilizadas por el sensor; 2. Inundación: se crea una enorme cantidad de tráfico que agota la memoria de los procesadores. Por todo ello, se deberán estudiar y aplicar nuevas técnicas mejoradas tales como protocolos seguros y de encaminamiento eficiente (Lin et al., 2017).

Confianza Digital: La confianza digital asegura que los objetivos de seguridad y privacidad son alcanzables durante la interacción de distintos objetos, diferentes capas IoT y diferentes aplicaciones. Cuando existe confianza digital, la seguridad y la privacidad pueden hacerse cumplir. Se requerirá diseñar sistemas de gestión de confianza digital para implementar los objetivos considerados (Lin et al., 2017).

Olvido Digital: La información personal recolectada por IoT puede retenerse indefinidamente y recuperada fácilmente mediante técnicas de *data mining* (Atzori et al., 2010), lo que comporta riesgos.

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

1.3.7. Modelos de Negocio y de Servicios

(Bittencourt et al., 2018) plantea interrogantes sobre cómo ofrecer, monitorizar y facturar servicios IoT mediante servicios de computación *fog* y *cloud* al existir diferentes *players* en distintos niveles.

1.4 Marco legal

La irrupción de la tecnología IoT en combinación con la Big Data y la Inteligencia Artificial comportan riesgos para la seguridad y la privacidad de las personas. Estas tecnologías pueden emplearse para usos no previstos, como la obtención no consentida de información, la creación de perfiles de diversa índole, la monitorización de la conducta de los usuarios (*profiling*), la toma de decisiones automatizada y finalmente, la manipulación individual y social.

En general, actualmente las políticas y procedimientos para la búsqueda de vulnerabilidades se apoyan en la Norma ISO 29147 *Information technology- Security techniques- Vulnerability disclosure*. Sin embargo, los problemas surgidos tras la irrupción de escenarios tecnológicos en los que se combinan la BigData y la Inteligencia Artificial (como motores de análisis masivos de datos e información en tiempo real) y la IoT (como proveedora masiva de información) plantean problemas que pueden requerir normativas y legislación novedosas.

Las cuestiones de seguridad a las que leyes y normativas debería hacer frente son (1) la posibilidad de ataques a dispositivos aprovechando vulnerabilidades, especialmente en espacios privados, (2) el acceso a información potencialmente sensible acerca de los usuarios, y (3) la recopilación, análisis y actuación maliciosa sobre datos dentro de los espacios privados.

En relación a estos temas es oportuno señalar que (a) en general los dispositivos no obligan a los usuarios a cambiar sus contraseñas por defecto, (b) que generalmente los recursos limitados de los dispositivos dificultan la creación de parches informáticos, (c) que los dispositivos pueden reprogramarse para usos no previstos, (d) que los dispositivos utilizan componentes comunes, y una vez conocida una vulnerabilidad en un componente, ésta se puede explotar maliciosamente en diferentes dispositivos. La UE es estricta en lo que hace a seguridad. Por ejemplo, se requiere la realización de evaluaciones, certificaciones y uso de estándares, a las organizaciones que traten datos personales en dispositivos IoT, así como proporcionar garantías cuando se sirvan de proveedores de servicios externos. Desde el Parlamento Europeo también se ha impulsado el establecimiento de incentivos regulatorios para las empresas que incorporen seguridad y privacidad "desde el diseño" (*by design*) por medio del Reglamento General de Protección de Datos. (Salazar & Silvestre, 2014).

Además, los problemas de privacidad planteados por la adopción de dispositivos IoT son: (1) la cantidad de información personal que se puede inferir de los sensores al disponerse de los perfiles de usuarios y datos de otras fuentes (personalidad, demografía, factores de salud, propensión a ciertas enfermedades), (2) la dificultad para que las personas puedan desenvolverse en forma anónima, (3) la falta de herramientas accesibles, visibles y eficaces para que el usuario pueda retirar, en cualquier momento, el consentimiento a la totalidad o parte de datos procesados por los sistemas. El aspecto de la privacidad es particularmente sensible en el ámbito de la UE. Estos países cuentan con un marco legal que incluye el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos personales (1981) y la Carta de Derechos Fundamentales de la UE (2000). En

septiembre de 2017, el Comité de Ministros del Consejo de Europa aceptó el pedido que hizo la República Argentina para adherir al Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos personales y la Ley 27.483 fue sancionada el 02/01/2019 en el Senado y la Cámara de Diputados de la Nación. Por otra parte, en EE.UU., la Comisión Federal de Comercio (FTC) es más flexible en lo que hace a los servicios IoT para la recolección de datos no requeridos inicialmente. (Salazar & Silvestre, 2014)

1.4.1. Los marcos regulatorios frente a la innovación

En el año 2016, la Secretaria de Tecnologías de la Información y las Comunicaciones (SeTIC) dictó la Resolución SeTIC N°8/2016 que creó el Grupo de Trabajo de Servicios de Internet para estudiar los principales aspectos vinculados a la evolución, desarrollo, utilización y promoción de Internet en la República Argentina. (Nación, 2017). En este contexto se organizó la jornada "Diálogo Público-Privado: Internet de las Cosas. Una Oportunidad para Argentina", se realizó una consulta pública para recabar información, necesidades, opiniones y propuestas de los distintos actores y sectores vinculados al desarrollo de IoT, con la finalidad de "elaborar políticas públicas o regulaciones que promuevan su desarrollo y que incentiven la inversión en aplicaciones y soluciones que contribuyan al crecimiento de nuestra economía y, particularmente, a aumentar su productividad y competitividad" (Nación, 2017).

La encuesta pública tuvo aportantes desde los sectores empresarios, consultoras, legislativo, y académico. En referencia a los aspectos regulatorios algunas de las conclusiones salientes son las siguientes: El Estado no debería regular, sino promover, facilitar e incentivar el uso de la IoT absteniéndose de crear regulaciones específicas o adicionales, tanto en el orden nacional, como en el provincial y/o municipal. El Estado debería licenciar el espectro para que los Operadores puedan ofrecer servicios IoT de calidad. El Estado no debería abordar un modelo regulatorio para garantizar la protección y privacidad de los datos en las comunicaciones diferente del que hace a la Ley de Protección de Datos Personales.

1.4.2. Ley 372 del estado de California

El 29 de septiembre de 2018, California se convirtió en el primer Estado con una ley de seguridad cibernética que cubre los dispositivos "inteligentes", al promulgar el proyecto de ley SB-327 *Information privacy: connected devices* que fue agregada a la Sección 1, Parte 4 de la División 3 del Código Civil, bajo el título *Title 1.81.26. Security of Connected Devices*, adelantándose así al resto del mundo. Este acto fue precedido por la presentación de propuestas de ley en las que se establecían los estándares mínimos que deberían cumplir los *dispositivos conectados* por parte de las agencias federales de los EE.UU., el pedido para desarrollar recursos de ciberseguridad en la educación y concientización de los consumidores en referencia a los dispositivos IoT, y la realización de un estudio acerca del estado de la industria de dispositivos conectados en ese país. En resumen, esta ley requiere que los fabricantes proporcionen funciones de seguridad a los dispositivos, que asimismo doten a los dispositivos de medios para solicitar a los usuarios el consentimiento para recopilar información e indicación explicita de cuándo ésta se lleva a cabo y, finalmente, que los vendedores informen a los consumidores, en los puntos de venta, acerca de las funciones de recopilación de datos que poseen los productos que venden. Aunque la ley tiene detractores, se sigue adelante con ella, a la luz de varios incidentes relacionados con dispositivos conectados, como captura de información mediante cámaras, juguetes y Smart TVs hackeados (Porcelli, 2019).

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

2. RESULTADOS, ANÁLISIS Y DISCUSIÓN

A continuación, se expondrá la metodología aplicada, los resultados del estudio y las reflexiones originadas por el mismo.

2.1 Materiales y métodos

El método utilizado para realizar este trabajo consiste en la obtención, el relevamiento, el análisis de literatura científica relevante y su posterior síntesis. Las fuentes principales de trabajos científicos han sido principalmente ScienceDirect (Elsevier), ResearchGate, arXiv, Google Academics, y páginas web en general. Los trabajos relevados son, en general, de acceso libre a la comunidad científica.

Algunas de las referencias bibliográficas datan de la década de 1990 o antes, y se han incorporado por ser trabajos clásicos. Sin embargo, en general, se ha tratado de hacer énfasis en el análisis de trabajos publicados durante los últimos cinco años para reflejar el estado del arte.

La literatura recopilada se organizó mediante Mendeley Desktop, una herramienta de gestión del conocimiento que facilita la editorial Elsevier. Asimismo, se empleó el *add-on* Mendeley Cite-O-Matic para MS Word para facilitar referenciación bibliográfica del documento.

El *site* de ScienceDirect permitió la obtención de literatura basada en el establecimiento de alertas por medio de palabras claves (tales como IoT AND Protocols, etc.).
Los recursos físicos, logísticos y económicos provienen del PI 29/A425-1, financiado por la Universidad Nacional de la Patagonia Austral.

2.2 Resultados

Se ha realizado el análisis de un número significativo de fuentes bibliográficas (>50). La cantidad de publicaciones disponibles para el análisis año a año es muy grande, y el campo de interés, muy dinámico. Por lo tanto, este trabajo se ha centrado en la obtención del conocimiento de temas considerados como centrales desde una perspectiva general.

Se ha encontrado que varios de los trabajos publicados en carácter de *surveys* o *reviews* coinciden en agrupar la temática del paradigma IoT aproximadamente del mismo modo que se ha realizado en este documento, a saber: Arquitecturas, Protocolos, Tecnologías, Aplicaciones, Problemas abiertos y Oportunidades (aunque no necesariamente en el mismo orden). En este trabajo se ha seguido una estructura similar cubriendo, en lo posible, todo el campo de estudio en una vista ‘a vuelo de pájaro’ para detectar oportunidades para la investigación, sin menoscabar el conocimiento de base necesario.

Existe una concepción que afirma que los dispositivos IoT están manifiestamente limitados desde el punto de vista de su reducida capacidad de memoria y/o procesamiento. Algunos autores consultados (Iova et al., 2016), (Farahzadi et al., 2018), (Atzori et al., 2010) se refieren a ello. Esto es cierto, en alguna medida, por la propia naturaleza de los dispositivos (pequeños, inalámbricos, etc.) y ha sido el impulsor para la creación (o empleo) de protocolos optimizados para IoT (ver 1.1.3.3.1.4-CoAP y 1.1.3.3.1.5-DDS). No obstante, la evolución tecnológica, en lo que concierne a la potencia del *hardware*, a los nuevos *frameworks* y a la disponibilidad de *middleware*, que potencia la creación de aplicaciones nuevas, está

ICT-UNPA-256-2020
ISSN: 1852-4516
Aprobado por Resolución N° 0535/20-R-UNPA
http://doi.org/10.22305/ict-unpa.v12.n3.744

permitiendo desplazar capacidades de alto nivel como la *inteligencia* desde los grandes servidores *cloud* hacia la internet *fog* y el *Edge* (Hu et al., 2017) (L. Bittencourt et al., 2018). Esta migración de servicios o capacidades, traccionada por nuevos requisitos de latencia y/o ancho de banda cerca de los dispositivos terminales, llega al punto de que la Inteligencia Artificial (IA) *en el borde* está ganando considerable fuerza día a día (Mocnej et al., 2018). Se puede afirmar, por tanto, que hoy en día los dispositivos IoT no son exclusivamente dispositivos de pequeña potencia computacional abriéndose entonces una ventana de oportunidad para la implementación de aplicaciones que requieran procesamientos complejos *in situ*.

Se ha visto que la industria es un campo naturalmente propicio para la implantación de aplicaciones que empleen sistemas *Cloud-Fog-Edge*-IoT. En el ámbito de la Patagonia Austral, los procesos productivos de la Agricultura, Ganadería, y Acuicultura plantean interesantes desafíos para los cuales, seguramente, se pueden desarrollar soluciones verticales de negocio en busca de la eficiencia. Este hecho se debe, en gran medida, a que los costos de infraestructura que conlleva la implantación de un sistema IoT son accesibles hasta para los más pequeños productores. En particular se han hallado dos aplicaciones interesantes que podrían ser replicables en nuestro ámbito regional. El primero de ellos (Guirado-Clavijo et al., 2018) es un sistema de información totalmente integrado que permite realizar la gestión completa del proceso productivo de vegetales de invernaderos, desde la venta de semillas al agricultor hasta la venta de los productos al cliente final, realizando la trazabilidad completa. El segundo es un sistema de acuaponía que combina la acuicultura tradicional con la hidroponía (Karimanzira & Rauschenbach, 2019) haciendo recircular los subproductos de los módulos acuicultural e hidropónico en un ciclo cerrado, buscando establecer condiciones de crecimiento óptimas en ambos componentes a la vez.

2.3 Discusión

IoT es un campo en manifiesta expansión. La revolución previa en tecnología de comunicaciones impulsada por la telefonía celular influyó en forma determinante en este proceso, desde las primeras aplicaciones M2M. El aumento en la complejidad de las tecnologías subyacentes hace posible la creación de aplicaciones novedosas con mayor valor añadido. Los dispositivos IoT ya no son sólo pequeñas piezas de hardware con capacidad de comunicación programadas en código ensamblador, sino que han evolucionado hacia dispositivos donde la complejidad debe, necesariamente, manejarse mediante más y más niveles de abstracción. ¿Significa esto que la limitación en recursos de los dispositivos IoT es una cuestión del pasado? Puede que la respuesta sea que no, al menos por el momento. Esta afirmación estriba en que, posiblemente, sólo haya crecido el espectro de complejidad de los dispositivos, habiendo lugar para dispositivos muy limitados en capacidades y dispositivos con capacidades muy grandes y crecientes. La razón es que, en la búsqueda de mayores capacidades, se requieren todavía dispositivos minúsculos que consuman cantidades de energía ínfimas. Piénsese, por ejemplo, en ciertos dispositivos que deban abandonarse en lugares remotos e inaccesibles para adquirir datos que luego deben ser recogidos o enviados empleando anchos de banda insignificantes.

Esta fase de la investigación se ha abordado desde la exploración de posibles usos y aplicaciones del paradigma IoT a nuestro medio. En tanto este es uno de nuestros principales objetivos, la tarea está necesariamente incompleta. Por otra parte, en este trabajo no se ha llegado a profundizar suficientemente en el estudio del modelado de sistemas IoT (necesario para nuestro enfoque en ingeniería de sistemas), ni de los protocolos de nivel de aplicación

para sistemas IIoT para tiempo real (necesarios para la creación de aplicaciones industriales de mayor impacto). Otro aspecto que se considera relevante para investigaciones futuras se relaciona con las arquitecturas IoT descentralizadas y las arquitectura eficiente en recursos (Mocnej et al., 2018).

Una mención aparte requiere el campo de la legislación y/o regulaciones referentes a este campo de vertiginoso crecimiento en nuestra disciplina. Este primer trabajo de relevamiento tendrá por resultado el establecimiento de unos cimientos iniciales desde los cuales realizar una búsqueda sistemática de líneas de investigación en el campo de la Internet de las Cosas.

3. CONCLUSIONES

Se ha realizado una primera exploración, relevamiento, y análisis de 58 fuentes bibliográficas para adquirir una visión general del estado del arte del universo IoT. Asimismo, se han identificado dos verticales de negocio posiblemente aplicables al contexto y particularidades de la Patagonia Austral. Como resultado, queda establecido un mapa preliminar para el abordaje al estudio en mayor profundidad de los diversos temas, cuestiones y desafíos que se plantean dentro del paradigma IoT, así como las oportunidades, desafíos y necesidades de investigación y desarrollo planteadas en la sección 1.3.

Además de los temas más clásicamente tocantes a las tecnologías TIC, este trabajo incluye un breve análisis sobre dos publicaciones interesantes (Porcelli, 2019) y (Nación, 2017), que atañen al marco legal y que ponen en evidencia la pugna entre regulación e innovación; la primera, necesaria para evitar situaciones de anarquía, la segunda, imprescindible para el crecimiento del ecosistema tecnológico.

4. RECOMENDACIONES

Los autores consideran que se debe insistir en la búsqueda de modelos de aplicaciones. Por otra parte, se entiende necesaria la profundización en el estudio del modelado de sistemas IoT y de protocolos de nivel de aplicación para sistemas industriales (IIoT) para tiempo real. Finalmente, y a la luz de la proliferación del *fog computing*, se considera relevante la investigación referente a *gateways* sin limitaciones importantes de recursos computacionales.

5. AGRADECIMIENTOS

Queremos expresar nuestro agradecimiento al Área de Investigación Forestales Silvopastoriles de la Estación Experimental Agropecuaria Santa Cruz de INTA, que nos dio acceso a un entorno de pruebas de hidroponía en la estación Marambio (Antártida Argentina), de la que llevamos a cabo numerosos y fructíferos ensayos sobre monitorización, control, almacenamiento y exposición gráfica de variables ambientales en tiempo real a distancia (INTA, 2019).

Asimismo, deseamos agradecer a la Secretaria de Ciencia y Técnica de la UNPA por el significativo aporte de dispositivos hardware IoT y sensores, con los que se realizaron valiosas experiencias. También al aporte de financiamiento y recursos realizado por la UNPA a través de las convocatorias a proyectos de investigación, en nuestro caso del PI 29/A425-1.

6. BIBLIOGRAFIA

AFZAAL, H., & ZAFAR, N. A. (2017). Modeling of IoT-based border protection system. *2017 First International Conference on Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT)*, 1–6. https://doi.org/10.1109/INTELLECT.2017.8277639

AL-FUQAHA, A., GUIZANI, M., MOHAMMADI, M., ALEDHARI, M., & AYYASH, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

ASHTON, K. (2009). In the real world, things matter more than ideas. In *RFID Journal* (Vol. 22). https://doi.org/http://www.rfidjournal.com/articles/view?4986

ATZORI, L., IERA, A., & MORABITO, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

AZIZ, B. (2016). A formal model and analysis of an IoT protocol. *Ad Hoc Networks*, *36*(June 2015), 49–57. https://doi.org/10.1016/j.adhoc.2015.05.013

BASSI, A., BAUER, M., FIEDLER, M., KRAMP, T., VAN KRANENBURG, R., LANGE, S., & MEISSNER, S. (2013). Enabling things to talk: Designing IoT solutions with the IoT architectural reference model. In *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*. https://doi.org/10.1007/978-3-642-40403-0

BITTENCOURT, L. F., IMMICH, R., SAKELLARIOU, R., DA FONSECA, N. L. S., MADEIRA, E. R. M., CURADO, M., … WESTERLUND, T. (2017). A survey on LoRa for IoT: Integrating edge computing. *IFAC-PapersOnLine*, *4*(2016), 249–254. https://doi.org/10.1109/JPROC.2019.2918951

BITTENCOURT, L., IMMICH, R., SAKELLARIOU, R., FONSECA, N., MADEIRA, E., CURADO, M., … RANA, O. (2018). The Internet of Things, Fog and Cloud continuum: Integration and challenges. *Internet of Things*, *3–4*, 134–155. https://doi.org/10.1016/j.iot.2018.09.005

BROWN, E. (2016a). 21 Open Source Projects for IoT. *Linux.Com*.

BROWN, E. (2016b). Who Needs the Internet of Things? Retrieved August 8, 2018, from The Linux Foundation website: https://www.linux.com/news/who-needs-internet-things

CMU Computer Science Department. (2005). *CMU SCS Coke Machine Home Page*. Retrieved from http://www.cs.cmu.edu/~coke/

COHEN, E. A., & GERSHENFELD, N. A. (1999). When Things Start to Think. In *Foreign Affairs* (Vol. 78). https://doi.org/10.2307/20049565

COMUNICACIONES, U. I. de las. (2012). ITU-T Y.2060 : Visión general de la Internet de las cosas. Retrieved August 4, 2018, from https://www.itu.int/rec/T-REC-Y.2060-201206-I/es

DERVAN, B. (2019). 10 Top Internet of Things Events to Attend in 2019. Retrieved from https://www.skyhook.com/blog/iot/internet-of-things-events-2019

ETEROVIC, T., KALJIC, E., DONKO, D., SALIHBEGOVIC, A., & RIBIC, S. (2015). An Internet of Things visual domain specific modeling language based on UML. *2015 25th International Conference on Information, Communication and Automation Technologies, ICAT 2015 - Proceedings*, 1–5. https://doi.org/10.1109/ICAT.2015.7340537

FARAHZADI, A., SHAMS, P., REZAZADEH, J., & FARAHBAKHSH, R. (2018). Middleware technologies for cloud of things: a survey. *Digital Communications and Networks*, *4*(3), 176–188. https://doi.org/10.1016/j.dcan.2017.04.005

FAROOQ, M. U., WASEEM, M., MAZHAR, S., KHAIRI, A., & KAMAL, T. (2015). A Review on Internet of Things (IoT). In *International Journal of Computer Applications* (Vol. 113). Retrieved from https://research.ijcaonline.org/volume113/number1/pxc3901571.pdf

FYSARAKIS, K., ASKOXYLAKIS, I., SOULTATOS, O., PAPAEFSTATHIOU, I., MANIFAVAS, C., & KATOS, V. (2016). Which IoT protocol? Comparing standardized approaches over a common M2M application. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, (October 2017). https://doi.org/10.1109/GLOCOM.2016.7842383

GAAMEL, A., SHELTAMI, T., AL-ROUBAIEY, A., & SHAKSHUKI, E. M. (2017). Broker-Less Middleware for WSAN Performance Evaluation. *Procedia Computer Science*, *110*, 369–377. https://doi.org/10.1016/j.procs.2017.06.079

GERSHENFELD, N., KRIKORIAN, R., & COHEN, D. (2004). The Internet of Things. In *Scientific American*. Retrieved from www.sciam.com

GONZÁLEZ, L., LAGUÍA, D., SANTOS, E., BIRGI, J., HALLAR, K., GESTO, E., & SOFÍA, O. (2019). LibreSeed : una sembradora de plantines con hardware y software libre. *48JAIIO-CAI*, 170–182.

GROTECK. (2015). Internet of Things World Forum. Retrieved from http://www.icenter.ru/docs/pilot_2016-1/vmiv.pdf

GUIRADO-CLAVIJO, R., SANCHEZ-MOLINA, J. A., WANG, H., & BIENVENIDO, F. (2018). Conceptual Data Model for IoT in a Chain-Integrated Greenhouse Production: Case of the Tomato Production in Almeria (Spain). *IFAC-PapersOnLine*, *51*(17), 102–107. https://doi.org/10.1016/j.ifacol.2018.08.069

HASAN, H. M., & MOHAMMED, B. K. (2018). Evaluation of MQTT Protocol for IoT Based Industrial Automation. *International Journal of Engineering Science and Computing*, (December). Retrieved from http://ijesc.org/

HEJAZI, H., RAJAB, H., CINKLER, T., & LENGYEL, L. (2018). Survey of platforms for massive IoT. *2018 IEEE International Conference on Future IoT Technologies, Future IoT 2018*, *2018-Janua*(May), 1–8. https://doi.org/10.1109/FIOT.2018.8325598

HOUIMLI, M., KAHLOUL, L., & BENAOUN, S. (2017). Formal specification, verification and evaluation of the MQTT protocol in the Internet of Things. *2017 International Conference on Mathematics and Information Technology (ICMIT)*, 214–221. https://doi.org/10.1109/MATHIT.2017.8259720

HOUIMLI, M., KAHLOUL, L., BENAOUN, S., AL-ROUBAIEY, A., HASAN, H. M., ALONSO, L., … ABDELLATIF, S. (2016). A Survey of Protocols and Standards for Internet of Things. *Ad Hoc Networks*, *29*(4), 48–54. https://doi.org/10.1016/j.adhoc.2015.01.020

HU, P., DHELIM, S., NING, H., & QIU, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of Network and Computer Applications*, *98*(April), 27–42. https://doi.org/10.1016/j.jnca.2017.09.002

IIOT STANDARDS | Object Management Group. (n.d.). Retrieved from https://www.omg.org/hot-topics/iot-standards.htm

INTA. (2019). El INTA instala un sistema hidropónico en la Antártida - INTA Informa. Retrieved from INTA Informa website: https://intainforma.inta.gob.ar/el-inta-instala-un-sistema-hidroponico-en-la-antartida/

IOVA, O., PICCO, P., ISTOMIN, T., & KIRALY, C. (2016). RPL: The Routing Standard for the Internet of Things... or Is It? *IEEE Communications Magazine*, *54*(11), 16–22. https://doi.org/10.1109/MCOM.2016.1600397CM

ITU. (2005). The Internet of Things [ITU Report]. In *Itu Internet Report 2005*. https://doi.org/10.2139/ssrn.2324902

KAMAL, Z., MOHAMMED, A., SAYED, E., & AHMED, A. (2017). Internet of Things Applications, Challenges and Related Future Technologies. *WSN World Scientific News*, *67*(672), 126–148. Retrieved from www.worldscientificnews.com

KARIMANZIRA, D., & RAUSCHENBACH, T. (2019). Enhancing aquaponics management with IoT-based Predictive Analytics for efficient information utilization. *Information Processing in Agriculture*, (xxxx). https://doi.org/10.1016/j.inpa.2018.12.003

KELSEY, R. (2015). *7/17/2015 RFC 6550 - RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks* (pp. 1–314). pp. 1–314. Retrieved from http://www.rfc-editor.org/info/rfc6550.

KHARRUFA, H., AL-KASHOASH, H. A. A., & KEMP, A. H. (2019). RPL-based routing protocols in IoT applications: A Review. *IEEE Sensors Journal*, *PP*(April), 1–1. https://doi.org/10.1109/JSEN.2019.2910881

LATIF, S. L., AFZAAL, H. A., & ZAFAR, N. A. (2017). Modeling of Sewerage System Using Internet of Things for Smart City. *2017 International Conference on Frontiers of Information Technology (FIT)*, 46–51. https://doi.org/10.1109/FIT.2017.00016

LIN, J., YU, W., ZHANG, N., YANG, X., ZHANG, H., & ZHAO, W. (2017). Architecture, enabling technologies, security and privacy, and applications of internet of things: A survey. *IEEE Internet of Things Journal*, *4*(5), 1125–1142.

LUETH, K. L. (2019). IoT 2019 in Review: The 10 Most Relevant IoT Developments of the Year. Retrieved from IoT Analytics website: https://iot-analytics.com/iot-2018-in-review/

MADAKAM, S., RAMASWAMY, R., & TRIPATHI, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, *03*(05), 164–173. https://doi.org/10.4236/jcc.2015.35021

MAZZINI, S., FAVARO, J., & BARACCHI, L. (2015). A Model-Based Approach Across the IoT Lifecycle for Scalable and Distributed Smart Applications. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, *2015-Octob*, 149–154. https://doi.org/10.1109/ITSC.2015.33

MEHBOOB, U., ZAIB, Q., & USAMA, C. (2016). *Survey of IoT Communication Protocols Techniques, Applications, and Issues*. Retrieved from http://xflowresearch.com/wp-content/uploads/2016/02/Survey-of-IoT-Communication-Protocols.pdf

MENDOZA, J. F., ORDÓÑEZ, H., ORDÓÑEZ, A., & JURADO, J. L. (2017). Architecture for embedded software in microcontrollers for Internet of Things (IoT) in fog water collection. *Procedia Computer Science*, *109*(2016), 1092–1097. https://doi.org/10.1016/j.procs.2017.05.395

MEYER, S., SPERNER, K., MAGERKURTH, C., DEBORTOLI, S., & THOMA, M. (2012). *Concepts for Modelling IoT-Aware Processes*. (257521)

MISIC, J., ALI, M. Z., & MISIC, V. B. (2018). Protocol Architectures for IoT Domains. *IEEE Network*, *32*(4), 81–87. https://doi.org/10.1109/MNET.2018.1700395

MOCNEJ, J., SEAH, W. K. G., PEKAR, A., & ZOLOTOVA, I. (2018). Decentralised IoT Architecture for Efficient Resources Utilisation. *IFAC-PapersOnLine*, *51*(6), 168–173. https://doi.org/10.1016/j.ifacol.2018.07.148

NACIÓN, P. de la. (2017). *Consulta pública sobre Internet de las Cosas*. Retrieved from https://www.argentina.gob.ar/sites/default/files/consulta_publica_internet_de_las_cosas.pdf

NIC. (2008). *Disruptive Civil Technologies: Six Technologies with Potential Impacts on US Interests Out to 2025 : Biogerontechnology, Energy Storage Materials, Biofuels and Bio-based Chemicals, Clean Coal Technologies, Service Robotics, the Internet of Things*. 34. Retrieved from https://books.google.com/books?id=6DmhAQAACAAJ

PAPKE, B. L. (2017). Enabling design of agile security in the IOT with MBSE. *2017 12th System of Systems Engineering Conference, SoSE 2017*, 1–6. https://doi.org/10.1109/SYSOSE.2017.7994938

PORCELLI, A. M. (2019). Alcances jurídicos, tecnológicos y comerciales de la primera legislación sobre internet de las cosas. *Lex Social*, *9*(1), 603–636. Retrieved from www.up.es/revistas/index.php/lex_social/index

REDMOND, A. M., & ZARLI, A. (2018). The concept selection of lean software and system engineering tools for smart cities. *2017 International Conference on Engineering, Technology and Innovation: Engineering, Technology and Innovation Management Beyond 2020: New Challenges, New Approaches, ICE/ITMC 2017 - Proceedings*, *2018-Janua*, 36–43. https://doi.org/10.1109/ICE.2017.8279866

ROBLES-RAMIREZ, D. A., ESCAMILLA-AMBROSIO, P. J., & TRYFONAS, T. (2017). IoTsec: UML extension for internet of things systems security modelling. *Proceedings - 2017 International Conference on Mechatronics, Electronics, and Automotive Engineering, ICMEAE 2017*, *2017-Janua*, 151–156. https://doi.org/10.1109/ICMEAE.2017.20

SALAZAR, J., & SILVESTRE, S. (2014). Internet de las cosas. *Universidad Católica*, 1–27.

SARKER, V. K., & PE, J. (2019). *LoRa for IoT : Integrating Edge Computing LoRa for IoT : Integrating Edge Computing*. (June).

TEICHER, J. (2018). The little-known story of the first IoT device - IBM Industries. Retrieved from Ibm website: https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/

VILLAGRA, A., ERRECALDE, M., MOLINA, D., VARAS, V., OROZCO, S., VALDÉZ, J., … PANDOLFI, D. (2018). *Soluciones inteligentes para el desarrollo urbano sostenible*. 50–55.

VILLAGRA A, ERRECALDE M, PANDOLFI D, MOLINA D, VARAS V, OROZCO S, … MONTENEGRO C. (2019). Hacia ciudades mas eficientes y sostenibles. *XXI Workshop de Investigadores En Ciencias de La Computación*.

WEISER, M. (1991). The Computer for the 21st Century. *Scientific American*, *265*(3), 94–104. https://doi.org/10.1038/scientificamerican0991-94