



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



Máster en Ingeniería de Computadores y Redes  
Trabajo Fin de Máster

# EVALUACIÓN DE SERVICIOS EN LA NUBE PARA EL DESARROLLO DE APLICACIONES IOT SOBRE REDES INALÁMBRICAS DE SENSORES

**Autor:** *Edison Fabricio Chuquimarca Sarango*

**Director(es):** *D. José Carlos Campelo Rivadulla*

*D. Alberto Bonastre Pina*

*15 de Septiembre del 2017*

# INDICE

## Resumen

<b>CAPITULO I: JUSTIFICACION Y OBJETIVOS.....</b>	<b>1</b>
1.1 Justificación: .....	1
1.2 Objetivos:.....	1
1.2.1 Objetivos Secundarios:.....	1
<b>CAPITULO II: ESTADO DEL ARTE DE IOT Y CLOUD COMPUTING.....</b>	<b>3</b>
2.1 <i>Internet of Things</i> .....	3
2.1.1 Arquitectura de <i>Internet of Things</i> .....	3
2.2 <i>Cloud Computing</i> .....	4
2.2.1 Arquitectura de <i>Cloud Computing</i> .....	5
2.3 Convergencia entre IoT y <i>Cloud Computing</i> .....	6
2.3.1 Ventajas de la convergencia entre IoT y <i>Cloud Computing</i> .....	7
2.3.2 Nuevos Modelos de Negocio .....	8
2.4 Desafíos y retos del paradigma CloudIoT .....	9
<b>CAPITULO III: SERVICIOS EN LA NUBE PARA IOT .....</b>	<b>11</b>
3.1 SOFIA2 .....	11
3.1.1 Breve Historia .....	11
3.1.2 Conceptos de Sofia2 .....	12
3.1.3 Características de Sofia2 .....	13
3.1.4 Arquitectura de Sofia2 .....	14
3.1.5 Modelo de negocio en Sofia2 .....	16
3.1.6 Aplicaciones con Sofia2 .....	16
3.1.7 Recursos para el desarrollador .....	17
3.1.8 Casos de Uso .....	17
3.2 FIWARE .....	18
3.2.1 Breve Historia .....	18
3.2.2 Conceptos de Fiware.....	18
3.2.2.1 Orion Context Broker.....	19
3.2.2.2 IDAS IoT Agent.....	20
3.2.2.3 Protocolo Ultralight2.0 .....	21
3.2.3 Arquitectura de Fiware.....	21
3.2.4 Modelo de Negocio en Fiware.....	21
3.2.5 Recursos para el desarrollador .....	22
3.2.6 Casos de Uso .....	22
3.3 WATSON IoT .....	23
3.3.1 Conceptos de Watson IoT .....	23
3.3.2 Características de Watson IoT .....	24
3.3.3 Arquitectura de Watson IoT .....	24
3.3.4 Modelo de Negocio en Watson IoT .....	25
3.3.5 Recursos para el Desarrollador.....	25
3.3.6 Casos de Uso .....	25
3.4 SAMSUNG ARTIK CLOUD.....	26
3.4.1 Conceptos de Samsung Artik Cloud.....	27
3.4.2 Características de Samsung Artik Cloud.....	28

3.4.3 Arquitectura de Samung Artik Cloud.....	29
3.4.4 Modelo de Negocio de Samsug Artik Cloud.....	29
3.4.5 Casos de Uso .....	30
3.5 MICROSOFT AZURE IOT SUITE.....	31
3.5.1 Conceptos de Microsoft Azure IoT Suite .....	31
3.5.2 Características de Microsoft Azure IoT Suite .....	32
3.5.3 Arquitectura de Microsoft Azure IoT Suite .....	33
3.5.4 Modelo de Negocio de Microsoft Azure IoT Suite .....	33
3.5.5 Casos de Uso .....	33
<b>CAPITULO IV: ENTORNO DE PRUEBAS PARA LA EVALUACIÓN DE LOS SERVICIOS EN LA NUBE PARA IOT. ....</b>	<b>35</b>
4.1 Implementación del servicio Sofia2.....	37
4.2 Implementación del servicio Fiware .....	39
4.3 Implementación del servicio Watson IoT.....	40
4.4 Implementación del servicio Samsung Artik Cloud .....	41
4.5 Implementación del servicio Microsoft Azure IoT .....	43
<b>CAPITULO V: RESULTADOS.....</b>	<b>45</b>
5.1 Resultados en Sofia2.....	45
5.2 Resultados en Fiware .....	48
5.3 Resultados en Watson IoT.....	49
5.4 Resultados en Samsung Artik .....	54
5.5 Resultados en Microsoft Azure IoT Suite.....	56
<b>CAPITULO VI: CONCLUSIONES.....</b>	<b>61</b>
<b>BIBLIOGRAFIA.....</b>	<b>64</b>
<b>ANEXOS.....</b>	<b>70</b>

## LISTA DE FIGURAS

Figura 1: Capas que conforman el paradigma IoT.....	4
Figura 2: Arquitectura genérica para Cloud Computing.....	5
Figura 3: Arquitectura genérica para CloudIoT.....	7
Figura 4: Encuadre de Sofia2 en el flujo típico de IoT.....	12
Figura 5: Diagrama de comunicación entre los diferentes conceptos de Sofia2. .	13
Figura 6: Representación en JSON de una ontología.....	13
Figura 7: Arquitectura de la versión Base Edition de Sofia2.....	15
Figura 8: Arquitectura de la versión IoT Edition de Sofia2.....	15
Figura 9: Arquitectura de la version Advance Edition de Sofia2.....	16
Figura 10: Modelo de Negocio de la plataforma Sofia2.....	17
Figura 11: Context Broker de Fiware.....	20
Figura 12: IoT Agent IDAS de Fiware.....	21
Figura 13: Arquitectura IoT de Fiware.....	22
Figura 14: Arquitectura de la plataforma Watson IoT.....	25
Figura 15: Arquitectura de la plataforma Samsung Artik.....	29
Figura 16: Modelo de Negocio de Samsung Artik.....	30
Figura 17: Arquitectura de la plataforma Microsoft Azure IoT Suite.....	33
Figura 18: Arquitectura genérica del entorno de pruebas.....	36
Figura 19: Diagrama de Bloques de la implementación en Sofia2.....	37
Figura 20: Plataforma Sofia2 mostrando información de los sensores.....	38
Figura 21: Diagrama de Bloques de la implementación en Fiware.....	39
Figura 22: Herramienta FreeBoard mostrando la información de los sensores. .	40
Figura 23: Diagrama de Bloques de la implementación en Watson IoT.....	40
Figura 24: Plataforma Watson IoT mostrando la información de los objetos.....	41
Figura 25: Diagrama de Bloques de la implementación en Artik Cloud.....	41
Figura 26: Plataforma Samsung Artik mostrando información de los sensores. .	42
Figura 27: Diagrama de bloques de la implementación en Azure IoT Suite.....	43
Figura 28: Aplicación Power BI mostrando información de los sensores.....	44
Figura 29: Plataforma Azure IoT mostrando métricas de los dispositivos.....	44
Figura 30: Herramienta de consulta de estado de Ontologías en Sofia2.....	47
Figura 31: Herramienta de creación de graficas de información en Sofia2.....	47
Figura 32: Herramienta de consulta de base de datos en Sofia2.....	48
Figura 33: Herramienta de estado de datos transferidos en Watson IoT.....	53
Figura 34: Herramienta de gestión de dispositivos en Watson IoT.....	53
Figura 35: Herramienta de gestión y consulta de bases de datos.....	53
Figura 36: Interfaz grafica de usuario en Artik Samsung.....	56
Figura 37: Métricas de uso de dispositivos en la Azure IoT.....	58
Figura 38: Aplicación Microsoft Azure Storage Explorer.....	59

## LISTA DE TABLAS

Tabla 1: Complementariedad e integración de IoT y Cloud Computing.....	6
Tabla 2: Variables a ser simuladas y enviadas por la Raspberry Pi. ....	37
Tabla 3: Relación del modelo SaaS y el entorno de pruebas. ....	37
Tabla 4: Mensajes por día enviados. ....	45
Tabla 5: Costo aproximado del servicio Watson IoT. ....	51
Tabla 6: Costo aproximado del servicio Samsung Artik.....	54
Tabla 7: Costo aproximado del servicio Azure IoT Suite. ....	57
Tabla 8: Mensajes Procesados por las plataformas IoT.....	59
Tabla 9: Características de los servicios en la nube para IoT.....	60

## **LISTA DE ACRONIMOS**

IoT	Internet of Things
M2M	Machine to Machine
SCADA	Supervisory Control And Data Acquisition
WSN	Wireless Sensor Networks
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
SAaaS	Sensing and Actuation as a Service
SEaaS	Sensor Event as a Service
SenaaS	Sensor as a Service
DBaaS	DataBase as a Service
DaaS	Data as a Service
VSaaS	Video Surveillance as a Service
API	Application Programming Interface
WBAN	Wireless Body Area Network
VANETS	Vehicular Ad Hoc Network
QoS	Quality of Service
SDK	Software Development Kit
SIB	Semantic Information Broker
KP	Knowledge Processor
SSAP	Smart Space Access Protocol
REST	Representational State Transfer
MQTT	Message Queue Telemetry Transport
JMS	Java Message Service

BDTR	Base de Datos Tiempo Real
NoSQL	Not Only Structured Query Language
BDH	Base de Datos Histórica
ODBC	Open Database Connectivity
JDBC	Java Database Connectivity
SP	Sensor Publishers
ESP	Extended Service Providers
SDK	Software Development Kit
SSMTP	Simple Mail Transfer Protoco
NGSI	Next Generation Services Interface
GE	Generic Enabler
FI-PPP	Future Internet Public-Private Partnership
LWM2M	Lightweight Machine to Machine
HTTP	Hypertext Transfer Protocol
SME	Small and Medium-sized Enterprises
SNCF	Société nationale des chemins de fer français
TLS	Transport Layer Security
COAP	Constrained Application Protocol
JSON	JavaScript Object Notation
JS	Java Script
BCA	Building and Construction Authority

## RESUMEN

En la década de los ochenta fueron surgiendo todo tipo de tecnologías inalámbricas y de sensores con el objetivo de obtener parámetros determinados del entorno; y que en sus inicios era solo aplicable a la industria militar y específica. A medida que se avanzaba hacia una miniaturización de los componentes electrónicos, la reducción de costos y el desarrollo de tecnologías más eficientes, estos sensores ya se podían aplicar a casi todo parámetro de nuestro entorno y en consecuencia a un uso masivo de los mismos. A finales de la década de los noventa se empieza a acuñar el termino Internet of Things (IoT) y de cómo esta tecnología podría ser el siguiente paso de lo que conocemos como Internet. La idea de que todo objeto de la vida real pueda tener presencia física en la red de redes, enviando y recibiendo información, mostraba un nuevo universo de oportunidades para usuarios, industrias, gobierno, academia, etc.

Otra tecnología que se ha establecido de manera casi irreversible es la llamada computación en la nube o Cloud Computing. En ese momento todo tipo de usuarios tiene algún tipo de contenido en la nube ya sea fotos, documentos, correos, etc. Empresas y gobiernos cada día confían más en almacenar su información y servicios en la nube, debido en gran medida al ahorro económico que supone este modelo de negocio y a las características alta disponibilidad, fiabilidad e integridad que proveen estas.

En los últimos años en la literatura científica se ha estudiado y se ha propuesto un nuevo modelo de servicio que intenta unir IoT y Cloud Computing. Esta convergencia permitirá desarrollar todo un ecosistema de nuevas e innovadoras oportunidades donde los desarrolladores de software y de hardware tendrán un rol primordial. Este presente trabajo de Fin de Máster busca estudiar los más prometedores servicios en la nube para IoT, tanto públicos y privados, que actualmente existen en el mercado. Se implementará un entorno de pruebas donde un dispositivo embebido enviará constantemente variables de sensores a los servicios en la nube. Al final, de los resultados observados se podrá determinar qué servicios son los más óptimos para IoT y cuáles son los más flexibles para que un desarrollador pueda construir sus aplicaciones.

## **CAPITULO I: JUSTIFICACION Y OBJETIVOS**

### **1.1 Justificación:**

IoT y Cloud Computing son paradigmas que tienen sus propias limitaciones tecnológicas debido a la naturaleza de su funcionamiento, pero estas limitaciones se pueden complementar fácilmente con la convergencia exitosa de los mismos. La considerable cantidad de información generada por los objetos puede ser tratada eficientemente por el poder de la nube, ya sea almacenando la información o procesándola con poderosos algoritmos. Además, la computación en la nube puede actuar de intermediario entre la compleja heterogeneidad de tecnologías existentes en IoT y las aplicaciones finales que consumen los usuarios. Este nuevo modelo que algunos han denominado CloudIoT amplía mucho más el universo de oportunidades que por sí solo generaba IoT.

Este nuevo universo de oportunidades se generará gracias a la inmensa cantidad de datos que se tendrá a disposición de los desarrolladores, y así ellos podrían crear las aplicaciones que los usuarios necesitan. El éxito o no de estas aplicaciones no solo dependerá del esfuerzo del desarrollador, si no también de las características particulares que pueda ofrecer el servicio en la nube para IoT. Es por ello que en este trabajo se busca evaluar diferentes servicios en la nube para IoT.

Con la implementación del entorno de pruebas se busca evaluar la complejidad de dichos servicios en su ejecución, sus características de disponibilidad de servicio, los mecanismos de seguridad que cada servicio pueda tener, las características diferenciadoras que sobresalen de cada servicio, así como también las diferencias entre los modelos de negocios que proporcionan. Al final se realizará una comparación entre los servicios estudiados, y se determinará las ventajas y desventajas propias de cada una, el entorno de aplicación según sus características y su coste de implementación, tanto en desarrollo como en el plano económico. El análisis de estos resultados ayudará a determinar qué servicios en la nube son los más prometedores actualmente y cuál o cuáles puedan convertirse en los referentes en un futuro próximo, además de proporcionar al lector un panorama más claro y general que le pueda ayudar a elegir entre un servicio u otro.

### **1.2 Objetivos:**

Estudiar y evaluar los más prometedores servicios en la nube para IoT que actualmente existen en el mercado a través de la implementación de dichos servicios usando un dispositivo embebido.

#### **1.2.1 Objetivos Secundarios:**

- Establecer el estado del arte actual de IoT y la computación en la nube para así entender sus generalidades y los desafíos que enfrentan.
- Detallar las características, modo de funcionamiento y modelo de negocio de los actuales servicios en la nube para IoT.

- Implementar una aplicación que envíe datos de sensores desde un dispositivo embebido hacia estos servicios en la nube haciendo uso de las herramientas que existen a disposición para los desarrolladores.
- Observar el comportamiento tanto del servicio en la nube como de la aplicación cuando éstas estén en funcionamiento.
- Componer recomendaciones que ayuden a otros desarrolladores de aplicaciones para IoT a elegir un servicio en la nube en base a sus requerimientos.

## CAPITULO II: ESTADO DEL ARTE DE IOT Y CLOUD COMPUTING

### 2.1 *Internet of Things*

En los años recientes la comunidad científica y la industria han mostrado particular interés en el paradigma de *Internet of Things* (IoT), también referido en [1] como *Internet of Everything* o *Internet with Things*. Este paradigma especifica que cualquier objeto de nuestro entorno puede estar conectado a Internet y tener presencia enviando o recibiendo información. La información de los objetos se puede recoger usando sensores que midan las características propias de dicho objeto y a través de una interfaz de comunicación enviar la información hacia Internet. De una manera más sofisticada se define a la IoT como nodos (objetos) inteligentes, auto-configurables e interconectados en una infraestructura de red dinámica y global [2]. Este paradigma abre un nuevo panorama donde se podrán encontrar ideas, oportunidades de negocios y soluciones que pueden tener aplicaciones en casi todo tipo de entornos como el hogar, la industria, la salud, movilidad, seguridad etc.

IoT no es un paradigma totalmente nuevo, sino que es el resultado de una evolución e integración de diferentes tecnologías basadas en M2M, desde los sistema SCADA en 1980 hasta las redes de sensores (WSN por sus siglas en inglés, *Wireless Sensor Networks*) a inicios 1990 [3]. Lo anterior descrito ha llevado a que IoT sea un paradigma heterogéneo sin hasta el momento un estándar definido para la interconexión entre objeto e Internet, sino que se tenga un gran número de estándares y tecnologías cada una con sus propias fortalezas y debilidades pero ninguna cuenta con un total apoyo de la industria y de la comunidad científica para una implementación masiva. Esto no ha detenido el uso de IoT, que ha experimentado un crecimiento exponencial. Para el año 2016 Gartner estimó que a nivel mundial 6.4 billones de objetos estuvieron conectados a IoT y que para el año 2020 la cifra aumentaría a 20.8 billones [4]. Además, el mercado de IoT para 2016 ha manejado la apabullante cifra de \$235 billones de dólares, y se espera que para el 2020 se alcance la cifra de \$1524 billones de dólares[4]. Estos datos demuestran el potencial que tiene IoT como catalizador de nuevas oportunidades de negocio que, enfocadas inteligentemente, pueden ser parte de soluciones totalmente innovadoras y con elevada presencia en el mercado.

#### 2.1.1 Arquitectura de *Internet of Things*

La arquitectura de IoT usualmente está constituida por cinco capas según como se describe en [5]:

- *Perception Layer*: Recolección de datos del entorno u objeto a través de sensores.
- *Transport Layer*: Los datos recolectados en la primera capa son gestionados aquí para ser enviados hacia la siguiente capa.
- *Processing Layer*: Aquí se gestiona, procesa y almacena la información de los sensores.

- Application Layer: Presenta la información ya gestionada por la capa inferior según las necesidades de cada entorno. Es donde se prestan los servicios al usuario final.
- Business Layer: Donde se monetizan los servicios de la capa aplicación.

Esta arquitectura de cinco capas basada en [5] puede observarse en la figura 1.

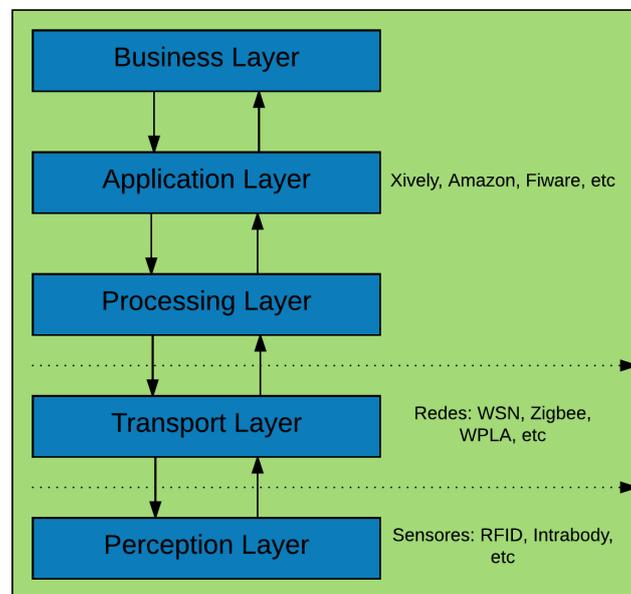


Figura 1: Capas que conforman el paradigma IoT.

En el modelo de IoT los objetos envían y reciben información, en ocasiones de manera continua. Por ello se requiere un manejo eficiente del consumo de energía, más aún cuando los sensores, como en la mayoría de casos, se alimenten mediante baterías. Esto ha llevado a la industria de IoT a diseñar sensores con bajo consumo de energía, sacrificando potencia de computación y capacidad de almacenamiento. Este tipo de sensores, denominados de bajo coste han sido una clave fundamental en la rápida adopción de IoT [6]. Esta fundamental característica de bajo consumo, que no debe ser considerada un detrimento, puede ser fácilmente complementada con la correcta implementación de *Cloud Computing*, la cual se detallara en el siguiente apartado.

## 2.2 Cloud Computing

*Cloud Computing* es un paradigma de entrega de servicios, prestaciones y recursos tanto de hardware y software a través de Internet [7], donde los servicios como tal son referidos como Software as a Service (SaaS) [8]. *Cloud Computing* como tal permite a los usuarios prescindir de instalar y mantener costosas infraestructuras, que en su mayoría solo proporcionan servicios específicos y optar por un nuevo modelo denominado *pay-as-you-use* [9] o también llamado *pay-as-you-go* [8], donde el usuario solo paga el coste de un servicio específico y según su uso. Este nuevo paradigma ofrece gran variedad de nuevas soluciones que van desde almacenamiento de contenidos web, datos y archivos en la nube, hasta procesamiento de complejos algoritmos con

inteligencia artificial y redes neuronales. Otro aspecto diferenciador de *Cloud Computing* es que los usuarios pueden acceder a recursos con alta capacidad de almacenamiento, computación, disponibilidad, confiabilidad y seguridad a un costo relativamente bajo.

### 2.2.1 Arquitectura de *Cloud Computing*

El paradigma de *Cloud Computing* se basa generalmente en la implementación de arquitecturas y diseños de *Data Centers* con computación distribuida, computación paralela y computación en grid [10]. Según lo descrito en [8] *Cloud Computing* de manera genérica está compuesta por tres capas de servicios: *Software as a Service* (SaaS), *Platform as a Service* (PaaS) e *Infraestructure as a Service* (IaaS). A continuación se describe cada una de estas capas:

- *Software as a Service* (SaaS): Son las aplicaciones que trabajan sobre internet, y a la cuales los usuarios acceden a través del modelo de negocio *pay-as-you-use*.
- *Platform as a Service* (PaaS): Plataforma donde las aplicaciones y servicios están implementados. Los desarrolladores de Software pueden diseñar sus propias aplicaciones en este capa.
- *Infraestructure as a Service* (IaaS): Los recursos de computación y almacenamiento que el usuario hace uso a través de las aplicaciones.

En la figura 2 se observa cada capa dentro de la arquitectura de *Cloud Computing* descrito en [8] teniendo como ejemplo el servicio de Cloud de Google.

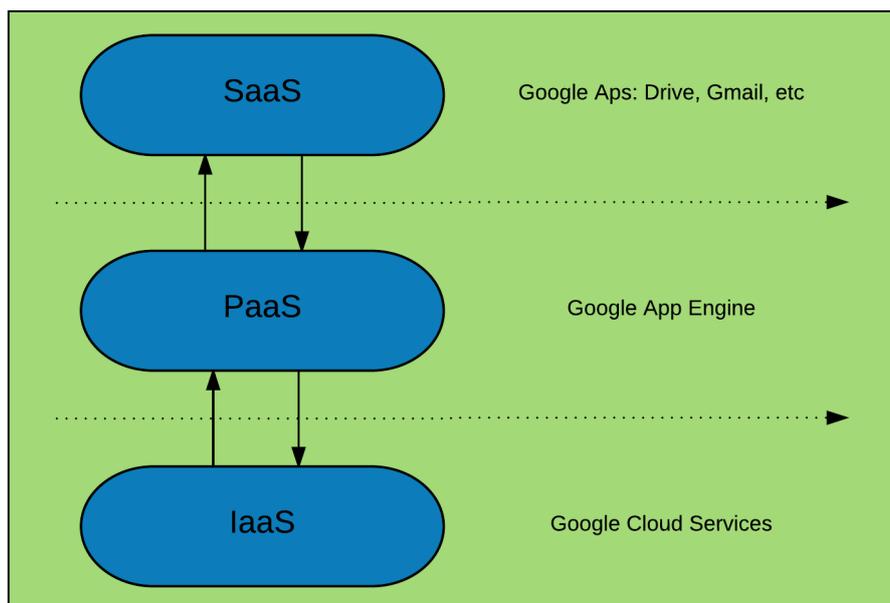


Figura 2: Arquitectura genérica para *Cloud Computing*.

La virtualmente ilimitada capacidad de cómputo y almacenamiento de la nube a bajo costo para los usuarios ha permitido el desarrollo de nuevas soluciones y aplicaciones. Incluso soluciones ya existentes puedan complementarse; un ejemplo claro es el caso de IoT. En el siguiente apartado se discutirá cómo la

convergencia entre IoT y *Cloud Computing* puede resultar beneficiosa, proporcionando el empujón definitivo que permita a IoT establecerse de forma irreversible.

### 2.3 Convergencia entre IoT y *Cloud Computing*

Como se ha visto anteriormente, IoT genera escenarios totalmente nuevos dentro del entorno de las tecnologías de información. Tenemos, por ejemplo, la prometedora computación ubicua la cual especifica que la informática puede estar presente en cualquier momento y en cualquier lugar, que en contraste con la computación de escritorio, la computación ubicua puede ocurrir en cualquier dispositivo, cualquier lugar y cualquier formato [11]. Pero IoT por sí sola no puede generar este prometedor escenario dada sus limitaciones. En cambio con *Cloud Computing* tenemos una tecnología que maneja cantidades ilimitadas en capacidad de cómputo y almacenamiento. Por lo tanto, estas dos tecnologías son complementarias entre sí, y se espera que su fusión marque un antes y después en el futuro de Internet [12]. En la tabla 1 se muestra cómo se complementa e integra IoT y Cloud Computing según [2].

Tabla 1: Complementariedad e integración de IoT y Cloud Computing.

IOT	CLOUD COMPUTING
Objetos en cualquier lugar	Ubicua: Recursos utilizables desde cualquier lugar
Objetos del mundo real	Recursos virtuales
Recursos de computación limitados	Recursos computacionales prácticamente ilimitados
Almacenamiento limitado	Recursos de almacenamiento prácticamente ilimitados
Internet como punto de convergencia	Internet para la prestación de servicios
Fuente de Big Data	Medios para gestionar Big Data

Este nuevo paradigma, que algunos han denominado *CloudIoT* [2] creará aún mejores escenarios para la industria e investigación de los que actualmente IoT y *Cloud Computing* puedan generar por separado. A diferencia de *Cloud Computing*, IoT tiene contacto directo con el mundo real y su comportamiento en todos los escenarios posibles. Toda la información generada por IoT puede ser gestionada y procesada de manera eficiente por *Cloud Computing*, lo cual permitirá implementar nuevas soluciones y servicios aplicables a multitud de situaciones en la vida real. En la figura 3 se puede observar un ejemplo genérico de cómo está compuesta la arquitectura del nuevo paradigma de CloudIoT. En ella podemos observar cómo *Cloud Computing* actúa de intermediario entre los objetos y las aplicaciones. Por ello puede considerarse como un *framework* o *middleware*, ya que actúa como mediador, ocultando la complejidad de los objetos, sus redes de sensores y las aplicaciones que se implementan sobre la Cloud Computing.

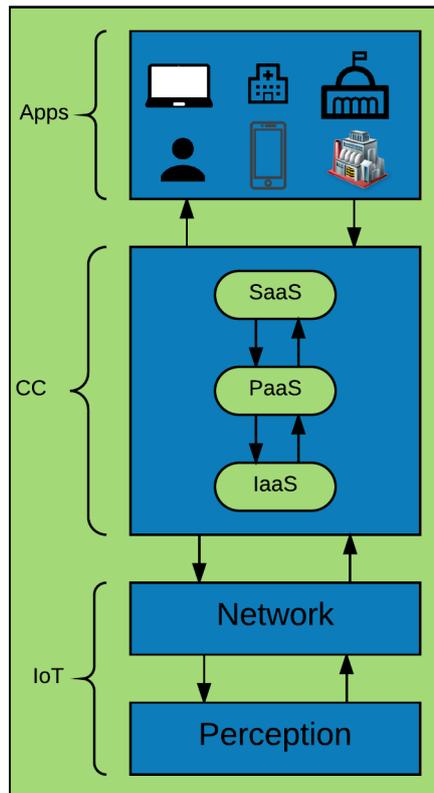


Figura 3: Arquitectura genérica para CloudIoT.

Además, la convergencia entre IoT y Cloud Computing generará nuevos servicios que se describen a continuación [2]:

- Sensing as a Service (SaaS): Proveyendo acceso ubicuo a los datos de los sensores.
- Sensing and Actuation as a Service (SAaaS): Implementación de lógica de control automático en la nube.
- Sensor Event as a Service (SEaaS): Servicio de envío de mensajes por eventos de sensores.
- Sensor as a Service (SenaaS): Gestión ubicua de sensores remotos.
- DataBase as a Service (DBaaS): Gestión ubicua de Base de Datos.
- Data as a Service (DaaS): Acceso ubicuo de todo tipo de datos.
- Video Surveillance as a Service (VSaaS): Acceso ubicuo de análisis complejo de video.

### 2.3.1 Ventajas de la convergencia entre IoT y Cloud Computing

La exitosa convergencia entre IoT y Cloud Computing desarrollará una amplio espectro de nuevas posibilidades, de las cuales se especifican las más importantes:

- Capacidad de Almacenamiento: IoT maneja gran cantidad de objetos y éstos, a su vez generan grandes volúmenes de información. Aquí es donde el poder de la nube puede aportar positivamente con sus casi ilimitados

recursos de almacenamiento además de proveer un trato homogéneo a los datos recibidos de diferentes sensores a través de APIs [13].

- Capacidad de Procesamiento: La deficiencia en la capacidad de procesamiento en los objetos puede ser complementada por la nube. Con la capacidad de computación en la nube es posible implementar complejos algoritmos de Big Data y así generar todo un ecosistema de nuevas soluciones de mercado aplicable tanto a la industria como al consumidor en general [2].
- Recursos de Comunicación: Al estar IoT y Cloud Computing basado en Internet se facilita la gestión, rastreo y conexión de objetos en tiempo real y desde cualquier lugar [14], lo cual minimiza costos de inversión en infraestructura dedicada.
- Nuevas y mejores Prestaciones: En IoT debido a la baja capacidad de computación y de almacenamiento no es posible garantizar que prestaciones como alta disponibilidad, eficiencia, seguridad, confiabilidad e interoperabilidad sean del todo alcanzadas [2]. Pero con la nube se puede generar un nuevo entorno donde estas prestaciones sean alcanzadas gracias al poder de computación propia de *Cloud Computing*.

### 2.3.2 Nuevos Modelos de Negocio

Gracias a las ventajas anteriormente descritas se pueden generar nuevos modelos de negocios, e incluso potenciar los actuales dando valor agregado a sus productos y servicios, los cuales los detallamos a continuación:

- Salud: Las soluciones en el campo de Salud actuales y futuras tendrán un repunte significativo al aumentar el número, variedad y grado de miniaturización de los sensores. Una tecnología prometedora son las redes de área corporal (*Wireless Body Area Network*, WBAN). Éstas permiten que los sensores se adhieran a la ropa, al cuerpo humano o incluso sean implantados bajo la piel. Dichos dispositivos son capaces de establecer enlaces de comunicaciones inalámbricos. Una red WBAN permite la monitorización de los estados físicos y de salud de los pacientes, buscando que la intrusión con las actividades de estos sea mínima [15]. Complejos algoritmos en la nube pueden ser aplicados a toda la información generada por los sensores, además de garantizar que los resultados sean confiables, seguros y con alta disponibilidad. Las soluciones pueden ir desde monitoreo de la actividad cardiaca y respiratoria de un paciente o grupo de pacientes, la detección temprana de anomalías, hasta incluso que toda una infraestructura hospitalaria esté dotada con sensores para una fácil y rápida gestión de la información.
- Ciudades Inteligentes: En la actualidad, las redes de sensores han tenido una fuerte penetración en soluciones para *Smart Cities* como el monitoreo de medio ambiente, tráfico vehicular, servicio de parking [3], etc. Al existir un ecosistema heterogéneo de tecnologías de redes inalámbricas, la nube puede proporcionar un middleware entre IoT y las aplicaciones, dando como resultado la posibilidad de que diferentes soluciones en IoT pueden converger en un mismo sistema de monitoreo en tiempo real y con capacidades de computación ubicua.

- Coches inteligentes y movilidad: La unión de IoT y *Cloud Computing* en el campo de coches inteligentes permitirá la innovación en soluciones que permitan mejorar la movilidad. Actualmente existe un gran número de sensores a bordo de un vehículo. Toda esta información puede ser enviada hacia la nube a través de, por ejemplo, redes de sensores vehiculares conocidas como VANETS [16]. El poder de la nube permitirá mejorar la seguridad y eficiencia a través de la detección temprana y prevención de tráfico, así como evitar accidentes, etc.
- Eficiencia energética: La convergencia entre IoT y *Cloud Computing* genera una mejora en el consumo de energía en los objetos. Los sensores solo se encargarán de las tareas de monitoreo y envío de mensajes generados por los diferentes eventos y el poder de la nube analizará la información y tomará las decisiones.
- Industria: Uno de los más prometedores modelos de negocios es el de la industria 4.0. Actualmente existe una infinidad de sensores presentes en la plantas de manufacturación, pero la comunicación en tiempo real, directa y bidireccional entre las máquinas y los sensores depende de soluciones propietarias costosas y no abiertas. IoT y *Cloud Computing* tienen la capacidad de superar estos inconvenientes en la industria, así como proporcionar nuevos servicios con capacidad de computación en tiempo real y en todo lado [6], así como mejorar la productividad y optimizar el manejo de inventario, permitiendo la trazabilidad de productos, desde la planta hasta al cliente y la automatización de tareas [6].

Hasta aquí solo se ha comentado algunos de los muchos nuevos modelos de negocios que ahora se contemplan y es muy probable que en los próximos años otros totalmente nuevo o más específicos surjan. La clave para estos modelos de negocios es que la convergencia entre IoT y *Cloud Computing* sea total, exitosa y sin mayores inconvenientes.

## 2.4 Desafíos y retos del paradigma CloudIoT

Para que el nuevo paradigma de *CloudIoT* pueda tener éxito y ser una tecnología que esté para quedarse, es necesario primero que supere algunos retos. Algunos de estos retos surgen de la naturaleza propia de la convergencia entre IoT y *Cloud Computing* y otros vienen acompañando a estas tecnologías desde la concepción de las mismas. Según [17] y [18], las siguientes capacidades deben ser alcanzadas para garantizar confianza y eficiencia en los servicios de *CloudIoT*: seguridad, privacidad, confiabilidad, disponibilidad, portabilidad e interoperabilidad semántica. Además de lo anterior hay algunas capacidades que han resultado ser un desafío en la literatura reciente según [2]:

- Prestación de servicios: La manera en cómo los servicios de *Cloud Computing* que tradicionalmente se proveen de manera vertical debe tener un nuevo enfoque y ser aprovechado por los nuevos modelos de servicios de *CloudIoT* que proveen eficiencia, escalabilidad y entrega de servicios IoT fácilmente extensibles [19].

- Protocolos de comunicación y red: IoT por el momento está compuesta por todo un conjunto heterogéneo de protocolos y tecnologías de comunicación inalámbricas. Esto supone un obstáculo al momento de implementar soluciones a gran escala y de bajo coste.
- Big Data: Como se ha mencionado anteriormente, el número de dispositivos conectado a internet crece exponencialmente. Todo este conjunto de objetos genera cantidades inmensas de información. El poder de la nube tiene la capacidad de analizar y almacenar estos datos. La característica de ubicuidad de los objetos y sensores hace necesario el uso de servicios escalables en la nube [20]. El reto a superar es el manejo eficiente de esta información y la creación de nuevas aplicaciones y servicios que obtengan provecho de las misma.
- Red de Sensores: Los sensores, según [21], serán los principales habilitadores de IoT. Actualmente hay en el mercado sensores de casi todo tipo y cada día se desarrollan nuevos tipos de sensores que generan datos de diferentes tipos. El reto a superar, según [22], es el oportuno procesamiento del enorme y continuo flujo de datos de los sensores, sujeto a las restricciones de consumo de energía y eficiencia de los protocolo de red .
- Calidad de Servicio (QoS): La calidad de servicio siempre ha sido un parámetro ha tener en cuenta en Internet. Ahora con IoT este parámetro se vuelve mas crucial a medida que la cantidad y tipo de información se incrementa. La información debe estar disponible y ser confiable en todo momento. QoS debería ser medido en términos de ancho de banda, retardo, jitter, y porcentaje de paquetes perdidos [9].
- Seguridad y Privacidad: La seguridad y privacidad siempre han estado presentes tanto en IoT como en Cloud Computing. Ahora con la computación ubicua se vuelve un desafío a tener en cuenta. CloudIoT debería proveer las herramientas para que la información cumpla con los requisitos indispensables de seguridad de la información como son: confiabilidad, integridad y disponibilidad. Además, debe contar con las políticas necesarias para que los datos sean solo conocidos por los usuarios permitidos.
- Implementación y desarrollo: Uno de los desafíos a tener en cuenta en el paradigma de CloudIoT es el relacionado a los costos de los servicios bajo el modelo *pay-as-you-use* o *pay-as-you-go*. Se busca que las soluciones y aplicaciones desarrolladas bajo este modelo sean de bajo costo y que su implementación sea relativamente fácil. Con esto se alcanzaría un espacio idóneo para que los desarrolladores, clientes y empresas empiecen a usar CloudIoT masivamente.

## CAPITULO III: SERVICIOS EN LA NUBE PARA IOT

En los últimos años se ha visto un crecimiento en el número de servicios y plataformas en la nube para IoT tanto públicos como privados. Estos tratan de servir como puente entre los objetos y la nube haciendo uso de *middlewares* y de API's hacia las aplicaciones [2]. Es necesario mencionar que las compañías propietarias de estos servicios ofrecen servicios adicionales en la nube, pero en este trabajo de fin de máster solo nos centraremos en aquellos relacionados con Internet of Things. En esta sección se tratará de explicar de manera resumida y concisa la historia, características principales, arquitectura, casos de éxito y el modelo de negocio de los más prometedores servicios en la nube para IoT que existen actualmente. Los servicios seleccionados para su análisis son los siguientes:

- Sofia2
- Fiware
- Watson IoT de IBM
- Artik Cloud de Samsung
- Azure IoT Suite de Microsoft

La elección de los servicios Fiware y Sofia2 se basa en el hecho de que son iniciativas europeas que han tenido gran impacto en el sector académico y empresarial. Siendo la primera una iniciativa de la Unión Europea y de acceso libre que se espera que sea la arquitectura estándar de el denominado Internet del Futuro [23]. Sofia2 en cambio nació como una iniciativa privada que busca ser una solución de infraestructura para el desarrollo de las Smart Cities con capacidades empresariales [24]. Ambas han sido implementadas masivamente tanto por el sector académico con fines de investigación y en soluciones empresariales para clientes de toda índole.

Para la elección de los servicios de IBM, Microsoft y Samsung se tuvo en cuenta que estas empresas han ingresado con mucha fuerza en el mercado de la computación en la nube no solo ofreciendo servicios si no también infraestructura que va desde almacenamiento de ficheros hasta aplicaciones complejas de inteligencia artificial y Big Data. Además de que ambas empresas por su nombre, infraestructura y trayectoria han sido la elección de numerosas soluciones para IoT en el sector empresarial de alta tecnología.

### 3.1 SOFIA2

#### 3.1.1 Breve Historia

Según se describe en [25] Sofia2 nace de un proyecto Europeo de investigación y desarrollo denominado SOFIA que es el acrónimo de *SMART OBJECTS FOR INTELLIGENT APPLICATIONS*. SOFIA es el resultado de un proyecto de investigación denominado Artemis, de tres años, en el que participaron varios partners de diferentes países de la Unión Europea entre los que destacan Nokia, Philips, Fiat, Acciona e Indra. Entre sus principales características tenemos que Sofia es *open-source*, multiplataforma, multilenguaje e independiente de las

comunicaciones. El propósito de Sofia es lograr la interoperabilidad entre diferentes aplicaciones que comparten conceptos semánticos. Una vez finalizada la investigación Artemis, Indra [26] tomó la plataforma SOFIA original y la desarrolló bajo enfoque empresarial dando como resultado Sofia2.

### 3.1.2 Conceptos de Sofia2

En [27] se describe a Sofia2 como la unión de un middleware y repositorio capaz de procesar miles de eventos por segundo, con almacenamiento en tiempo real y Big Data, con análisis, modelado visual y reglas integradas, multiplataforma con interfaces multiprotocolo y todo operable desde una Consola Web. Todo esto permite que diferentes dispositivos IoT heterogéneos puedan convivir en un mismo ecosistema a través del SDK y las API's que la plataforma proporciona. Según [28] Sofia2 está centrada en ofrecer servicios de IoT en la nube, donde pueden implementarse aplicaciones (con la información proporcionada por los sensores) que la procesen y la ponga a disposición de los clientes, ver figura 4.

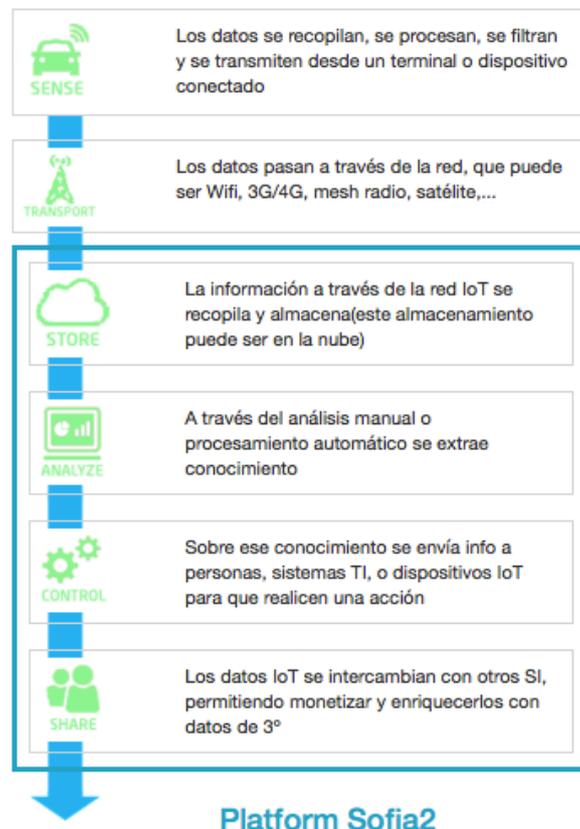


Figura 4: Encuadre de Sofia2 en el flujo típico de IoT.

Dentro de la plataforma Sofia2 se manejan cuatro conceptos: *Smart Space*, *Semantic Information Broker*, *Knowledge Processor*, *Smart Space Access Protocol*. Estos cuatro conceptos se puede observar en la figura 5 [25].

- **Smart Space:** Entorno en el cual las aplicaciones se comunican entre sí para proporcionar características más elaboradas. Lo componen los diferentes SIB.

- **Semantic Information Broker (SIB):** Núcleo de la plataforma que actúa como bus intercambiador recibiendo, procesando y almacenando toda la información de las aplicaciones conectadas a Sofia2. Para el intercambio de la información Sofia2 usa JSON (SSAP).
- **Knowledge Processor (KP):** Son las aplicaciones que, gracias al SIB, pueden comunicarse con otras aplicaciones en el Smart Space. Se pueden implementar en diversos lenguajes como Java, Python, C/C++, etc. Se definen tres tipos de KPs:
  - Productor: Solo envía información hacia el SIB.
  - Consumidor: Solo recibe información desde el SIB.
  - Prosumer: Envía y recibe información del SIB.
- **Smart Space Access Protocol (SSAP):** Protocolo de mensajería lógico para comunicar los SIB y los KP. Se admiten tanto implementaciones XML como JSON. El primero JSON es el más eficiente ya que consume menor ancho de banda frente a XML.

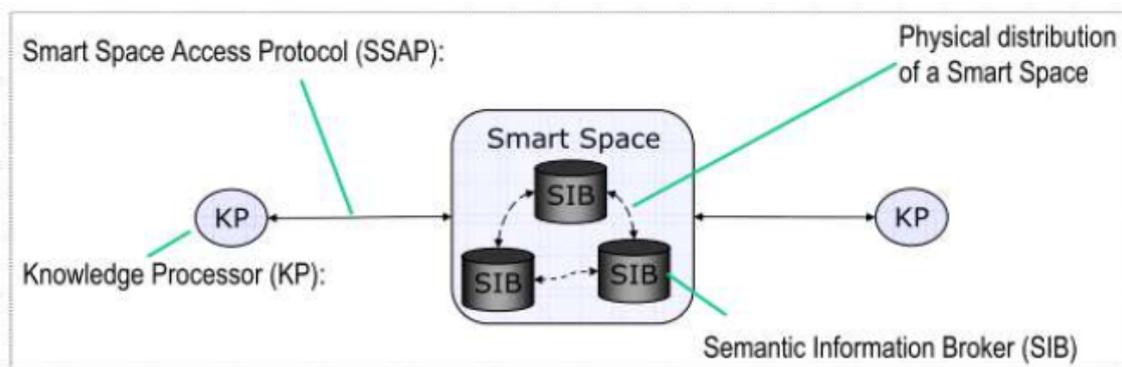


Figura 5: Diagrama de comunicación entre los diferentes conceptos de Sofia2.

Un concepto adicional que maneja Sofia2 son las denominadas ontologías, que son las descripciones semánticas que representan las entidades del sistema las cuales se reflejan en JSON. Por ejemplo un sensor, que es una ontología, se representaría según se muestra en la figura 6.

```

1  |"SensorTemperatura": {
2  |    "coordenadaGps": {
3  |      "altitud": 0,
4  |      "latitud": 40.512274,
5  |      "longitud": -3.675679
6  |    },
7  |    "identificador": "S_Temperatura_00001", "medida": 19,
8  |    "timestamp": 1373887443001,
9  |    "unidad": "C"
10 |  }
11 | },

```

Figura 6: Representación en JSON de una ontología.

### 3.1.3 Características de Sofia2

Entre las principales características de Sofia2 se desatacan [28]:

- Seguridad Integrada: En todos los niveles y elementos de la arquitectura.

- Multi-dispositivo: Omnicanalidad de la plataforma.
- Interoperabilidad: Capacidad de operar con diversas soluciones.
- UI + API Gestión centralizada: Panel de Control Centralizado.
- Enfoque Big Data: Ingesta, análisis y procesamiento Big Data.
- On Premise & On Cloud: Instalado en la infraestructura del cliente o en la nube.
- Personalizable y extensible: Adaptable a la necesidades.
- Visión Semántica: Modelado de la semántica visualmente.
- Open Source & Commercial: Versiones comerciales con soporte o abiertas sin soporte.

### 3.1.4 Arquitectura de Sofia2

Sofia2 cuenta actualmente con tres versiones: la Base Edition, IoT Edition y la Advanced Edition. Cada una de ellas ofrece sus propias características y funcionalidades que se detallarán a continuación:

- **Base Edition:** Esta versión es ideal para la implementación de aplicaciones que hagan uso de información generada por sensores. Entre sus principales características tenemos:
  - Consola centralizada para gestión de aplicación y módulos.
  - Ontologías y modelado asistido: desde Excel, wizard, visualmente...
  - APIs multilenguaje
  - Reglas
  - Comunicaciones bidireccionales REST, MQTT, JMS, WebSockets.
  - Base Datos NoSQL (MongoDB) o relacional como BDTR
  - Dashboards e Informes.

La arquitectura de esta versión se puede observar en la figura 7 tomado de [29] .

- **IoT Edition:** Versión diseñada especialmente para las características propias de IoT, como es la gestión de gran cantidad de datos en poco tiempo. Entre sus principales características tenemos:
  - Integración dispositivos y redes sociales.
  - Infraestructura Big Data sobre Hadoop como BDH.
  - API Manager para publicación de información como APIS REST.
  - Notebooks Web para hacer analítica interactiva.
  - Migración de BDTR a BDH automática y configurable.

La arquitectura de esta versión la podemos observar en la figura 8 tomado de [29] .

- **Advanced Analytics Edition:** Es la versión mas completa de Sofia2. Es una extensión del IoT Edition que añade el modulo de Analytics of Things para analizar la información generada por los sensores. Entre sus principales características tenemos:
  - Integración de cualquier fuente de datos de forma visual y asistida.
  - Módulo Machine Learning integrado que permite lanzar algoritmos.

- Acceso a la información través de interfaces ODBC y JDBC.

En la figura 9 se puede observar la arquitectura de esta versión tomado de [29].

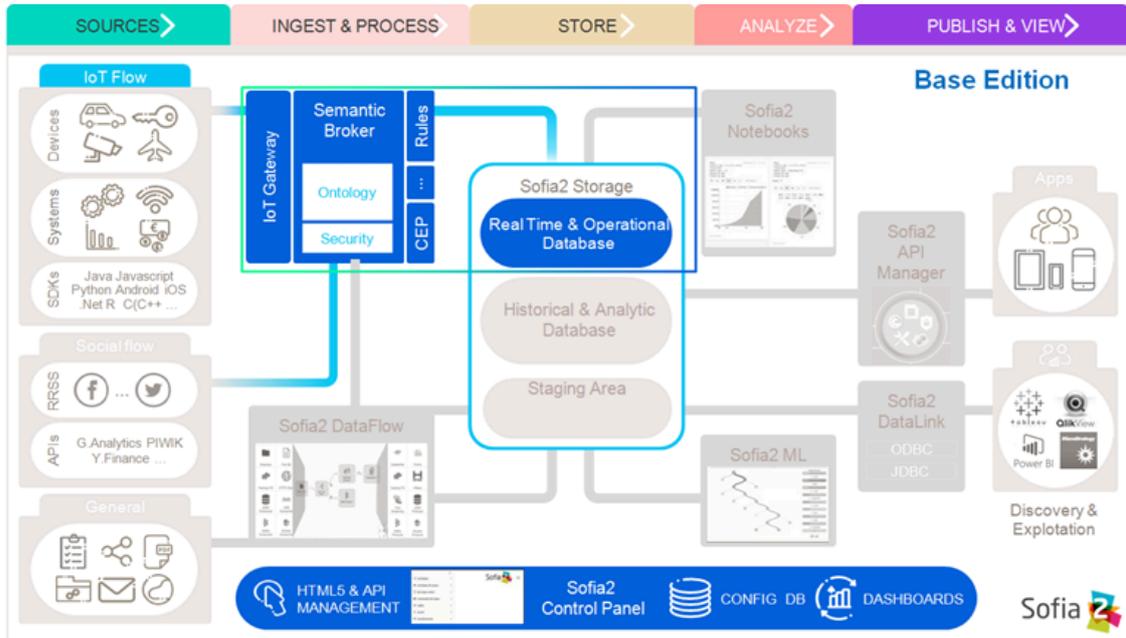


Figura 7: Arquitectura de la versión Base Edition de Sofia2.

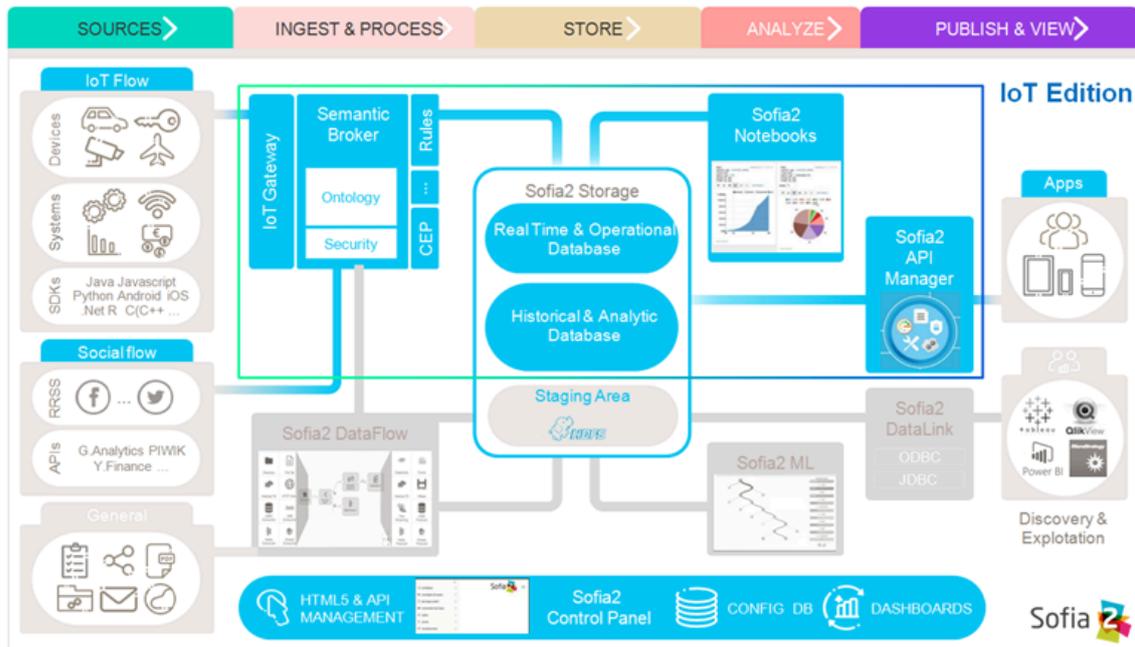


Figura 8: Arquitectura de la versión IoT Edition de Sofia2.

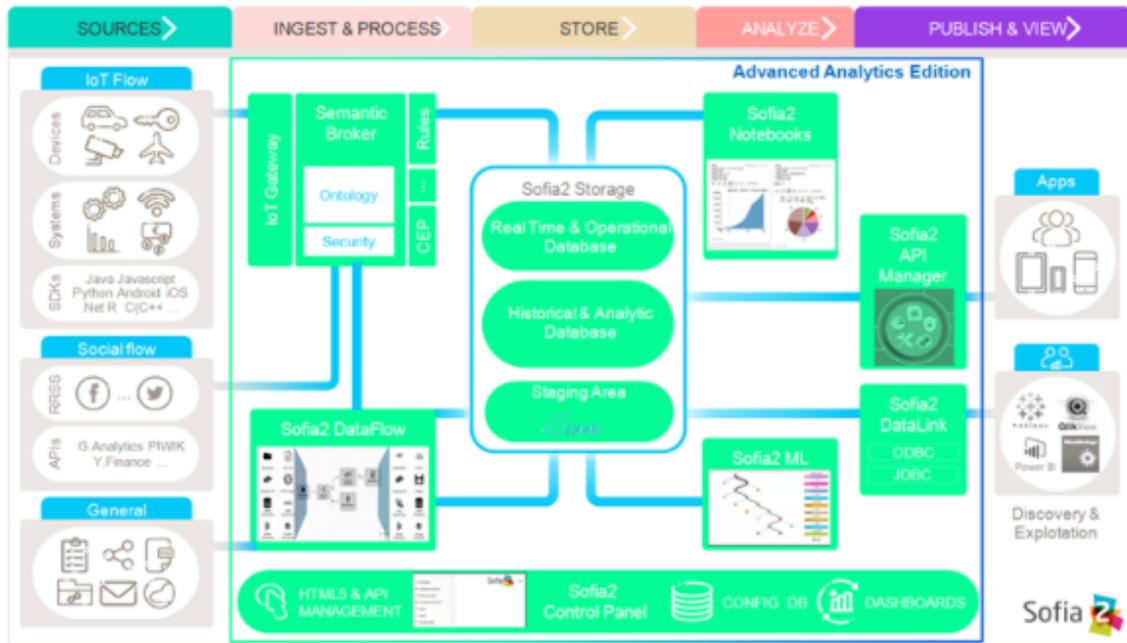


Figura 9: Arquitectura de la version Advance Edition de Sofia2.

### 3.1.5 Modelo de negocio en Sofia2

Sofia2 brinda tres modelos de implementación de su plataforma: Cloud Labs o PoC, OnPremise y el modelo PaaS-SaaS Cloud.

- **CloudLab o PoC:** Modelo gratuito localizado en la nube ideal para experimentación e implementación de aplicaciones piloto para usuarios que quieren probar la plataforma. Infraestructura proporcionada por Indra.
- **On Premise:** Modelo de pago donde una plataforma personalizada de Sofia2 se instala en los CPD de los clientes.
- **PaaS-SaaS Cloud:** Servicio disponible en la nube bajo el modelo pay-as-you-use. Este servicio puede ser o no operado por Indra.

En la figura 10 tomada de [30] se muestra detalladamente las características de cada modelo de negocios en la plataforma Sofia2.

### 3.1.6 Aplicaciones con Sofia2

Sofia2 ofrece al usuario varias aplicaciones listas para usar y las herramientas necesarias para que el desarrollador pueda implementar sus propias aplicaciones.

- *Dashboard:* Aplicación donde se puede implementar *widgets* ya existentes de Sofia2 o desarrollados por el usuario que muestren información de las propiedades de las diferentes ontologías. Es ideal para mostrar información de sensores.

MODELO COMERCIAL				
	Cloud Labs o PoC		On Premise	Cloud (SaaS)
Modalidad de Licencia	Gratis ( <a href="http://sofia.com">http://sofia.com</a> )	Fijo (por mes)	Module x Core (Anual + mantenimiento)	Mensajes (miles) & Almacenamiento (TB)
Soporte	Correo Electrónico & web	8x5 incluido	8x5 incluido 24x7 extendido	8x5 incluido 24x7 extendido
Nuevas versiones, updates, fixes,...	Incluido	Incluido	Incluido	Incluido
SSPP	Elección	Min 50 FTEs	Elección	Elección
Alta Disponibilidad	No HA	No HA	HA	HA
SLA	no SLA	no SLA	No incluido	SLA 99% incluido 99.5% extendido
Entorno Compartido	Si	No	No	No
Infraestructura	Compartida	Dedicada (fija)	Dedicada (configurable)	Dedicada (a demanda)
Funcionalidades	Todo menos: - Acceso directo al sistema de almacenamiento - Capacidades de administración - Documentación premium	Todo	Todo	Todo

Figura 10: Modelo de Negocio de la plataforma Sofia2.

- *Social Media Analysis*: Sofia2 ofrece la posibilidad de realizar seguimiento de la actividad de usuarios en redes sociales como análisis de actividad, palabras más usadas, horario de más tráfico, etc.
- *Storing*: Almacenamiento de información de las ontologías en base de datos ya sean estas históricas o no.
- *Modulo Machine Learning*: Permite lanzar algoritmos, crear modelos, etc. con la información de las ontologías
- Infraestructura Big Data y Analítica Interactiva.

### 3.1.7 Recursos para el desarrollador

Sofia2 cuenta con todo un conjunto de documentación, tutoriales, API's, etc. donde los desarrolladores pueden obtener información acerca de cómo desarrollar sus propias aplicaciones. Por ejemplo, Sofia2 cuenta con soporte para lenguajes tan variados como Java, JavaScript, Android, Swift (IOS), Python, Node.js, C/C++, Arduino, etc. En cada una de ellas se encuentran las herramientas necesarias para poder interactuar con cada una de las ontologías, los KP y las bases de datos.

### 3.1.8 Casos de Uso

La plataforma Sofia2 ha sido usada en la implementación de varios proyectos IoT europeos por parte de instituciones tanto publicas como privadas [31]. A continuación se resumen algunos proyectos donde se emplea Sofia2.

#### Smart Cities Coruña:

Este proyecto liderado por el Ayuntamiento de Coruña e INDRA permite que los usuarios por medio de medios electrónicos puedan acceder a la información de

los sensores de la ciudad, así como también poder realizar procesos administrativos y de servicios. Sofia2 como plataforma ofrece información centralizada y sistema de control que permite mejoras en la gestión de la ciudad, personalización de servicios, sostenibilidad y competitividad.

#### Smart Energy ENDESA:

En este proyecto Sofia2 actúa como plataforma de adquisición de datos y control de dispositivos ubicados en el cliente. La empresa ENDESA se encarga de la comercialización de esta solución, además de proveer dispositivos que miden el consumo de energía y que son fácilmente integrables con Sofia2. Cerca de 10000 dispositivos envían información a Sofia2 donde se almacena y se monitorea. EDESA ofrece a los usuarios la posibilidad de consultar el consumo a través de una aplicación móvil.

#### Smart Health Zurich:

En este proyecto a través de dispositivos *wearables* se busca monitorear el estado de salud de los clientes de seguros médicos. La información está disponible tanto para el usuario como para la empresa en una plataforma web y móvil. Pero no solo la información del dispositivo del *wearable* se envía a Sofia2, sino que además es posible realizar la integración con la información de las redes sociales de los clientes y así aplicar reglas de Big Data.

#### Smart Health SERVICIO GALEGO DE SAÚDE:

Este proyecto liderado por TELEVES e INDRA para el *Servicio Gallego de Salud* consiste en un “concentrador inteligente”, desarrollado y fabricado por TELEVES, conectado de manera interrumpida a Sofia2 [31]. Sofia2 actúa como plataforma mediadora entre los diferentes sensores en el hospital ofreciendo monitoreo de diversos parámetros así como comunicación con los pacientes a través de alarmas, recordatorios, etc.

## **3.2 FIWARE**

### **3.2.1 Breve Historia**

Fiware nace como iniciativa de la Unión Europea a través de la FI-PPP (Future Internet Public Private Partnership) que tiene como objetivo avanzar en la competitividad de Europa en las tecnologías de Internet del Futuro y apoyar la aparición de mejores futuras aplicaciones de relevancia pública y de carácter social [32]. En el año 2012 las empresas Telefónica, Orange, Enginerring, y Atos empezaron un proyecto para el desarrollo de estándares de Fiware para Smart Cities [33].

### **3.2.2 Conceptos de Fiware**

Fiware es una arquitectura que permite construir un ecosistema abierto y sostenible en torno a estándares de plataforma de software públicos, libres de

derechos y basados en la implementación que facilitarán el desarrollo de nuevas aplicaciones inteligentes en múltiples sectores [34]. Fiware maneja el concepto de GE (Generic Enabler) que es una librería de servicios de propósito general que cubren funcionalidades comunes en campos como seguridad, almacenamiento, cloud, data context e Internet of Things. Estos servicios están disponibles a través de API'S disponibles para que los desarrolladores las puedan adoptar en la construcción de aplicaciones. Cada GE puede ser considerado un bloque que contiene un conjunto de API's para la construcción de aplicaciones inteligentes. Estos GE están divididos en 7 capítulos técnicos:

- **Cloud Hosting:** Gestión del modelo IaaS/PaaS, Monitoreo, Políticas de Gestión, Portal de gestión de políticas y herramientas para servicios en la nube, etc.
- **Data/Context Management:** Manejo de datos a larga escala y su respectiva transformación en conocimiento, Análisis de Big Data, Manejo de comunicaciones entre diferentes entidades, Manejo y procesamiento de eventos masivos, etc.
- **Interfaces to Network and Devices:** Acceso desde cualquier lugar usando interfaces de red.
- **Advanced Web-based User Interfaces:** Gráficos 3D para la web, Aplicaciones 3D colaborativas, Infraestructura para la interacción de con objetos reales, etc.
- **Security:** Gestión de la identidad, Control de Acceso, Análisis y Monitorización de Seguridad.
- **Internet Of Things:** Conexión de aplicaciones al mundo físico, descubrimientos de sensores, Administrador de configuración, Manejo de Datos de Gateway, etc.
- **Applications/Services and Data Delivery:** Alcanzar usuarios objetivos para monetizar aplicaciones y servicios.

Ahondar en cada una de las características de los GE va mas allá de este trabajo de fin de master por lo que solo se hablara de las GE usados en el campo de IoT como son el Orion Context Broker y el IDAS Agent IoT.

### 3.2.2.1 Orion Context Broker

Este GE es una implementación de Publicación/Suscripción que proporciona interfaces NGSI9 y NGSI10 con las cuales los clientes pueden realizar las siguientes operaciones [35]:

- Registro de aplicaciones productoras de información de contexto, como por ejemplo un sensor de temperatura en un cuarto.
- Actualización de la información contextual, por ejemplo el envío de la temperatura actualizada por parte del sensor.
- Notificaciones cuando ocurran cambios en la información contextual.
- Consultas de la información contextual. El Orion Context Broker almacena la ultima actualización de la información contextual.

La información contextual se representa mediante valores asignados a atributos que caracterizan a aquellas entidades relevantes para una aplicación. En la figura 11, basada en [36], podemos observar cómo el Context Broker puede modelar y obtener acceso a la información contextual de manera independiente a la fuente de información.

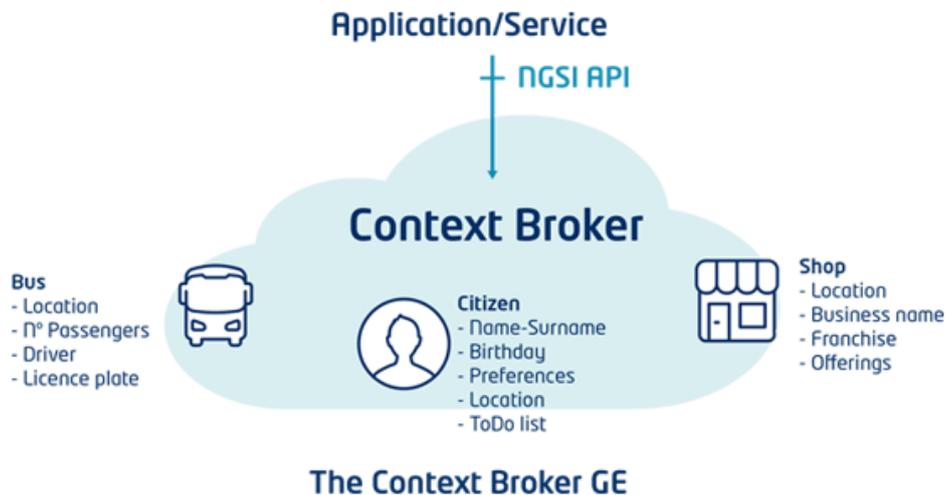


Figura 11: Context Broker de Fiware.

### 3.2.2.2 IDAS IoT Agent

Este GE provee de las siguientes opciones [35]:

- REST API para desarrolladores de aplicaciones M2M.
- API de comunicación para dispositivos como sensores, actuadores y gateway.
- Interfaz NGSI9 y NGSI10 para comunicación con brokers NGSI, implementado por el IoT Agent.
- Herramienta desarrollo FIGWAY, a disposición de desarrolladores para ser usados en dispositivos embebidos.

Según [37] IDAS actúa como intermediario entre el heterogéneo ecosistema de sensores y Orion Context Broker. Este último permite a los desarrolladores acceder de manera fácil y simple a los atributos de las entidades que representan los objetos reales, además de ofrecer la posibilidad de enviar órdenes hacia los dispositivos para llevar a cabo determinadas acciones. Todo lo anterior se representa en la figura 12.

IDAS soporta varios protocolos IoT con una arquitectura modular denominada "IoT Agents" [37], esto es, cada IoT Agent pueden manejar un protocolo independientemente del resto. Actualmente IDAS tiene soporte para los protocolos Ultralight2.0, MQTT y LWM2M. Esto último convierte a IDAS en un servicio muy flexible ya que puede instalarse en un dispositivo embebido con soporte Linux e inmediatamente comenzar a enviar los atributos de los objetos hacia el *Context Broker*.

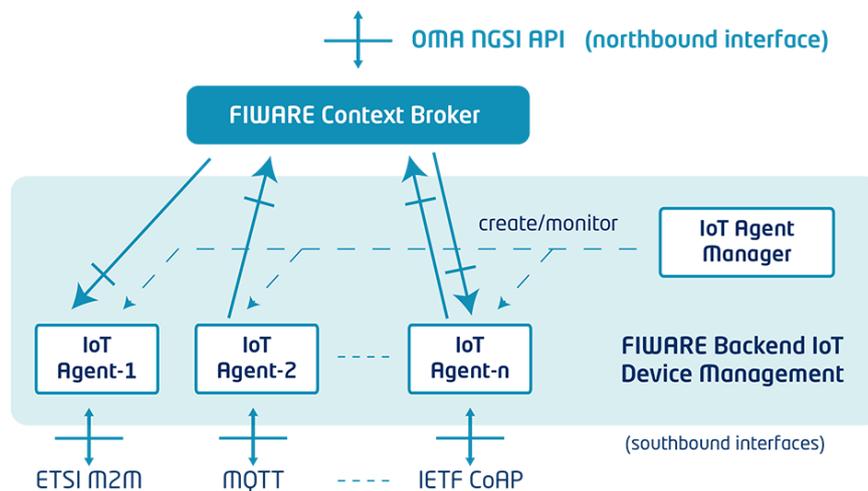


Figura 12: IoT Agent IDAS de Fiware.

### 3.2.2.3 Protocolo Ultralight2.0

Este protocolo ha sido definido por la comunidad Fiware y su evolución es impulsada por la misma comunidad. En [38] se lo define como un protocolo basado en texto ligero destinado a dispositivos restringidos y comunicaciones donde el ancho de banda y la memoria del dispositivo pueden ser recursos limitados. Puede ser usado con los protocolos de aplicación HTTP y de transporte MQTT.

### 3.2.3 Arquitectura de Fiware

La arquitectura de Fiware por si sola es muy extensa y vas mas allá del objetivo de este trabajo de fin de máster por lo que solo se hará énfasis en la arquitectura de IoT que la propia Fiware proporciona para motivos académicos [39]. En la figura 13 se puede observar esta arquitectura donde tenemos el *IoT Device Management* (IDAS), el *Orion Context Broker*, el IoT Gateway y las aplicaciones. El *Gateway Logic GE* es un componente opcional que proporciona funciones de gestión de la IoT Edge API y actúa como puerta de enlace entre el API y las funciones.

### 3.2.4 Modelo de Negocio en Fiware

Como se ha mencionado anteriormente, Fiware es totalmente libre. Los GE y API pueden ser usados de manera libre y sin restricciones por los desarrolladores para la construcción de sus aplicaciones, incluso Fiware provee de servicios en la nube donde alojar estos GE y así puedan ser accesibles vía internet. Esto es de suma importancia en la expansión de Fiware como plataforma universal para aplicaciones inteligentes en IoT.

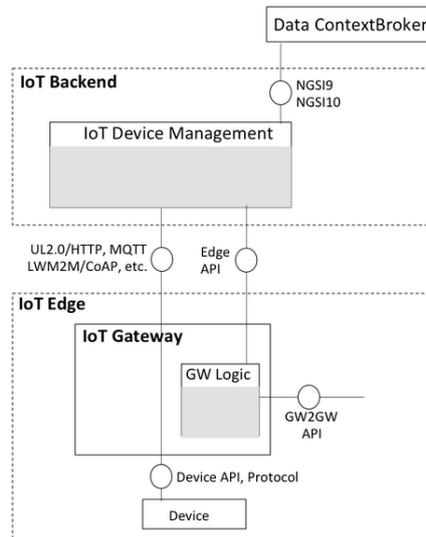


Figura 13: Arquitectura IoT de Fiware.

### 3.2.5 Recursos para el desarrollador

Fiware, como plataforma libre, provee un ingente número de recursos que van desde documentación académica, tutoriales, API's, y foros donde los desarrolladores puedan indagar cómo usar los GE en sus diferentes aplicaciones. Fiware ofrece soporte para lenguajes como Python, Java, C/C++, Node.js, HTML5, etc.

### 3.2.6 Casos de Uso

Muchos proyectos y emprendimientos han elegido a Fiware como plataforma IoT para el desarrollo de sus soluciones. A continuación se listan las soluciones más destacables que hacen uso de Fiware [40].

#### Torino Wireless Smart City:

Este proyecto de Smart City nacido en 2003 en la ciudad de Torino provee soluciones en movilidad, energía, gobierno electrónico, inclusión social, vida y salud. La aplicación Fiware desarrollada se enfoca en los problemas de seguridad percibida por los ciudadanos. La aplicación recoge las advertencias y quejas que cada centro de contacto policial hace acerca de disturbios, comportamientos sospechosos y daños a la propiedad pública. La tecnología Fiware permite organizar y analizar los datos proveyendo un tablero interactivo con las actividades críticas geo-localizadas en un mapa. También permite enviar notificaciones en tiempo real a la policía y proporciona estadísticas actualizadas de las actividades críticas.

#### Agricolus:

*TeamDev* es un SME italiano que ha desarrollado el servicio Agricolus que tiene como objetivo ayudar a agricultores a incrementar su productividad y ahorrar tiempo disminuyendo la contaminación ambiental. Este servicio hace uso de la

tecnología Fiware para recolectar y organizar la información de diferentes fuentes en un cultivo como: sensores, satélites, drones de inspección de campo, maquinaria, dispositivos móviles, estaciones meteorológicas y mas. A estos datos recolectados se le aplican técnicas de Big Data que proporcionan información valiosa sobre el comportamiento actual y futuro de los cultivos a sus clientes para que ellos puedan tomar decisiones correctas en la administración de sus cultivos.

#### Any Solution:

Este SME español desarrolla metodologías y proyectos estratégicos en diferentes campos, siendo uno de éstos las *Smart Cities*. Su principal proyecto llamado *SmartLock* proporciona a usuarios y organizaciones el acceso a una aplicación para controlar quién y cuándo determinada persona puede acceder a un recinto (hogar u oficina). Desarrollar la aplicación con Fiware les ha permitido controlar y monitorizar los diferentes sensores instalados en un hogar u oficina así como de mecanismos de autenticación y notificación de actividades en los mismos.

#### Aplicación “Improve your City”:

Esta aplicación desarrollada en Madrid permite una comunicación directa de los ciudadanos con el ayuntamiento y los servicios públicos. Los ciudadanos haciendo uso de sus dispositivos móviles pueden convertirse en sensores de la ciudad. Con esto se genera información que ayuda a manejar eficientemente los recursos de una ciudad. La tecnología Fiware provee de herramientas para el contexto de la información así como su almacenamiento y análisis.

### **3.3 WATSON IoT**

La plataforma Watson IoT pertenece al conjunto de soluciones provista por IBM través de su programa Bluemix. Esta plataforma permite administrar dispositivos IoT así como el almacenamiento y el acceso a la información de dichos dispositivos. Con esta información y las herramientas propias de IBM es posible construir aplicaciones analíticas, paneles de visualización y aplicaciones IoT móviles [41].

#### **3.3.1 Conceptos de Watson IoT**

Dentro de la plataforma Watson IoT se manejan los siguientes conceptos [41]:

- **Organización:** Una organización es el conjunto de aplicaciones, dispositivos y servicios pertenecientes a un solo administrador en la plataforma Watson IoT. Un administrador puede manejar varias organizaciones pero por motivos de seguridad la información de una organización no es accesible de manera directa por otra organización. Una organización puede crear una aplicación que ponga a disposición la información para que otras aplicaciones de diferentes organizaciones puedan tener acceso a ella.

- **Dispositivo:** Un dispositivo es cualquier elemento que pueda conectarse a internet. Estos dispositivos no pueden comunicarse con otros dispositivos, pero sí enviar y recibir información de las aplicaciones. Estos dispositivos manejan un token único para su identificación y acceso a la plataforma Watson IoT.
- **Gateways:** Un gateway es un dispositivo que sirve como punto de acceso a otros dispositivos que no pueden conectarse directamente a internet.
- **Aplicaciones:** Se define como aplicación a cualquier entidad que tenga conexión a Internet y pueda interactuar con la información y el comportamiento de los dispositivos. Las aplicaciones se identifican y acceden a la plataforma Watson IoT haciendo uso de un API key.
- **Eventos:** Son los mensajes que los dispositivos o gateways envían a la plataforma Watson IoT. Las aplicaciones pueden acceder a la información relacionado con estos eventos.
- **Orden:** Una orden es el mecanismo con que las aplicaciones se comunican con los dispositivos.

### 3.3.2 Características de Watson IoT

La plataforma Watson IoT se enfoca en las siguientes áreas [42]:

- **Conexión:** La conexión de dispositivos es el punto fuerte de la plataforma IoT. No solo un dispositivo o gateway puede enviar o recibir información de Watson IoT sino que también se puede implementar en los dispositivos compatibles un *Agente de gestión de Dispositivos* que permite realizar acciones tales como el reinicio, las actualizaciones de firmware, etc.
- **Gestión de la información:** La información proporcionada por los dispositivos se puede almacenar, gestionar y transformar en la plataforma Watson IoT. Para ello Watson IoT proporciona el servicio de base de datos para almacenamiento histórico de la información de los sensores.
- **Analítica:** Watson IoT proporciona las herramientas para que la información de los dispositivos pueda ser visualizada en gráficos de tiempo real. Además se puede implementar reglas basadas en la información de los dispositivos para cuando se cumpla cierta condición enviar alertas o tomar acciones previamente determinadas.
- **Gestión de Riesgos:** La seguridad de la conexión entre el dispositivo y la plataforma Watson IoT se basa en un token único e identificador de dispositivo único. Además de esto Watson IoT provee un complemento denominado *Gestión de Riesgos y Seguridad* que provee de mecanismos de seguridad adicionales como certificados de capa de transporte (TSL) .

### 3.3.3 Arquitectura de Watson IoT

La plataforma Watson IoT se comunica con las aplicaciones y dispositivos usando un API y protocolos de comunicación como MQTT y HTTP. Las aplicaciones y servicios dentro de *Bluemix* también se pueden comunicar con la plataforma haciendo uso de los mismos protocolos de comunicación. Esto último

permite una fácil integración con los diversos servicios que IBM tiene disponibles en su programa BLUEMIX como por ejemplo servicios de bases de datos, análisis de Big Data, aplicación de inteligencia artificial, etc. En la figura 14 [41] se muestra el diagrama de bloques de la arquitectura de Watson IoT.

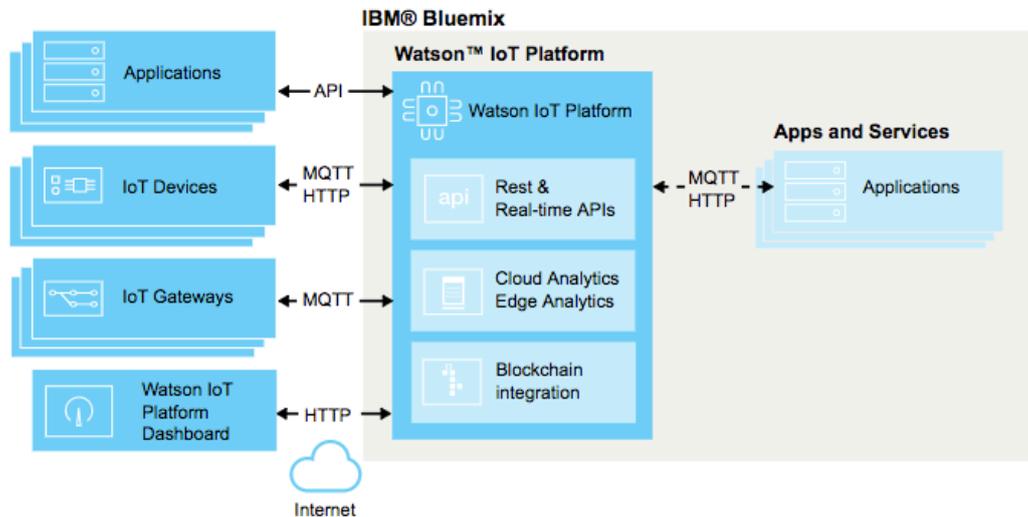


Figura 14: Arquitectura de la plataforma Watson IoT.

### 3.3.4 Modelo de Negocio en Watson IoT

El modelo de negocio de Watson IoT se basa en el modelo *pay-as-you-go*, es decir según el número de servicios o aplicaciones usados y el tamaño de la información almacenada en la plataforma se paga una membresía mensual o anual. Dentro del abanico de productos de Watson IoT también se proporciona el servicio de soporte técnico especializado que es adicional a los servicios anteriormente mencionados.

### 3.3.5 Recursos para el Desarrollador

IBM, como responsable directo de la plataforma Watson IoT ha contribuido en el desarrollo de múltiples recursos y documentación que está disponible online y son accesibles a todos los desarrolladores. Esta documentación está dirigida tanto a desarrolladores experimentados como también a personas carecen de conocimientos básicos en conceptos IoT y desarrollo web. IBM, además, ha hecho esfuerzos para establecer una comunidad de desarrolladores con la creación de foros y blogs donde se pueden consultar dudas sobre la plataforma Watson IoT. Las API's y SDK's que proporciona Watson IoT para el desarrollo de aplicaciones incluyen los lenguajes más comunes como es Java, Node.js, C/C++, Python, C#, etc.

### 3.3.6 Casos de Uso

Watson IoT como plataforma perteneciente a IBM ha recibido el respaldo y confianza de innumerables empresas y proyectos IoT a nivel mundial. A

continuación se enumeran los proyectos que más impacto han tenido usando los servicios de Watson IoT:

#### Visa International Service Association (VISA):

VISA ha establecido una alianza con IBM para permitir que todo tipo de empresas puedan implementar métodos de pagos seguros en cualquier dispositivo conectado a Internet. Por ejemplo un reloj, anillos inteligentes, automóviles, etc.

En el ámbito de los coches inteligentes los conductores podrían recibir alertas si un seguro esta a punto de vencer o si una pieza especifica necesita ser reemplazada. El conductor tendría el control desde su coche de programar una cita con servicio técnico o comprar una pieza nueva. En este nuevo modelo de comercio basado en IoT es fundamental la seguridad de los pagos[43]. Aquí es donde la plataforma de Watson IoT es fundamental para que VISA pueda ofrecer a sus clientes la seguridad de que las transacciones son confiables. Los objetos conectados a Watson IoT podrán usar la tecnología de *Visa Token Security* que reemplaza el método obsoleto del identificador único de tarjetas de crédito.

#### Salas Cognitivas con Watson IoT:

Las empresas privadas HARMAN, JBL y AMX AV que se especializan en micrófonos, altavoces y sistema de control y conmutación respectivamente han desarrollado una solución usando la plataforma Watson IoT y la inteligencia artificial de Watson IBM. Esta solución permite ofrecer a usuarios de hoteles, hospitales, salas de conferencia y similares control total de los dispositivos por ordenes de voz [44].

#### Compañía Ferroviaria Nacional Francesa:

El operador de ferrocarriles francés SNCF actualmente está usando la plataforma Watson IoT para ofrecer a sus clientes mayor eficiencia operativa y mejores estándares de seguridad para sus 13.5 millones de pasajeros diarios [45]. SNCF esta conectando a Watson IoT todo su sistema ferroviario( trenes, vías férreas y estaciones de trenes) para obtener información en tiempo real que permita aumentar la seguridad, disponibilidad y calidad de su servicio de trenes. Por ejemplo, los trenes de nueva generación están equipados con 2000 sensores que envían 70000 datos por mes los cuales son remotamente monitoreados con la plataforma Watson IoT.

### **3.4 SAMSUNG ARTIK CLOUD**

Samsung Artik es un proyecto de la multinacional surcoreana Samsung Electronics. Esta plataforma abierta de intercambio de datos para internet de las cosas (IoT), permite conectar dispositivos y habilitar nuevos servicios y aplicaciones [46]. Samsung Artik proporciona a desarrolladores y empresas API's abiertos, SDK's y las herramientas necesarias para recolectar, almacenar y actuar sobre cualquier dispositivo que genere información y este conectado a

Internet. Pero Artik no solo se enfoca hacia servicios de Software para IoT, sino que también provee soluciones hardware totalmente compatibles y listas para usar. Estas soluciones se denominan *Samsung Artik Modules* [47].

### 3.4.1 Conceptos de Samsung Artik Cloud

A continuación se describen algunos conceptos básicos que la plataforma Artik maneja para la comunicación efectiva de los dispositivos, plataforma y servicios [48].

- **Autorización:** Cada API tiene modelos de autorización basadas en permisos de escritura y lectura para los usuarios y servicios de la plataforma. Un usuario puede realizar determinadas actividades a través de una llamada a la respectiva API.
- **Mensajes:** La información de los dispositivos o servicios es almacenada en mensajes. Estos mensajes se pueden clasificar en dos tipos: mensajes que solo contienen información o mensajes que contienen acciones para determinados dispositivos. Cada mensaje tiene asociada *metadata* como identificador de dispositivo, identificador de usuario, e identificador de aplicación.
- **Identificador de Usuario:** Este identificador esta asociado a los usuarios creados en la plataforma Artik. Con este identificador las diferentes aplicaciones pueden solicitar la información de los dispositivos asociados al mismo.
- **Identificador de Dispositivo y Tipo de Dispositivo:** Cualquier elemento que provea información a Artik se denomina *Dispositivo*. Éstos, a su vez, pueden ser sensores, un sistema embebido, objetos, aplicaciones o servicios. Estos dispositivos tienen un identificador único que les permite diferenciarse de los otros dispositivos dentro de la plataforma. El Tipo de Dispositivo diferencia la categoría a la que pertenece uno o varios dispositivos.
- **Identificador de Aplicación:** Todas las aplicaciones que interactúan con la plataforma Artik tienen asignado un identificador. Este identificador permite obtener un acceso token tipo *Oauth2* para solicitar datos de una determinada aplicación.
- **Normalización de la información:** La información recibida por Artik de los sensores es denominada *Raw Data*, información en el formato y estructura original sin sufrir modificaciones por parte del sistema. Después de la recolección la información es procesada y convertida en información normalizada como es el formato JSON.
- **Manifest:** Artik Cloud esta diseñado para ser independiente de la información enviada ya sea por los dispositivos o aplicaciones [48]. Artik, para procesar correctamente la información de los dispositivos, necesita un *Manifest* en el que se asocia el tipo de dispositivo y la estructura de la información
- **Acciones:** Las acciones son un tipo de mensaje que envían una orden en específico hacia un dispositivo para que lleve a cabo determinada acción. Estas acciones están definidas en el *Manifest*.

- **Reglas:** Las reglas permiten llevar a cabo determinadas tareas cuando se cumple un evento en específico. Por ejemplo, es posible crear una regla que basándose en la información que envían los dispositivos, envíe un mensaje (por ejemplo, una acción para reiniciar un dispositivo cuando este supere un umbral determinado).
- **Herramientas Artik Cloud Tools:** Artik provee a desarrolladores e investigadores herramientas web para observar y administrar la información que envían los dispositivos, así como también interfaces web gráficas donde ver métricas útiles del comportamiento de dispositivos y aplicaciones.

### 3.4.2 Características de Samsung Artik Cloud

Las características fundamentales de la plataforma Artik [49] se describen a continuación:

- **Módulos IoT:** Samsung Artik no solo entrega soluciones en software sino también soluciones en Hardware que pueden ser desplegadas como dispositivos de tipo *Edge* o *gateways*. Estos dispositivos, denominados *Ready-to-Use*, cuentan con soporte para comunicación tipo Ethernet, Wi-Fi, ZigBee y Bluetooth. Esto no quiere decir que otro tipo de dispositivos no propietarios de Samsung no puedan conectarse a la plataforma ya que Artik permite que cualquier dispositivo con conexión a Internet pueda interactuar con la misma.
- **Interoperabilidad de dispositivos y datos:** Samsung Artik permite que dispositivos puedan comunicarse con otros dispositivos o servicios en la nube. Existe una variedad enorme de *Built-in Cloud Connectors* que permiten que diferentes servicios, dispositivos y aplicaciones interactúen con Artik. La información que se genera puede ser almacenada y normalizada en Artik. Además, Artik provee las herramientas para poder actuar sobre los dispositivos y ejecutar determinadas acciones, generar alertas o emails.
- **Interacción de Dispositivos:** Cualquier dispositivo puede ser conectado a Artik e interactuar con la plataforma. Artik permite que dispositivos puedan entablar comunicaciones de dos vías usando protocolos como MQTT, HTTP/REST, Websockets, CoAP, etc. Ya sea a través de código o por la interfaz gráfica, es posible describir los estados de los dispositivos o realizar acciones sobre ellos.
- **Seguridad y Privacidad:** Tanto los módulos ARTIK, dispositivos de terceros y las aplicaciones pueden usar mecanismos de seguridad extremo a extremo. Cada uno de ellos se conecta de manera segura usando el protocolo TLS, elementos seguros y certificados de seguridad.
- **Administración de Dispositivos:** Artik ofrece herramientas web para el monitoreo y administración de dispositivos. Estas herramientas permiten observar las propiedades de los dispositivos, sus servicios, ejecución de tareas, administración de permisos y certificados de seguridad.
- **Interoperabilidad de Análisis y Visualización:** La información generada por los dispositivos puede ser analizada y visualizada en tiempo

real. Artik ofrece métricas de uso, log de errores, accesos, etc, ya sea por dispositivo o por conjunto de dispositivos.

- **Herramientas para el desarrollador:** Artik cuenta con todo un conjunto de API's para recolectar, almacenar y consultar información de los dispositivos. Los desarrolladores pueden construir sus aplicaciones usando los diferentes SDK's que ARTIK ofrece.
- **Escalabilidad y Latencia:** La plataforma Artik esta diseñada para administrar billones de dispositivos sin incrementar la latencia y manteniendo altos estándares de disponibilidad en el servicio.

### 3.4.3 Arquitectura de Samung Artik Cloud

La figura 15 muestra el diagrama de la arquitectura genérica de la plataforma Artik de Samsung [46]. En ella se especifica cómo Artik Cloud sirve de intermediario entre los dispositivos y las aplicaciones construidas por los desarrolladores para proporcionar servicios a los usuarios. Ésto permite que tanto desarrolladores como usuarios no se preocupen por la compleja heterogeneidad de tecnologías en IoT sino solo en la información que esta presente en la nube.

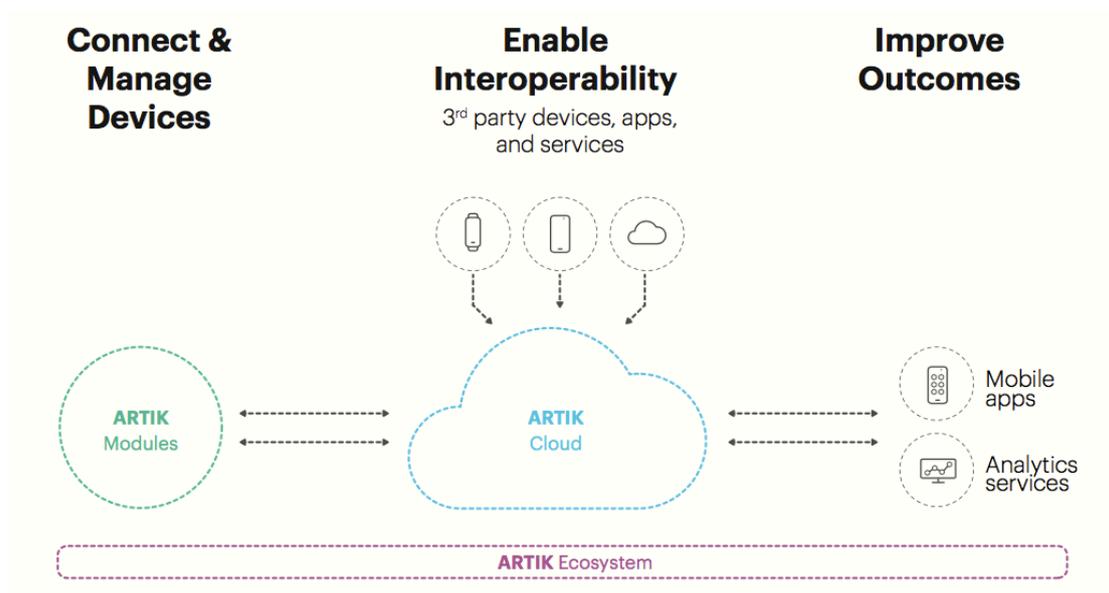


Figura 15: Arquitectura de la plataforma Samsung Artik.

### 3.4.4 Modelo de Negocio de Samsug Artik Cloud

Artik maneja un modelo de negocio conocido como *pay-as-you-go*, donde, se diferencia sus servicios para dos tipos de clientes: *Small Bussines* y *Enterprise*. En la figura 16 se puede observar una comparación entre estos dos modelos, además de mostrar el modelo *Free*, disponible para desarrolladores que quieran experimentar con la plataforma.

### 3.4.5 Casos de Uso

Artik Cloud es una plataforma relativamente nueva en el mercado de IoT [50] ya que fue anunciada a inicios de el año 2016. La plataforma, por ahora, esta sufriendo una transición de uso meramente experimental a un uso masivo. Es por ello que Artik Cloud es usado mayoritariamente en proyectos experimentales y de desarrollo y aún no sea usado a gran escala. A continuación se especifica varios proyectos experimentales en los que se esta usando la plataforma Artik Cloud

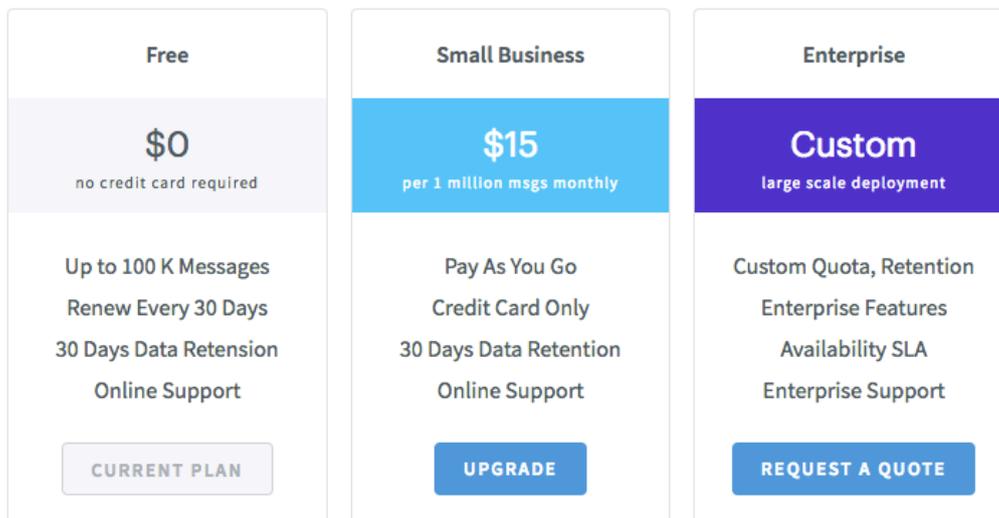


Figura 16: Modelo de Negocio de Samsung Artik.

- Artik Cloud y Peugeot

Samsung y la empresa automotriz Peugeot están trabajando en un concepto experimental de coche inteligente denominado *Peugeot Instinct Concept* [51]. Este coche está conectado a la nube Artik Cloud y a una casa inteligente experimental. Se permite que el coche pueda tener acceso a la información de los dispositivos del hogar como wearables, termostatos, altavoces, cerraduras, etc. y de la misma manera desde el coche administrar y monitorear los dispositivos del hogar. Asimismo desde una aplicación el usuario puede acceder a las diferentes métricas del coche.

- Samsung y Kontak.io Gateway

Este es un ejemplo de implementación de los servicios de hardware y software de Artik. Kontak.io, una empresa polaca especializada en soluciones hardware de IoT, esta empezando a usar los módulos Artik como núcleo de sus dispositivos Gateway [52]. De esta manera los diferentes sensores IoT pueden fácilmente interactuar con Artik Cloud a través de este gateway.

- Artik Cloud, T-Mobile y Breezie:

Breezie es una plataforma abierta que facilita que empresas y organizaciones especializadas en brindar cuidados a mayores puedan ofrecer sus servicios a través de aplicaciones móviles. Con la ayuda de los servicios de Artik Cloud y la plataforma de dispositivos IoT de T-Mobile, los diferentes dispositivos y aplicaciones pueden trabajar de manera coordinada y además de extender el número de dispositivos que pueden interactuar con Breezie [53].

### 3.5 MICROSOFT AZURE IOT SUITE

Azure IoT Suite es un conjunto de servicios y soluciones pre-configuradas en la nube perteneciente a la familia Azure de la multinacional Microsoft. Estos servicios y soluciones empresariales permiten la comunicación bidireccional entre el *back-end* de la solución y millones de dispositivos, recibir telemetría, distribución de datos de dispositivos a un procesador de eventos de transmisión, recepción de cargas de archivos de los dispositivos, almacenamiento de datos de dispositivos, supervisión, herramientas para implementación de comunicaciones seguras, reglas, etc.[54].

Existe una infinidad de soluciones pre-configuradas y sus múltiples variaciones según los requerimientos de cada usuario, pero se hará énfasis en la solución de monitoreo remoto ya que comparte servicios de Azure que son comunes a muchas otras soluciones [55].

#### 3.5.1 Conceptos de Microsoft Azure IoT Suite

Los siguientes conceptos son fundamentales para un entendimiento crítico del conjunto de soluciones IoT Azure que Microsoft proporciona [56].

- **Dispositivos y modelos de datos:** Los modelos permiten modelar metadatos descriptiva acerca de los dispositivos. Esta metadatos está conformada por características como número serial, los datos que el dispositivo envía, acciones que el dispositivo pueda ejecutar, eventos que este midiendo, etc.
- **Flujo de Datos:** Es la información que fluye a través de los servicios IoT de Azure. El formato de este flujo de datos depende del tipo de datos que se está transportando en ese momento. Los tipos más comunes son :
  - Telemetría de dispositivos: Las señales digitales de las observaciones realizadas en un periodo definido por los dispositivos.
  - Estados, alertas y acciones: Un estado es el último valor conocido de un dispositivo representado por el último registro que lleva ese parámetro específico. Una alerta es un mensaje desencadenado por un evento que cumple ciertas condiciones y reglas. Las acciones son los mensajes enviados desde Azure hasta los dispositivos para reportar estados o alertas que activan alguna acción.

- **Timestamps:** Las marcas de tiempo de cada flujo de datos generalmente en formato UTC.
- **Interacción del dispositivo:** Para establecer una comunicación bidireccional segura con diferentes dispositivos, Azure IoT Suite adopta los principios del enfoque *Service Assited Communication* [57]:
  - Los dispositivos solo aceptan conexiones de red solicitadas.
  - Los dispositivos solo se conectan o establecen comunicación con gateways conocidos o emparejados.
  - La comunicación entre dispositivo y servicio esta asegurada por los protocolos de la capa transporte y aplicación (MQTT y TLS).
  - Las autorizaciones y autenticación a nivel de sistema deben basarse en identificadores y credenciales de dispositivo que deben ser revocables en caso de síntomas de abuso.
- **Protocolos de comunicación:** En la actualidad Azure soporta un numero enorme de protocolos de comunicación para IoT. Cada uno de ellos permite enviar la información de un dispositivo a los diferentes servicios en la nube. Por ejemplo tenemos los protocolos AMQP y MQTT para la capa de transporte y JSON para el formato nativo de los mensajes. Azure IoT se adapta a la mayoría de ellos y tiene módulos que se integran en la mayoría de dispositivos.

### 3.5.2 Características de Microsoft Azure IoT Suite

Microsoft Azure IoT Suite, al igual que la mayoría de servicios IoT en la nube, dispone de una extensa variedad de servicios de comunicación para dispositivos así como herramientas de almacenamiento y análisis de la información generada por los mismos. De todo lo anterior se pueden añadir las siguientes características [58]:

- **Dispositivos gemelos:** Cada dispositivo físico conectado a Azure IoT tiene su par en la plataforma en forma de documento JSON.
- **Autenticación y Seguridad:** Cada dispositivo tiene asociado un identificador y clave que le permite autenticarse con la plataforma.
- **Enrutamiento de mensajes:** Azure IoT permite definir reglas con rutas de mensajes para administrar hacia dónde y desde dónde se están enviando los mensajes. Esta característica no requiere implementación de código.
- **Supervisión de Dispositivos:** Opción que permite tener métricas y registros de las actividades y estado de los dispositivos como eventos de conectividad, identidad, *throughput* de mensajes, etc.
- **Bibliotecas para dispositivos:** Disposición de SDK's y API's para la mayoría de sistemas embebidos y lenguajes.
- **Módulos para los diferentes protocolos IoT:** Azure IoT dispone de bibliotecas donde se pueden implementar soluciones en sistemas embebidos usando protocolos como MQTT, HTTP AMQP, etc. de forma nativa.
- **Escalabilidad:** Escalabilidad de hasta millones de dispositivos con sus respectivos eventos y propiedades.

### 3.5.3 Arquitectura de Microsoft Azure IoT Suite

La figura 17 muestra un arquitectura conceptual de alto nivel de los componentes que intervienen en la plataforma de Microsoft Azure IoT [56]. Esta arquitectura esta compuesta por servicios centrales y otros de nivel de aplicación que facilitan el procesamiento de la información IoT en tres áreas:

- **Conectividad de Dispositivos:** Los diferentes dispositivos IoT pueden contactarse directamente o vía gateway. En ambos casos se puede añadir inteligencia con diferentes niveles de procesamiento de datos.
- **Procesamiento, análisis y administración de datos:** Este nivel de *back-end* suministra capacidades de registro y descubrimiento de dispositivos, recolección de datos, transformación y analítica de datos como también lógica a nivel de negocios y visualización de datos.
- **Presentación y Conectividad de Negocios:** En este nivel se realiza la interacción de la datos IoT con los procesos de una empresa. Una empresa puede integrar Azure IoT con una solución existente a través de módulos denominados Enterprise Integration (EAI) y Bussines-to-Bussines (B2B)

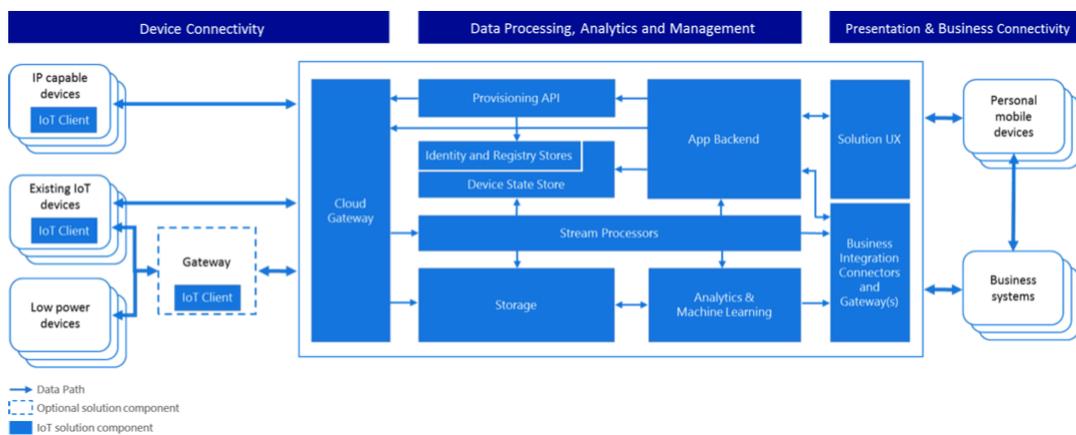


Figura 17: Arquitectura de la plataforma Microsoft Azure IoT Suite.

### 3.5.4 Modelo de Negocio de Microsoft Azure IoT Suite

La plataforma de Microsoft Azure IoT Suite tiene como mercado objetivo el sector empresarial e industrial. Es por ello que su plataforma en la nube Azure, y todos los servicios y aplicaciones que la conforman, se manejan bajo el modelo *pay-as-you-go*. Dependiendo del número de servicios, el tipo de infraestructura usada y la cantidad de información que será almacenada y procesada, dependerá el costo de una determinada solución.

### 3.5.5 Casos de Uso

Azure IoT Suite, como solución enfocada al sector empresarial e industrial tiene amplia presencia en soluciones de este tipo [59]. A continuación se hablara de las casos de éxitos mas prominentes donde Azure IoT esta siendo usada como plataforma.

### Rolls-Royce:

La reconocida empresa de motores de aviones comerciales esta usando los servicios de Microsoft Azure IoT para obtener y analizar la información de los diferentes equipos aeronáuticos que tiene a disposición en su flota. Esto permite a la empresa obtener valiosos datos de predicción que permiten mejorar la eficiencia en los programas de mantenimiento, ahorrando tiempo y dinero a la empresa [60].

### Edificios inteligentes en Singapur:

La BCA del Ministerio de Desarrollo Nacional del gobierno de Singapur escogió el conjunto de soluciones de Microsoft Azure IoT para implementar una solución que permite mejorar la eficiencia en los sistemas de refrigeración de edificios comerciales y no comerciales de gran altura. Mediante reportes de métricas e informes, la solución permite ahorro energético y de costes. [61]

### Transporte inteligente:

*Fathym* es una empresa proveedora de soluciones IoT que ha desarrollado una aplicación denominada *WeatherCloud* que permite obtener actualizaciones en tiempo real del estado de las carreteras. Dicha aplicación esta construida bajo la plataforma Azure IoT y sus diferentes servicios. La aplicación es usada por organizaciones gubernamentales como el Centro Nacional para la Investigación Atmosférica de Alaska, el departamento de transporte de Alaska, Utah, Colorado y en Nueva Zelanda. La aplicación permite a los operadores ver las condiciones actuales de la carretera, pronósticos futuros y alertas que ayudan en la toma de decisiones estratégicas para mantener la seguridad en las vías [62].

### Rockwell Automation:

La multinacional *Rockwell Automation*, especializada en soluciones de automatización e información industrial, ha desarrollado una solución IoT para monitorear equipos que participan en actividades de minería, de transporte, y distribución de derivados de petróleo y gas. Esta, solución provista de características de análisis predictivo, permite a sus clientes obtener información en tiempo real de cada aspecto en la cadena de suministro, lo que ayuda a predecir problemas incluso antes de que estos ocurran. Esta solución, implementada con los servicios de Microsoft Azure IoT, permite a los operadores a través de gráficos históricos monitorear el estado de los equipos y sus variables[63].

## CAPITULO IV: ENTORNO DE PRUEBAS PARA LA EVALUACIÓN DE LOS SERVICIOS EN LA NUBE PARA IOT.

Para la implementación del entorno de pruebas este trabajo de fin de máster se basó en el modelo *Sensing as a Service* detallado en [64]. En este modelo se especifica que los datos de los sensores se envían primeramente a un gateway local, que se comunica con los servicios en la nube, y cuando un usuario los requiera estos son provistos de manera inmediata. El usuario no tiene contacto directo con los sensores o infraestructura, solo con la información generada por los sensores. En este modelo de servicio se especifican cuatro capas:

- *Sensors and Sensor Owners Layer*: Los sensores que miden las características particulares de los objetos. Los Sensor Owners toman la decisión final de publicar o no la información que poseen en la nube.
- *Sensor Publishers Layer (SP)*: Donde se detectan los sensores disponibles y se establece si se dispone o no de los permisos para publicar la información de los sensores en la nube.
- *Extended Service Providers Layer (ESP)*: Es la capa mas inteligente. Aquí los servicios pueden variar de un proveedor a otro. Cuando un consumidor requiere la información de un determinado sensor, la ESP puede proveer la información comunicando con otros ESP, SP o la información que esta almacenada en la nube.
- *Sensor Data Consumers Layer*: En esta capa están los datos de los sensores disponibles para los consumidores como gobiernos, empresas, instituciones académicas, etc. Los consumidores no acceden directamente a los sensores sino que lo hacen a través del ESP o SP correspondiente.

Para implementar este modelo se desarrolló una arquitectura que está compuesta principalmente de una Raspberry Pi que actúa como gateway entre los objetos y los servicios en la nube. Con este entorno de pruebas se envía la información de los sensores hacia la nube para su respectivo almacenamiento y visualización. La arquitectura se muestra de manera detallada en la figura 4 y se explica su composición a continuación:

- Grupo de Sensores:

En la arquitectura no se implementó ninguna clase de sensores, pero para que el estudio esté lo mas cercano a un escenario real se simulará la carga de los datos proporcionado por un entorno de sensores en huertos fotovoltaicos [65]. En este entorno se va a monitorizar variables eléctricas, térmicas y ambientales de 16 bits cada una. En la tabla 2 se muestra las cinco variables que por cada panel solar que serán simuladas. El grupo de paneles lo conforman una carga de 5Kw, que corresponden a 20 paneles de 250w. De este grupo de paneles solares hay que monitorizar dos variables adicionales, que son temperatura ambiente y radiación solar (ver tabla 2) lo cual da como resultado un carga de datos igual a 102 variables. Normalmente, los paneles solares están activos solo diez horas al día por motivos de disponibilidad de luz solar, pero, como estamos en un entorno de pruebas controlado asumiremos que los paneles solares trabajan las 24 horas del día.

- Red inalámbrica:

La red inalámbrica no será implementada y se dará por válido que los sensores están enviando información fiable y constante a la Raspberry Pi.

- Gateway - Cloud:

La Raspberry Pi enviará los datos de los sensores cada 5 minutos por lo tanto tendremos que los servicios en la nube soportaran una carga 29376 variables al día. El numero de días que se estará enviando las variables dependerá enormemente de las características propias del modelo gratuito que ofrezcan los servicios en la nube.

Estas variables serán generadas aleatoriamente dentro de un rango válido por un script en la Raspberry Pi, que a través de las API's correspondientes de cada servicio en la nube serán enviados y almacenados en los mismos. Además, la Raspberry Pi hará uso de dos herramientas *crontab* y *ssmtp*. La primera ejecutara de manera automática los scripts que enviaran la información a la nube y la segunda enviará reportes por correo cuando exista alguna anomalía en el envío de la información de los sensores y que servirá como información adicional para el momento de la evaluación de los servicios en la nube.

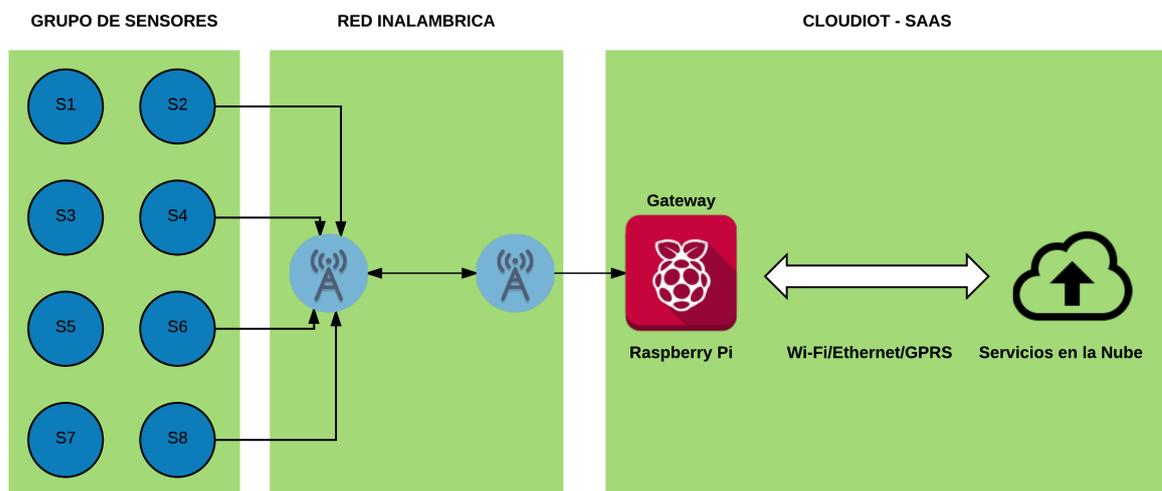


Figura 18: Arquitectura genérica del entorno de pruebas.

Con este entorno de pruebas será posible evaluar el comportamiento de cada servicio en la nube, así como explorar cada una de sus características, herramientas, configuraciones y demás opciones que las mismas ofrecen a clientes y desarrolladores. Además proporcionará una visión general del posible grado de complejidad al implementar aplicaciones IoT usando los respectivos servicios en la nube.

Tabla 2: Variables a ser simuladas y enviadas por la Raspberry Pi.

Variables Panel Solar		
VARIABLE	RANGO	UNIDADES
Voltaje Uno	20 - 40	Voltios
Voltaje Dos	20 - 35	Voltios
Intensidad Uno	5 - 12	Amperios
Intensidad Dos	5 - 15	Amperios
Temperatura Modulo Solar	40 - 50	º Centígrados
Variables ambientales		
Temperatura ambiente	20 - 30	º Centígrados
Radiación Solar	2 - 3	watt/m <sup>2</sup>

En la tabla 4 se muestra la relación entre el modelo SaaS detallado en [64] y la arquitectura del entorno de pruebas montada.

Tabla 3: Relación del modelo SaaS y el entorno de pruebas.

SaaS	Arquitectura de entorno de pruebas
Sensors and Sensor Owners	Grupo de Sensores
Sensor Publishers (SP)	Raspberry Pi
Extended Service Providers (ESP)	Servicios públicos y privados de CloudIoT
Sensor Data Consumers	Usuarios finales y las aplicaciones.

#### 4.1 Implementación del servicio Sofia2

Para entender un poco mejor la implementación en Sofia2 se muestra en la figura 20 un diagrama de bloques de cada una de las partes involucradas en esta implementación. Cabe mencionar que se uso el modelo de servicio *CloudLab*, el cual es gratuito en Sofia2.

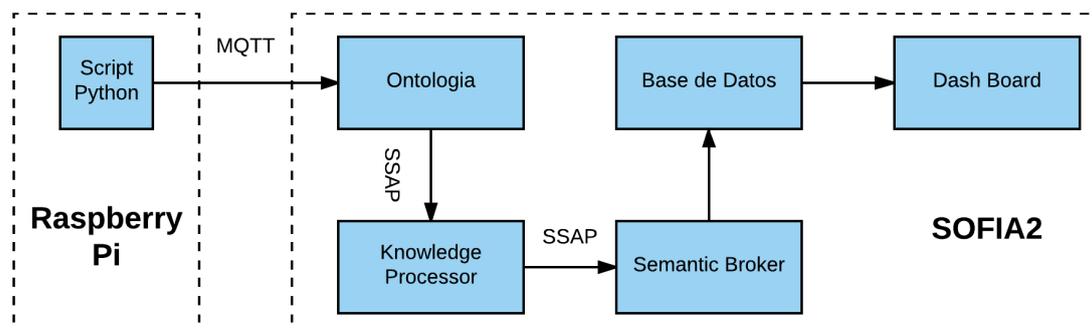


Figura 19: Diagrama de Bloques de la implementación en Sofia2

Sofia2 maneja el concepto de ontologías. Una ontología puede ser un objeto que tiene diferentes atributos o propiedades. En este caso un panel solar representa una ontología con 5 propiedades: voltaje uno, voltaje dos, intensidad uno, intensidad dos y temperatura panel. Estas ontologías se definen en Sofia2.

Las ontologías se comunican por medio del protocolo SSAP con el Semantic Broker para entablar la conexión con el respectivo Knowledge Processor (KP) que consumen la información de la ontología. Como mecanismo de seguridad, cada ontología debe autenticarse con el KP usando tokens. El KP registra cada cambio en los valores de la ontología en la base de datos de tipo BDH donde la herramienta DashBoard realiza las consultas a la base de datos para representar gráficamente los valores de los sensores.

La Raspberry Pi, usando al API Python de Sofia2, y con la información del nombre de ontología, valores de las propiedades, KP y el token puede empezar a enviar la información de la ontología a la plataforma Sofia2. Esta comunicación usa el protocolo MQTT y su payload es un mensaje en formato JSON que contiene la información de las propiedades de la ontología. Podemos observar la DashBoard mostrando información de los sensores en la figura 21. En el anexo 1 se encuentra una guía paso a paso de la implementación en la Raspberry Pi y el código respectivo.

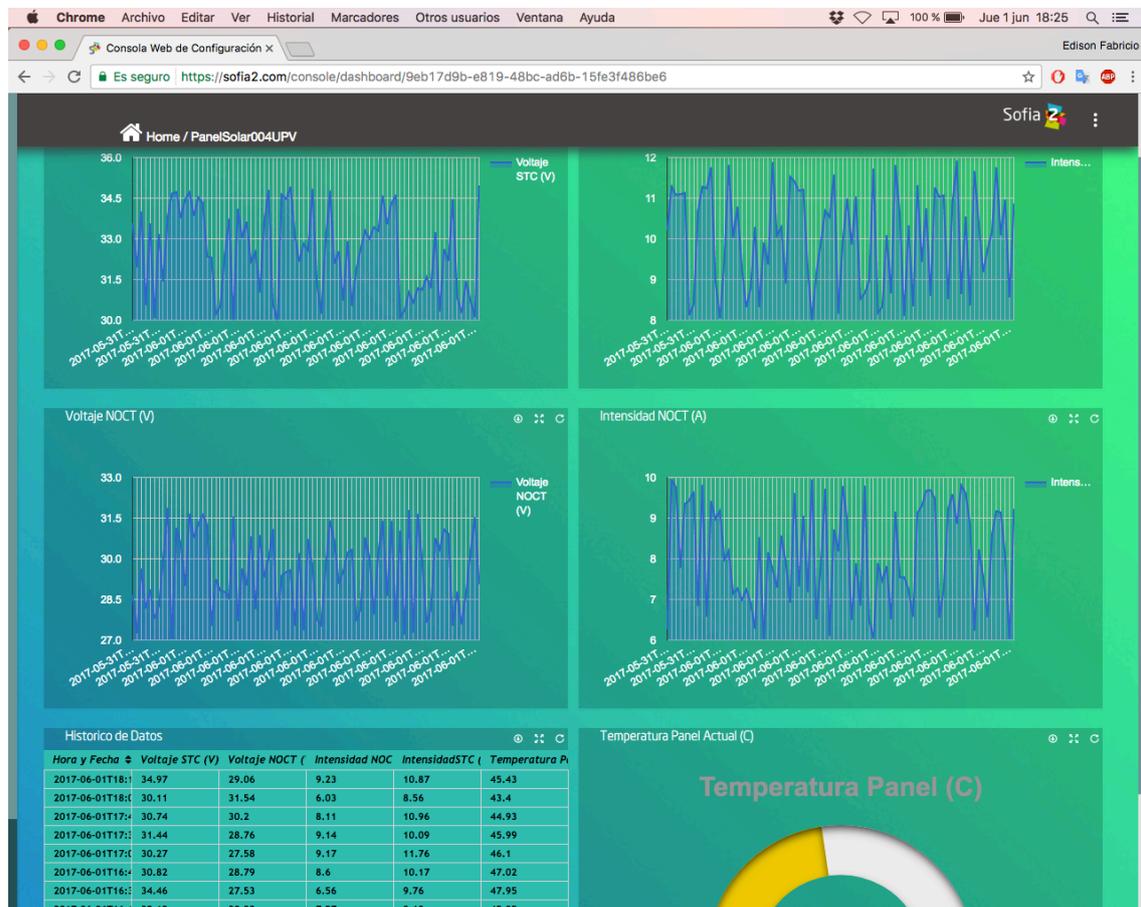


Figura 20: Plataforma Sofia2 mostrando información de los sensores.

## 4.2 Implementación del servicio Fiware

En la figura 22 se muestra un diagrama de bloques donde se detalla los componentes usados en la implementación de Fiware.

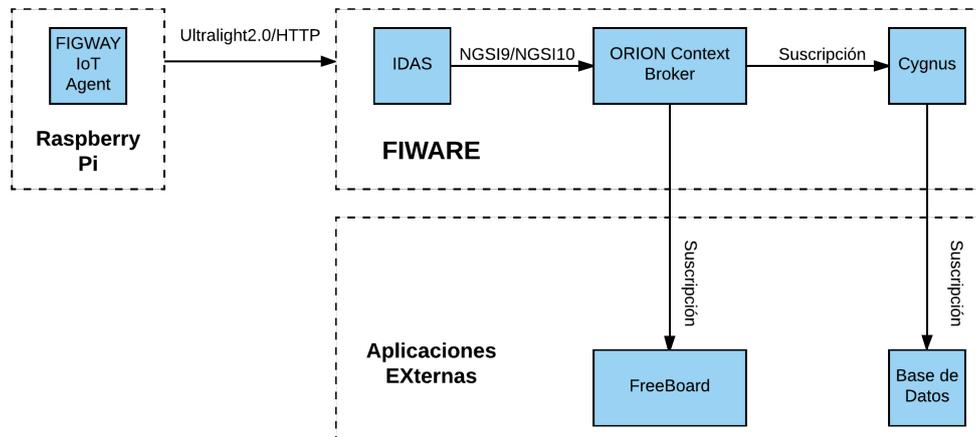


Figura 21: Diagrama de Bloques de la implementación en Fiware.

Fiware maneja el conceptos de entidades que representan los objetos del mundo real. Estas mismas entidades tienen propiedades o atributos que caracterizan al objeto. En este caso los paneles solares se representan como entidades con sus cinco propiedades: voltaje uno, voltaje dos, intensidad uno, intensidad dos y temperatura panel.

La Raspberry, por medio de un script en Python, genera dichas propiedades de manera aleatoria y usando la herramienta FIGWAY, que actúa como IoT Agent, envía la información de la entidad y de sus propiedades hacia el IDAS. Para esta comunicación FIGWAY hace uso del protocolo Ultralight2.0/HTTP . El IDAS a su vez envía la información al Context Broker. Tanto el IDAS como el Context Broker están instalados en la infraestructura de nube publica de Fiware que está a disposición de los desarrolladores para que prueben sus aplicaciones.

El Orion Context Broker ya teniendo registrado las entidades y sus atributos puede ser consultado sobre las mismas. En este caso FreeBoard, que es una herramienta online de visualización de sensores IoT, consulta las entidades del Context Broker y muestra la información en su pagina web. Además, tenemos un GE llamado Cygnus de Fiware que actúa como conector entre el Context Broker y una base de datos para darle persistencia a los datos, en esta caso la usada es MySql. En la figura 18 se muestra la herramienta FreeBoard con la información correspondiente de los objetos. En el anexo 2 se encuentra una guía paso a paso de la implementación en la Raspberry Pi y el código respectivo.

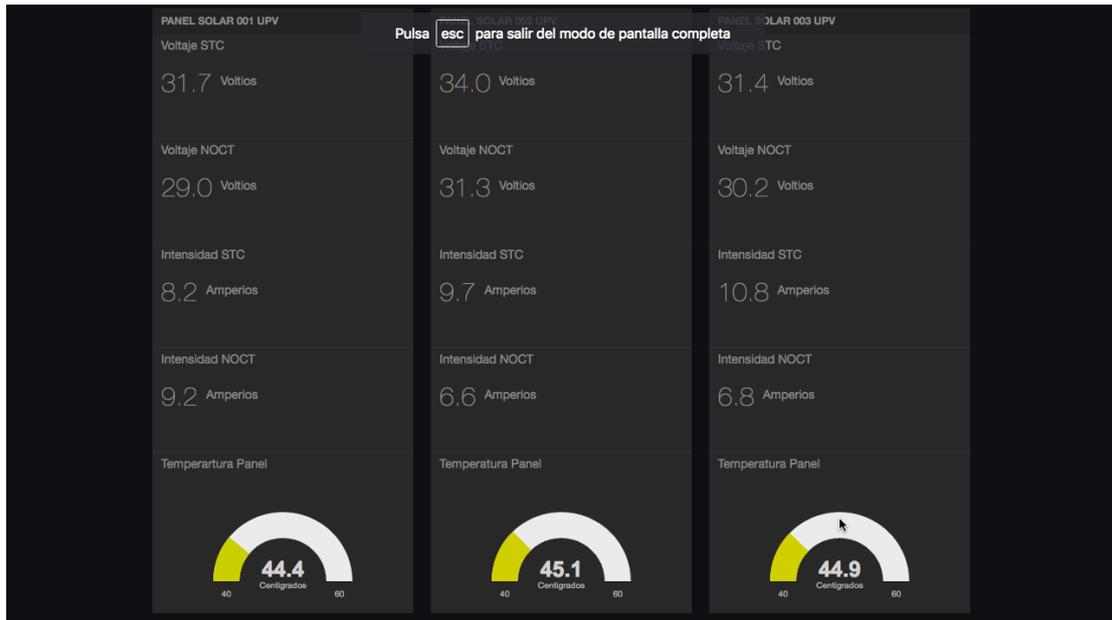


Figura 22: Herramienta FreeBoard mostrando la información de los sensores.

### 4.3 Implementación del servicio Watson IoT

En la figura 23 se muestra el diagrama de bloques de los componentes usados en la implementación de Watson IoT. La implementación se basó en el modelo de suscripción gratuita de IBM Watson.

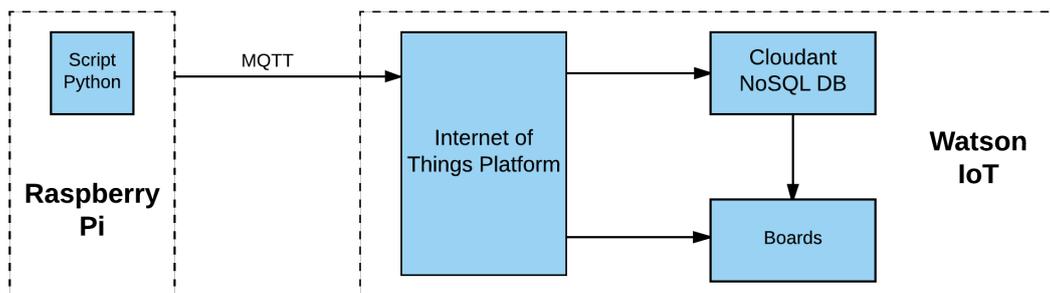


Figura 23: Diagrama de Bloques de la implementación en Watson IoT.

La plataforma de Watson IoT maneja el concepto de dispositivos para identificar los objetos y sus atributos. En este caso cada panel solar es un dispositivo con sus respectivas atributos voltaje uno, voltaje dos, intensidad uno, intensidad 3 y temperatura ambiente.

La Raspberry Pi, por medio del API de Python, se comunica con la plataforma Watson IoT usando el protocolo MQTT. En esta comunicación se envía los atributos de cada uno de los objetos. En esta comunicación se usa como el estándar JSON para el formato de los mensajes. El servicio Internet of Things Platform administra estos dispositivos y sus atributos, que a su vez son consultados por el servicio de base de datos Cloudant para tener un registro histórico de los datos. De la misma manera, la aplicación Boards consulta tanto a

la base de datos como al servicio de Platform Watson IoT acerca de los atributos de los objetos para poder representarlos de manera grafica. Tal como se muestra en la figura 24. En el anexo 3 se muestran los pasos de manera mas detallada de la implementación de esta plataforma y su código respectivo.

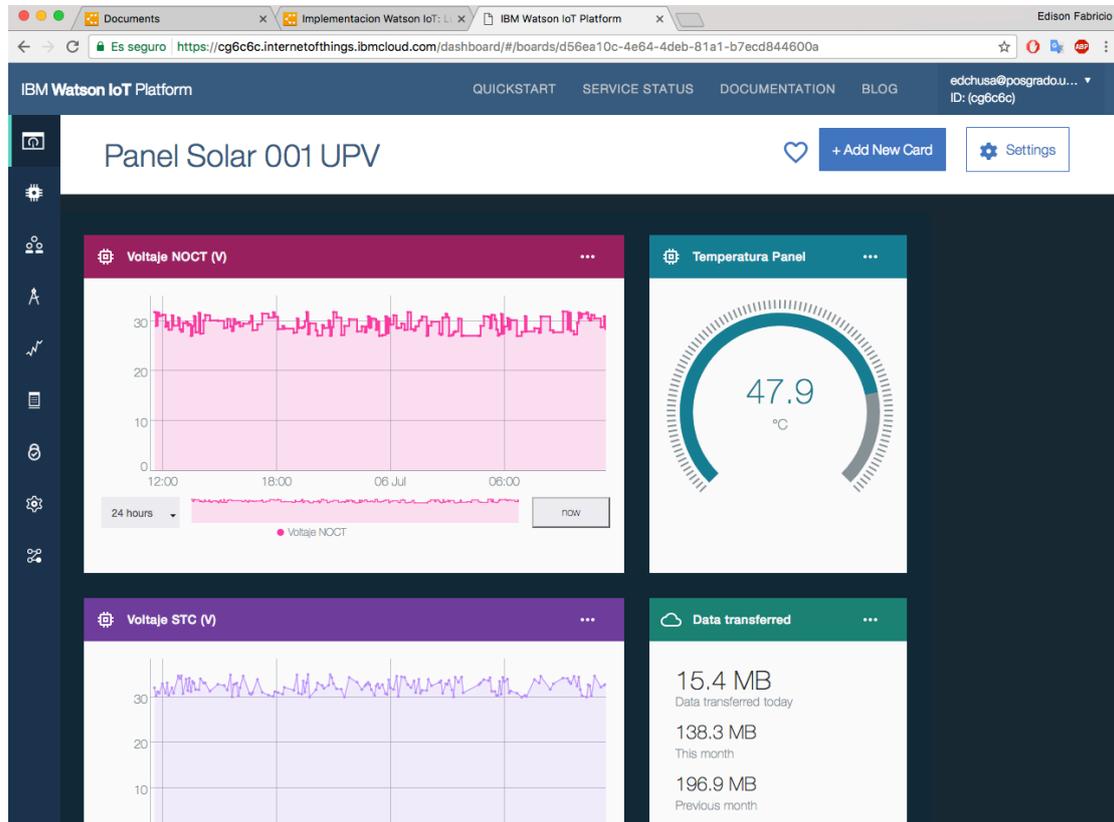


Figura 24: Plataforma Watson IoT mostrando la información de los objetos.

#### 4.4 Implementación del servicio Samsung Artik Cloud

En la figura 25 se observa el diagrama de bloques de los componentes usados en la implementación de la plataforma Artik. La implementación se basó en el modelo de suscripción gratuita de Samsung Artik Cloud.

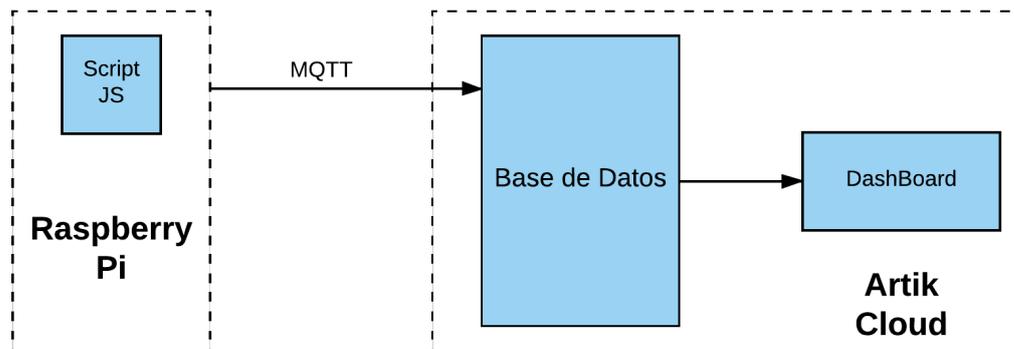


Figura 25: Diagrama de Bloques de la implementación en Artik Cloud.

Dentro de la plataforma Artik los objetos del mundo real se identifican como dispositivos. Cada dispositivo se caracteriza por campos que representan las propiedades del objeto en el mundo real (por ejemplo, las variables de los sensores del objeto). Es por ello que cada panel solar se identifica como un dispositivo con sus respectivos campos o variables.

En la Raspberry Pi, el script escrito en JS genera aleatoriamente los valores para cada variable y las integra en un cadena de texto en formato JSON que será el mensaje a enviar a la plataforma Artik por medio del protocolo MQTT. Este mensaje se identifica en la plataforma usando un identificador único y un token, parámetros que son diferentes de un dispositivo a otro. Una vez la instancia del dispositivo en la nube empieza a recibir mensajes, los almacena en la base de datos. Desde esta base de datos se generan gráficas con los valores históricos de los variables, así como métricas correspondientes a los dispositivos y a sus diferentes propiedades. En la figura 25 se muestra el denominado *DashBoard* que refleja gráficamente la información histórica de los sensores. En el anexo 4 se encuentra una guía y el código respectivo de la implementación de este servicio en la Raspberry Pi.

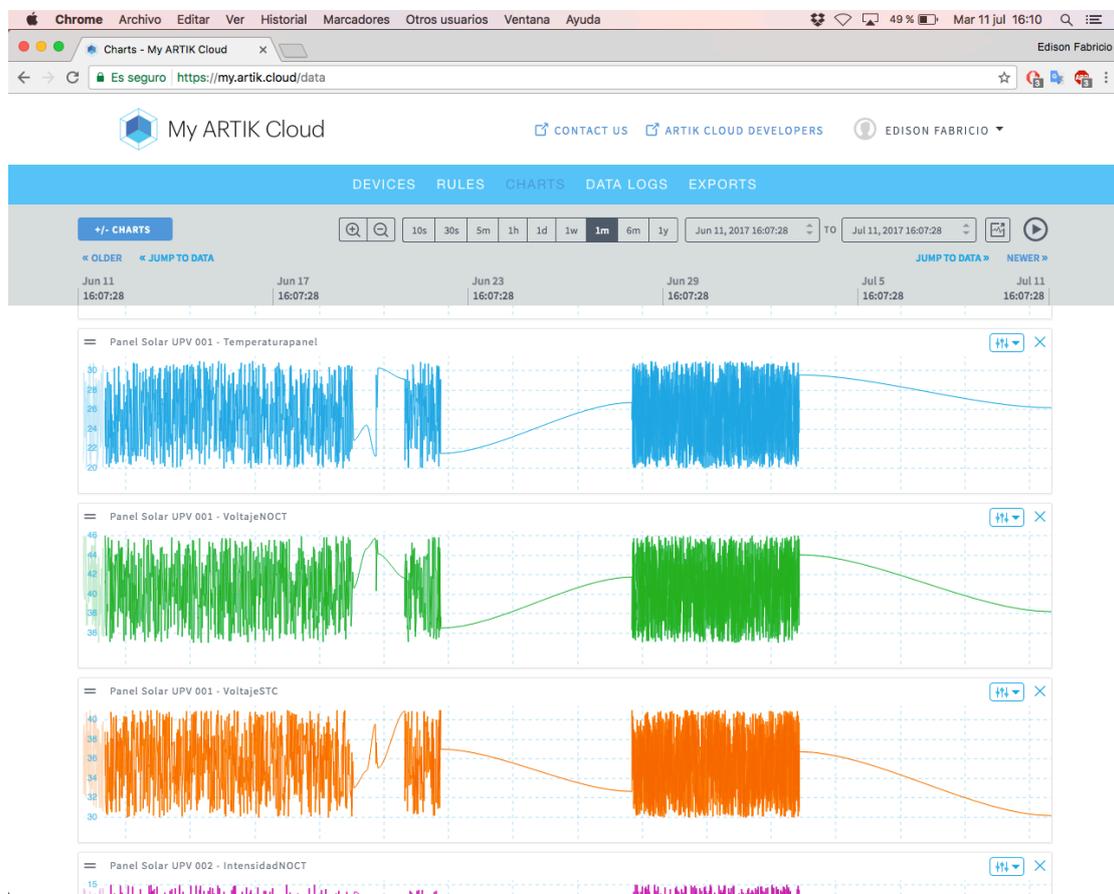


Figura 26: Plataforma Samsung Artik mostrando información de los sensores.

## 4.5 Implementación del servicio Microsoft Azure IoT

En la figura 27 se muestra un diagrama de bloques donde se muestra cada uno de los servicios que intervienen para la solución de monitoreo remoto en Azure IoT.

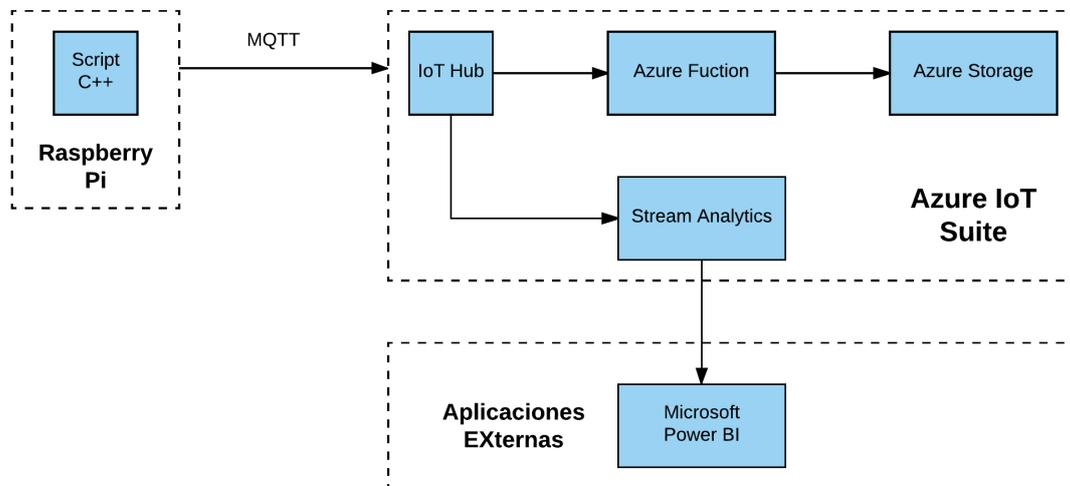


Figura 27: Diagrama de bloques de la implementación en Azure IoT Suite.

La Raspberry Pi, usando un script escrito en C++, envía la información del dispositivo y sus diferentes atributos (en este caso del panel solar y sus diferentes variables). Para la autenticación con la plataforma usa un identificador único de dispositivo y su respectivo token. El servicio IoT Hub es una solución pre-configurada que recibe la telemetría de los dispositivos y actúa como concentrador de comunicaciones y eventos de los mismos sirviendo de puente entre los dispositivos IoT y los diferentes servicios de Azure.

El servicio Azure Function permite escribir y ejecutar fragmentos de código. Aquí se implementó una función en JavaScript que, basada en los eventos del IoT Hub, cuando se recibe telemetría de algún dispositivo almacena ese mensaje en una base de datos en el servicio de Azure Storage.

Por otra lado, tenemos los servicios de *Stream Analytics*, el motor de procesamiento de eventos y de análisis de información en tiempo real. Cuando un evento de telemetría de algún dispositivo se dispara en el IoT Hub, esta función recoge el mensaje y actúa de intermediario entre ésta y la aplicación de Microsoft Power BI, donde recoge el mensaje y lo representa de manera gráfica.

En la figura 28 se muestra la aplicación Power BI mostrando la información de los sensores y en la figura 29 el servicio IoT Hub. En el anexo 5 se muestra el código y los pasos detallados de cómo se implementó en la plataforma Azure IoT.

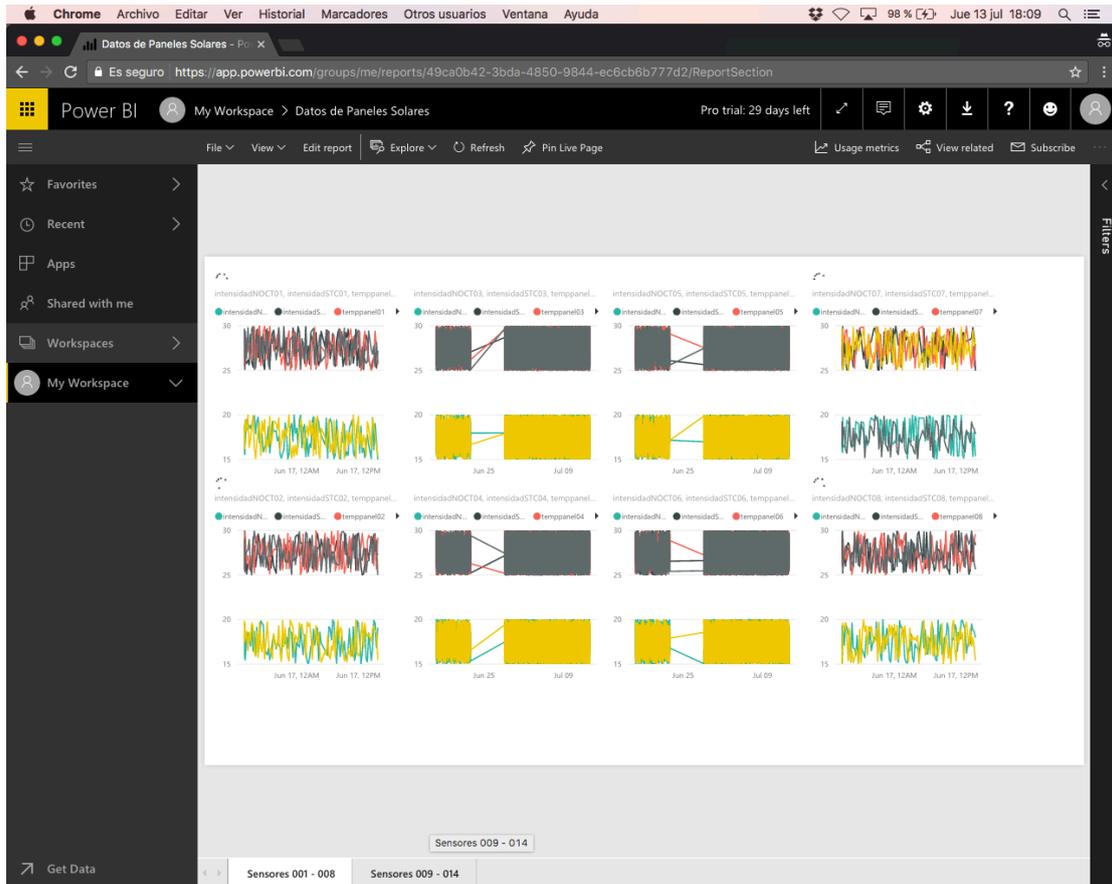


Figura 28: Aplicación Power BI mostrando información de los sensores.

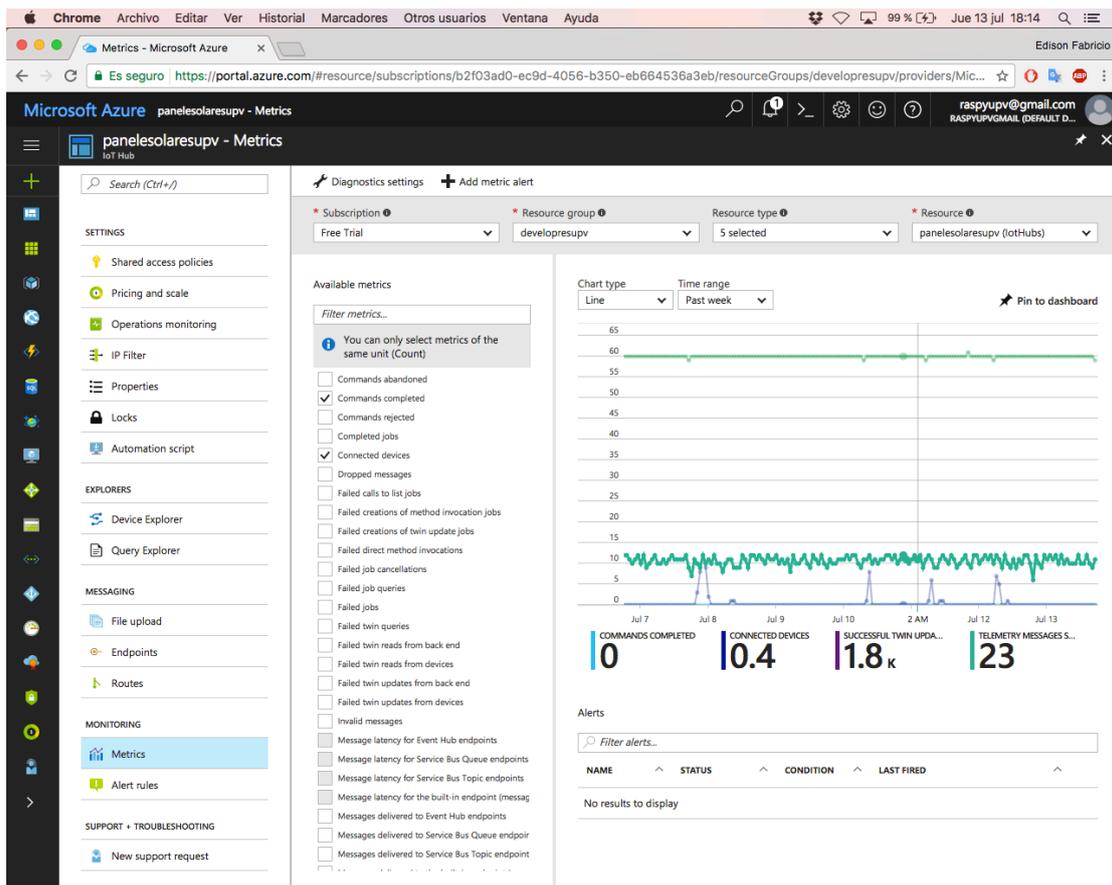


Figura 29: Plataforma Azure IoT mostrando métricas de los dispositivos.

## CAPITULO V: RESULTADOS

Una de las características a evaluar en cada plataforma es su capacidad de recibir, procesar y almacenar las peticiones de los diferentes clientes o dispositivos. Estas peticiones contienen información de los sensores, credenciales de autenticación, metadata, etc. Estas peticiones o mensajes están definidas bajo el protocolo JSON para los servicios de Sofia2, Watson IoT, Artik Cloud y Azure IoT. Mientras que para el servicio de Fiware se implementa el protocolo Ultralight 2.0 que tiene similares características a JSON.

La información de los sensores esta conformada por 5 variables o dos dependiendo del objeto lo cual da como resultado que se envíen por día 6048 mensajes. Para un mejor entendimiento, la tabla 4 muestra de manera mas detallada esta cuestión.

Tabla 4: Mensajes por día enviados.

Dispositivos	Cantidad	Variables	Mensaje por dispositivo	Mensajes/día por dispositivo	Mensajes/día Total
Paneles Solares	20	5	1	288	5760
Sensor de variables ambientales	1	2	1	288	288
				<b>TOTAL</b>	<b>6048</b>

De la información de la tabla 4 se deduce que los servicios tienen que aceptar diariamente este número de mensajes. Con la herramienta *sstmp* se construyó un *datalog* donde, si por alguna razón un mensaje no era procesado por los servicios, este evento queda registrado. Con estos datos es posible cuantificar el número de peticiones enviadas versus el número de peticiones procesadas o descartadas lo cual será de gran ayuda para estimar el grado de eficiencia de cada plataforma.

### 5.1 Resultados en Sofia2

La plataforma de Sofia2 fue sometida a la evaluación durante 30 días, que es el tiempo máximo que la base de datos en tiempo real puede almacenar información de una ontología antes de borrarla bajo el modelo de suscripción gratuita.

- Mensajes procesados por la plataforma:

En base al archivo *datalog* respectivo se pudo extraer la siguiente información: De los 181440 mensajes procesados por 30 días solo el 0,02% fueron mensajes no procesados o no aceptados por la plataforma lo cual le da un porcentaje de eficiencia del 99,98% (ver tabla 8).

- Seguridad en Sofia2:

Sofia2 permite que los clientes, es decir, los dispositivos, se registren a la plataforma mediante un token de autenticación asociado a un KP. Además, cada KP tiene asociada una instancia que identifica al cliente que se conecta a la plataforma. Por lo tanto, cada ontología (dispositivo) maneja su propio token. Esto puede resultar un poco tedioso si son muchas ontologías, pero es un método seguro que usa Sofia2 para verificar que solo los clientes autorizados pueden enviar o recibir información de las ontologías. Además Sofia2 tiene implementado por defecto los protocolos TLS/SSL a nivel de dispositivos para la comunicación con el exterior.

- Modelo de Negocio en Sofia2:

Sofia2 en su modelo de negocios maneja el concepto de *pay-as-you-go* para su prestación de servicios e infraestructura en la nube, además Sofia2 ofrece la posibilidad de 'implementar' la solución Sofia2 en la infraestructura del cliente de manera local.

Al momento de redactar este trabajo de fin de máster Sofia2 aún no implementan un modelo de suscripción mensual o anual de prestación de servicios en la nube sino que según las características y requerimientos de hardware que haga uso una determinada aplicación, Sofia2 presenta al desarrollador o cliente al valor a pagar por la misma. Para este trabajo de fin de master la aplicación hizo uso del modelo de suscripción gratuita.

- Entorno de desarrollo en Sofia2:

La implementación de manera general en Sofia2 no tiene una alta dificultad técnica, lo cual lo hace muy atractiva para todo tipo de desarrolladores, ya que hay API's disponibles para la mayoría de plataformas que existen actualmente. La única dificultad que se encontró fue la falta de información concisa y clara de cómo usar las respectivas API's. Algo que también se notó durante la implementación de este servicio fue la falta de una comunidad establecida de desarrolladores y que Sofia2 no haga ninguna mención de la existencia de foros donde se hagan consultas técnicas, lo que en este tipo de desarrollos es fundamental. Otro aspecto interesante de Sofia2 es que una plataforma muy flexible ya que permite al desarrollador construir su propia aplicación externa la cual, a través del API correspondiente, puede realizar consultas a la información semántica almacenada en la nube. Esto último da la posibilidad a que desarrolladores pueden implementar una multitud de aplicaciones sin preocuparse por la infraestructura o servicios que corren en la nube ya que este servicio lo proporciona Sofia2 en su modelo de negocio. En el modelo de servicio *Advanced Analytics Edition* Sofia2 implementa los módulos necesarios para desarrollar soluciones Big Data. En cuanto a la privacidad de los datos Sofia2 especifica que la información que los clientes intercambian con la plataforma no es pública, a menos que el cliente especifique lo contrario. Sofia2 no usará esta información con otros fines que se no sea extraer estadísticas para mejorar el rendimiento de la plataforma.

Además Sofia2 ofrece un entorno grafico amigable e intuitivo donde se puede:

- Crear, modificar y ver el estado de las ontologías, así como gestionar las mismas y las bases de datos asociadas a ellas. Ver figura 30 y figura 32.
- Administración de cada uno de los tokens y de los permisos asociados a los KP que consumen la información de las ontologías.
- Herramientas para creación y gestión de *Dashboard* para visualizar la información de los diferentes objetos (ver figura 31), así como la implementación de *Dashboards* de manera publica para que cualquier usuario en la web pueda consultar la información de los sensores.

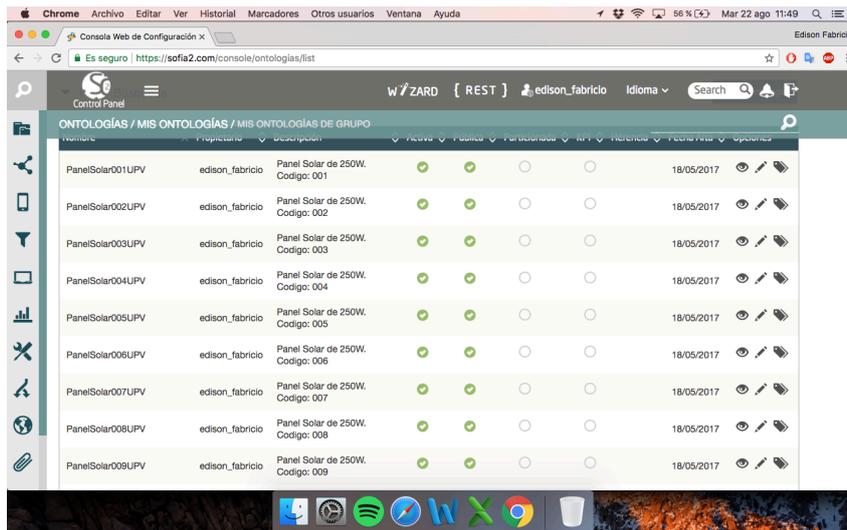


Figura 30: Herramienta de consulta de estado de Ontologías en Sofia2.

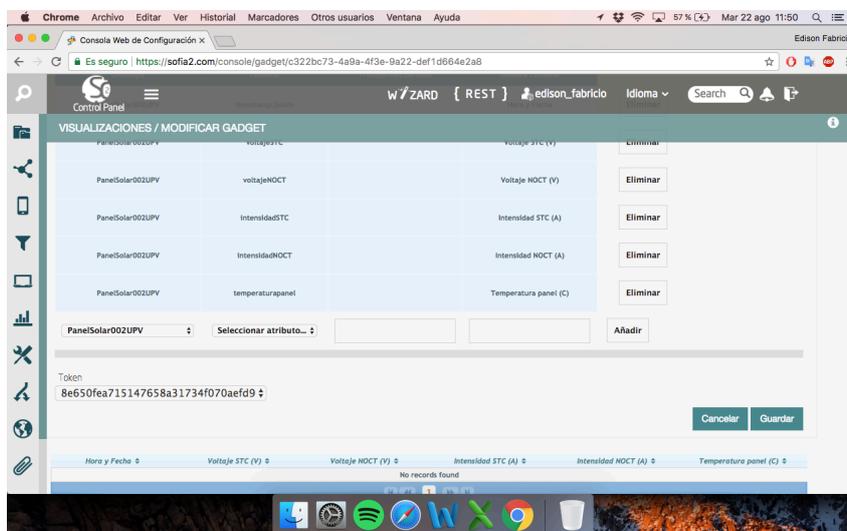


Figura 31: Herramienta de creación de graficas de información en Sofia2.

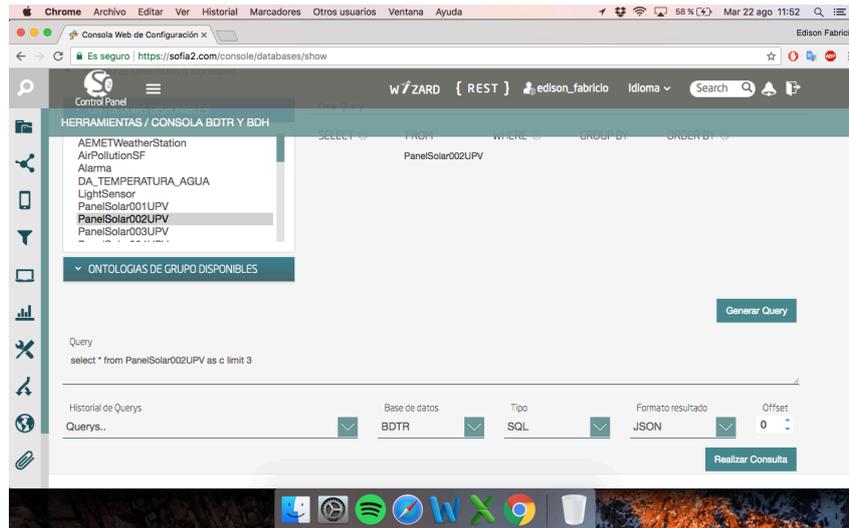


Figura 32: Herramienta de consulta de base de datos en Sofia2.

## 5.2 Resultados en Fiware

Los GE de Fiware son de acceso libre así, que en ese aspecto no existe limitaciones. Por lo tanto se eligió un tiempo igual a 30 días para la evaluación del servicio.

- Mensajes procesados por la plataforma:

Fiware usa tanto el protocolo Ultralight2.0 y JSON para el formato de los mensajes, con lo cual se aplica el mismo procedimiento que en la tabla 4. Como resultado, la plataforma Fiware debe procesar por día 6048 mensajes. La información del *datalog* correspondiente muestra que de los 181440 mensajes solo el 0,11% fueron mensajes no procesados con lo cual el 99,89% fueron mensajes exitosamente procesados por la plataforma Fiware (ver tabla 8).

- Seguridad en Fiware:

Fiware como método de seguridad implementa el sistema de autenticación por tokens. Este token es usado por el GE, ya sea el Orion Context Broker o el IDAS, y no por dispositivo. Por lo tanto, todo dispositivo que quiera conectarse con ellos deberá tener el mismo token. Esto podría traducirse como un desventaja en parámetros de seguridad, ya que si alguien no autorizado tiene acceso al token de un dispositivo, se pone en riesgo a todos los demás así como a los GE del sistema. Fiware además hace uso del protocolo TLS a nivel de GE para proteger la comunicaciones dentro de su plataforma.

Para que un GE cualquiera de Fiware o aplicaciones externas quieran consultar la información del *Context Broker* es necesario que esta conozca tanto el token, el nombre del servicio asignado (*service-path*), y el respectivo API Key.

- Modelo de Negocio en Fiware:

Como se ha hecho mención, FIWARE es una plataforma totalmente abierta y libre por lo que sus GE se pueden ser usados libremente por los desarrolladores sin necesidad de pago por licencias.

- Entorno de desarrollo en Fiware:

La plataforma Fiware ofrece en su pagina web gran variedad de recursos que el desarrollador puede explorar para conocer el funcionamiento de la plataforma. La abundante documentación es quizás muy académica y ahonda mucho en descripción de conceptos. Por ello, los desarrolladores primerizos que estén buscando información más precisa y clara de cómo empezar a construir sus aplicaciones vean esto como un inconveniente. Pero por otro lado Fiware ha hecho continuos esfuerzos de consolidar una comunidad de desarrolladores donde se puede acudir cuando la documentación se vuelve un poco dificultosa en su implementación.

Otra aspecto a tener en cuenta es que con estos GE el desarrollador tiene la opción de tener esos servicios en la nube o disponer de ellos manera local en su propia infraestructura. Esto último dota de flexibilidad a la plataforma Fiware ya que se puede adaptar a casi cualquier tipo de ambiente de aplicación y desarrollo. Dentro de los GE ofrecidos por Fiware existe una denominado COSMOS que permite implementar características de Big Data a las soluciones. Este GE trabaja de manera conjunta con el Context Broker.

En cuanto a la privacidad de la información, Fiware al ser una plataforma libre y sin licencias, que además puede ser implementada en lugar que el desarrollador desee, no usa o tiene acceso a la información que los dispositivos generan. Fiware dispone de un GE denominado CKAN que permite publicar la información que el *Context Broker* bajo el modelo de *Open Data*. Fiware es compatible con aplicaciones de terceros que hacen posible publicar la información de un *Context Broker* a través de un pagina web publica donde cualquier usuario puede acceder de manera fácil.

A pesar de todo lo anterior Fiware, no ofrece ningún tipo de entorno gráfico donde se pueda gestionar las entidades, bases de datos, seguridades, etc. Para todas estas opciones el desarrollador tiene que tener los conocimientos mínimos requeridos ya que esto es accesible a través de una consola de administración. Es posible crear las herramientas gráficas que permitan gestionar de manera mas intuitiva y fácil lo anterior, pero ello depende enormemente de los esfuerzos del desarrollador en construir dichas aplicaciones.

### **5.3 Resultados en Watson IoT**

El tiempo de evaluación de la plataforma Watson IoT es diferente al tiempo empleado en las plataformas Sofia2 y Fiware debido a que en Watson tenemos un limite en la cantidad de datos que puede procesar la plataforma en el modelo de suscripción gratuita, el cual es de 200MB. Como cada dispositivo intercambia

información de aproximadamente 2.15 MB diarios (esta información basada en las propias métricas que Watson IoT proporciona) al final del día se tiene que los datos manejados por la plataforma Watson son de 45 MB con lo cual da un tiempo de funcionamiento de 4 días bajo el modelo de suscripción gratuita.

- Mensajes procesados por la plataforma:

En base al archivo *datalog* se puede observar que durante el periodo de pruebas de 4 días la plataforma aceptó el 100% de las peticiones. Pero para no dejar este experimento limitado a este número de días se, modificó el tiempo de envío de los mensajes de cinco minutos a quince. De este modo la plataforma recibe 1890 peticiones al día, lo cual es una carga de datos correspondiente a 15 Mb aproximadamente. Con ello se puede extender el número de días a trece. Los resultados de esta nueva evaluación se muestran que de igual manera que en el caso anterior el 100% de las peticiones son aceptadas por la plataforma (ver tabla 8).

- Seguridad en Watson IoT:

Watson IoT permite que cada dispositivo maneje su propio token de autenticación para la comunicación con la plataforma. Además de ello, Watson IoT permite implementar el protocolo TLS que refuerza la poca seguridad que MQTT implementa en la mayoría de casos. Esto último asegura a los desarrolladores que los datos están encriptados y validados en todo el transcurso de la comunicación. Dentro de la plataforma Watson cada servicio dispone de un API KEY específico para consultar o modificar la información. Esto último puede ser realizado por aplicaciones externas como de otros servicios propios de Watson.

- Modelo de Negocio en Watson IoT:

Como se había mencionado anteriormente, el modelo de negocio de Watson IoT se basa en el conocido *pay-as-you-go*. En [66] la misma plataforma provee de una herramienta para calcular el costo aproximado del servicio. Este cálculo se basa en la cantidad de datos que la plataforma va a administrar, la cantidad de información que se almacenará en la base de datos, el tipo de soporte técnico que se desea recibir por parte de IBM, si se opta o no por Hardware dedicado, etc. Para clarificar de mejor manera todo lo anterior en la tabla 5 se muestran los costos de dos posibles escenarios bajo el modelo de suscripción anual. De la tabla 5, el escenario con menor costo es el primero con un valor aproximado de € 3,313.12 en relación con el segundo escenario con un valor de € 50,957.74 donde el precio más alto recae en el hardware dedicado perteneciente al servicio de la base de datos. Cabe recordar que solo se están tomando en cuenta dos servicios: el de administración de la información de los dispositivos y el almacenamiento de los mismos. Se excluye los demás servicios que integra Bluemix como son, por ejemplo, capacidades de Big Data, componentes de seguridad avanzada, integración con los servicios de inteligencia artificial de Watson IBM, entre muchos otros servicios e infraestructura que ofrece Bluemix de IBM.

- Entorno de desarrollo para Watson IoT:

IBM con Watson IoT ofrece una plataforma intuitiva, rápida, flexible y fácil de usar pero sin dejar de lado todas las características en disponibilidad, fiabilidad y seguridad que han hecho a IBM un referente en las tecnologías de la información. La documentación sobre Watson IoT es abundante, variada y fácil de usar, de forma que los desarrolladores con cualquier nivel de conocimientos en programación no tendrán en dificultades en implementar sus aplicaciones de IoT. Además de que IBM ha hecho esfuerzos por establecer una sólida comunidad de desarrolladores con la cual se compromete íntegramente a solucionar cualquier inconveniente con la que ellos se encuentren.

Tabla 5: Costo aproximado del servicio Watson IoT.

<b>ESCENARIO 1</b>			
<b>Servicio</b>	Internet of Things Platform	<b>Servicio</b>	Cloudant NoSQLDB
<b>Tipo de Suscripción</b>	Estándar	<b>Tipo de Suscripción</b>	Estándar
<b>Tiempo de Suscripción</b>	Anual	<b>Tiempo de suscripción</b>	Anual
<b>Numero de dispositivos</b>	21	<b>GB de datos almacenados</b>	1
<b>Numero de mensajes mensual por dispositivo</b>	181440	<b>Búsquedas por segundo</b>	20
<b>Tamaño del Mensaje</b>	7.45KB	<b>Escrituras por segundo</b>	10
<b>Porcentaje de datos analizados por la plataforma</b>	100%	<b>Consultas por segundo</b>	5
<b>Porcentaje de datos analizados en el Dispositivo</b>	100%		
<b>PRECIO</b>	€ 1,188.25	<b>PRECIO</b>	€ 324.88
<b>Soporte Técnico anual para ambos servicios</b>	€ 1,800.00		
<b>ESCENARIO 2</b>			
<b>Servicio</b>	Internet of Things Platform	<b>Servicio</b>	Cloudant NoSQLDB
<b>Tipo de Suscripción</b>	Seguridad Avanzada	<b>Tipo de Suscripción</b>	Hardware Dedicado
<b>Tiempo de Suscripción</b>	Anual	<b>Tiempo de suscripción</b>	Anual
<b>Numero de dispositivos</b>	21		
<b>Numero de mensajes mensual por dispositivo</b>	181440		
<b>Tamaño del Mensaje</b>	7.45KB		
<b>Porcentaje de datos analizados por la plataforma</b>	100%		
<b>Porcentaje de datos analizados en el Dispositivo</b>	100%		
<b>PRECIO</b>	€ 1,192.54	<b>PRECIO</b>	€ 45,132.00
<b>Soporte Técnico anual para ambos servicios</b>	€ 4,672.80		

Pero este servicio no es del todo accesible para todo tipo de desarrolladores, especialmente para los emprendimientos, ya que los costos que implica mantener un servicio en esta plataforma son altos. IoT Watson esta más pensando para soluciones empresariales donde se requiera altos estándares de seguridad, integridad de los datos, disponibilidad y fiabilidad de la información.

La privacidad de la información de en Watson IoT es de suma importancia para IBM. Solo los usuarios específicos pueden acceder a la información almacenada dentro de la plataforma. IBM no hace uso de la información con otros fines que no sean los de extraer estadísticas de uso para mejorar la experiencia de usuario y el rendimiento de la plataforma.

IBM Watson no ofrece una manera sencilla de hacer publica la información generada por los sensores, como por ejemplo ocurre en Sofia2, sino que es necesario construir una aplicación web que haga consultas a la base de datos respectiva por medio de un API KEY. Esto ultimo supone una ventaja en la que los desarrolladores tengan mas libertad creativa al momento de hacer publica la información, pero un inconveniente en usuarios poco experimentados en implementación de paginas web y administración de base de datos.

Watson IoT y la gama de servicios de Bluemix ofrecen una serie de herramientas adicionales, entre las que se destaca las capacidad de Big Data, que permiten al desarrollador o administrador de una solución IoT tener más control y seguridad sobre los dispositivos y datos que se están generando. Estas herramientas están disponibles en un entorno grafico intuitivo y fácil de usar, entre ellas tenemos:

- Creación de reglas específicas para cuando se cumplan determinados eventos en un dispositivo. Por ejemplo, si el valor de temperatura de un sensor sobrepasa un valor la plataforma Watson IoT puede o enviar un email de notificación o apagar/reiniciar el dispositivo.
- Métricas de la cantidad de datos transferidos por cada dispositivo. Ver figura 33.
- Gestión y consulta de estado de los dispositivos conectados a Watson IoT. Ver figura 34.
- Reglas de seguridad, donde se puede gestionar qué dispositivos están autorizados para enviar o no información a la plataforma. Así como configurar para cada dispositivo si usan o no el protocolo TLS.
- Fácil integración con los servicios de Bluemix que permitan aplicar reglas de Big Data a la información de los sensores e inteligencia artificial.
- Posibilidad de selección de la infraestructura física en diferentes zonas geográficas.
- Consulta y gestión de bases de datos. Ver figura 35.

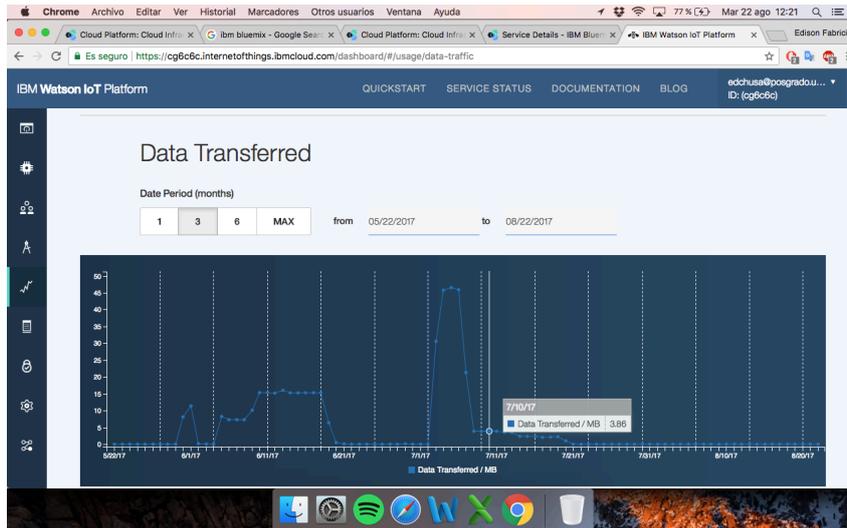


Figura 33: Herramienta de estado de datos transferidos en Watson IoT.

The screenshot shows the 'Devices' dashboard in the IBM Watson IoT Platform. The interface includes a navigation bar with 'QUICKSTART', 'SERVICE STATUS', 'DOCUMENTATION', and 'BLOG'. Below the navigation bar, there are tabs for 'Browse', 'Diagnose', 'Action', 'Device Types', and 'Manage Schemas'. A 'Refresh' button and a '+ Add Device' button are visible. The main area displays a table of devices with the following columns: Device ID, Device Type, Class ID, Date Added, and Location. The table shows 6 devices of type 'panelsolarupv'.

Device ID	Device Type	Class ID	Date Added	Location
panelsolarupv001	panelsolarupv	Device	May 31, 2017 10:13:52 AM	UPV - ITACA
panelsolarupv002	panelsolarupv	Device	May 31, 2017 10:52:33 AM	UPV - ITACA
panelsolarupv003	panelsolarupv	Device	May 31, 2017 11:14:22 AM	UPV - ITACA
panelsolarupv004	panelsolarupv	Device	May 31, 2017 11:01:29 AM	UPV - ITACA
panelsolarupv005	panelsolarupv	Device	May 31, 2017 11:02:38 AM	UPV - ITACA
panelsolarupv006	panelsolarupv	Device	May 31, 2017 11:02:27 AM	UPV - ITACA

Figura 34: Herramienta de gestión de dispositivos en Watson IoT.

The screenshot shows the 'Databases' dashboard in the IBM Watson IoT Platform. The interface includes a navigation bar with 'QUICKSTART', 'SERVICE STATUS', 'DOCUMENTATION', and 'BLOG'. Below the navigation bar, there are tabs for 'Your Databases', 'Create Database', and 'JSON'. The main area displays a table of databases with the following columns: Name, Size, # of Docs, and Actions. The table shows 8 databases.

Name	Size	# of Docs	Actions
iotp_cg6c6c_upvsolarstest_2017-w22	0.9 MB	1796	[+][-][x]
iotp_cg6c6c_upvsolarstest_2017-w23	4.2 MB	9105	[+][-][x]
iotp_cg6c6c_upvsolarstest_2017-w24	6.4 MB	14063	[+][-][x]
iotp_cg6c6c_upvsolarstest_2017-w25	0.5 MB	1066	[+][-][x]
iotp_cg6c6c_upvsolarstest_2017-w26	5.0 KB	1	[+][-][x]
iotp_cg6c6c_upvsolarstest_2017-w27	11.8 MB	25910	[+][-][x]
iotp_cg6c6c_upvsolarstest_2017-w28	1.4 MB	2859	[+][-][x]
iotp_cg6c6c_upvsolarstest_2017-w29	494.3 KB	939	[+][-][x]

Figura 35: Herramienta de gestión y consulta de bases de datos.

## 5.4 Resultados en Samsung Artik

La plataforma Artik fue sometida a una evaluación de 30 días, que es el tiempo máximo para retener la información de los sensores en la nube bajo el modelo de suscripción gratuita.

- Mensajes procesados por la plataforma:

De la información extraída del archivo *datalog*, ver tabla 8, se observa que el 100% de las peticiones han sido aceptadas por la plataforma Artik Cloud. En todo el periodo de treinta días la plataforma Artik estuvo siempre aceptando las peticiones de mensajes entrantes desde la Raspberry Pi sin rechazar ninguno. Esto demuestra los altos valores en disponibilidad y fiabilidad que la plataforma pone a disposición de los usuarios.

- Seguridad en Samsung Artik:

Artik como medida de seguridad dispone que cada dispositivo que esté registrado en la plataforma cuente con un token de seguridad. Este token y un identificador único serán necesarios para que los dispositivos puedan empezar a interactuar con la plataforma. Las aplicaciones de terceros que hagan llamados a través de una API también tendrán que usar un token para realizar la autenticación con la plataforma. Además Artik ofrece un API para implementar el protocolo de seguridad TLS en sus comunicaciones, opción solo disponible en el modelo de negocio *Enterprise*.

- Modelo de negocio en Samsung Artik:

Los servicios de Artik están disponibles bajo el modelo de negocio *pay-as-you-go* donde se diferencia si la aplicación es de tipo *Small Bussines* o *Enterprise* (ver figura 16). En el modelo *Small Bussines* se paga un valor fijo por determinados servicios y características, que también, son fijas y no variables. Este modelo es perfecto cuando el desarrollador este seguro que su aplicación no supera la característica del millón de mensajes procesados por mes y no sea necesario almacenar esta información por mas de treinta días. En la tabla 6 se muestra el valor aproximado a solventar correspondiente a un año bajo el modelo *Small Bussines*.

El modelo *Enterprise* está dirigido para usuarios corporativos y con necesidades un poco más específicas. Es por ello que, para acceder a este servicio, Samsung primero evalúa los requerimientos de la aplicación y emite el respectivo valor a solventar por el servicio.

Tabla 6: Costo aproximado del servicio Samsung Artik.

TIPO DE SUSCRIPCIÓN	TIEMPO	VALOR POR MES	TOTAL
Small Bussines	12 meses	€ 13.25	€ 159

-

- Entorno de desarrollo para Artik Samsung:

El desarrollo de aplicaciones en Artik no supone un alto grado de complejidad ya que la abundante documentación a disposición es clara y concisa. Así que los desarrolladores no tendrán mayores inconvenientes en el desarrollo de la aplicaciones además de la existencia de una solida comunidad de desarrolladores.

Dependiendo de la aplicación y de los requerimientos de la misma el desarrollador o usuario podrá elegir dentro del modelo *Small Bussines* o *Enterprise* siendo el primero el más accesible para la mayoría de desarrolladores. El segundo modelo está enfocado en soluciones a gran escala y que requieran características específicas es por ello que Samsung para este modelo de negocio no ofrece un precio estándar. De momento Artik no dispone de herramientas de Big Data en su plataforma por lo que los usuarios tienen que recurrir a plataformas o servicios externos para disponer de esta característica en sus aplicaciones.

Para la publicación abierta de la información Artik, de la misma manera que Watson IoT, dispone un API KEY para realizar consultas a la base datos. Por lo tanto el usuario debe desarrollar las herramientas, por ejemplo una pagina web, donde se cualquier usuario pueda acceder a los datos de los dispositivos.

Artik manifiesta que los datos generados por los dispositivos solo puede ser consultada y modificada por los usuarios dueños de los mismas y de terceros usuarios o aplicaciones que estén debidamente autenticados. Samsung no dispone de esta información para si misma ni la comparte con empresas terceras, cualquier que ésta sea.

Artik pone a disposición de los desarrolladores y usuarios de la plataforma una serie de herramientas que son accesibles a través de la interfaz gráfica de usuario en la web:

- Administración de los dispositivos
- Métricas del uso y propiedades de los dispositivos
- Administración de permisos y seguridades para aplicaciones y dispositivos
- Creación y administración de reglas cuando se cumplan determinadas premisas previas.
- Gráficas históricas de las propiedades de los dispositivos.
- Consulta a la base de datos.
- Métricas de uso de los diferentes servicios.
- Administración y gestión de las aplicaciones que interactúan con la plataforma Artik.

Todas estas herramientas, acompañadas de una interfaz simple, clara e intuitiva que hará que tanto desarrolladores experimentados como usuarios promedios puedan fácilmente adaptarse a la plataforma y usarla sin mayores inconvenientes (ver figura 36).

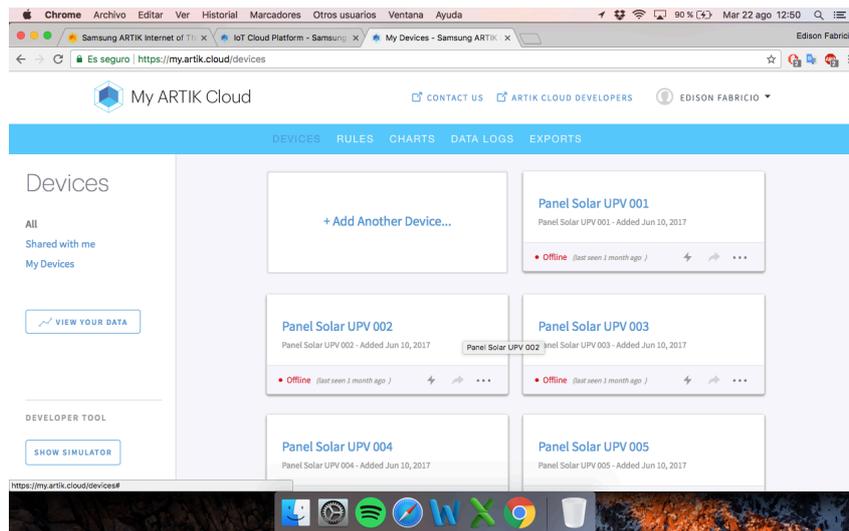


Figura 36: Interfaz grafica de usuario en Artik Samsung.

## 5.5 Resultados en Microsoft Azure IoT Suite

La plataforma Azure IoT Suite estuvo funcionando durante un periodo de 30 días bajo el modelo de suscripción gratuita que Microsoft proporciona para que desarrolladores puedan poner a pruebas sus aplicaciones y soluciones.

- Mensajes procesados por la plataforma:

En la tabla 8 se muestra las peticiones aceptadas y peticiones erróneas durante el periodo de 30 días, extraídas del respectivo archivo *datalog*. Como se puede observar en dicha tabla el 99,87% de los mensajes totales han sido aceptados y procesados por la plataforma.

- Seguridad en Microsoft Azure IoT Suite:

Los mecanismos de seguridad que Azure IoT ofrece se basan en un método de autenticación por identificador y token único de cada dispositivo. Además, permite implementar de manera nativa en cada dispositivo comunicación bidireccional usando el protocolo TLS. El servicio IoT Hub posee herramientas visuales donde se pueden administrar tokens e identificadores, métricas de accesos identificados y no identificados, intentos de acceso, etc. Esto último otorga al desarrollador o administrador de una solución IoT poderosa información sobre los parámetros de seguridad de sus dispositivos y servicios.

- Modelo de Negocio en Microsoft Azure IoT Suite:

Los servicios en la nube que Microsoft proporciona se manejan bajo el modelo *pay-as-you-go*. Microsoft en [67] ofrece una herramienta online donde los futuros clientes pueden obtener un estimado del costo anual de una determinada solución que dependerá del número de servicios usados, las características técnicas de dichos servicios y el tipo de soporte técnico que se desea recibir. En la tabla 7 se muestra el costo aproximado de la solución IoT anual que usa los mismos

Tabla 7: Costo aproximado del servicio Azure IoT Suite.

Servicio	Características	Precio Mensual	Precio Anual
<b>IoT Hub</b>	- Ilimitado numero de Dispositivos - 400000 Mensajes diarios	€ 42.17	€ 506.04
<b>Stream Analytics</b>	- 744 horas de funcionamiento	€ 75.29	€ 903.48
<b>App Fuctions</b>	- 128 en tamaño memoria de ejecución - 1 000 000 ejecuciones	€ 7.46	€ 89.52
<b>Azure Storage</b>	- Almacenamiento de 3GB - Redundancia de Datos - Acceso Frecuente	€ 0,05	€ 0.6
		<b>TOTAL</b>	<b>€ 1,499.64</b>
<b>SERVICIO TÉCNICO</b>			
<b>Gratuito</b>	- Facturación y administración de suscripciones - Panel de servicios - Envío de incidentes web	€ 0.00	€ 0.00
<b>Desarrollador</b>	- Envío de incidentes web - Break/fix ilimitado e ininterrumpido - Tiempo de respuesta más rápido (< 8 horas)	€ 24.46	€ 293.52
<b>Estandar</b>	- Envío de incidentes web - Soporte telefónico - Tiempo de respuesta más rápido (< 2 horas)	€ 252.99	€ 3,035.88
<b>Professional Direct</b>	- Atención prioritaria - Línea telefónica para remisión a instancia superior - Tiempo de respuesta más rápido (< 1 hora)	€ 843.30	€ 10,119.60

servicios que se usaron en el periodo de pruebas. Como se puede observar en la tabla 7 al costo del servicio anual de una solución estándar de IoT hay que añadir, si se prefiere, el tipo de soporte técnico que se desea recibir por parte de Microsoft.

Como se puede observar en la tabla 7 el costo del servicio anual es relativamente bajo si lo comparamos con el soporte técnico *Professional Direct* por el mismo periodo de tiempo. Cabe destacar que este último es para soluciones de tipo empresarial en donde se requiera tiempos de respuesta instantáneos en la resolución de inconvenientes.

- Entorno de desarrollo en Microsoft Azure IoT:

Microsoft pone a disposición una infinidad de documentación para ser consultada por desarrolladores o investigadores, además de una comunidad bien establecida de desarrolladores. La dificultad de la implementación de una solución IoT dependerá enormemente de las características diferenciadores de una aplicación u otra. Por ejemplo una solución solamente enfocada en recolección de datos de sensores, almacenamiento y visualización será relativamente de menor complejidad comparada con una solución que implemente características de Big Data o inteligencia artificial.

En cuanto a la privacidad de la información Microsoft, de la misma manera que los anteriores servicios en la nube, dispone que la información pertenece a la usuarios que suben dicha información y tanto aplicaciones u otros usuarios pueden acceder cuando los usuarios dueños así lo dispongan. Microsoft no comparte esta información con terceras personas o empresas.

Para la publicación de la información generada por los sensores Azure IoT dispone de un API KEY en la cual terceras aplicaciones puedan consultar la base de datos donde la información esta siendo almacenada, así como también los eventos que se activan cuando mensajes desde los sensores son enviados hacia la plataforma. De esta manera los desarrolladores pueden implementar una pagina web donde hacer publica la información generado por los dispositivos conector a los sensores.

Microsoft dispone de herramientas web online para la administración de cada uno de los recursos y sus características. Entre ellas tenemos:

- Métricas de uso de dispositivos como número de mensajes, número de conexiones. Ver figura 37.
- Gestión de permisos y seguridad de los dispositivos conectados.
- Reglas y gestión de eventos.
- Gestión de permisos y exportación de información con otros servicios de Microsoft Azure.
- Consulta de base la base datos haciendo uso de la aplicación *Microsoft Azure Storage Explorer*. Ver figura 38.
- Herramienta de gestión de errores y eventos relacionados a la los servicios que se implementen

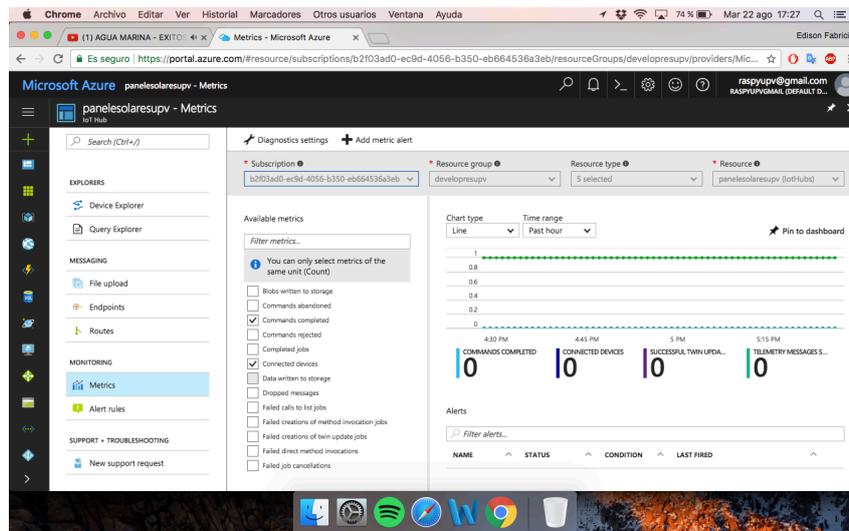


Figura 37: Métricas de uso de dispositivos en la Azure IoT.

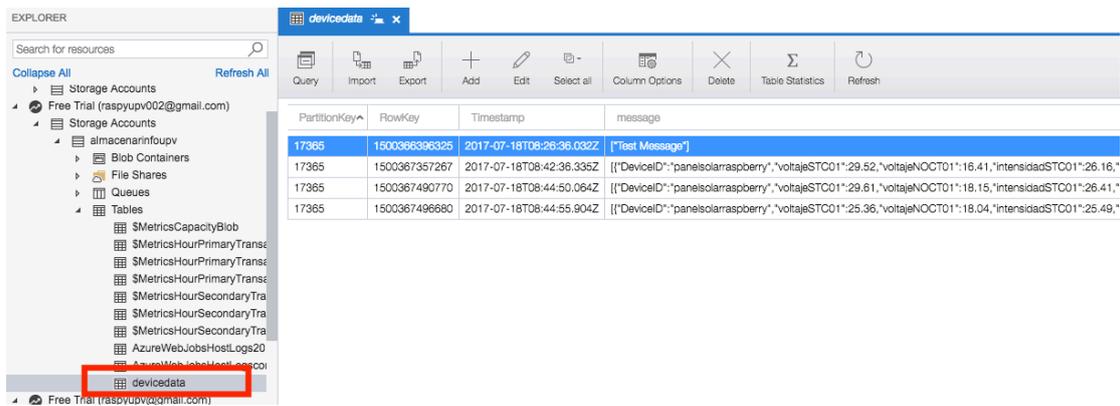


Figura 38: Aplicación Microsoft Azure Storage Explorer.

La tabla 8 recoge los resultados de los mensajes procesados por cada una de las plataformas IoT. En esta tabla se observa el tiempo de evaluación, número de mensajes, y el porcentaje de mensajes recibidos de forma satisfactoria por las plataformas IoT.

Tabla 8: Mensajes Procesados por las plataformas IoT.

SERVICIO EN LA NUBE IoT	Tiempo de evaluación	Mensajes totales	Mensajes Recibidos	Mensajes rechazados
<b>SOPIA2</b>	30 días	181440	181402 (99,98%)	38 (0,02%)
<b>FIWARE</b>	30 días	181440	181236 (99,89%)	204 (0,11%)
<b>WATSON IoT</b>	13 días	78622	78622 (100%)	0 (0%)
<b>ARTIK CLOUD</b>	30 días	181440	181440 (100%)	0 (0%)
<b>AZURE IoT</b>	30 días	181440	180972 (99,87%)	234 (0,13%)

Para finalizar, en la tabla 9 se muestra un cuadro comparativo donde se detalla de manera resumida las principales características de los servicios en la nube estudiados en este trabajo de Master. El objetivo de esta tabla es la de brindar un herramienta de comparación de los servicios IoT a los desarrolladores de aplicaciones y soluciones que estén buscando un servicio que se adapte a sus necesidades específicas.

Tabla 9: Características de los servicios en la nube para IoT.

	<b>SOFIA2</b>	<b>FIWARE</b>	<b>WATSON IoT</b>	<b>ARTIK CLOUD</b>	<b>AZURE IoT</b>
<b>Iniciativa</b>	Inicialmente Pública-europea ahora publica-privada	Pública-Europea	Privada	Privada	Privada
<b>Modelo de Negocio</b>	Modelo gratuito y pay-as-you-go	Gratuita	pay-as-you-go	pay-as-you-go	pay-as-you-go
<b>Ubicación Infraestructura</b>	En la nube y localmente	En la nube y localmente	En la nube	En la nube	En la nube
<b>Seguridad en comunicaciones</b>	- Protocolo TLS/SSL a nivel de dispositivos - Tokens de Autenticación por ontología.	- Protocolo TLS a nivel de GE - Tokens de autenticación por usuario	- Protocolo TLS/SSL a nivel de dispositivos - Tokens de autenticación por dispositivo.	- Protocolo TLS/SSL a nivel de dispositivos. - Tokens de autenticación por dispositivo .	- Protocolo TLS/SSL a nivel de dispositivos. - Tokens de autenticación por dispositivo.
<b>Protocolos de Comunicación</b>	- MQTT - HTTP - TCP - Ajax Push	- HTTP - MQTT - CoAP - Ultralight 2.0	- MQTT	- MQTT	- MQTT - AMQP - HTTP
<b>Herramientas de Big y Analytics</b>	Sí, incluida en la edición Advanced Analytics Edition	Sí, incluida en el GE Cosmos	Sí, incluida en los servicios proporcionados por Bluemix de IBM: Real Time Analytics, Machine Learning, Cognitive Analytics	No, solo almacenamiento de datos y administración de dispositivos.	Sí, incluida en los servicios proporcionados de Microsoft: Data Analytics, Real Time Analysis, Machine Learning, Data-At-REst Analysis
<b>Interoperabilidad con otras plataformas</b>	No	No	No	No	No
<b>Herramientas con Entorno Grafico</b>	Sí	No	Sí	Sí	Sí

## CAPITULO VI: CONCLUSIONES

- Actualmente la convergencia entre los paradigma de IoT y Cloud Computing ya no es un objetivo a conseguir en un futuro sino todo lo contrario. Servicios como los estudiados y evaluados en este trabajo de fin de máster demuestran que estos paradigmas son totalmente complementarios entre sí y que su unión expande aún más las posibilidades que puedan tener por separado estos paradigmas. Aunque la convergencia ya ha tenido lugar, los retos iniciales han ido cambiando y con eso nuevos desafíos han surgido y es probable que en el futuro próximo nuevos desafíos tengan que ser enfrentados para alcanzar la total convergencia.
- Como se ha observado, de los resultados del número de peticiones enviadas versus el numero de peticiones aceptadas por las plataforma en su modelo de suscripción gratuita, se puede concluir que la disponibilidad de las plataformas es un parámetro plenamente alcanzado por cada una de los servicios IoT. Aunque con el numero de mensajes diarios elegido nunca se alcanza el punto de saturación de las plataformas, esta cantidad es una muestra clara que en condiciones de uso normal estas plataformas son perfectamente viables para uso en la mayoría de aplicaciones IoT.
- Uno de los desafíos actuales y futuros es el de la seguridad tanto en las comunicaciones como en los dispositivos IoT. Aunque la mayoría de servicios IoT cuentan con mecanismos de seguridad éstos en esencia son adaptaciones de los que actualmente se usan en Internet. Por ello es necesario que se hagan esfuerzos en desarrollar e implementar nuevos mecanismos y protocolos que se adapten al entorno y necesidades propios de IoT.
- Aunque en este trabajo de fin de master solo se han evaluado cinco servicios de IoT, en el mercado actual existe una amplia variedad de los mismos. De los servicios estudiados en este trabajo de fin de master no se puede concluir fehacientemente que de los cinco servicios estudiados exista alguno que pueda convertirse en un estándar de tipo de servicio para IoT, ya que todos con sus fortalezas y debilidades están enfocados para alcanzar un mercado objetivo específico. Esto desde el punto de vista de los usuarios de dichos servicios resulta ventajoso pues se tiene a disposición una amplia variedad de servicios para elegir.
- Aunque la posibilidad de que en un futuro pueda existir un servicio IoT modelo, se puede concluir que protocolos como JSON, MQTT y TLS se han convertido en protocolos estándar dentro de IoT y Cloud Computing. La amplia aceptación de JSON y MQTT se debe a que éstos están diseñados desde su concepción para IoT aportando características de bajo consumo de potencia y recursos para su procesamiento.
- De los servicios estudiados, excepto Artik de Samsung, todos han hecho énfasis en proveer a su plataformas de capacidades de Big Data. La importancia se debe a que la enorme cantidad de información, generada por los objetos y almacenada en los servicios IoT, puede ser explotada y aplicada a un infinidad de situaciones en la vida real, por ejemplo comercio electrónico, en la cual ya no es suficiente tener datos

almacenados de los objetos sino otorgarle contexto a la información generados por esos objetos.

- La elección de un servicio IoT u otro dependerá enormemente de los requisitos propios de cada usuario o desarrollador quiera para determinada solución. Primeramente tenemos a Sofia2 que es un servicio enfocado a soluciones IoT de tipo empresarial en el que su mercado objetivo son las aplicaciones para Smart Cities. El desarrollador puede empezar con un proyecto piloto usando el modelo de suscripción gratuito y después implementar una solución con características un poco más específicas bajo el modelo pay-as-you-go. Sofia2 permite esta migración de forma amigable y segura.
- Por su parte la plataforma Fiware es ideal para fines de investigación académica y como base de proyectos de emprendimiento de todo tipo. La Unión Europea impulsa el uso profesional de la plataforma a través de varios programas de acompañamiento para desarrolladores. El modelo de licencias libre hace a Fiware ideal para su uso en todo ámbito. Aun así Fiware no ha tenido una amplia aceptación ya que la mayoría de soluciones que la emplean son de países pertenecientes a la Unión Europea. Empresas de alto grado de industrialización y tecnología por lo general no han confiado totalmente en Fiware para implementar sus diferentes servicios.
- Los servicios IoT de IBM y Microsoft por otra parte están enfocados a un mercado objetivo de tipo empresarial e industrial. Por lo tanto es de esperar que sus servicios tengan un costo alto y dependiendo del número de recursos a usar se paga un precio. Es por ello que grandes empresas de tecnología, gobiernos e industria avanzada confían en estas plataformas para implementar sus servicios. Tanto IBM y Microsoft tienen a sus espaldas años de prestigio y confianza con lo cual es más factible para una gran empresa confiar en ellos.
- Samsung, al ser una plataforma nueva y aún buscando afianzarse en el mercado de servicios IoT tiene un largo camino por recorrer aún. A pesar de que por ahora la plataforma solo es usada en proyectos pilotos cabe mencionar que en el momento en que Samsung decida implementar en cada una de su gama de productos una conexión con su propia plataforma IoT y una vez que su hardware dedicado para IoT empiece a ser utilizado masivamente, la plataforma Artik empezara a tener relevancia y más reconocimiento en la comunidad de desarrolladores.
- De las cinco plataformas en la nube estudiadas en este trabajo de fin de máster no se puede exponer de manera determinante cual de ellas es la mejor opción para un desarrollador sino que esto depende de las características que cada desarrollador este buscando para determinada aplicación. En el aspecto de prestaciones y características técnicas todas son muy similares. La diferencia radica en su modelo de prestación de servicios. Por ejemplo Fiware es ideal para proyectos de investigación científica y aplicaciones pilotos para emprendimientos en las que se requiera, durante todo el desarrollo, no pagar ningún tipo de tributo por el uso de todas sus características. Con lo cual Fiware tiene ventaja sobre otras plataformas que son de pago y solo ofrecen cortas versiones de prueba. Las ventajas de plataformas como Watson IoT, Azure y Artik

sobre Fiware es que tienen un modelo de negocio donde dependiendo del tipo de servicio y tamaño de uso en términos de hardware se debe pagar una suscripción con lo cual el desarrollador no debe preocuparse por implementación o mantenimiento de infraestructura sino solo en operar los servicios ya instalados en la infraestructura de las plataformas. Además de que estas últimas plataformas IoT ofrecen una más rápida personalización. Sofia2, en cambio, une estas dos características: es tanto libre de uso en algunos aspectos y cuenta con un modelo de pago *pay-as-you-go*. Por tanto puede resultar muy atractiva para desarrolladores que estén buscando un modelo gratuito donde implementar su proyecto piloto y poder migrar de manera fácil hacia un modelo de negocio bajo suscripción.

## BIBLIOGRAFIA

- [1] W. M. S. Stout and V. E. Urias, "Challenges to securing the Internet of Things," in *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, 2016, pp. 1–8.
- [2] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "On the Integration of Cloud Computing and Internet of Things," in *2014 International Conference on Future Internet of Things and Cloud*, 2014, pp. 23–30.
- [3] S. Andreev *et al.*, "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 32–40, Sep. 2015.
- [4] Rob van der Meulen, "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015," *Gartner webpage*, 2015. .
- [5] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du, "Research on the architecture of Internet of Things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 2010, vol. 5, pp. V5-484-V5-487.
- [6] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, "Internet of Things and Edge Cloud Computing Roadmap for Manufacturing," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 66–73, Jul. 2016.
- [7] G. Suciú, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciú, "Smart cities built on resilient cloud computing and secure internet of things," in *Proceedings - 19th International Conference on Control Systems and Computer Science, CSCS 2013*, 2013.
- [8] S. Patidar, D. Rane, and P. Jain, "A survey paper on cloud computing," in *Proceedings - 2012 2nd International Conference on Advanced Computing and Communication Technologies, ACCT 2012*, 2011.
- [9] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved," in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014*, 2014, no. January, pp. 414–419.
- [10] S. Z. S. Zhang, S. Z. S. Zhang, X. C. X. Chen, and X. H. X. Huo, "Cloud Computing Research and Development Trend," *Futur. Networks, 2010. ICFN '10. Second Int. Conf.*, pp. 93–97, 2010.
- [11] J. Krumm, *Ubiquitous Computing*. 2009.
- [12] J. Zhou *et al.*, "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," in *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2013, pp. 651–657.
- [13] G. C. Fox, S. Kamburugamuve, and R. D. Hartman, "Architecture and measured characteristics of a cloud based internet of things API," in *2012 International Conference on Collaboration Technologies and Systems (CTS)*, 2012, pp. 6–12.

- [14] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds," in *2011 IEEE 4th International Conference on Cloud Computing*, 2011, pp. 582–589.
- [15] S. Ullah *et al.*, "A comprehensive survey of wireless body area networks on PHY, MAC, and network layers solutions," *J. Med. Syst.*, vol. 36, no. 3, pp. 1065–1094, 2012.
- [16] R. Karim, N. Ithnin, S. A. Razak, and S. Najafzadeh, "DTN Routing Protocols for VANETs : Issues and Approaches," *Int. J. Comput. Sci.*, vol. 8, no. 6, pp. 89–93, 2011.
- [17] T. Bhattasali, R. Chaki, and N. Chaki, "Secure and trusted cloud of things," in *2013 Annual IEEE India Conference (INDICON)*, 2013, pp. 1–6.
- [18] S. Aguzzi *et al.*, *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination | Digital Agenda for Europe | European Commission*. 2014.
- [19] F. Li, M. Voegler, M. Claessens, and S. Dustdar, "Efficient and scalable IoT service delivery on cloud," *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 740–747, 2013.
- [20] C. Dobre and F. Xhafa, "Intelligent services for Big data science," *Futur. Gener. Comput. Syst.*, vol. 37, pp. 267–281, 2014.
- [21] A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a Service and Big Data," *Proc. Int. Conf. Adv. Cloud Comput.*, pp. 21–29, 2012.
- [22] F. Zhao, "Sensors meet the Cloud: Planetary-scale distributed sensing and decision making," *Cogn. Informatics (ICCI), 2010 9th IEEE Int. Conf.*, p. 998, 2010.
- [23] Applica2, "FIWARE: ¿Que es Fiware?" [Online]. Available: <http://www.applica2.com/es/fiware>. [Accessed: 27-Jul-2017].
- [24] INDRA, "SOFIA2, LA SOLUCIÓN DE INTEGRACIÓN PARA SMART CITIES DE INDRA, AYUDA A LOS EMPRENDEDORES A DISEÑAR IDEAS DESDE LA NUBE," 2014. [Online]. Available: <http://www.indracompany.com/es/noticia/sofia2-solucion-integracion-smart-cities-indra-ayuda-emprendedores-disenar-ideas-nube>. [Accessed: 27-Jul-2017].
- [25] INDRA, "Sofia2 Conceptos Basicos." [Online]. Available: <http://sofia2.com/docs/SOFIA2-Conceptos SOFIA2.pdf>. [Accessed: 31-May-2017].
- [26] INDRA, "Indra Pagina Oficial." [Online]. Available: <http://www.indracompany.com/es/indra>.
- [27] INDRA, "Sofia2 Welcome Pack." [Online]. Available: <http://sofia2.com/docs/Sofia2-Welcome Pack-v03.pdf>. [Accessed: 31-May-2017].
- [28] INDRA, "Sofia 2: Capacidades," 2016. [Online]. Available: <http://sofia2.com>. [Accessed: 31-May-2017].
- [29] INDRA, "Sofia2 Iot Platform," 2016. [Online]. Available:

- [http://sofia2.com/docs/Sofia2\\_IoT\\_Platform-Vista\\_Tecnica\(nov\\_2016\).pdf](http://sofia2.com/docs/Sofia2_IoT_Platform-Vista_Tecnica(nov_2016).pdf). [Accessed: 31-May-2017].
- [30] INDRA, "Modelo Comercial Plataforma Sofia2." [Online]. Available: [https://www.slideshare.net/IndraSofia2SmartPlatform/modelo-comercial-plataforma-sofia2?from\\_action=save](https://www.slideshare.net/IndraSofia2SmartPlatform/modelo-comercial-plataforma-sofia2?from_action=save). [Accessed: 31-May-2017].
- [31] Sofia2, "Sofia2: Casos de Uso," 2016. [Online]. Available: <http://sofia2.readthedocs.io/en/latest/casosdeuso.html>. [Accessed: 03-Jul-2017].
- [32] European Commission, "Future Internet Public Private Partnership." [Online]. Available: <https://ec.europa.eu/digital-single-market/future-internet-public-private-partnership>. [Accessed: 26-Jun-2017].
- [33] Atos, "Telefónica, Orange, Engineering y Atos unen fuerzas para impulsar estándares comunes para Smart Cities basados en la plataforma FIWARE." [Online]. Available: [https://atos.net/es/2015/comunicados-de-prensa-es\\_2015\\_03\\_03/es-pr-2015\\_03\\_03\\_01?utm\\_source=es.atos.net/es-es/home/quienes-somos/noticias-y-eventos/noticias/2015/pr-2015\\_03\\_03\\_01.html&utm\\_medium=301](https://atos.net/es/2015/comunicados-de-prensa-es_2015_03_03/es-pr-2015_03_03_01?utm_source=es.atos.net/es-es/home/quienes-somos/noticias-y-eventos/noticias/2015/pr-2015_03_03_01.html&utm_medium=301). [Accessed: 26-Jun-2017].
- [34] Fiware, "Fiware: About Us." [Online]. Available: <https://www.fiware.org/about-us/>. [Accessed: 26-Jun-2017].
- [35] M. G. González, "FINODEX introduces FIWARE," 2015. [Online]. Available: <https://www.slideshare.net/finodexproject/fiware-summary>. [Accessed: 26-Jun-2016].
- [36] Fiware, "Development of context-aware applications: Introduction." [Online]. Available: <http://fiwaretourguide.readthedocs.io/en/latest/development-context-aware-applications/introduction/>. [Accessed: 26-Jun-2017].
- [37] Fiware, "Connection to the Internet of Things: Introduction." [Online]. Available: <http://fiwaretourguide.readthedocs.io/en/latest/connection-to-the-internet-of-things/introduction/>. [Accessed: 27-Jun-2017].
- [38] Fiware, "User & Programmers Manual: API Walkthrough & Development intro." [Online]. Available: <http://fiware-iotagent-ul.readthedocs.io/en/latest/usermanual/index.html>. [Accessed: 29-Jun-2017].
- [39] Fiware, "Internet of Things (IoT) Services Enablement Architecture." [Online]. Available: [http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Internet\\_of\\_Things\\_%28IoT%29\\_Services\\_Enablement\\_Architecture](http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Internet_of_Things_%28IoT%29_Services_Enablement_Architecture). [Accessed: 27-Jun-2017].
- [40] Fiware, "Fiware: Success Stories," 2016. [Online]. Available: [https://www.fiware.org/success\\_stories](https://www.fiware.org/success_stories). [Accessed: 03-Jul-2017].
- [41] IBM Bluemix, "Bluemix Docs: Internet of Things Platform - About Watson IoT Platform," 2017. [Online]. Available: [https://console-regional.ng.bluemix.net/docs/services/IoT/iotplatform\\_overview.html#about\\_iotplatform](https://console-regional.ng.bluemix.net/docs/services/IoT/iotplatform_overview.html#about_iotplatform). [Accessed: 04-Jul-2017].

- [42] IBM Bluemix, "Bluemix Docs: Internet of Things Platform - Watson IoT Platform Feature Overview," 2017. [Online]. Available: [https://console-regional.ng.bluemix.net/docs/services/IoT/feature\\_overview.html#feature\\_overview](https://console-regional.ng.bluemix.net/docs/services/IoT/feature_overview.html#feature_overview). [Accessed: 04-Jul-2017].
- [43] J. McCarthy, "How Visa Embraced IoT to Advance Commerce," 2017. [Online]. Available: <https://www.ibm.com/blogs/think/2017/02/visa-iot/>. [Accessed: 04-Jul-2017].
- [44] N. & N. ARMONK, "HARMAN and IBM Watson Internet of Things Introduce Cognitive Rooms that Bring Connected Experiences to the Consumer," 2017. [Online]. Available: <http://www-03.ibm.com/press/us/en/pressrelease/51958.wss>. [Accessed: 04-Jul-2017].
- [45] IBM, "French National Railway Company Accelerates Innovation with Watson Internet of Things on IBM Cloud," 2017. [Online]. Available: <http://www-03.ibm.com/press/us/en/pressrelease/51570.wss>. [Accessed: 04-Jul-2017].
- [46] Samsung, "Artik Cloud: The fastest way to connect siloed devices and enable new services.," 2017. [Online]. Available: [https://www.artik.io/library/?q=cloud&hPP=10&idx=Download\\_production&p=0&dFR%5Bdocument\\_types%5D%5B0%5D=Product Briefs&is\\_v=1](https://www.artik.io/library/?q=cloud&hPP=10&idx=Download_production&p=0&dFR%5Bdocument_types%5D%5B0%5D=Product Briefs&is_v=1). [Accessed: 10-Jul-2017].
- [47] Samsung, "Samsung ARTIK End-to-end IoT," 2017. [Online]. Available: <https://www.artik.io/overview/samsung-artik-end-end-iot/>. [Accessed: 10-Jul-2017].
- [48] Samsung, "Artik Cloud Developers: Basics," 2017. [Online]. Available: <https://developer.artik.cloud/documentation/getting-started/basics.html>. [Accessed: 10-Jul-2017].
- [49] Samsung, "Samsung ARTIK Platform Overview," 2016. [Online]. Available: <http://developer.artik.io/downloads/c72ee2af-c78a-4bac-a9e8-d0be00f8ddb9/download>. [Accessed: 10-Jul-2017].
- [50] Samsung, "Samsung Announces Commercially Available IoT Cloud Platform to Deliver Interoperability Between Devices and Applications," USA, 27-Apr-2016.
- [51] R. Kuo, "Watch a video of Peugeot's ARTIK Cloud enabled car," 2017. [Online]. Available: <https://www.artik.io/blog/2017/05/peugeots-artik-cloud-enabled-car/>. [Accessed: 10-Jul-2017].
- [52] F. Patton, "Samsung ARTIK Case Study – The Kontakt.io Gateway," 2016. [Online]. Available: <https://www.artik.io/blog/2016/10/case-study-kontakt-io-gateway/>. [Accessed: 10-Jul-2017].
- [53] A. Team, "ARTIK Cloud + T-Mobile + Breezie = improving senior care," 2017. [Online]. Available: <https://www.artik.io/blog/2017/02/artik-cloud-t-mobile-breezie-improving-senior-care/>. [Accessed: 10-Jul-2017].
- [54] Microsoft, "Azure y el Internet de las cosas," 2017. [Online]. Available: <https://docs.microsoft.com/es-es/azure/iot-hub/iot-hub-what-is-azure-iot>. [Accessed: 12-Jul-2017].

- [55] Microsoft, "What are the Azure IoT Suite preconfigured solutions?," 2017. [Online]. Available: <https://docs.microsoft.com/en-us/azure/iot-suite/iot-suite-what-are-preconfigured-solutions>. [Accessed: 12-Jul-2017].
- [56] Microsoft Docs, "Microsoft Azure IoT Reference Architecture Azure," no. November, p. 231, 2016.
- [57] C. Vasters, "'Service Assisted Communication' for Connected Devices," 2014. [Online]. Available: <https://blogs.msdn.microsoft.com/clemensv/2014/02/09/service-assisted-communication-for-connected-devices/>. [Accessed: 12-Jul-2017].
- [58] Microsoft Docs, "Introducción al servicio Azure IoT Hub," 2017. [Online]. Available: <https://docs.microsoft.com/es-es/azure/iot-hub/iot-hub-what-is-iot-hub>. [Accessed: 12-Jul-2017].
- [59] Microsoft, "Casos de éxito de Microsoft IoT," 2017. [Online]. Available: <https://www.microsoft.com/es-es/internet-of-things/customer-stories#manufacturing&rollsroyce>. [Accessed: 13-Jul-2017].
- [60] Microsoft, "Rolls-Royce and Microsoft collaborate to create new digital capabilities," 2016. [Online]. Available: <https://customers.microsoft.com/en-US/story/rollsroycestory>. [Accessed: 13-Jul-2017].
- [61] Microsoft, "BCA partners Microsoft to leverage IoT, data analytics and the cloud for next-generation Green Mark buildings," 2016. [Online]. Available: <https://news.microsoft.com/en-sg/2016/09/07/bca-partners-microsoft-to-leverage-iot-data-analytics-and-the-cloud-for-next-generation-green-mark-buildings/#sm.0002m8g83164iegevdh1fgvzcxz9a%23b10sylSLzekuSWri.97>. [Accessed: 13-Jul-2017].
- [62] Microsoft, "Fathym's IoT-enabled WeatherCloud enhances driver safety during inclement weather," 2016. [Online]. Available: <https://blogs.microsoft.com/iot/2016/12/09/fathyms-iot-enabled-weathercloud-enhances-driver-safety-during-inclement-weather/>. [Accessed: 13-Jul-2017].
- [63] Microsoft, "Fueling the oil and gas industry with IoT," 2015. [Online]. Available: <https://customers.microsoft.com/en-US/story/fueling-the-oil-and-gas-industry-with-iot-1>. [Accessed: 13-Jul-2017].
- [64] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a Service Model for Smart Cities Supported by Internet of Things," *Eur. Trans. Telecommun.*, vol. 25, no. 3, pp. 294–307, Jul. 2013.
- [65] A. Molina-García, J. C. Campelo, S. Blanc, J. J. Serrano, T. García-Sánchez, and M. C. Bueso, "A decentralized wireless solution to monitor and diagnose PV solar module performance based on symmetrized-shifted gompertz functions," *Sensors (Switzerland)*, vol. 15, no. 8, pp. 18459–18479, 2015.
- [66] IBM, "IBM Bluemix: Pricing Calculator." [Online]. Available: <http://iot-cost-calculator.ng.bluemix.net/customise>. [Accessed: 06-Jul-2017].

- [67] Microsoft, "Microsoft Azure: Calculadora de precios," 2017. [Online]. Available: <https://azure.microsoft.com/es-es/pricing/calculator/>. [Accessed: 14-Jul-2017].

## **ANEXOS**