

UNIVERSIDAD POLITECNICA DE VALENCIA
ESCUELA POLITECNICA SUPERIOR DE GANDIA
Grado en Ing. Sist. de Telecom., Sonido e Imagen



UNIVERSIDAD
POLITECNICA
DE VALENCIA



ESCUELA POLITECNICA
SUPERIOR DE GANDIA

**“INTERCONEXIÓN DE
DISPOSITIVOS IoT
(Internet Of Things) CON
PLATAFORMA SOFIA2”**

TRABAJO FINAL DE GRADO

Autor/a:
Víctor Vicente Cebrián

Tutor/a:
María Consuelo Part Escrivá

GANDIA, 2017

RESUMEN

Las siglas IoT hacen referencia al concepto Internet Of Things, también conocido en castellano como Internet De Las Cosas. Las tecnologías IoT hacen que sea fácil conectar todo tipo de cosas a la red y desarrollar aplicaciones para controlar y administrar estas 'things'. Todas las complejidades de habilitar la conectividad, los servicios y el despliegue para estos dispositivos es tarea de la plataforma IoT.

Una plataforma IoT se encarga de garantizar la integración con diferentes dispositivos hardware soportando una amplia gama de protocolos de comunicación. A través de los interfaces de integración proporcionados por la plataforma, también puede gestionar los datos IoT recopilados hacia sistemas específicos de almacenamiento y visualización de datos, así como transmitir datos a dispositivos conectados (configuración, notificaciones) o entre ellos (controles, eventos).

El presente proyecto versa en torno a estos dos conceptos y muestra el uso de dispositivos capaces de medir diferentes parámetros y cómo se conectan mediante gateways a la plataforma IoT y Big Data Sofia2.

Se explicará el estado del arte del IoT, qué protocolos son los más usados en estas tecnologías, y cuáles son los pasos a seguir para recoger datos, transportarlos, transformarlos y visualizarlos en la plataforma Sofia2.

Palabras clave: Internet Of Things, plataforma IoT, dispositivo, protocolo, datos.

ABSTRACT

The acronym IoT stands for the concept Internet Of Things. IoT technologies make it easy to connect all kinds of things to the network and develop applications to control and manage them. All the complexities of enabling connectivity, services and deployment for these devices is the task of the IoT platform.

An IoT platform ensures integration with different hardware devices supporting a wide range of communication protocols. Through the integration interfaces provided by the platform, it can also manage IoT data collected to specific data storage and visualization systems, as well as transmit data to connected devices (configuration, notifications) or between them (tests, events).

The present project revolves around these two concepts and shows the use of devices capable of measuring different parameters and how they are connected through gateways to the IoT and Big Data Sofia2 platform.

The state of the art of IoT will be explained, which protocols are the most used in these technologies, and which the steps are to follow to collect data, to transport them, to transform them and to visualize them in Sofia2 platform.

Keywords: Internet Of Things, IoT platform, device, protocol, data.

ÍNDICE

1. Introducción.....	1
1.1 Objetivos.....	1
1.2 Metodología.....	2
1.3 Etapas.....	2
2. Estado del Arte de las tecnologías IoT.....	3
3. Plataformas IoT	7
3.1 Capacidades de una plataforma IoT	7
3.2 Comparativa entre plataformas IoT.....	8
3.3 Elección de plataforma IoT: Sofia2	9
4. Protocolos de comunicación.....	17
4.1 MQTT	18
4.2 Restful Services	20
4.3 Comparativa de protocolos de comunicación.....	21
5. Hardware empleado	22
5.1 SensorTag CC2650	23
5.2 Gateway. Smartphone Android Xiaomi Redmi Note 4	23
6. Aplicación práctica	25
6.1 Crear un usuario en Sofia2	25
6.2 Crear una Ontología	26
6.3 Crear un ThinkKP	28
6.4 Descarga y configuración del archivo .APK Sofia2	29
6.5 Caso de uso: Acelerómetro y geolocalización	30
6.5.1 Comprobación de datos recibidos en la plataforma	31
6.5.2 Creación de gadgets y dashboard	32
6.6 Caso de uso: Detección de Beacon y notificación automática.....	40
7. Conclusiones	43
8. Índice de figuras	44
9. Bibliografía y referencias	46

1 INTRODUCCIÓN

Este trabajo Final de Grado surge de la necesidad de indagar sobre las posibilidades que nos presentan las nuevas tecnologías emergentes como son el IoT y el Big Data e intentar discernir cómo son capaces de mejorar nuestras vidas, ya que se están integrando en todos los aspectos de nuestro día a día.

En el último año de mi vida he tenido la oportunidad de aprender lo que significa formar parte del núcleo de desarrollo de una plataforma IoT trabajando en la empresa Indra y ayudando al crecimiento de Sofia2, su plataforma IoT y Big Data.

El presente trabajo se tratará desde un punto de vista teórico-práctico. Por un lado, se realizará un estudio del momento actual de éstas tecnologías, los protocolos más usados y algunas de las plataformas existentes y sus características y por otro lado, se mostrará paso a paso cómo conectar dispositivos a la plataforma Sofia2 y cómo enviar datos, tratarlos, crear visualizaciones de estos datos y establecer alarmas ante la aparición de eventos.

1.1 OBJETIVOS

Objetivo principal

Partiendo de un conocimiento general de las tecnologías, nos adentraremos en un hands on donde descubriremos cómo conectar dispositivos con una plataforma IoT como es Sofia2.

Mostraremos los elementos que componen el sistema y veremos paso a paso como enlazar con la plataforma, y como realizar todo el flujo que seguirán los datos, desde su captación sensorial hasta la toma de decisiones por mediación de Scripts en la plataforma.

Objetivos secundarios

- Definición de los protocolos usados en IoT
- Conocimiento de las plataformas más usadas actualmente
- Descripción y uso de los parámetros de un beacon
- Definición de la arquitectura usada en una plataforma IoT
- Visión de las capacidades y funcionamiento de una plataforma IoT
- Uso del acelerómetro y del sistema de geolocalización de un dispositivo.

1.2 METODOLOGÍA

Tras conocer el estado del arte del IoT y lo que representan las plataformas dentro del mundo IoT, procederemos a la elección del dispositivo y al hardware que usaremos en nuestra aplicación práctica. A continuación se realizará un primer testeo de funcionamiento de los dispositivos elegidos y se iniciará el flujo que se seguirá para implementar su conexión con la plataforma y posterior procesado de los datos obtenidos.

1.3 ETAPAS

A continuación se resumen los principales pasos de ejecución del TFG:

1. Investigación, búsqueda bibliográfica y estudio del estado del arte de las tecnologías IoT.
2. Elección de los elementos hardware (gateways, sensores, beacons...) y compra de los mismos.
3. Aprendizaje del uso del beacon CC2650 SensorTag de Texas Instruments y de los parámetros que ofrece.
4. Comparativa de distintas plataformas de IoT (Internet of Things) para la adquisición, almacenamiento y visualización de datos recogidos por el SensorTag. Elección de Sofia2 como plataforma.
5. Aprendizaje del funcionamiento de la plataforma Sofia2 y pruebas de uso.
6. Descarga de la Apk Sofia2 IoT, sus parámetros y cómo configurarla.
7. Primeras pruebas de interconexión entre el Gateway (uso del smartphone Xiaomi Redmi Note 4) y la plataforma.
8. Pruebas de interconexión del Beacon con el Gateway.
9. Creación de todo el flujo para envío y visualización de datos procedentes del beacon y el Gateway. Creación de Ontologías, ThinkKP, Gadgets y Dashboard.
10. Creación de Script para envío de email ante un evento de localización del beacon.
11. Estudio pormenorizado de los distintos protocolos existentes para IoT.
12. Redacción de la memoria del proyecto.

2 ESTADO DEL ARTE DE LAS TECNOLOGÍAS IoT

Gartner es la Consultora de referencia en investigaciones sobre las tecnologías de la información. Mediante sus informes periódicos como son el Hype Cycle o sus famosos Cuadrantes Mágicos presenta tendencias en cada uno de los sectores relacionados con el mundo tecnológico.

El Hype Cycle de Tecnologías Emergentes de Gartner es una representación gráfica de la madurez, adopción y aplicación comercial de tecnologías específicas. El informe Hype Cycle se publica de forma anual y proporciona una perspectiva transversal de las tendencias de la industrias tecnológicas emergentes, ayudando a discernir si nos encontramos ante una sobreexpectación o ante una tecnología viable.

En su último Hype Cycle de Tecnologías Emergentes [1] publicado en Julio de 2017, podemos observar que las tecnologías directamente relacionadas con el IoT y las plataformas IoT se sitúan en lo que ellos denominan Peak of Inflated Expectations:

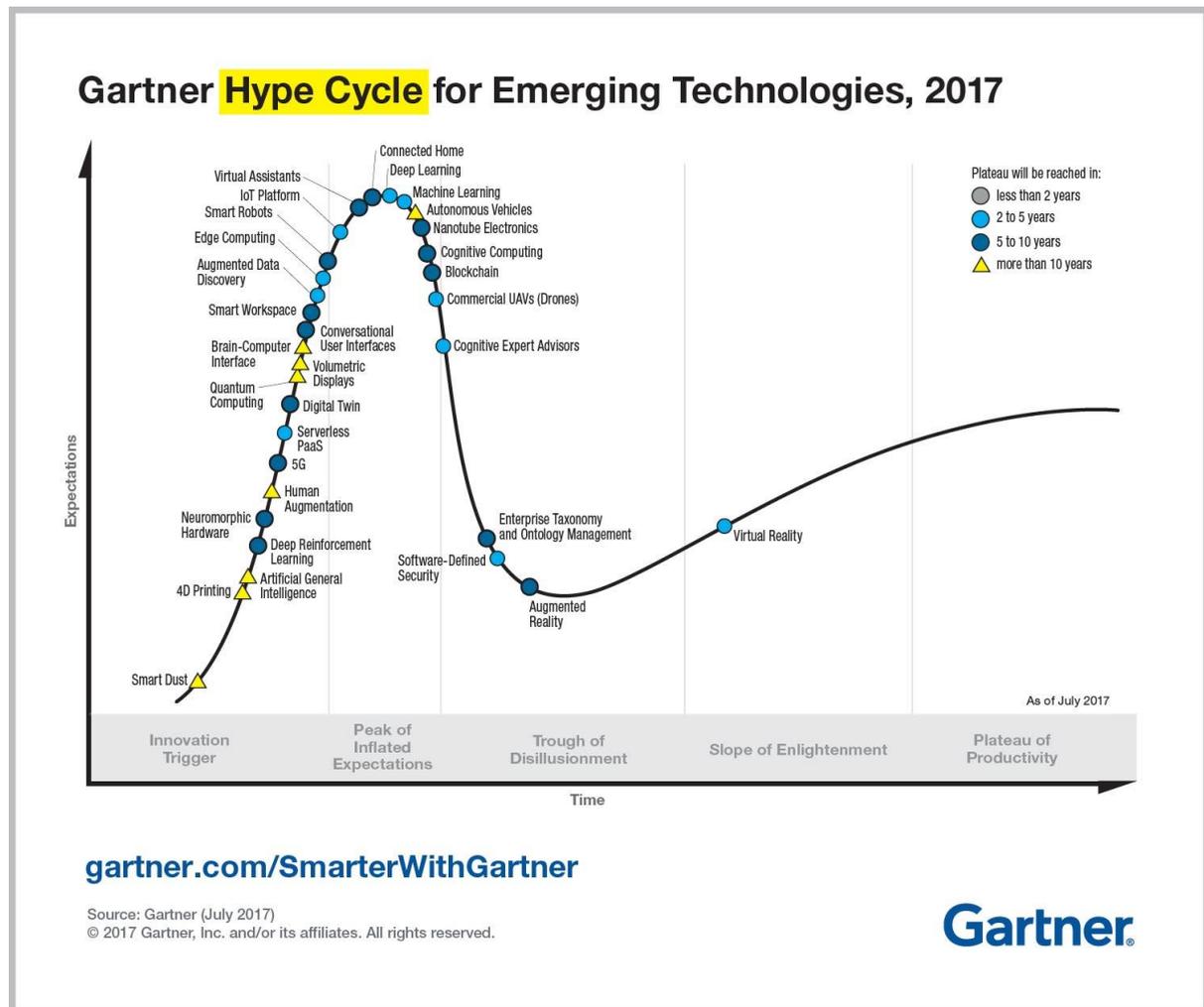


Figura 1. Gartner Hype Cycle para tecnologías emergentes. Julio 2017 [1]

La gráfica se divide en los diferentes ciclos de vida de las tecnologías:

- **Innovation Trigger:** cualquier avance, demostración, lanzamiento de producto o evento genera interés por parte de la industria y la prensa.
- **Peak of Inflated Expectations:** durante esta fase de sobreentusiasmo y proyecciones no realistas algunos líderes consiguen éxitos pero hay más fracasos al encontrar los límites de la tecnología. Las empresas que hacen dinero son los organizadores de conferencias y magazines.
- **Through of Disillusionment:** desilusión porque la tecnología no está a la altura de sus expectativas y rápidamente se pasa de moda. El interés de los medios disminuye.
- **Slope of Enlightenment:** experimentos enfocados y un trabajo sólido lleva a un verdadero entendimiento de la aplicabilidad de la tecnología, riesgos, y beneficios por parte de un amplio rango de organizaciones. Aparecen herramientas y tecnologías estándares que facilitan el proceso de desarrollo.
- **Plateau of Productivity:** los beneficios reales de la tecnología son demostrados y aceptados. Las herramientas y metodologías se estabilizan entrando en segundas y terceras generaciones. Crece el número de organizaciones que lo usan al reducirse el nivel de riesgo, la adopción crece rápidamente. Aproximadamente el 20% de la audiencia target adopta o está adoptando la tecnología en esta fase.

Como vemos, Gartner pone el foco en varias tecnologías íntimamente ligadas al Internet Of Things. Mientras que el Hogar Conectado (Connected Home), alcanzará el Plateau of Productivity en cuestión de 5 a 10 años, los Vehículos Autónomos (Autonomous Vehicles) se demorarán más de 10 años debido a su relación con la Inteligencia Artificial y a la adaptación de infraestructuras que se deben realizar en las Smart Cities. Por otra parte, se estima que las Plataformas IoT alcancen este hito en menos tiempo, entre 2 y 5 años.

Internet Of Things nos abre un gran abanico de posibilidades para mejorar nuestras vidas desarrollando soluciones en cada uno de los campos en los que interviene:

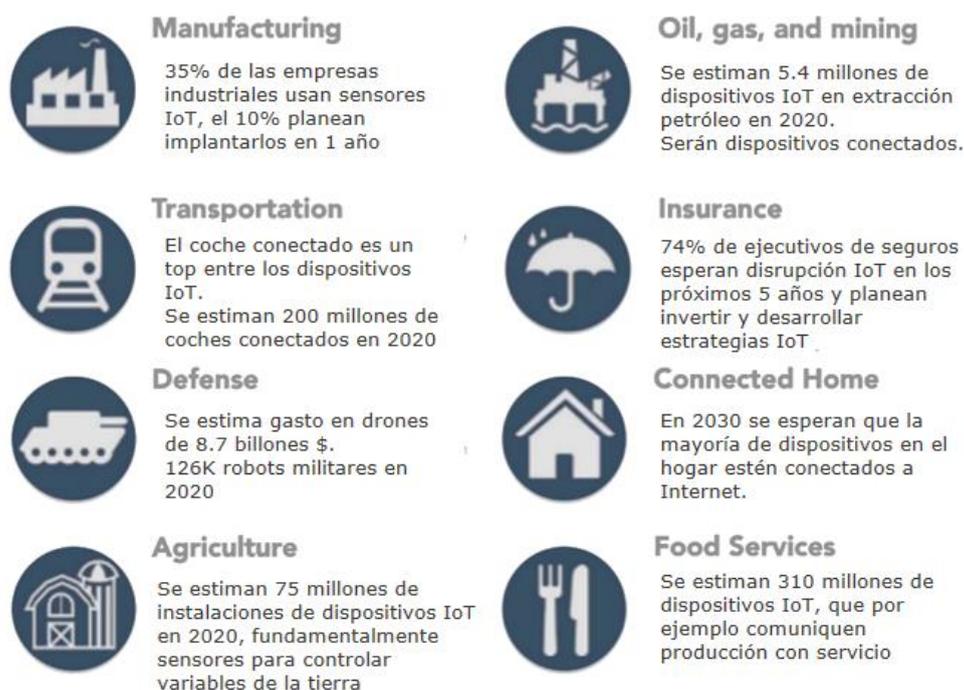


Figura 2. Estimación del crecimiento IoT por sectores. Parte 1



Figura 3. Estimación del crecimiento IoT por sectores. Parte 2

Por otro lado, Gartner identifica [2] que las 10 principales tecnologías IoT para 2017 y 2018 serán:

- 1. Seguridad IoT.** IoT introduce nuevos riesgos y desafíos de seguridad a nivel de dispositivos, plataformas, sistemas operativos, comunicaciones y sistemas conectados. La seguridad IoT es aún más complicada en "things" básicas que no permiten sofisticados mecanismos de seguridad.
- 2. Analítica IoT.** Los modelos de negocio IoT explotarán la información recolectada de las "things" de muchas formas: entender el comportamiento de clientes, mejorar productos, prestar nuevos servicios. IoT requiere nuevas aproximaciones analíticas, con nuevas herramientas y algoritmos.
- 3. Gestión de dispositivos IoT.** Las "things" de larga vida requieren gestión y monitorización, tanto del dispositivo, del firmware, de las actualizaciones de software, reporting, gestión de la seguridad... Las herramientas deben escalar para miles y millones de dispositivos.
- 4. Redes de baja potencia y corto alcance.** Seleccionar una red inalámbrica para un dispositivo IoT requiere balancear diversos requisitos contradictorios, como la vida de la batería, ancho de banda, rango, costes de los dispositivos, costes operacionales... Estas redes de baja potencia y corto alcance dominarán la conectividad IoT wireless en el futuro, coexistiendo varias sin una única ganadora.
- 5. Redes de baja potencia y largo alcance.** Las redes celulares tradicionales no son las más adecuadas, cuando hablamos de redes IoT wide-area se buscan ratios de transferencia de Kbps, cobertura global, vida de la batería de hasta 10 años, coste del hardware sobre los 5\$ y soportando conexiones de cientos de miles de dispositivos a una estación base. En el largo plazo el estándar NB-IoT (Narrowband IoT) dominará este espacio.

6. Procesadores IoT. Los procesadores y arquitecturas para dispositivos IoT definen sus capacidades. Hay que sopesar las diferentes características buscadas: coste del HW, coste del SW, actualizaciones, encriptado...

7. Sistemas Operativos IoT. Los sistemas tradicionales no fueron diseñados para aplicaciones IoT, ya que consumen mucha potencia, necesitan procesadores potentes, necesitan mucha memoria y no garantizan respuesta en tiempo real. Existen y existirán un amplio conjunto de sistemas operativos IoT para adecuarse a los diferentes HW y capacidades necesarios.

8. Event Stream Processing. Muchas aplicaciones IoT generarán muchos datos en tiempo real que deben ser analizados. Para cubrir estos requisitos han emergido plataformas DSCP (plataformas de computación de stream distribuido).

9. Plataformas IoT. Las plataformas IoT encapsulan muchos de los componentes de infraestructura de un sistema IoT en un único producto. Los servicios de estas plataformas se pueden clasificar en 3 categorías: Control del dispositivo a bajo nivel, monitorización y gestión del dispositivo, comunicación y seguridad. Adquisición, transformación y gestión de datos en IoT. Desarrollo de aplicaciones IoT incluyendo visualización, lógica event-driven, programación de aplicaciones, analítica y adaptadores para conectar con sistemas empresariales.

10. Estándares y ecosistemas IoT. Los estándares y sus APIs son esenciales para que los dispositivos IoT puedan interoperar y comunicar. Emergerán diversos ecosistemas IoT. Las organizaciones que crean productos pueden necesitar desarrollar variaciones soportando diversos estándares y estar preparadas para actualizar productos durante su ciclo de vida según evolucionan los estándares.

Como vemos en la siguiente infografía [3] basada en información proporcionada por la empresa Cisco, el crecimiento e implantación de dispositivos IoT crece de una forma exponencial, abriendo grandes posibilidades, no solo de negocio, sino de una mejora cualitativa de nuestra vida cotidiana.

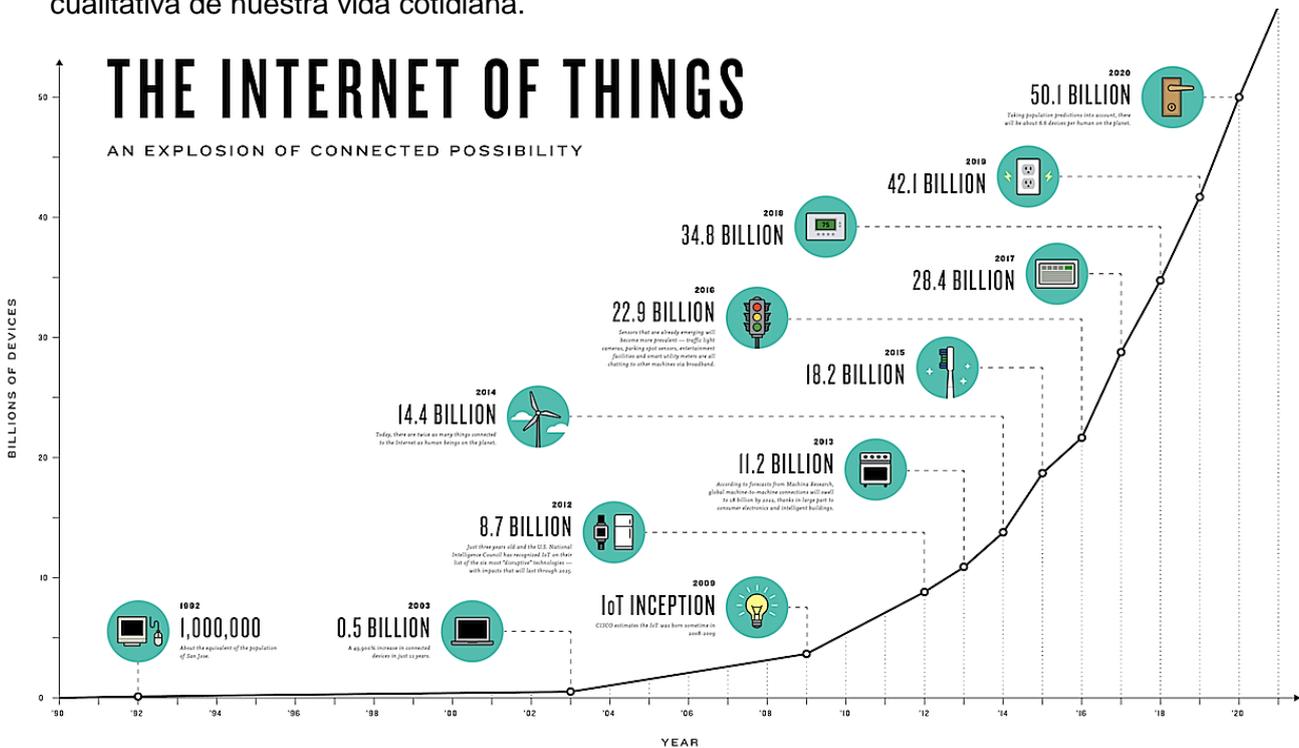


Figura 4. Infografía sobre el crecimiento previsto de los dispositivos IoT [3]

3 PLATAFORMAS IoT

En el informe Market Guide for IoT Platforms [4], se recomiendan una serie de características que deben contener las plataformas IoT. Como hemos comentado, todas las complejidades de habilitar la conectividad, los servicios y el despliegue para los dispositivos es tarea de la plataforma IoT.

3.1 CAPACIDADES DE UNA PLATAFORMA IoT

Una plataforma IoT generalmente incorpora soluciones que involucran endpoints IoT (sensores), Gateways IoT y aplicaciones empresariales back-end.

La plataforma tiene la capacidad de:

- Supervisar los flujos de eventos IoT
- Permitir la agregación de datos
- Análisis especializados
- Desarrollo de aplicaciones
- Integración con sistemas y servicios TI de back-end

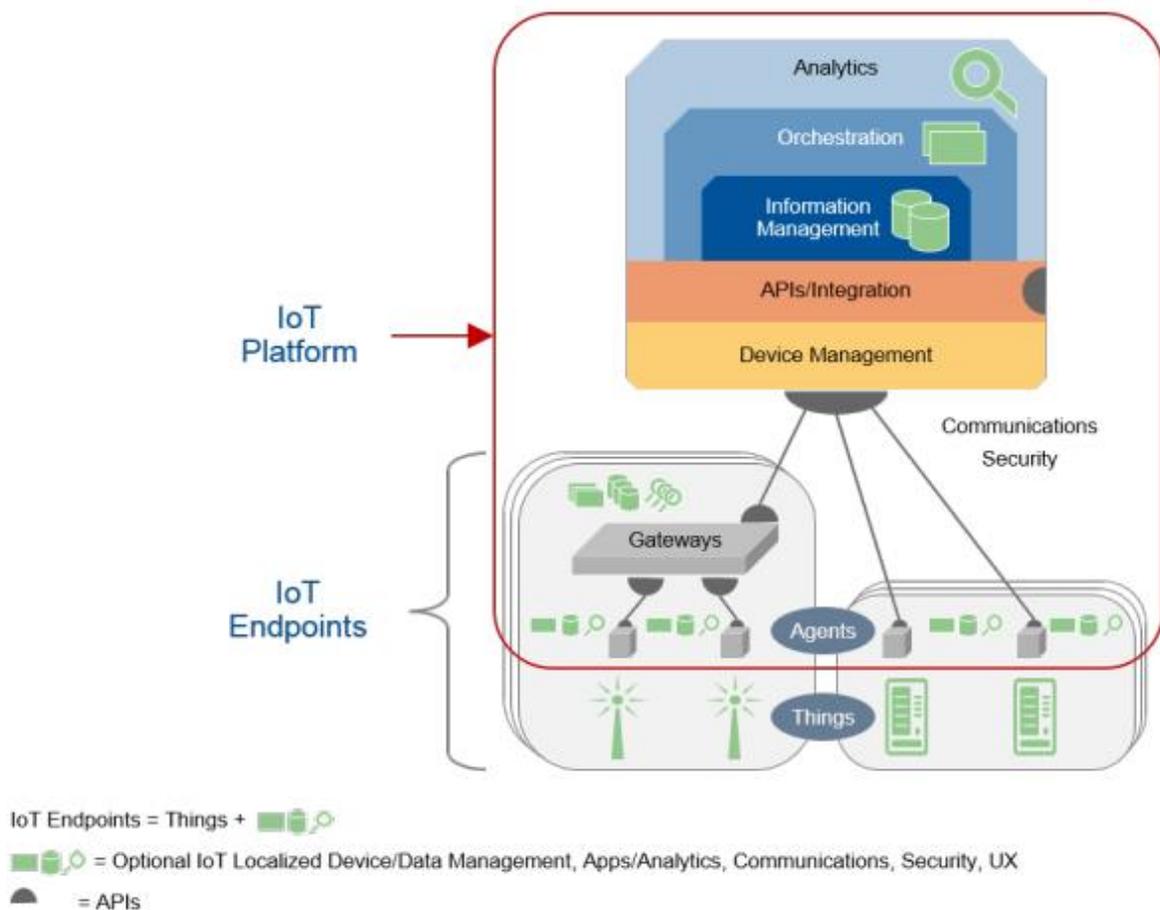


Figura 5. Capacidades de una plataforma IoT [4]

Las capacidades de una plataforma IoT incluyen:

- Aprovisionamiento y administración de endpoints IoT (Things) y Gateways IoT
- Personalización y construcción de aplicaciones (incluyendo SDK, IDE, AppServer...)
- Procesamiento de eventos: flujo de eventos y agregación de datos, streaming analytics, almacenamiento y gestión de la información
- Toma de decisiones: motores de reglas, orquestación de flujos de trabajo y proceso de negocio (BPM)
- Análisis: Análisis y visualización de datos IoT (incluyendo cuadros de mando).
- Ciberseguridad: autenticación, encriptación, gestión de certificados...
- Comunicaciones con dispositivos IoT (capa física como WIFI y capa de datos, como MQTT o HTTP)
- Integración: publicación y suscripción de APIs, transformaciones, adaptadores, para conectar con aplicaciones empresariales y fuentes de datos, servicios en la nube, aplicaciones móviles, legacy...
- Adaptadores
- Interfaces de usuario, tanto para usuarios finales como para desarrolladores

3.2 COMPARATIVA ENTRE PLATAFORMAS IoT

Veamos, en la siguiente tabla, una comparativa entre las plataformas IoT más influyentes del mercado en la actualidad: Azure IoT Hub, AWS IoT, Watson IoT Foundation y Sofia2 IoT Platform. En ella, observamos las cualidades más importantes de cada una de ellas:

	Azure IoT Hub	AWS IoT	Watson IoT Platform	Sofia2 IoT Platform
Protocolos	HTTP, AMQP, MQTT y protocolos a medida usando Protocol Gateway	HTTP, MQTT	HTTP, MQTT	HTTP, MQTT, AMQP, JMS, OPC y protocolos a medida vía Gateway Plugin
Patrones de comunicación	Telemetry, Command	Telemetry, Command	Telemetry, Command	Telemetry, Command
Plataformas certificadas	Intel, Raspberry Pi, Freescale, Texas Instruments, MinnowBoard, BeagleBoard, Seeed, resin.io	Broadcom Marvell, Reneses, Texas Instruments, Microchip, Intel, Mediatek, Qualcomm, Seeed, BeagleBoard	ARM mbed, Texas Instruments, Intel, Raspberry Pi, Arduino Uno	Intel, ARM, Raspberry Pi, Arduino, Texas Instruments, Seeed, Cisco, BeagleBoard, Texas Instruments
SDK/Lenguaje	.Net y UWP, Java, C, NodeJS	C, NodeJS, Javascript, Arduino, Java, Python, iOS, Android	C#, C, Python, Java, NodeJS	Java, Javascript, C, NodeJS, iOS, Android, Python, .Net, Arduino
Seguridad	TLS (Server Authentication)	TLS (Mutual Authentication)	TLS	TLS
Autenticación	Por dispositivos con SAS token	Certificado X.509 con autenticación cliente, IAM Service, Cognito Service	Per-device con token	Per-device/system con token, certificado X509, user/password
Precio	Pago por unidad IoT Hub según número de dispositivos y mensajes por días	Pago por tráfico en millones de mensajes (publicados de dispositivos y entregados a dispositivos)	Pago por número de dispositivos, tráfico de datos y almacenamiento	Modo SaaS: pago por tráfico de datos y almacenamiento Modo PaaS: pago por VMs

Figura 6. Tabla comparativa entre plataformas IoT

3.3 ELECCIÓN DE PLATAFORMA IoT: SOFIA2

A las plataformas IoT también se las conoce como Middleware IoT, lo que subraya su rol funcional como el de mediador entre hardware y las capas de aplicación. Un flujo tipo IoT y los componentes que intervienen podría ser el siguiente:

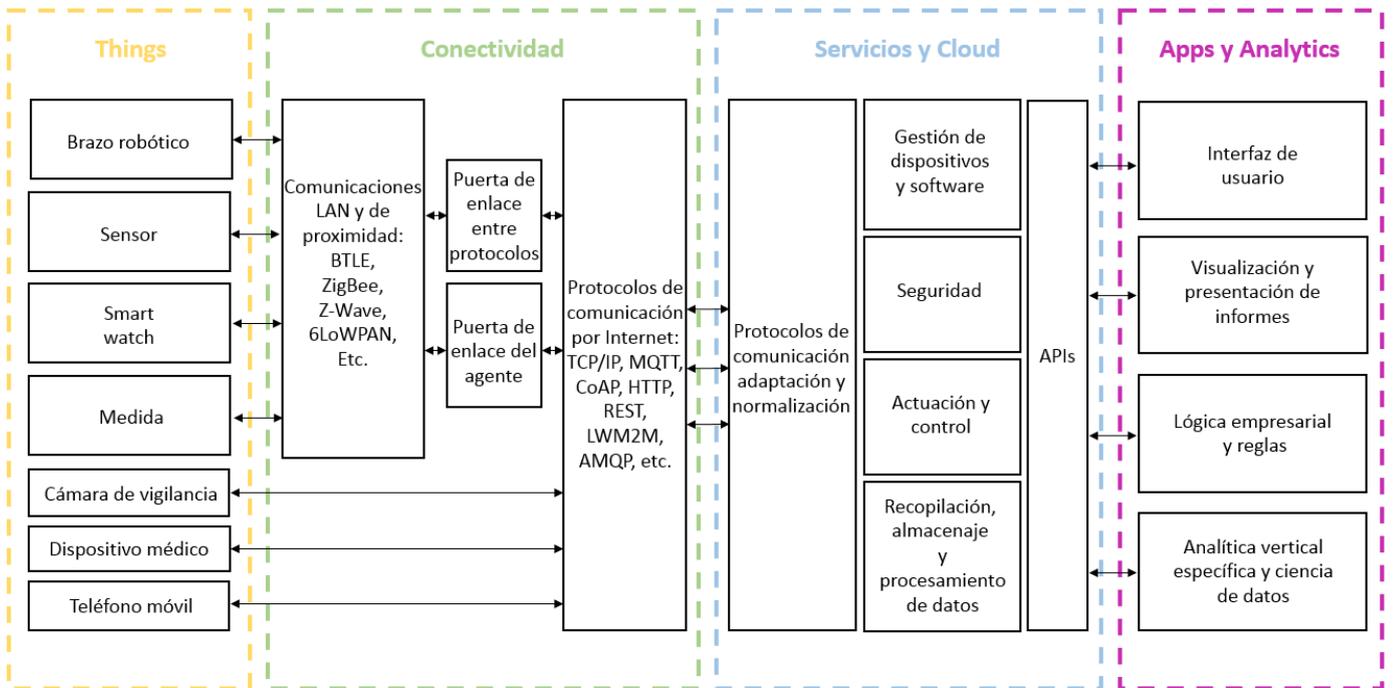


Figura 7. Flujo IoT genérico

Sofia2 soporta todos y cada uno de los módulos del diagrama anterior de la siguiente forma:

Plataforma IoT Genérica

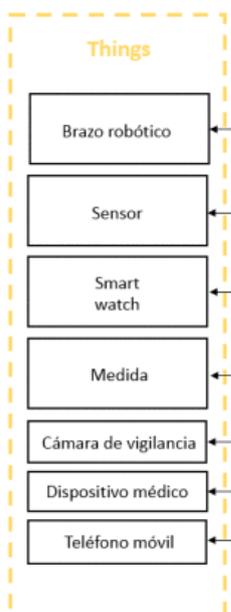


Figura 8. Things en plataforma genérica

Things

Plataforma IoT Sofia2

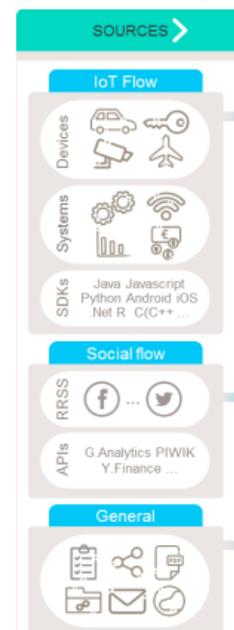


Figura 9. Things en plataforma Sofia2

Como Things entendemos cualquier dispositivo que es capaz de enviar datos, ya sean sensores, cámaras de vigilancia, brazos robóticos, Smart watch... Algunos de los dispositivos soportados por Sofia2 son:

Dispositivos	Sensor apertura y cierre puertas: CLIMAX, Leedarson, Nyce, Wulian, Centralite
Smart Home /	Sensor de presencia: CLIMAX, Leedarson, Nyce, Wulian, Centralite, DEVELCO
Smart Building /	Smart Plug: Meazon, 4-Noks
Smart Retail	Pinza Amperimétrica: Meazon, 4-Noks
	Termostato: 4-Noks, Centralite
	Cámara IP: D-LINK, Panasonic
	Sensor Temperatura y Humedad: Wulian, Centralite, Leedarson
	Sensor de Humo y Gas: CLIMAX, DEVELCO, Leedarson, Wulian
	Sensor de inundación: Centralite, CLIMAX, DEVELCO, Wulian
	Sensor de Luminosidad: Leedarson
	Smoke Listener: Centralite
	Sirena: Metalligence, Wulian
	Iluminación LED: LG, Leedarson
	Interruptores: CLIMAX, Centralite
	Válvula Termostática: CLIMAX
	Estacion Meteorologica: Sensores Adafruit
	Beacon: Indra, Estimote
	Botón del Pánico: CLIMAX, Centralite
	Smart Meters: Varios fabricantes
Dispositivos	Termómetro ambiental - Varios fabricantes
Smart Cities /	Sensor de humedad ambiental - Varios fabricantes
Smart Traffic /	Sensor de Consumo de Energía - Varios fabricantes
Smart Agro /	Caudalímetro - Varios fabricantes
Smart Tourism	Tensiómetro - Varios fabricantes
	Potenciómetro - Varios fabricantes
	Smart metering - Varios fabricantes
	Semáforo: Cross
	Iluminación Inteligente: UVAX
	Iluminación Inteligente: LUX
	Sensores Libelium (una vez integrado con Meshlium se puede conectar cualquier tipo de sensor de Libelium. Los siguientes son los que se han probado):
	Air Quality
	Atmospheric pressure
	Temperature
	Humidity
	Luminosity
	Waspote internal temperature, battery level, accelerometer
Dispositivos	Pulsoxímetros: Varios fabricantes usando protocolo IEEE
Smart Health /	Básculas: Varios fabricantes usando protocolo IEEE
Smart Insurance:	Tensiómetros: Varios fabricantes usando protocolo IEEE
	Electrocardiograma: Cardioscout
	Termómetro: Fora
	Glucómetro: Fora
	Nociceptor: varios fabricantes
	Torre de Anestesia (750 variables clínicas) – Dräger
	Torre de Anestesia (750 variables clínicas) – General Electric
	Sensor de presión en cama - (pendiente conocer fabricante)
	Sensor de caídas - (pendiente conocer fabricante)
	SmartBand – Withings

Otros	Quadrirotor/Drone – Indra / 3DRobotics / Microsoft IPCam
	Rover/Drone – Indra
	Raspberry PI / BeagleBone
	Arduino

Figura 10. Dispositivos soportados por Sofia2

Además de soportar la recogida de datos de todos estos dispositivos, Sofia2 también permite la ingesta de datos desde otro tipo de fuentes, como son RRSS, APIs y archivos de carácter general.

People As Sensors	Android devices
	iOS devices
	Smart TV
	Twitter
	Facebook
	Instagram
	Web crawlers

Figura 11. Otras fuentes de datos soportadas por Sofia2

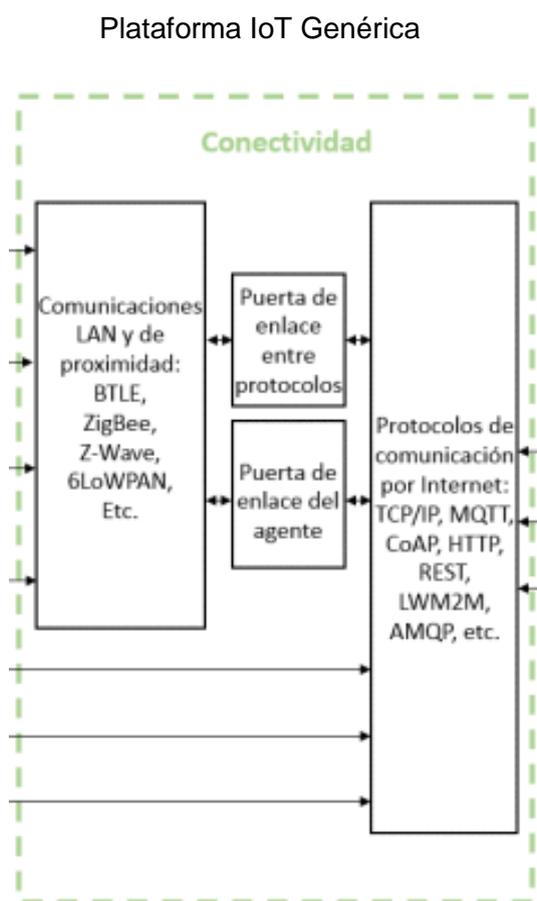


Figura 12. Conectividad en plataforma genérica

Conectividad

Plataforma IoT Sofia2

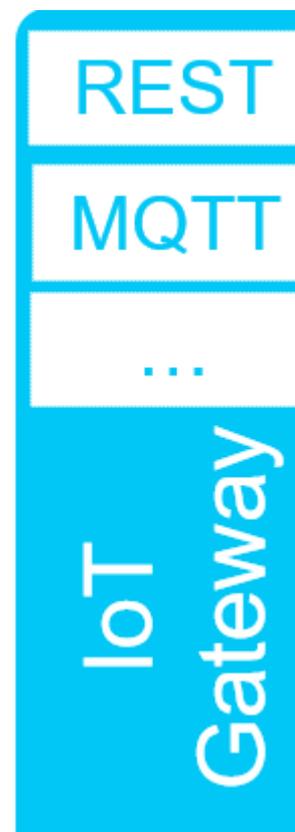


Figura 13. Conectividad en plataforma Sofia2

Sofia2 es agnóstica de las comunicaciones, con implementaciones en múltiples protocolos de comunicación ligeros (REST, OPC, MODBUS, WebSockets, MQTT, WS, JMS, AMQP...)

Además, entre otros, los gateways soportados por Sofia2 son:

Gateways	Indra Node#1
	Android devices
	Otros dataloggers ámbito edificios e industrial: Carlo Gavazzi,
	Cisco 819 (Fog Computing)
	Extreme Networks
	Intel DK100, Intel DK300
	iOS devices
	Libelium Meshlium
	R
	Raspberry Pi
	Televés

Figura 14. Gateways soportados por Sofia2

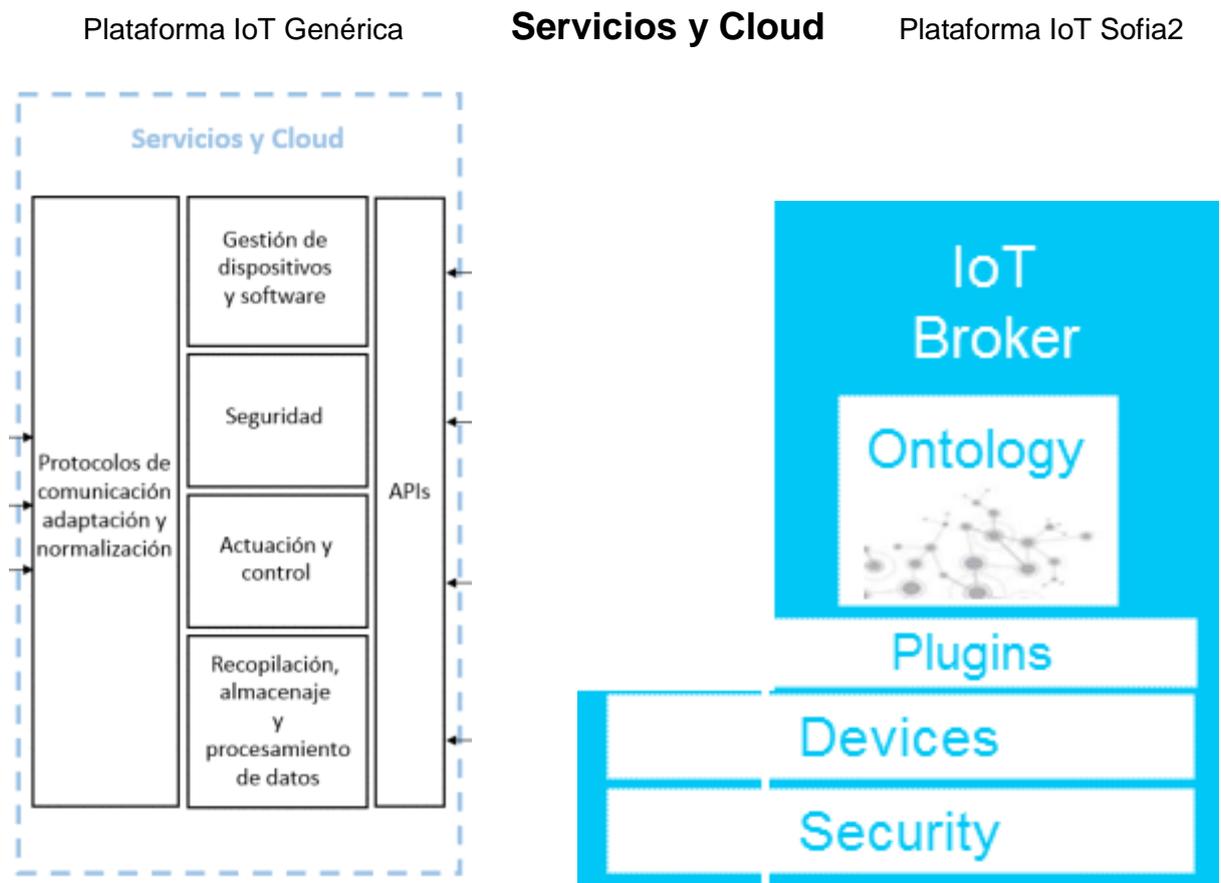


Figura 15. Servicios y Cloud en plataforma genérica Figura 16. Servicios y Cloud en plataforma Sofia2

En la plataforma Sofia2 se definen los siguientes conceptos elementales:

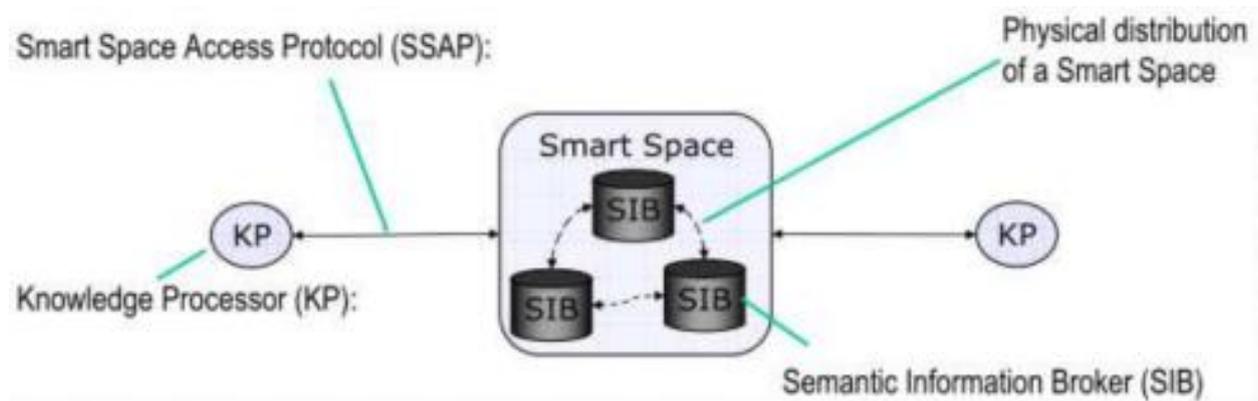


Figura 17. Conceptos elementales en Sofia2

SmartSpace. Es el universo colaborativo de sistemas y/o dispositivos (KPs o ThinkKPs) que intercambian información entre ellos. El núcleo de un Smart Space es el SIB (Semantic Information Broker).

SIB. Es el core del Smart Space. Actúa como elemento de integración de la información intercambiada por los dispositivos. Puede haber varios en un Smart Space.

KP o ThinKP (Knowledge Processor). Cada uno de los sistemas y/o aplicaciones que interoperan en el Smart Space a través del SIB deben estar definidos y configurados como KPs en el mismo. El KP es un elemento desplegado en el Smart Space que puede consumir y/o producir información.

Ontologías. Elemento atómico semántico con el cual se modelan los diferentes sistemas de información que interoperan en el dominio del Smart Space.

Las ontologías son descripciones semánticas de un conjunto de clases. De esta manera, las aplicaciones que compartan clases (normalmente denominadas conceptos) de la misma ontología, pueden intercambiar información mediante instancias concretas de dichas clases comunes.

En Sofia2, estas ontologías están representadas en formatos **JSON-Schema**, que las definen y validan.

En cuanto al almacenamiento de datos en Sofia2 distinguimos entre:

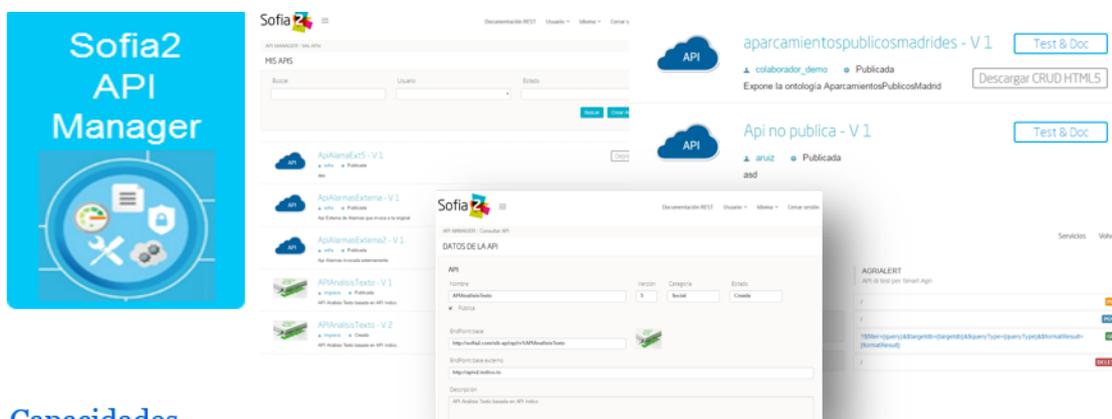


Figura 18. Almacenamiento en Sofia2

Por cada ontología se puede configurar una ventana de tiempo a partir de la cual la información se considera 'histórica'. La información permanecerá en esta base de datos hasta que automáticamente sea migrada al repositorio de información histórica.

La información almacenada estará disponible como origen de datos para los distintos módulos de la plataforma: Integración, Machine Learning, APIManager...

Sofia2 dispone de un API Manager con las siguientes capacidades:



Capacidades

Seguridad integrada con el resto de elementos de la plataforma (autenticación, autorización, cifrado, ...)

Integración transparente de **APIs de terceros**.
Open Data y Monetización

Publicación de datos **independientemente** del **repositorio** (tiempo real o histórico)

Control completo del **ciclo de vida de las APIs** (Creada, en Desarrollo, Publicada, Deprecada, Eliminada)

Métodos Custom Query, clonado de APIs, generación automática de CRUDs...

Control de Throttling (gestión del número de peticiones que podrá realizar cada usuario por minuto.)

Figura 19. Api Manager en Sofia2

Plataforma IoT Genérica

Apps y Analytics

Plataforma IoT Sofia2

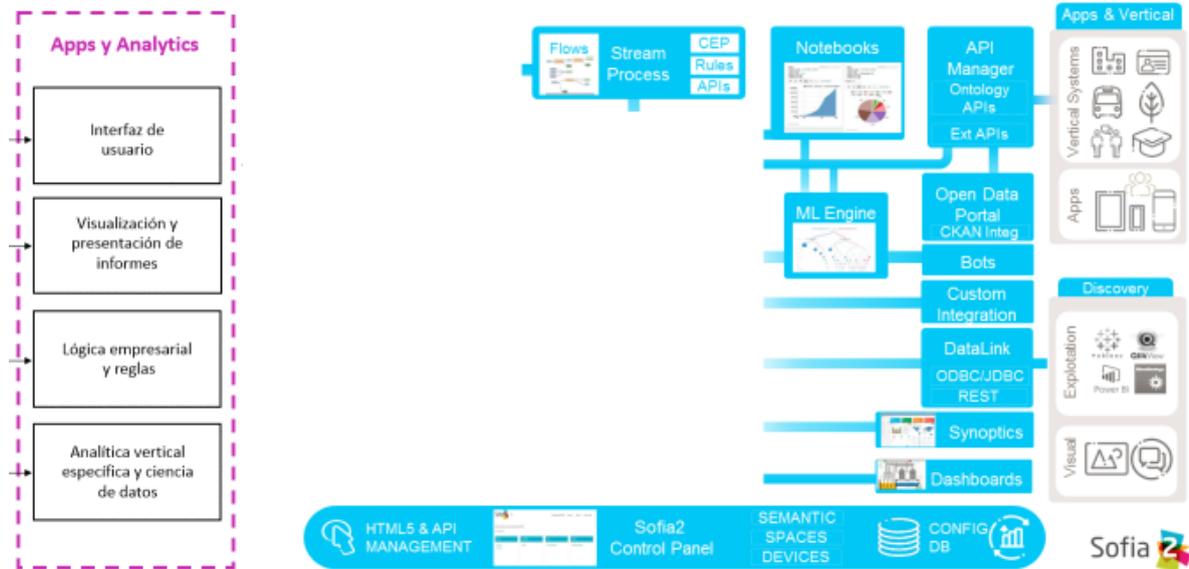


Figura 20. Apps y Analytics en plataforma genérica Figura 21. Apps y Analytics en plataforma Sofia2

En [sofia2/console](#) encontraremos la interfaz de usuario y entorno de experimentación con todas las capacidades de la plataforma. De manera gratuita y de forma bastante intuitiva podremos no sólo crear Ontologías para modelizar nuestros datos, ThinkKPs o ingestar datos de archivos o RRSS, sino que además podremos crear reglas (Scripts) para procesar toda esta información de la manera que más nos interese, visualizar estos datos en Gadgets y Dashboards o publicar Ontologías via API. Por todo ello, será la plataforma elegida para realizar la demostración práctica del TFG.

Además disponemos de los módulos de Analytics que nos permitirán crear Pipelines y Notebooks, o crear flujos de Machine Learning:

Capacidades		
Carga de ficheros locales	Definición visual de flujos	Inferencia y deep learning
Parseo de datos en diversos formatos (ARFF, XLS, XLSX, CSV, SVMLight)	Publicación de modelos	Visualización de resultados
Algoritmos: K-means, Generalized Linear Model, Distributed RF, Naive Bayes, Principal Component Analysis, Gradient Boosting Machine y Deep Learning		

Figura 22. Módulos Analytics en Sofia2

En la siguiente infografía podemos observar la arquitectura de la plataforma Sofia2:

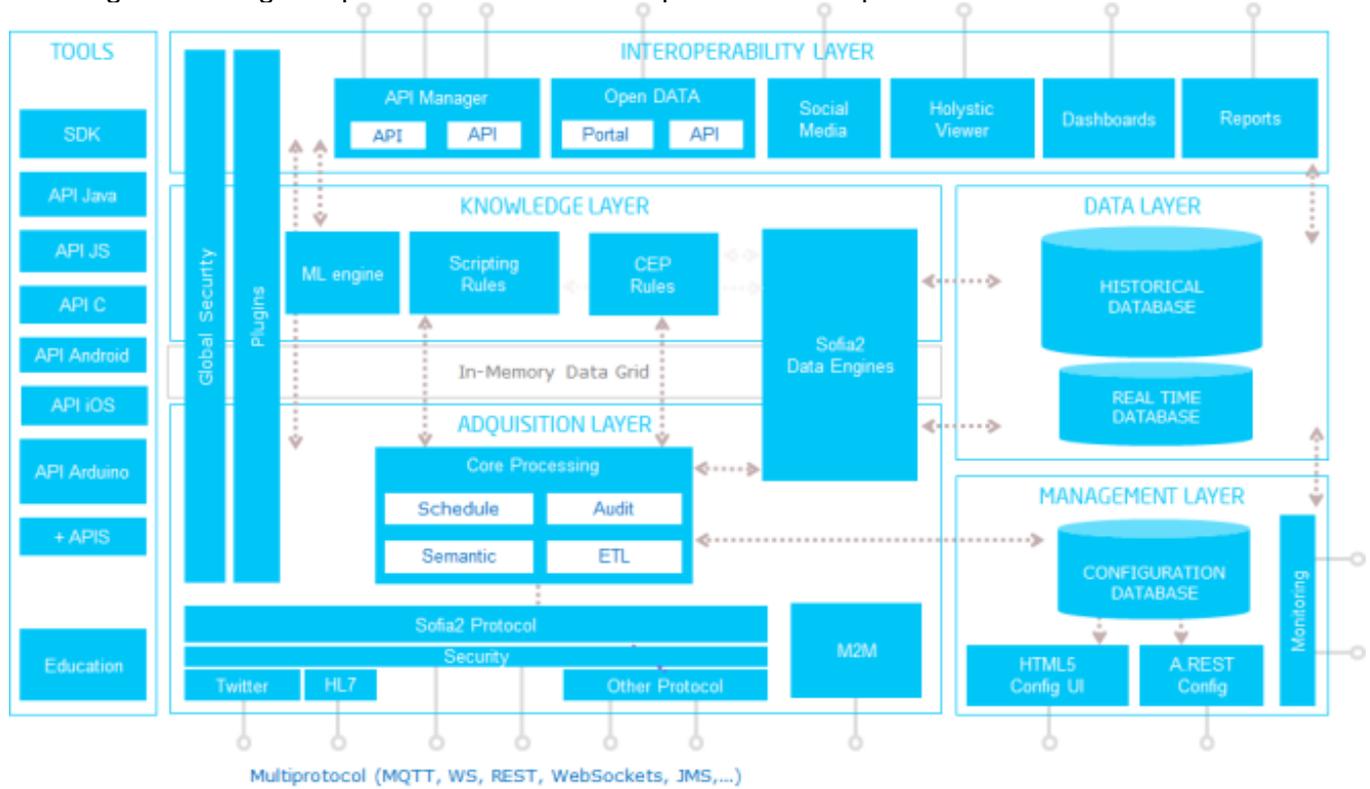


Figura 23. Infografía arquitectura Sofia2

Y aquí disponemos de una vista global de los componentes Sofia2:

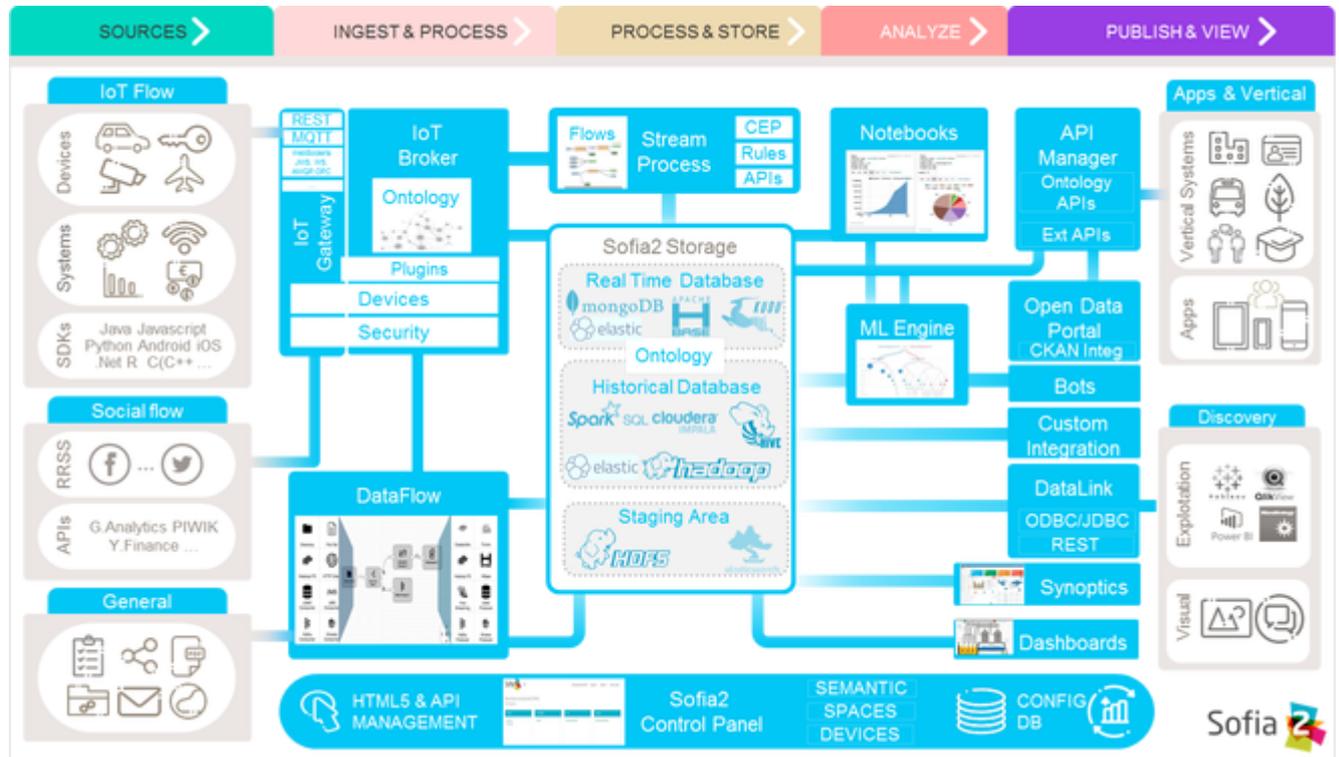


Figura 24. Componentes Sofia2

4 PROTOCOLOS DE COMUNICACIÓN

Un ecosistema IoT podría definirse mediante un modelo de 7 capas [6]. Veámoslo gráficamente:



Figura 25. Ecosistema IoT [6]

En la capa inferior está el dominio del mercado o de la aplicación, que puede ser red inteligente, casa conectada, salud inteligente, etc. La segunda capa consta de sensores que permiten la aplicación. Ejemplos de tales sensores son sensores de temperatura, sensores de humedad, contadores de electricidad o cámaras.

La tercera capa consiste en una capa de interconexión que permite que los datos generados por los sensores sean comunicados, usualmente a una instalación de cómputo, centro de datos o datos en la nube. Allí los datos se agregan con otros conjuntos de datos conocidos, tales como datos geográficos, datos de población o datos económicos. Los datos combinados se analizan a continuación mediante el aprendizaje automático y las técnicas de minería de datos. Para habilitar estas aplicaciones distribuidas de gran tamaño, también necesitamos el último software de colaboración y comunicación de nivel de aplicación, definido como SDN (Software Defined Networking), arquitectura orientada a servicios (SOA), etc.

Finalmente, la capa superior consiste en servicios que pueden incluir la gestión de la energía, la gestión de la salud, la educación, el transporte, etc.

Además de estas 7 capas, existen aplicaciones de seguridad y gestión que se requieren para cada una de las capas.

Centrándonos en la capa de interconexión, encontramos las siguientes subcapas:

Session		MQTT, SMQTT, CoRE, DDS, AMQP, XMPP, CoAP, ...	Security	Management
Network	Encapsulation	6LoWPAN, 6TiSCH, 6Lo, Thread, ...		
	Routing	RPL, CORPL, CARP, ...		
Datalink		WiFi, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.11ah, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, ...		

Figura 26. Protocolos IoT [6]

La capa Datalink, o de enlace de datos, conecta dos elementos IoT que generalmente podrían ser dos sensores o el sensor y el dispositivo de puerta de enlace (gateway) que conecta un conjunto de sensores a Internet.

A menudo es necesario que varios sensores se comuniquen y agreguen información antes de llegar a Internet. Se han diseñado protocolos especializados para el encaminamiento entre sensores y forman parte de la capa de enrutamiento. Los protocolos de la capa de sesión permiten la mensajería entre varios elementos del subsistema de comunicación IoT.

También se han desarrollado varios protocolos de seguridad y gestión para IoT, como se muestra en la figura.

Tal y como vimos en la figura 6, la mayoría de plataformas IoT soportan los protocolos HTTP y MQTT, además de otros. Nos centraremos en ellos.

4.1 MQTT

Message Queue Telemetry Transport (MQTT) es un protocolo de mensajería de tipo publicación/suscripción.

- Es ligero, abierto, simple, y fácil de implementar.
- Está diseñado para tener una mínima sobrecarga, lo que hace que sea una buena opción para aplicaciones M2M (Machine to Machine) y de Internet de las cosas, sobre todo cuando aparecen sistemas embebidos o limitados.
- MQTT utiliza características del transporte TCP, por lo que el requisito mínimo para el uso de MQTT es el uso de TCP.

MQTT es especialmente interesante en escenarios en los que la entrega de mensajes confiable es crucial para una aplicación, pero no se dispone de una conexión de red fiable (por ejemplo una red móvil). Ejemplos de aplicación: Telemetría, automotriz, casa inteligente, monitorización de energía, aplicaciones de chat, Notification Services.

Como hemos comentado, utiliza un modelo de comunicación publicación/suscripción. Este patrón desacopla el cliente que envía un mensaje (publicador) de otros clientes que puedan consumirla (suscriptores)

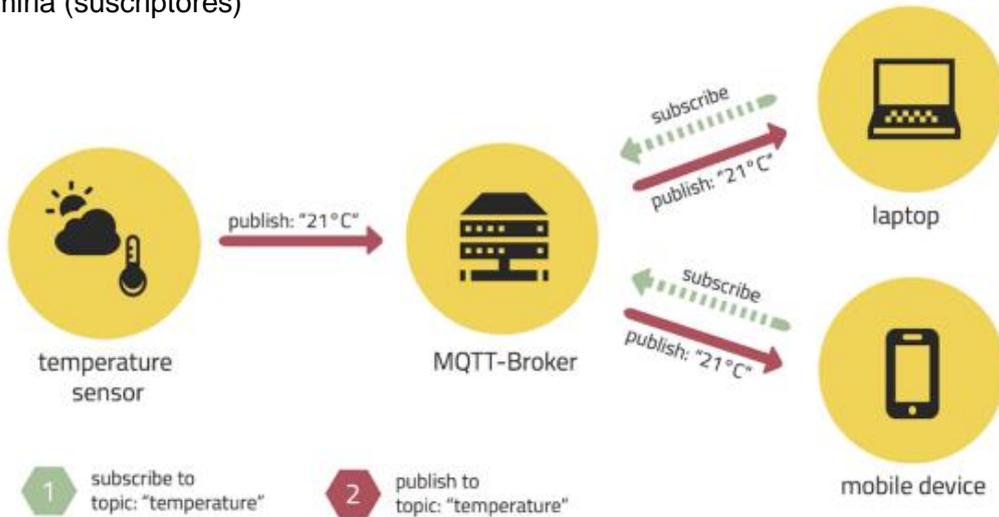


Figura 27. Esquema protocolo MQTT

De esta forma los publicadores y suscriptores no tienen que conocerse y sólo tienen que conocer el Message Broker.

Los mensajes más usados son CONNECT, PUBLISH, SUBSCRIBE Y UNSUBSCRIBE, pero existen también otros tipos de mensaje MQTT:

MESSAGE TYPE	DESCRIPTION
CONNECT	Client request to connect to Server
CONNACK	Connection Acknowledgement
PUBLISH	A message which represents a new/separate publish
PUBACK	QoS 1 Response to a PUBLISH message
PUBREC	First part of QoS 2 message flow
PUBREL	Second part of QoS 2 message flow
PUBCOMP	Last part of the QoS 2 message flow
SUBSCRIBE	A message used by clients to subscribe to specific topics
SUBACK	Acknowledgement of a SUBSCRIBE message
UNSUBSCRIBE	A message used by clients to unsubscribe from specific topics
UNSUBACK	Acknowledgement of an UNSUBSCRIBE message
PINGREQ	Heartbeat message
PINGRESP	Heartbeat message acknowledgement
DISCONNECT	Graceful disconnect message sent by clients before disconnecting.

Figura 28. Mensajes MQTT

MQTT soporta 3 Calidades del Servicio (QoS). Cada mensaje publicado se envía con uno de estos niveles de Quality of Service (QoS). Estos niveles representan las diferentes garantías en la entrega del mensaje.

QOS LEVEL	DESCRIPTION
0	At most once delivery: The sender tries with best effort to send the message and relies on the reliability of TCP. No retransmission takes place.
1	At least once delivery: The receiver will get the message at least once. If the receiver does not acknowledge the message or the acknowledge gets lost on the way, it will be resent until the sender gets an acknowledgement. Duplicate messages can occur.
2	Exactly once delivery: The protocol makes sure that the message will arrive exactly once at the receiver. This increases communication overhead but is the best option when neither loss nor duplication of messages are acceptable.

Figura 29. QoS MQTT

Es muy importante la seguridad en escenarios IoT, en el que se comunican objetos entre sí. MQTT confía en tecnologías estándares para esto:

- Autenticación usuario/Password
- Seguridad TLS

4.2 RESTFUL SERVICES

Representational State Transfer (REST) no es realmente un protocolo, más bien es un estilo de arquitectura. REST utiliza los métodos HTTP GET, POST, PUT y DELETE para proporcionar un sistema de mensajes orientado a recursos donde todas las acciones se pueden realizar simplemente usando los comandos HTTP síncronos request/response.

El tipo de contenido puede ser XML o JSON (JavaScript Object Notation) y depende del servidor HTTP y su configuración. REST es una parte importante del IoT porque está respaldada por plataformas comerciales de nube M2M (Machine To Machine).

Las características de HTTP pueden ser completamente utilizadas en la arquitectura REST.

Los servicios de RESTful utilizan el seguro y fiable protocolo HTTP. También, puede hacer uso de TLS/SSL para seguridad. Sin embargo, hoy en día la mayoría de las plataformas comerciales M2M no admiten peticiones HTTPS. En su lugar, proporcionan claves de autenticación que deben estar en el encabezado de cada solicitud para lograr algún nivel de seguridad.

Aunque REST ya se utiliza ampliamente en plataformas M2M comerciales, es improbable que se convierta en un protocolo dominante debido a no ser fácilmente implementable.

Dada la tendencia actual de las aplicaciones que se ejecutan en smartphones y tablets, la sobrecarga adicional asociada a los protocolos de request/response afecta al uso de la batería.

4.3 COMPARATIVA DE PROTOCOLOS DE COMUNICACIÓN

A continuación podemos comprobar las diferencias entre los diferentes protocolos de comunicación más usados en la tecnología IoT [7], qué tipo de protocolos de transporte usan, si tienen capacidad para usar la calidad de servicio (QoS), cómo es su arquitectura, o los sistemas de seguridad que proporcionan.

Protocol	Transport	QoS options	Architecture	Security
CoAP	UDP	YES	Request/Response	DTLS
MQTT	TCP	YES	Publish/Subscribe	TLS/SSL
XMPP	TCP	NO	Request/Response Publish/Subscribe	TLS/SSL
REST	HTTP	NO	Request/Response	HTTPS
AMQP	TCP	YES	Publish/Subscribe	TLS/SSL
Web socket	TCP	NO	Client/Server Publish/Subscribe	TLS/SSL

Figura 30. Tabla comparativa protocolos de comunicación [7]

5 HARDWARE EMPLEADO

Existe una gran variedad de dispositivos y sensores creados para múltiples propósitos. La mayoría de ellos se pueden conectar a una plataforma IoT. Algunos de ellos, clasificados según su generación, son:

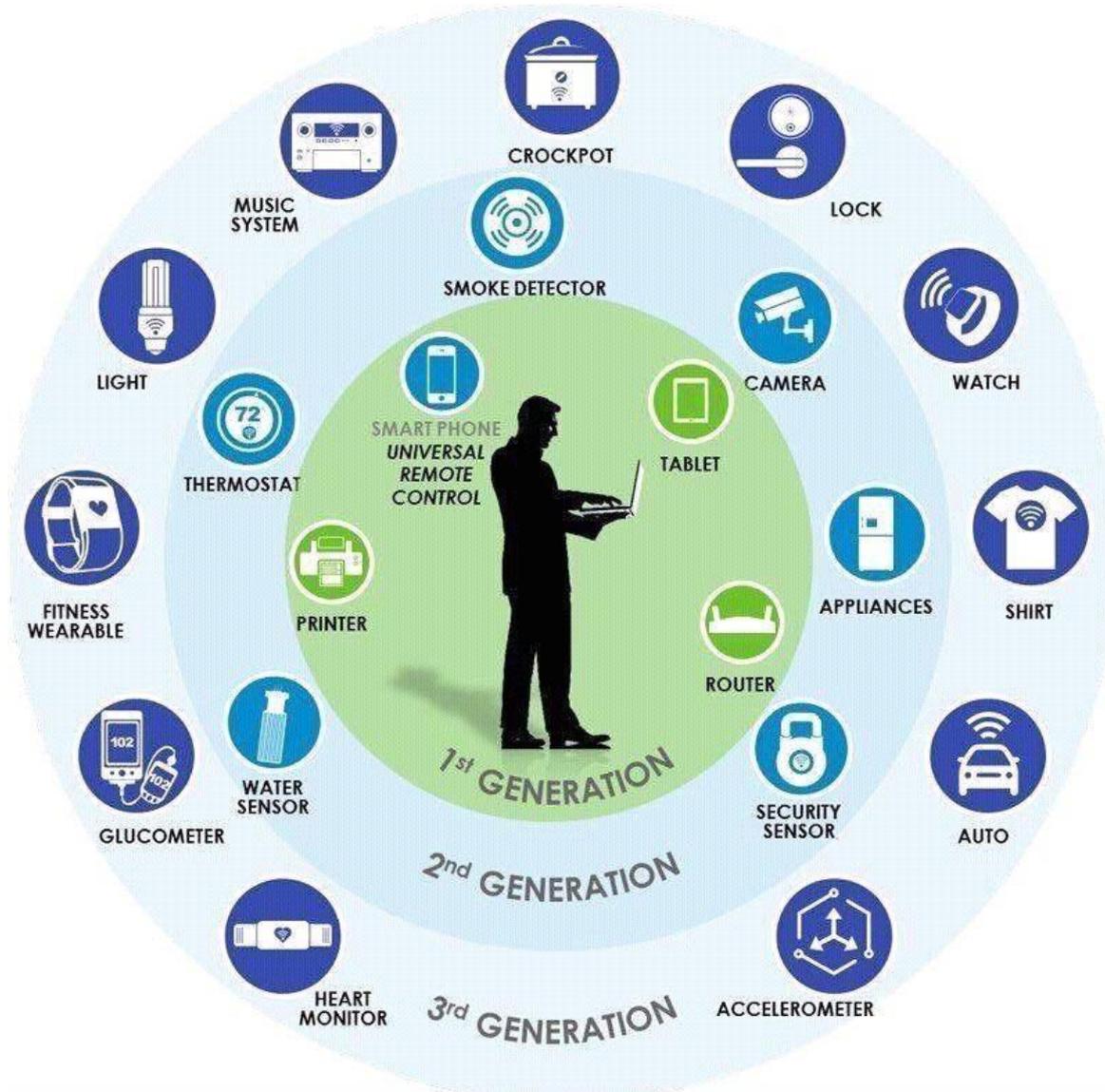


Figura 31. Dispositivos y sensores

5.1 SENSORTAG CC2650

Como hemos especificado con anterioridad, utilizaremos para nuestra aplicación práctica un dispositivo con múltiples sensores, programable y con interfaz de Bluetooth Low Energy (BLE) de comunicaciones, el SensorTag de Texas Instruments [8].



Figura 32. SensorTag CC2650 de Texas Instruments [8]

El SensorTag dispone de los siguientes sensores:

- Sensor de temperatura ambiente (x2)
- Sensor de temperatura de objeto cercano (infrarrojos)
- Sensor de movimiento de 9-ejes
- Sensor de humedad
- Sensor de presión atmosférica
- Sensor de luz ambiental
- Sensor magnético
- Además de micrófono digital, buzzer y botones

Para nuestra demostración práctica utilizaremos alguna de las capacidades del sensorTag, recogiendo datos en Sofia2, representándolos, y realizando acciones asociadas a los valores obtenidos.

5.2 GATEWAY. SMARTPHONE ANDROID XIAOMI REDMI NOTE 4

El Gateway, o puerta de enlace, actúa de proxy entre los dispositivos y la Plataforma IoT.

La necesidad de introducir gateways [9] en una arquitectura IoT nace de las siguientes limitaciones:

- Normalmente los sensores y dispositivos tienen capacidades de interconexión muy limitadas, utilizando protocolos de bajo consumo y relativamente corto alcance (Bluetooth Low Energy, Zigbee...), y conectándose a redes de área local (LAN) o residencial (HAN). Es necesario un Gateway para coordinar la red de sensores y actuar de proxy con la red de área ancha (WAN) donde la plataforma IoT expone sus interfaces para recibir y proporcionar información.

- El tratamiento de la información en bruto procedente de sensores y dispositivos, directamente en la plataforma IoT, puede ser en ocasiones ineficiente en términos de rendimiento y ancho de banda. Por lo que es necesario disponer de Gateways con capacidad de almacenamiento temporal de la información y procesamiento de la misma. De este modo es posible filtrar y agregar la información antes de enviarla a la plataforma, así como garantizar que no se pierde información en caso de interrupción temporal de las comunicaciones.
- Disponer de un Gateway que centralice las operaciones de monitorización de todos los dispositivos conectados a su red de sensores, reduce la complejidad del sistema de monitorización, que solo se tiene que conectar al Gateway.

El software de un Gateway es el componente que realiza la lógica de tratamiento de la información recopilada de la red de sensores o dispositivos para enviarla a la plataforma IoT, así como de comandado, permitiendo a la plataforma IoT interactuar con el entorno cubierto por dichos sensores y dispositivos.

En este sentido, el software de un Gateway es el encargado de consultar periódicamente o bajo demanda las distintas medidas de los sensores o dispositivos, agruparlas en entidades mayores de información y enviarlas a la plataforma IoT. Recibir órdenes de comandado desde la plataforma y dirigirla al actuador correspondiente. Consultar el estado de los sensores o dispositivos y ofrecerlos al software de monitorización.

El software de un Gateway debe estar diseñado para soportar al menos estos tres criterios:

- Recuperación ante fallos: Interrupción de la alimentación, caída de comunicaciones, fallos en sensores o dispositivos...
- Soporte para actualizaciones automáticas, gestionadas desde entorno remoto centralizado.
- Soporte para configuración centralizada, gestionada desde entorno remoto centralizado.

Usando un Smartphone Android (Xiami Redmi Note 4) como Gateway, se establecerá una conexión Bluetooth con el SensorTag, y se realizará un mapeo de los valores medidos por los sensores. El Smartphone será el encargado de encapsular la información y transmitirla a Sofia2 usando redes de telefonía móvil o una red WiFi.



Figura 33. Esquema de conectividad de los dispositivos

6 APLICACIÓN PRÁCTICA

Llegados a este punto implementaremos todo lo que hemos visto en una aplicación práctica, en la que crearemos todo el flujo IoT para realizar el envío y la visualización de datos procedentes del beacon y el Gateway. Crearemos la Ontología, el ThinkKP, los Gadgets, y el Dashboard que nos servirá para visualizar estos datos.

Veamos los componentes y capacidades de la plataforma Sofia2 que usaremos y los pasos que seguiremos:

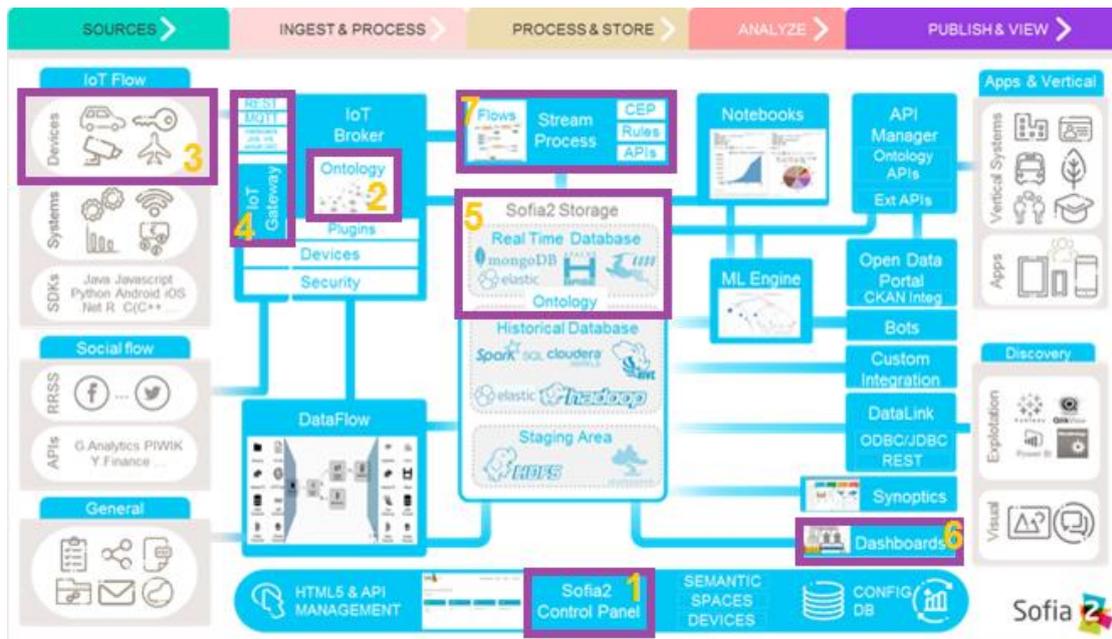


Figura 34. Componentes y capacidades de Sofia2 utilizados

6.1 CREAR UN USUARIO EN SOFIA2

Comenzaremos por acceder al Panel de Control de Sofia2. Si estamos en la [Plataforma de Experimentación](#) y no tenemos usuario, pulsaremos en **Crear una cuenta nueva**.



Figura 35. Acceso al panel de control de Sofia2

Una vez hecho el LOGIN si nuestro rol es USUARIO: **victor_usuario [ROL_USUARIO]** solicitaremos el **Paso a Colaborador** para poder crear Ontologías.



Figura 36. Solicitud paso a colaborador

Una gran ventaja que ofrece Sofia2 IoT Platform es que podremos usar el entorno de experimentación de forma gratuita sin límite de tiempo.

6.2 CREAR UNA ONTOLOGÍA

El término Ontología aplica en Sofia2 al modelo de datos. Podemos definir ésta como un esquema JSON que definirá de forma explícita los datos de las distintas magnitudes obtenidas tanto del dispositivo SensorTag como del Smartphone y que almacenará en la plataforma.

Para ello, pulsaremos sobre la opción de menú "Creación guiada Ontología".

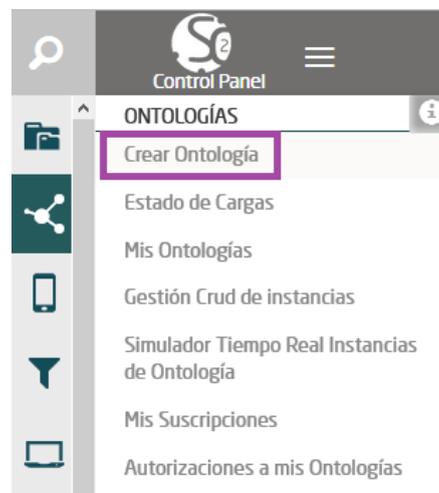


Figura 37. Acceso para la creación de Ontologías

Seleccionaremos "Crear Ontología paso a paso" y definiremos los siguientes parámetros:

- Nombre: En nuestro caso la denominaremos "tfgvvc"
- Descripción
- Meta_inf: tfg
- Categoría: General
- Plantilla: EmptyBase

Pulsando sobre "Añadir Nuevas Propiedades" podremos definir los datos que se desean manejar. Para este caso, se crearán los siguientes campos:

Campo	Descripción	Fuente	Tipo
geometry	Coordenadas de geoposición	Smartphone	Geometry
email	Email a la que se le enviará la alerta	Smartphone	String
accelX	Aceleración en G's sobre el eje X	Smartphone	Number
accelY	Aceleración en G's sobre el eje Y	Smartphone	Number
accelZ	Aceleración en G's sobre el eje Z	Smartphone	Number
event	Indica si hay evento que hace saltar la alarma	SensorTag	Number

Figura 38. Propiedades Ontología

Añadiéndolas obtendremos:

The screenshot shows a web interface for adding new properties to an ontology. At the top, there is a header "AÑADIR NUEVAS PROPIEDADES" and a sub-header "Nueva Propiedad Ontología". Below this, there are two dropdown menus: "Propiedad" (empty) and "T.datos" (set to "string"). To the right, there are two checkboxes: "requerido" (checked) and "no requerido" (unchecked). A blue "Añadir" button is located on the right side. Below these controls is a table listing the added properties:

Propiedad	T.datos	requerido	
geometry	geometry	requerido	🗑️
email	string	requerido	🗑️
accelX	number	requerido	🗑️
accelY	number	requerido	🗑️
accelZ	number	requerido	🗑️
event	boolean	requerido	🗑️

Figura 39. Propiedades añadidas a la Ontología

Pulsamos sobre "Generador Esquema e Instancia JSON" y "Generar Esquema". Obteniendo el esquema JSON.

Finalmente pulsamos sobre "Crear".

Una vez hecho esto, ya tendremos disponible nuestra Ontología "tfgvvc" con la definición de los atributos y el resto de parámetros que la definen.

6.3 CREAR UN THINKP

Una vez hayamos definido el modelo de datos y lo hayamos plasmado en una ontología, tendremos que crear el ThinkP, que es la configuración lógica de los dispositivos que van a interactuar con nuestra ontología.

Para ello accedemos al menú "Mis ThinkPs".



Figura 40. Acceso para la creación de ThinkPs

Y pulsamos sobre el botón "Nuevo ThinkP"



Figura 41. Botón de creación de un nuevo ThinkP

Aparecerá el cuadro de creación del nuevo ThinkP requiriéndonos introducir un identificador y una breve descripción. Además, será necesario asociar al menos una ontología al ThinkP. En este caso, tan solo le asociaremos la ontología que hemos creado en el paso anterior "tfgvvc" y pulsaremos sobre "crear".



Figura 42. Cuadro de creación de un nuevo ThinkP

Pulsando en “modificar” podremos ver las pestañas “Mis tokens” y “Mis instancias”, donde deberemos pulsar sobre “Nueva Instancia de ThinkP”, añadiendo una nueva instancia de ThinkP denominada “tfgvvc_01”:

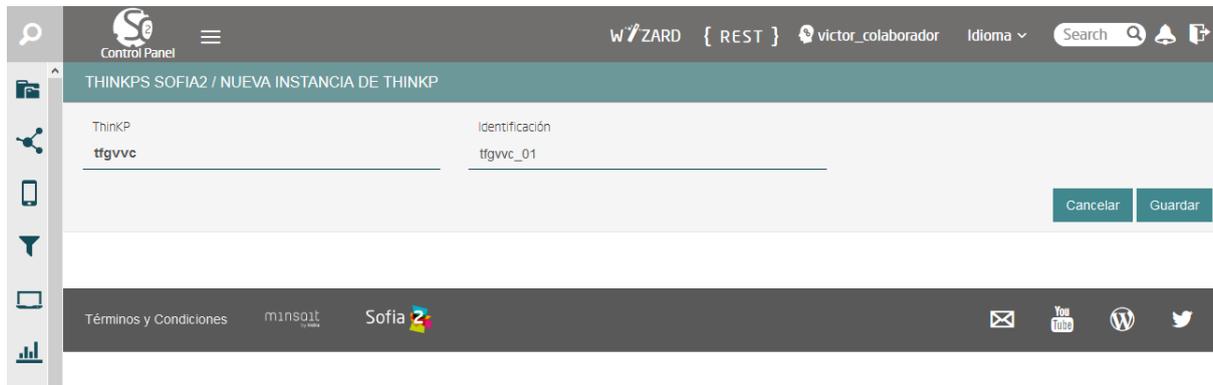


Figura 43. Adición de Instancia de ThinkP

Esta instancia de ThinkP, habilitará la inserción, lectura y en definitiva, el uso de las capacidades de Sofia2.

Pulsaremos en “Guardar” y ya dispondremos de la configuración lógica para poder recibir datos.

6.4 DESCARGA Y CONFIGURACIÓN DEL ARCHIVO .APK SOFIA2

Un archivo .APK, por sus siglas en inglés “Android Application Package” consiste en una aplicación empaquetada para el sistema operativo Android. En este caso, accederemos a [este](#) enlace para descargarnos el .APK que está listo para instalarse y usarse en nuestra aplicación práctica.

Una vez descargado, lo abriremos en nuestro Smartphone Android y se arrancará la aplicación Sofia2 IoT, donde podremos pulsar sobre el botón correspondiente para acceder a su configuración.

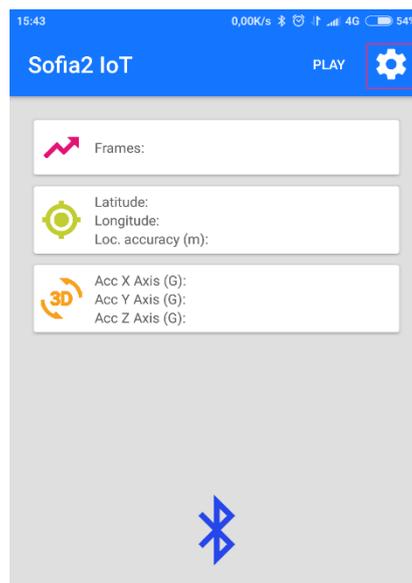


Figura 44. Acceso a la configuración de Sofia2 IoT

A continuación, introduciremos los siguientes valores en cada uno de los ajustes:

Sensor selection

24:71:89:BC:0D:04

CANCELAR ACEPTAR

ThinkKP name

tfgvvc:tfgvvc_01

CANCELAR ACEPTAR

Ontology name

tfgvvc

CANCELAR ACEPTAR

Token

eccefd805807438f81e776fbe2bcc038

CANCELAR ACEPTAR

Figura 45. Configuración de ajustes en Sofia2 IoT

6.5 CASO DE USO: ACELERÓMETRO Y GEOLOCALIZACIÓN

En el primer caso de uso que mostraremos, haremos uso de los sensores que lleva incorporados el Smartphone, actuando así como dispositivo IoT. También nos servirá como gateway de conexión con la plataforma.

Una vez hemos definido los parámetros de configuración de nuestra apk, pulsaremos sobre "play" y observaremos cómo empiezan a aparecer datos en la pantalla principal.

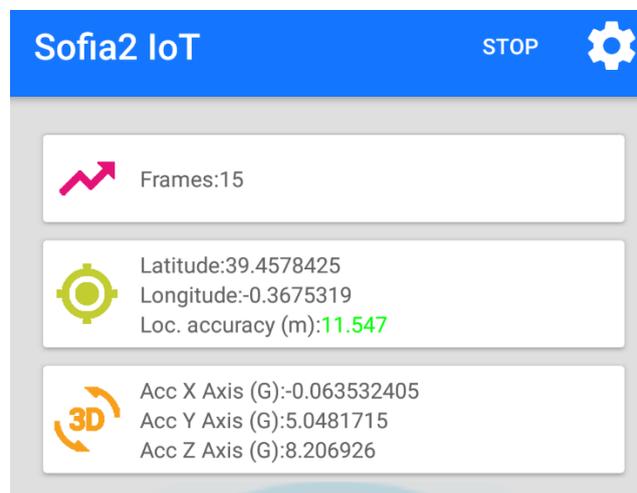
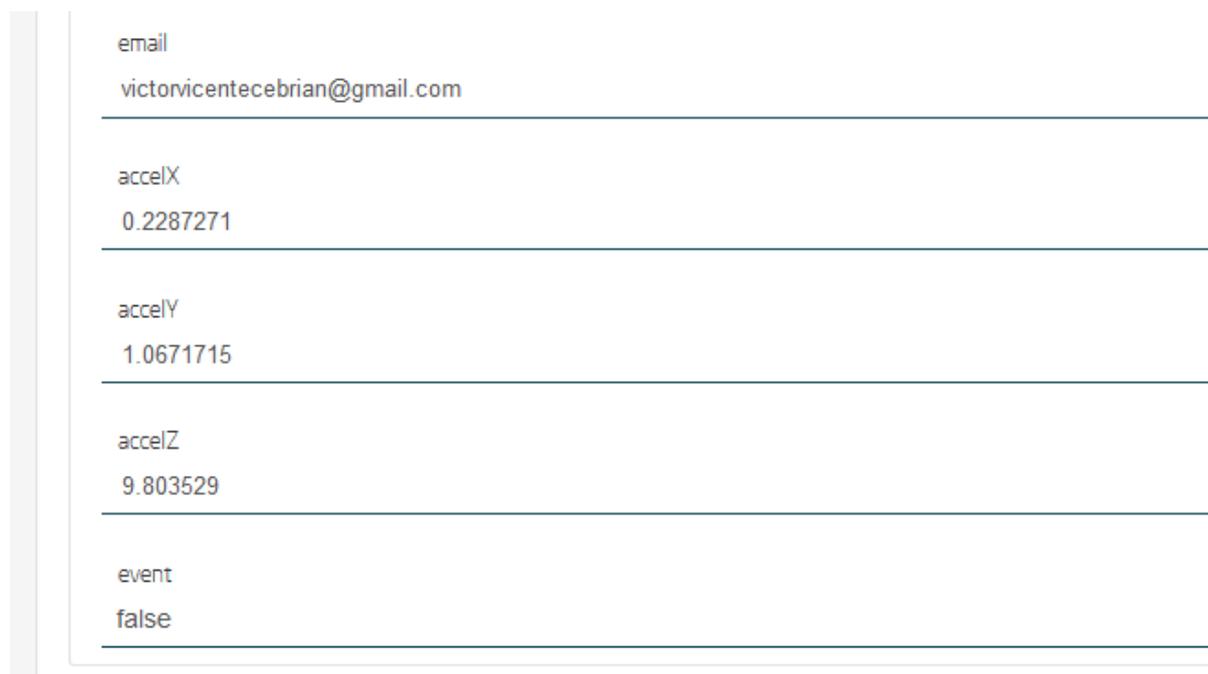


Figura 46. Datos de acelerómetro y geolocalización

Por otro lado, vemos cómo hemos obtenido datos de email, los 3 ejes que definen el acelerómetro, y un parámetro llamado "event" que nos indica si ha sido lanzado algún evento; en este caso, no.



email
victorvicentecebrian@gmail.com
accelX
0.2287271
accelY
1.0671715
accelZ
9.803529
event
false

Figura 49. Datos de email, acelerómetro y evento

6.5.2 CREACIÓN DE GADGETS Y DASHBOARD

Una vez que existen datos en la plataforma y a medida que los dispositivos u otras aplicaciones se conectan con Sofia2 es posible crear aplicaciones que interoperen entre sí y exploten la información existente.

Las herramientas de visualización de Sofia2 permiten explotar de forma sencilla y gráfica la información almacenada dentro de la plataforma.

Puedo crear elementos de visualización unitaria (Gadgets), unirlos en una página web (Dashboard) o incluso crear complejos sinópticos al estilo SCADA representando la evolución de las señales (Instances).

En el primer caso de uso crearemos un cuadro de mando usando las capacidades de presentación gráfica de la plataforma. En primer lugar, crearemos un gadget para mostrar en un gráfico en forma de barras, los datos obtenidos del acelerómetro. En segundo lugar, crearemos otro gadget de tipo mapa, en el que mostraremos la geolocalización del dispositivo en un mapa. Por último, integraremos estos dos gadgets en una página web, en un dashboard.

Accedemos mediante el panel de control de la plataforma a la pestaña "Mis Gadgets", dentro de "Visualización".

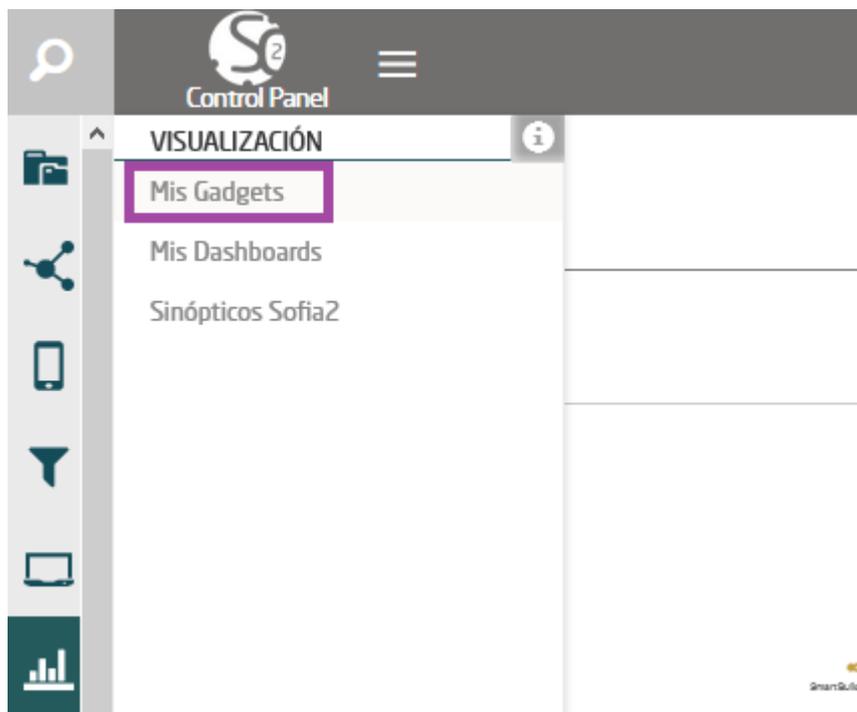


Figura 50. Acceso a Mis Gadgets

Pulsando sobre "Crear Gadget" y sobre "Básico", elegimos el gadget de tipo "Columna".

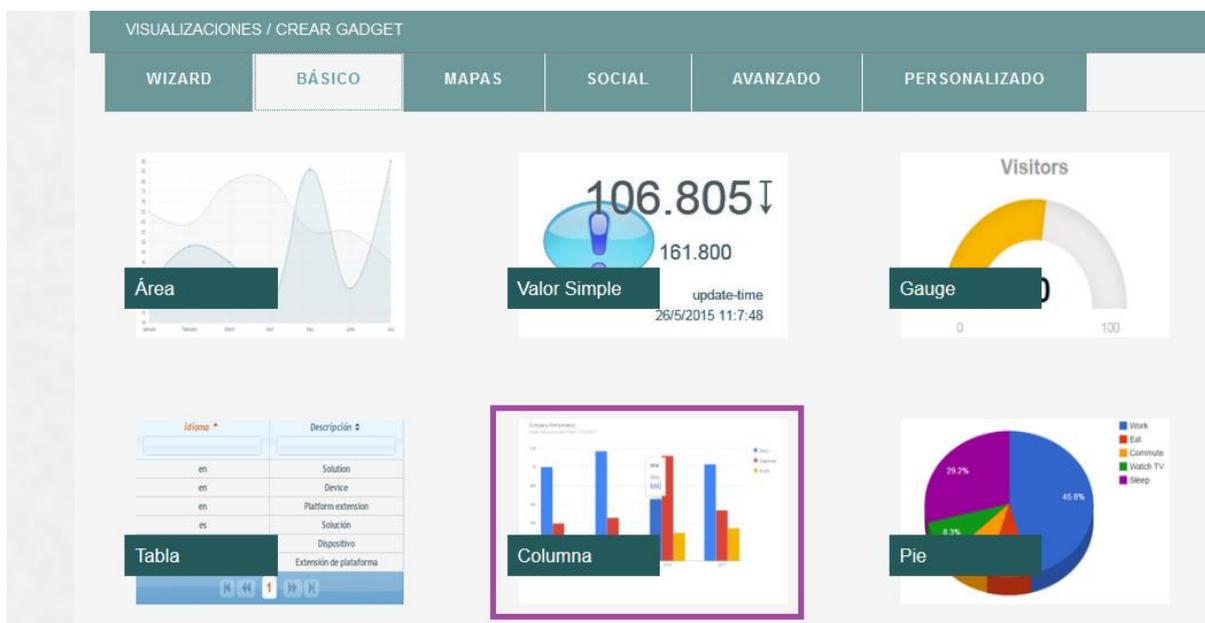


Figura 51. Gadget tipo columna

Escribiremos como nombre del gadget “tfgvvcacelerometro” y seleccionaremos “tfgvvc” como nuestro KP. Pondremos a 1 el atributo “Máximos valores a representar” para elegir la última Instancia de Ontología que ha llegado a la plataforma.

Seleccionaremos la ontología “tfgvvc”, en el eje X escribiremos “ContextData.Timestamp”, para tener en el eje de coordenadas X el tiempo y fecha en el que nos han llegado las muestras y en el eje Y escribiremos “accelX”, “accelY” y “accelZ” respectivamente. En el campo “Nombre Serie” escribiremos “Eje X”, “Eje Y” y “Eje Z”, para cada uno de los ejes de coordenadas del acelerómetro.

Al elegir el token que pertenece a nuestro ThinkKP nos aparecerá una previsualización de nuestro gadget.

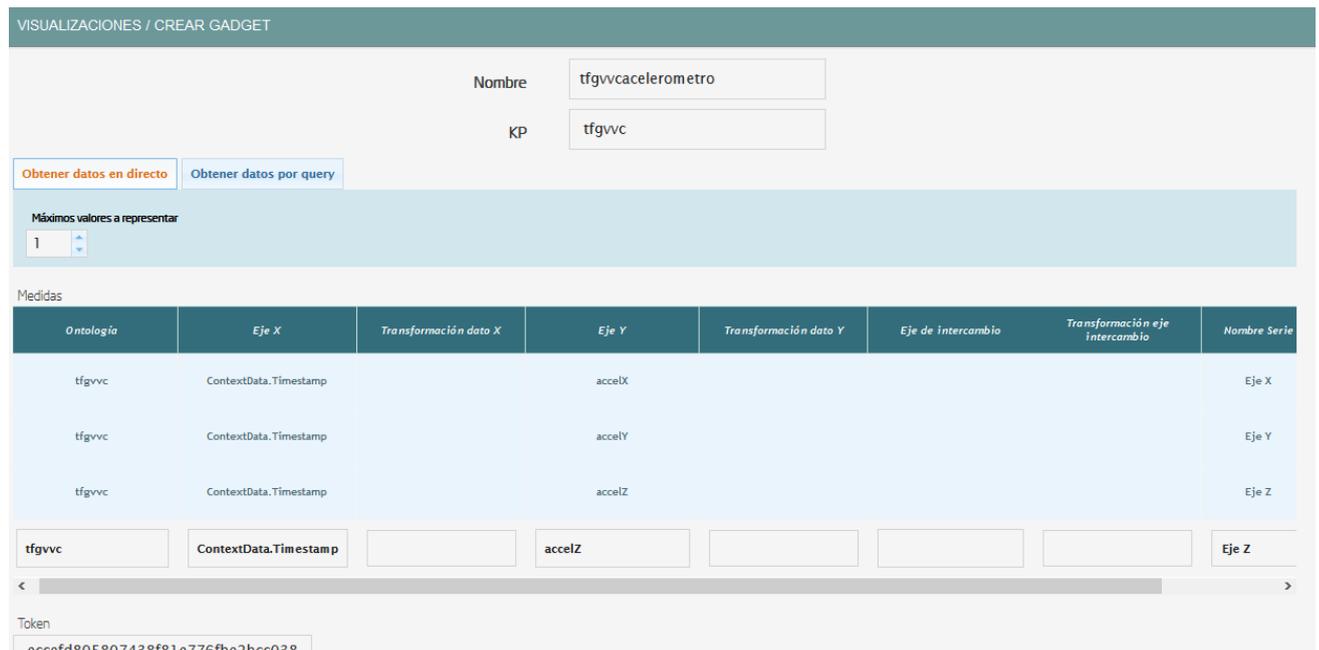


Figura 52. Parámetros gadget columna

Volviendo a la pantalla principal de “Mis gadgets” seleccionamos “Ver Gadget” (símbolo del ojo) en el gadget “tfgvvcacelerometro” que acabamos de crear.



Figura 53. Acceso a visualización del gadget

Manteniendo la aplicación del Smartphone Sofia2 IoT encendida, dejando el móvil en posición horizontal, y apretando a F5 en la visualización del gadget, veremos cómo cambia la gráfica, obteniendo un máximo en el eje Z y dos mínimos en los ejes X e Y.

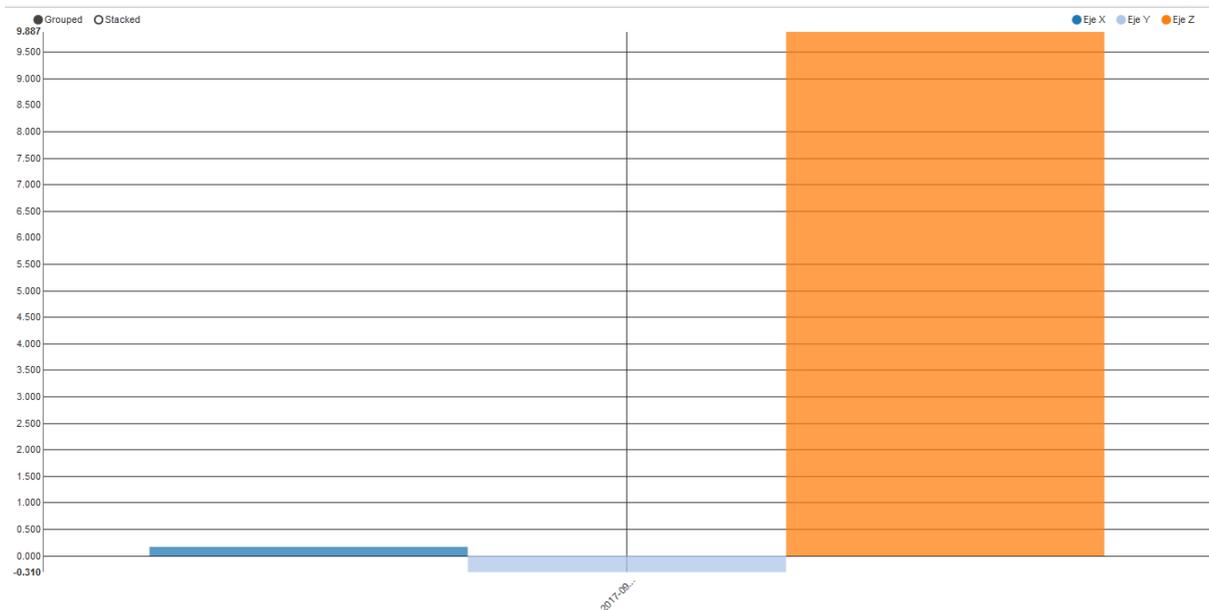


Figura 54. Visualización gadget acelerómetro con móvil en posición horizontal

Si ponemos el móvil en posición vertical y pulsamos sobre F5 en el gadget, observaremos una gráfica con un máximo en el eje Y y dos mínimos en los ejes X y Z.

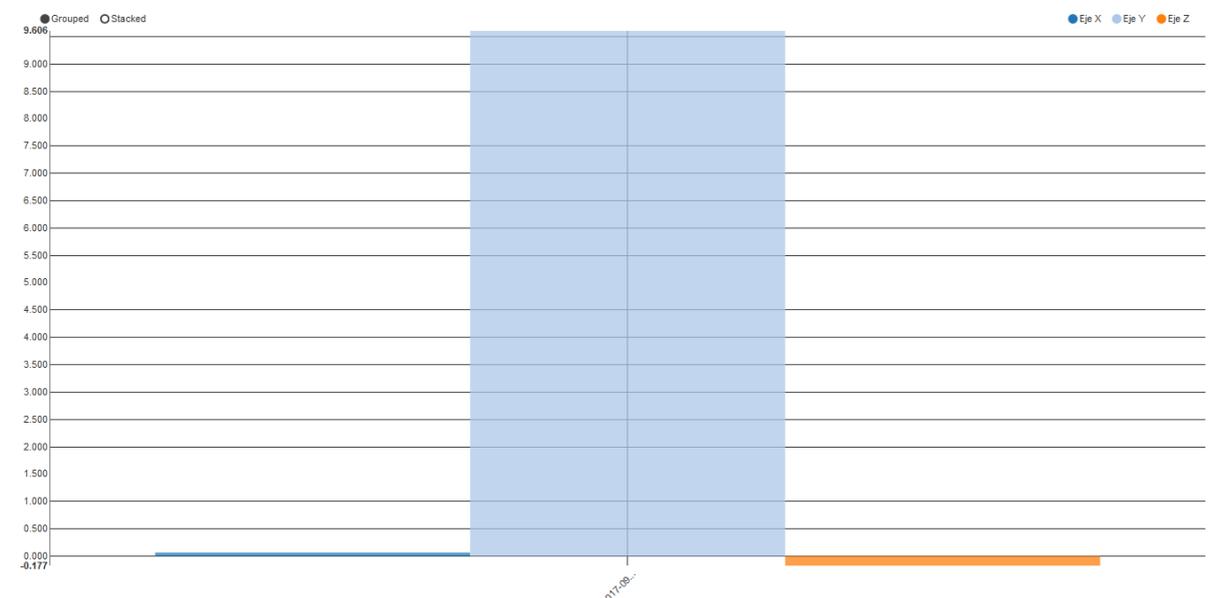


Figura 55. Visualización gadget acelerómetro con móvil en posición vertical

Por último, si situamos el móvil en dirección lateral, obtendremos en la gráfica un máximo en el eje X y dos mínimos en los ejes Y y Z al pulsar F5.

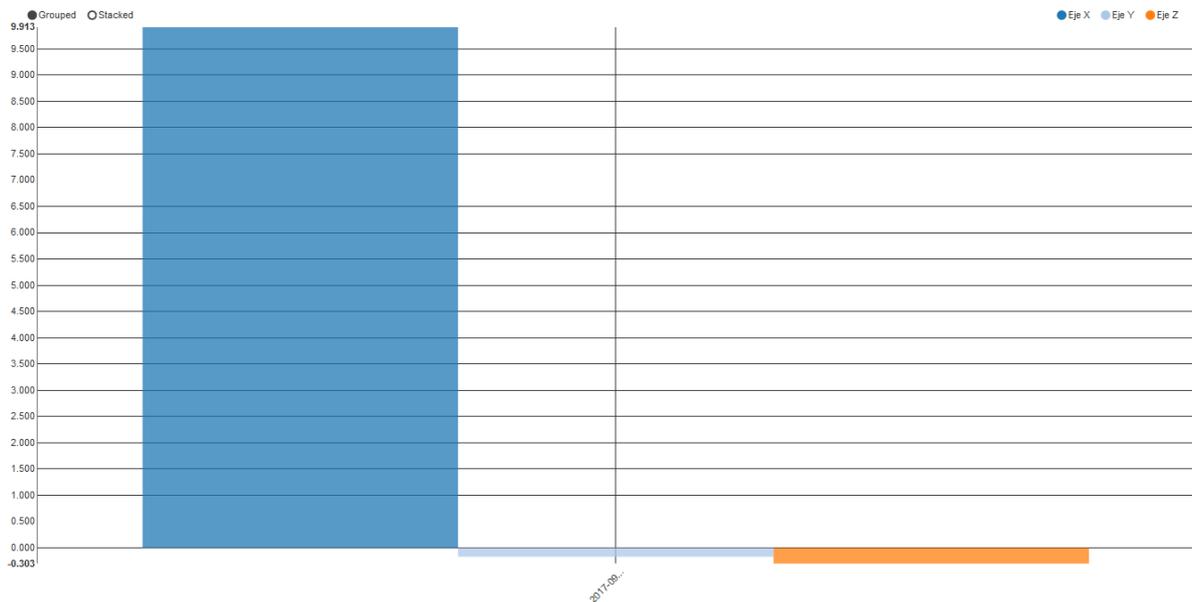


Figura 56. Visualización gadget acelerómetro con móvil en posición lateral

Una vez visto el funcionamiento del sensor acelerómetro, y la visualización de sus datos recogidos en la plataforma, vamos a probar el funcionamiento del sensor de geolocalización embebido en el smartphone.

Para ello crearemos un gadget de tipo mapa.

Accedemos mediante el panel de control de la plataforma a la pestaña "Mis Gadgets" dentro de "Visualización". Pulsando sobre "Crear Gadget" y sobre "Mapas", elegimos el gadget de tipo "Maps".

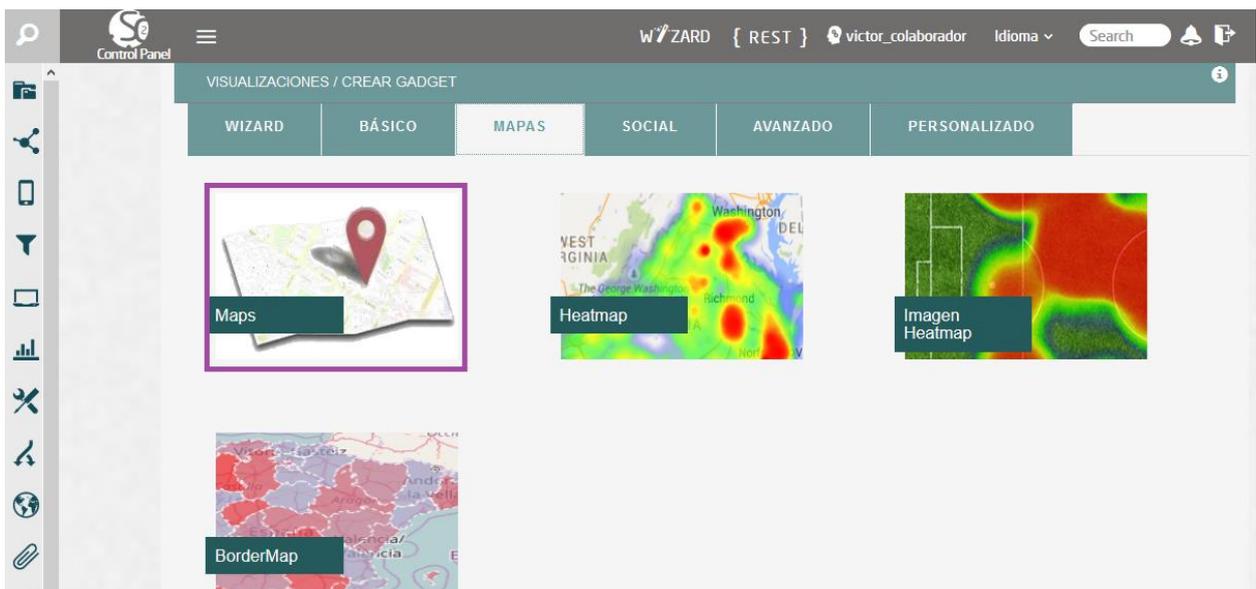


Figura 57. Gadget tipo maps

Escribiremos como nombre del gadget "tfgvvcmap" y seleccionaremos "tfgvvc" como nuestro KP. Pulsaremos la pestaña "Obtener datos por query", seleccionaremos la ontología "tfgvvc" y en el campo "Consulta" escribiremos "select * from tfgvvc limit 300;". Pulsaremos el botón "añadir".

En "Medidas" seleccionaremos la query1, escribiendo en el atributo "Campo" "geometry.coordinates" y en el atributo "Transformación de dato" "{coordinates:\$0,type:'Point'}". Si pulsamos "Añadir" y seleccionamos el token, aparecerá la previsualización del gadget.

Finalmente, si pulsamos sobre "Crear" obtendremos el gadget de mapa que geolocalizará la posición exacta del smartphone.

Volviendo a la pantalla principal de "Mis gadgets" seleccionamos "Ver Gadget" (símbolo del ojo) en el gadget "tfgvvcmap" que acabamos de crear.

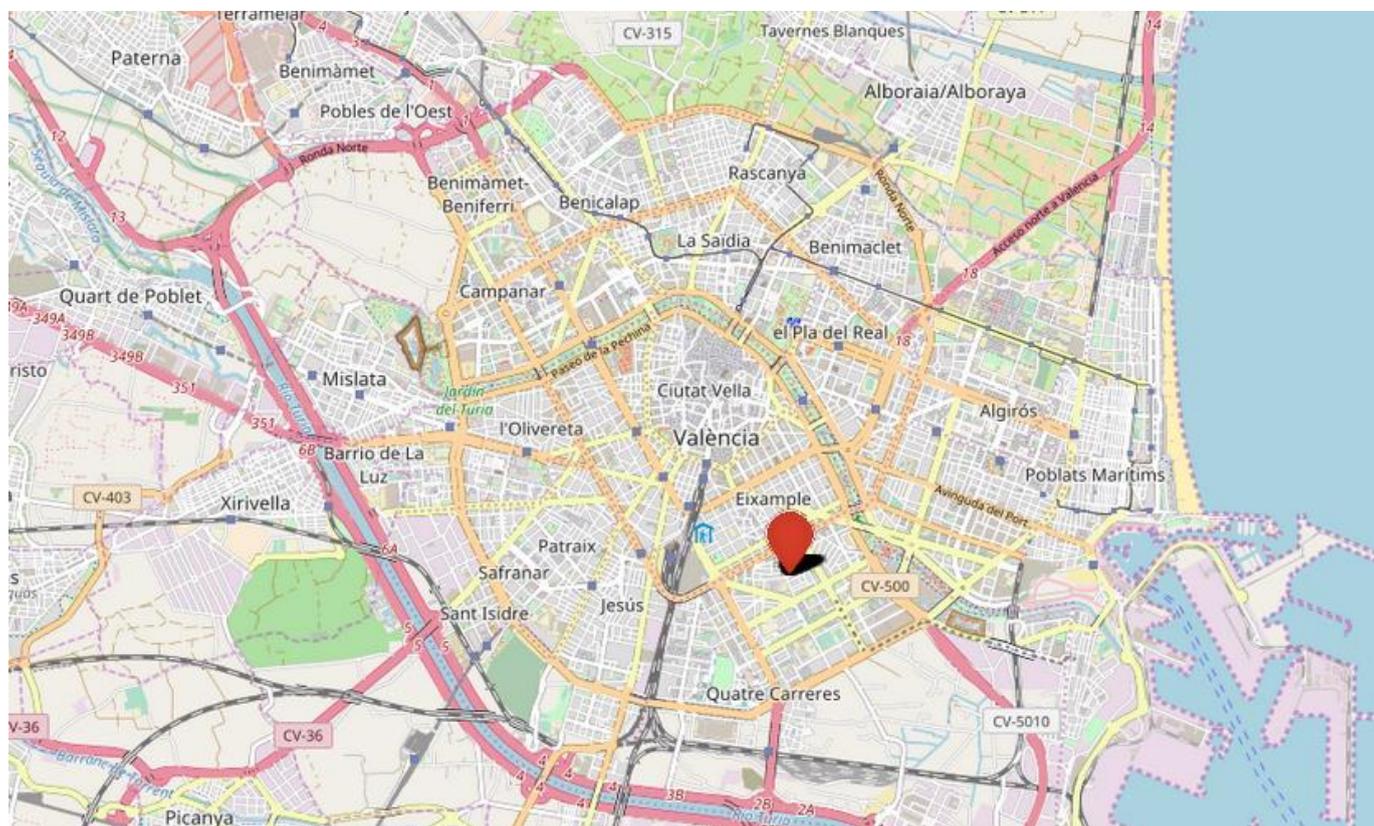


Figura 58. Gadget tfgvvcmap

Finalmente, integraremos los dos gadgets que hemos creado en un Dashboard.

Para ello, accederemos a la pestaña "Mis Dashboards" dentro de "Visualización".

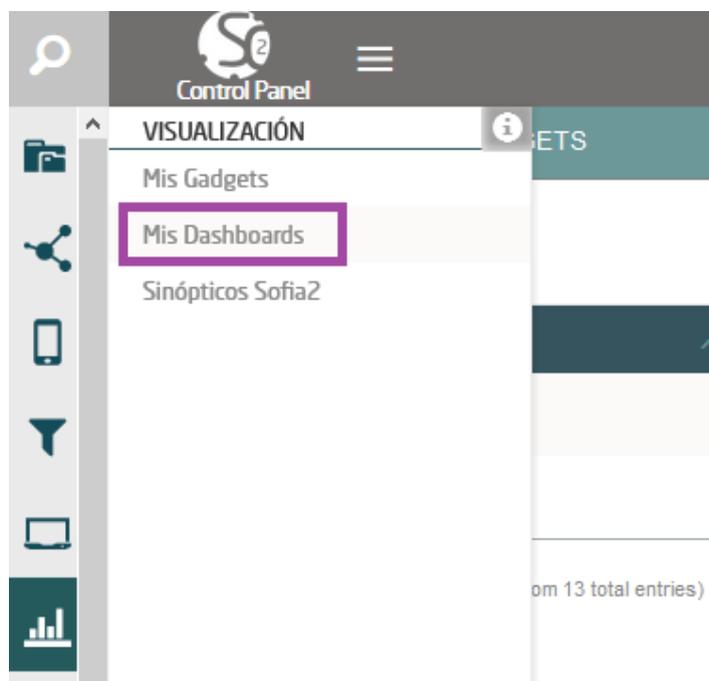


Figura 59. Acceso a Mis Dashboards

Pulsando sobre "Crear Dashboard", lo nombraremos como "tfgvvc", seleccionaremos el "Dark Theme" y pulsaremos sobre "Nueva página".

Seleccionando "+" nos dará la opción de añadir un gadget.



Figura 60. Adición de gadget a dashboard

Elegiremos el gadget "tfgvvcacelerómetro" y posteriormente realizaremos la misma acción con el gadget "tfgvvcmap".

Seleccionaremos una imagen de fondo mediante el menú de opciones.

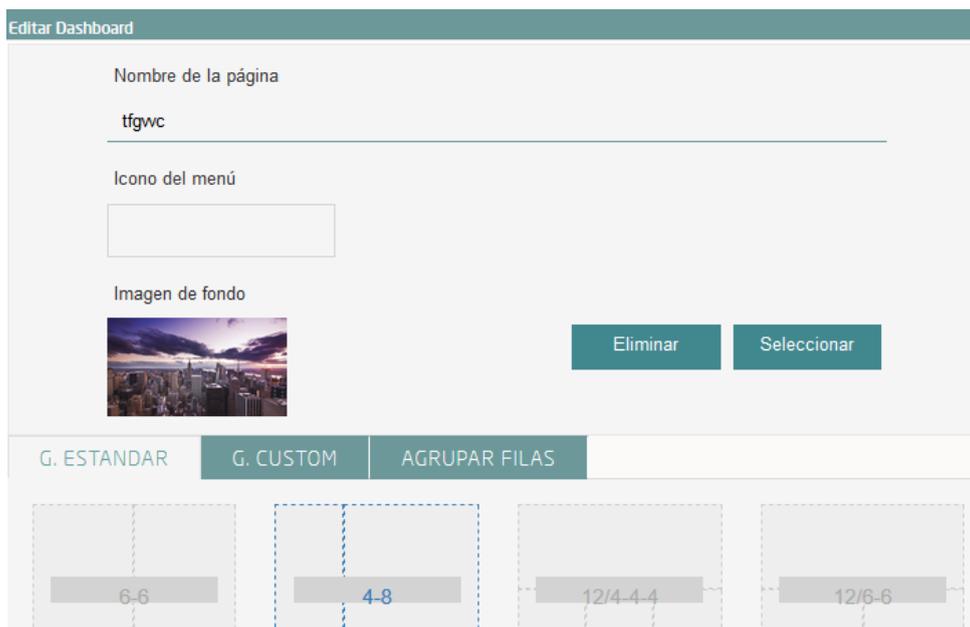


Figura 61. Selección de imagen de fondo

Finalmente obtendremos el Dashboard con los dos gadgets.

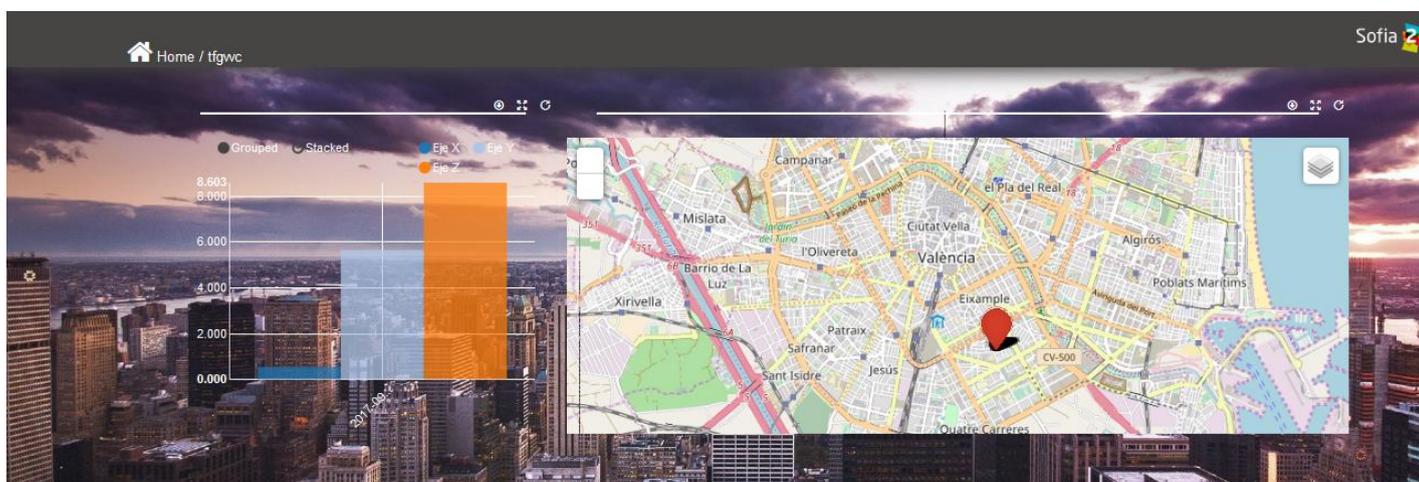


Figura 62. Dashboard completo integrando los dos gadgets

6.6 CASO DE USO: DETECCIÓN DE BEACON Y NOTIFICACIÓN AUTOMÁTICA

Para este último caso de uso, combinaremos la capacidad del sensorTag para actuar como beacon, y el smartphone, que actuará como puerta de enlace entre el dispositivo IoT y la plataforma.

A su vez, crearemos un código de alarma en la plataforma (Script), que realizará un envío al email que hayamos configurado en el apk, diciéndonos que la puerta de enlace ha detectado el beacon.

En primer lugar, crearemos el Script. Para ello, accedemos mediante el panel de control de la plataforma a la pestaña "Mis Reglas Scripts" dentro de "Reglas".

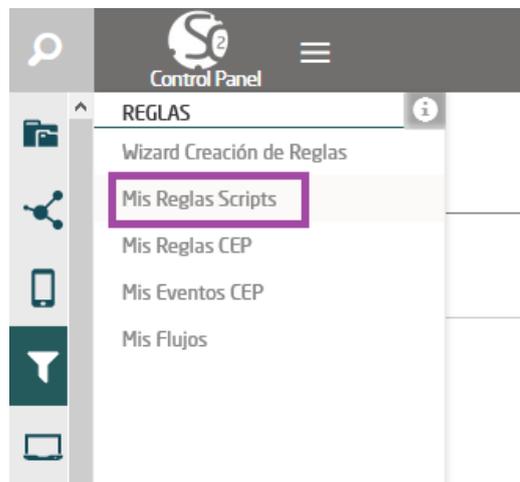


Figura 63. Acceso a Mis Reglas Scripts

Pulsaremos en "Crear Script" y nos aparecerá la pantalla para escribir y seleccionar los atributos y el código del script.

Lo llamaremos "tfgvvc", le daremos un timeout de "10", seleccionaremos el tipo "Ontología", seleccionando la ontología "tfgvvc" y escribiremos el código en lenguaje "Groovy" (que es muy similar al lenguaje "Java"). En la pestaña "If" escribiremos el código:

 A screenshot of a script editor interface. At the top, there are four tabs: 'if', 'Then', 'Else', and 'Error'. The 'if' tab is selected and highlighted in orange. Below the tabs, there is a dark background with white text representing Groovy code. The code is as follows:


```

1 def apiutils = new APIUtils();
2
3 def event=apiutils.getValueJson(ontology, "tfgvvc.event");
4 if (event=="true"){
5     return true;
6 }else{
7     return false;
8 }
9
  
```

Figura 64. Código Groovy pestaña If

Este código comprobará si hemos recibido el atributo "event" como verdadero, que significará que el gateway ha detectado el beacon, con lo que pasará a ejecutarse el código de la pestaña "Then". En caso de ser "false" el "event", no pasaría a ejecutarse el código de la pestaña "Then" y se acabaría el Script sin hacer ninguna acción.

En la pestaña "Then" escribiremos:



```

1 def apiutils = new APIUtils();
2 def apimail = new APIMail();
3 String [] to = [apiutils.getValueJson(ontology,"tfgvvc.email")];
4 def subject="Detección del beacon SensorTag en Sofia2 IoT";
5 def msg="Tienes el Beacon Sofia2.. Pásalo!";
6
7 apimail.sendMail(to, subject, msg);
8
    
```

Figura 65. Código Groovy pestaña Then

Este código tendrá la función de enviar un email con el sujeto "Detectado el beacon SensorTag en Sofia2 IoT" y el mensaje "Tienes el Beacon Sofia2.. Pasalo!" en caso de cumplirse la condición "If", y esto significaría que se ha detectado el sensorTag en el gateway. En la siguiente imagen vemos cómo el apk ha reconocido al beacon.

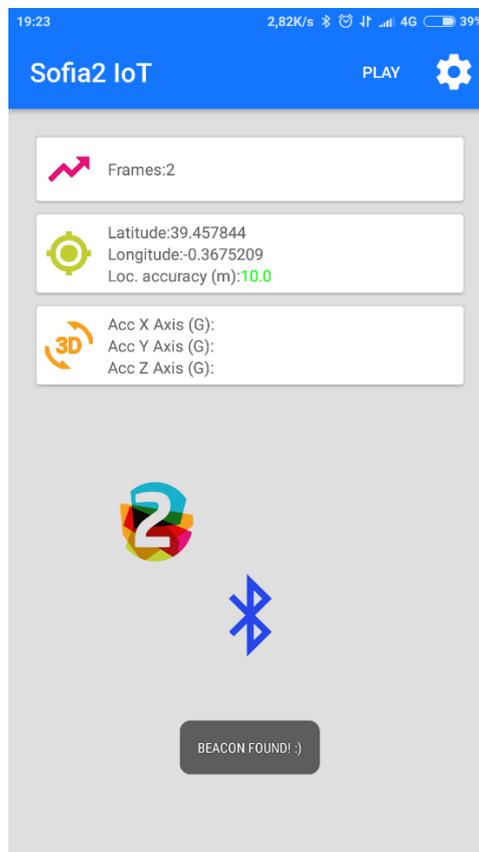


Figura 66. Detección del beacon en Sofia2 IoT

Por último, se muestra el email generado automáticamente que ha recibido la persona, teniendo el apk en funcionamiento, y una vez se ha detectado el beacon.

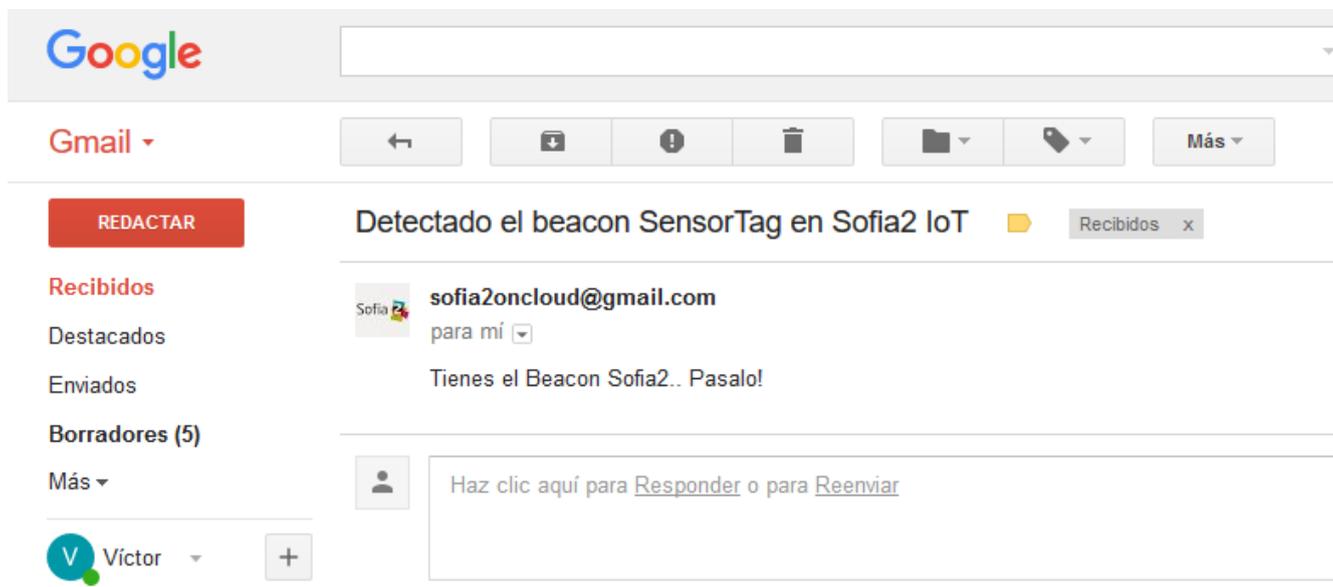


Figura 67. Envío automático de email

7 CONCLUSIONES

El presente trabajo ha definido las características, el ámbito de aplicación y la situación actual y previsiones futuras de las tecnologías IoT. También ha hecho énfasis en las capacidades de una plataforma IoT genérica y cómo Sofia2 cumple con las características que debe poseer cualquiera de ellas. Además, se han presentado los protocolos de comunicación más utilizados actualmente y una comparativa entre sus características más relevantes.

Por otra parte, y después de hacer una búsqueda en cuanto a los dispositivos IoT y sensores existentes en el mercado, se ha decidido seleccionar un microcontrolador de la empresa Texas Instruments, referente en el sector, el sensorTag CC2650. Con él, hemos conseguido cubrir las necesidades para desarrollar la aplicación práctica presentada y abrir la posibilidad a seguir profundizando en la materia con el desarrollo de nuevos casos de uso.

Con todo lo anterior, se ha cumplido con los objetivos secundarios que pertenecen al ámbito teórico del trabajo. Posteriormente se han realizado y explicado todos los pasos pertinentes para conseguir el objetivo principal, que consistía en conectar los dispositivos a la plataforma IoT y gestionar y visualizar los datos obtenidos. Por mediación de la creación de la ontología se ha modelado la estructura de datos, con el thinkP se ha configurado la lógica de los dispositivos, se ha descargado y configurado la aplicación Sofia2 IoT que nos ha permitido enlazar con la plataforma y se han creado los casos de uso.

El trabajo me ha permitido afianzar conocimientos adquiridos en mi reciente experiencia profesional y ampliar otros muchos. Además, aplicar estos conocimientos a la práctica experimental con casos de uso cercanos a aplicaciones de mercado (por ejemplo el sistema de geolocalización de flotas de camiones en soluciones de logística, el cambio de posición de visionado del smartphone en imágenes o películas de vídeo gracias al acelerómetro embebido, o el envío de mensajes automatizados) ha acrecentado mi interés por seguir creando más aplicaciones prácticas.

El ecosistema de innovación alrededor de Internet de las Cosas se encuentra en plena expansión con más de 8.400 millones de objetos conectados en 2017, un 31% más que en el pasado año. Los expertos prevén que la implementación tecnológica de IoT alcance los 30.000 millones de dispositivos en los próximos tres años, generando un valor de mercado por encima de los 14 mil millones de dólares en 2022, por lo que muchas empresas han empezado a capitalizar las ventajas del IoT como pieza clave de su transformación digital.

Todo ello, abre un futuro esperanzador para las tecnologías IoT y las plataformas ligadas a ellas, generando un inmenso volumen de datos que gestionará el denominado Big Data. Será importante gestionar correctamente la protección de datos y priorizar la seguridad en las conexiones de los dispositivos, puesto que son dos de los elementos críticos en la actualidad. Están emergiendo aplicaciones en todos los ámbitos de nuestra vida cotidiana y aparecerán muchas otras que aún somos incapaces de imaginar.

8 ÍNDICE DE FIGURAS

Figura 1. Gartner Hype Cycle para tecnologías emergentes. Julio 2017 [1].....	4
Figura 2. Estimación del crecimiento IoT por sectores. Parte 1.....	4
Figura 3. Estimación del crecimiento IoT por sectores. Parte 2.....	5
Figura 4. Infografía sobre el crecimiento previsto de los dispositivos IoT [3].....	6
Figura 5. Capacidades de una plataforma IoT [4].....	7
Figura 6. Tabla comparativa entre plataformas IoT.....	8
Figura 7. Flujo IoT genérico.....	9
Figura 8. Things en plataforma genérica	9
Figura 9. Things en plataforma Sofia2.....	9
Figura 10. Dispositivos soportados por Sofia2.....	10-11
Figura 11. Otras fuentes de datos soportadas por Sofia2.....	11
Figura 12. Conectividad en plataforma genérica	11
Figura 13. Conectividad en plataforma Sofia2	11
Figura 14. Gateways soportados por Sofia2.....	12
Figura 15. Servicios y Cloud en plataforma genérica.....	12
Figura 16. Servicios y Cloud en plataforma Sofia2.....	12
Figura 17. Conceptos elementales en Sofia2.....	13
Figura 18. Almacenamiento en Sofia2.....	14
Figura 19. Api Manager en Sofia2.....	14
Figura 20. Apps y Analytics en plataforma genérica	15
Figura 21. Apps y Analytics en plataforma Sofia2	15
Figura 22. Módulos Analytics en Sofia2.....	15
Figura 23. Infografía arquitectura Sofia2.....	16
Figura 24. Componentes Sofia2.....	16
Figura 25. Ecosistema IoT [6].....	17
Figura 26. Protocolos IoT [6].....	18
Figura 27. Esquema protocolo MQTT.....	19
Figura 28. Mensajes MQTT.....	19
Figura 29. QoS MQTT.....	20
Figura 30. Tabla comparativa protocolos de comunicación [7].....	21
Figura 31. Dispositivos y sensores.....	22
Figura 32. SensorTag CC2650 de Texas Instruments [8].....	23
Figura 33. Esquema de conectividad de los dispositivos.....	24
Figura 34. Componentes y capacidades de Sofia2 utilizados	25
Figura 35. Acceso al panel de control de Sofia2	25
Figura 36. Solicitud paso a colaborador.....	26
Figura 37. Acceso para la creación de Ontologías	26
Figura 38. Propiedades Ontología	27
Figura 39. Propiedades añadidas a la Ontología	27
Figura 40. Acceso para la creación de ThinKPs.....	28
Figura 41. Botón de creación de un nuevo ThinKP	28
Figura 42. Cuadro de creación de un nuevo ThinKP.....	28
Figura 43. Adición de Instancia de ThinKP	29
Figura 44. Acceso a la configuración de Sofia2 IoT	29
Figura 45. Configuración de ajustes en Sofia2 IoT	30
Figura 46. Datos de acelerómetro y geolocalización	30
Figura 47. Acceso a Gestión Crud de Instancias de Ontología.....	31
Figura 48. Datos de geolocalización	31
Figura 49. Datos de email, acelerómetro y evento.....	32
Figura 50. Acceso a Mis Gadgets.....	33
Figura 51. Gadget tipo columna.....	33
Figura 52. Parámetros gadget columna	34

Figura 53. Acceso a visualización del gadget.....	34
Figura 54. Visualización gadget acelerómetro con móvil en posición horizontal.....	35
Figura 55. Visualización gadget acelerómetro con móvil en posición vertical.....	35
Figura 56. Visualización gadget acelerómetro con móvil en posición lateral.....	36
Figura 57. Gadget tipo maps.....	36
Figura 58. Gadget tfgvvcmap.....	37
Figura 59. Acceso a Mis Dashboards	38
Figura 60. Adición de gadget a dashboard.....	38
Figura 61. Selección de imagen de fondo.....	39
Figura 62. Dashboard completo integrando los dos gadgets.....	39
Figura 63. Acceso a Mis Reglas Scripts.....	40
Figura 64. Código Groovy pestaña If.....	40
Figura 65. Código Groovy pestaña Then.....	41
Figura 66. Detección del beacon en Sofia2 IoT.....	41
Figura 67. Envío automático de email.....	42

9 BIBLIOGRAFÍA Y REFERENCIAS

- [1] Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017
<<http://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/>>
- [2] Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018<<http://www.gartner.com/newsroom/id/3221818>>
- [3] Internet of Things – the complete online guide to the IoT < <https://www.i-scoop.eu/internet-of-things-guide/>>
- [4] Market Guide for IoT Platforms <<https://www.gartner.com/doc/3380746/market-guide-iot-platforms>>
- [5] Tabla comparativa Plataformas IoT: Azure IoT Hub vs AWS IoT vs Watson IoT Foundation vs Sofia2 IoT Platform <<https://about.sofia2.com/2016/11/02/tabla-comparativa-plataformas-iot-azure-iot-hub-vs-aws-iot-vs-watson-iot-foundation-vs-sofia2-iot-platform/>>
- [6] Salman, Tara. Networking Protocols and Standards for Internet of Things. 2015
- [7] Karagiannis, Vasileios. Chatzimisios, Periklis. Vazquez-Gallego, Francisco, Alonso-Zarate, Jesus. A Survey on Application Layer Protocols for the Internet of Things.
- [8] SensorTag CC2650. Texas Instruments
<http://www.ti.com/ww/en/wireless_connectivity/sensortag/>
- [9] DZone's Guide to The Internet of Things <<https://dzone.com/guides/internet-of-things-1>>