**Internet de las Cosas**

Desde la llegada de Internet a nuestras vidas, éste ha evolucionado de una forma veloz y apabullante, desde aquellos rudimentarios módems de 56 KB hasta las rapidísimas y eficaces líneas de fibra óptica actuales. A día de hoy podemos conectar a Internet nuestros móviles, impresoras, Smart TV, cámaras vía IP, GPS y multitud de dispositivos electrónicos que poseen esta funcionalidad, pero, ¿hemos tocado techo o esto no es más que el inicio de una nueva era Internet?

Desde hace ya unos años se empezó a hablar del IoT (Internet de las cosas), no siendo más que una apuesta de futuro y comenzando a ser en la actualidad una absoluta realidad.   
Cada vez es más frecuente encontrarse con nuevos dispositivos capaces de conectarse a Internet y permitir al usuario un control y manejo de forma remota desde cualquier parte del mundo, pero esto no ha hecho más que comenzar.



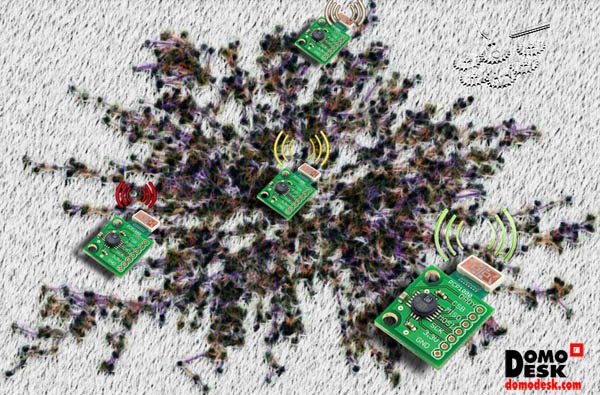
**¿Qué es exactamente el IoT Internet de las Cosas?**

Podríamos definir el Internet de las cosas como la consolidación a través de la red de redes de una "red" que alojase una gran multitud de objetos o dispositivos, es decir, poder tener conectada a esta todas las cosas de este mundo como podrían ser vehículos, electrodomésticos, dispositivos mecánicos, o simplemente objetos tales como calzado, muebles, maletas, dispositivos de medición, biosensores, o cualquier objeto que nos podamos imaginar.

**¿Qué nos ofrecerá?**

Como la gran mayoría de los avances tecnológicos el objetivo que pretende alcanzar esta tecnología es hacer más cómodas nuestras vidas y proporcionar una mayor seguridad en diversos ámbitos.

Un ejemplo seria si imaginamos a una nevera que fuese capaz de avisarnos cuando perdiese temperatura o indicarnos que algún alimento ha caducado o se ha pasado, o un escritorio que dejará constancia de donde se ha dejado cada cosa, o que pudiésemos saber dónde se encuentra cada objeto, que nos pertenezca, en cada momento, o controlar toda nuestra vivienda desde un Smartphone o PC (desde la puerta de entrada, hasta la cadena de WC), o que estemos avisados de los alérgenos y su concentración en el aire en una pulserita para alérgicos, o millones de escenarios por descubrir. Estos son algunos ejemplos del uso de la domótica y control.



**¿Es posible realmente conectar todo a la red?**

La respuesta es sí, no ahora mismo, pero si en muy poco tiempo. El principal inconveniente que está retrasando este avance es la limitación de direccionamiento que ofrece el actual protocolo ipv4, donde no sería posible interconectar tal cantidad de dispositivos y objetos. Por este motivo es ya inminente la transición a ipv6, el nuevo protocolo de direccionamiento que permitirá la interconexión casi ilimitada de cualquier objeto y la evolución e implementación del Internet of Things.  
Una vez esquivado dicho obstáculo, y con el progresivo abaratamiento de esta tecnología con el tiempo, no solo va a ser posible, si no necesario debido a su utilidad y la gran cantidad de aplicaciones que podremos realizar con el Internet de las cosas. Piensa en ropa inteligente, en artilugios implantados en nuestro cuerpo velando por nuestra salud, o ¿por qué no? en bolsas de snacks en los supermercados negándonos su compra por contener contraindicaciones en nuestro registro de salud.

**¿De qué forma repercute el Internet de las cosas respecto a temas de seguridad o privacidad, en nuestras vidas?**

Pues aquí, como siempre nos encontramos con la eterna dicotomía, si interpretamos las ventajas en cuanto a seguridad física o de bienes, indudablemente vamos hacia un entorno más seguro, si por el contrario nos percatamos que todo ese intercambio de información acaba por ser muy particular, y personal, de cada uno de nosotros, y que habla de tendencias, gustos, anhelos, pasiones...datos médicos, aficiones, sensaciones, variables actuales,..., pues entonces la seguridad se vuelve en un "control en manos ajenas" (eufemísticamente LA NUBE) que nos hace cada vez más vulnerables (eufemísticamente BIG DATA).

De tal forma, enfocando la seguridad física y de bienes en la vida de cualquier persona, ya sea sobre su persona, sobre su negocio, hogar, entre otros, tendrá un papel importantísimo, ya sea aumentando la seguridad en viviendas, vehículos, y bienes personales o simplemente sobre las personas.   
Volviendo a uno de los ejemplos anteriores, si todos y cada uno de los objetos tuviesen su particular conexión a Internet podríamos saber en cada momento dónde se encuentra dicho objeto y por lo tanto reducir prácticamente a cero la posibilidad de perderlo. Por otro lado, se vería incrementada de forma exponencial la seguridad en edificios, viviendas y fábricas, ya que con un sinfín de objetos sensorizados y monitorizados no habrá detalle que se escape, avisos por intrusión, escapes de agua, incendios, bases de datos con todo lo que ha ocurrido en una vivienda son algunas de las múltiples funciones que seremos capaces de realizar. En cuanto a la seguridad personal también se verá incrementada con objetos tales como relojes que pudiesen tomar el pulso y actuar en consecuencia, por ejemplo que en caso de paro cardíaco llamasen directamente a emergencias, dispositivos que nos alerten antes de sufrir una crisis por asma p.ej.. , todo esto y mucho más es lo que se podría conseguir con las nuevas tecnologías y todos estos nuevos conceptos, da igual que les llamen domótica, inmótica, AmI, Ambiance Intelligence, Objetos Inteligentes,Smartcities, Smart Grid, IoT…. o “un mundo feliz”.  
Como todo en esta vida, la avalancha tecnológica es imparable, los beneficios inexcusables....y el resto de la sociedad tendrá que poner coto a factores que tengan que ver con la privacidad, los derechos y deberes, y todo lo relacionado al reconocimiento de la dignidad personal.

**¿De qué capacidades estará dotado?**

- Comunicación y cooperación: los objetos tendrán la capacidad de conectarse a los servicios de Internet y/o entre sí, pudiendo intercambiar y actualizar datos entre ellos y  establecer comunicaciones con los servidores.  
- Capacidad de direccionamiento: Esta clase de dispositivos podrán ser configurados y localizables desde cualquier lugar de la red.  
- Identificación: Los objetos podrán ser identificados mediante tecnologías tales como RFID (Radio Frecuency Identification), NFC (Near Field Communication), códigos de barra de lectura óptica, o cientos de otras formas de identificar a un dispositivo en una red.  
- Localización: Tendrán en todo momento conocimiento sobre su ubicación física, pudiendo saber dónde se encuentra en todo momento.  
- Actuación: Determinados objetos serán capaces de manipular su entorno.

**¿Cuáles serán los niveles de inteligencia de estos dispositivos?**

Según los expertos existirán al menos 4 niveles de inteligencia:

- Nivel 1: Identidad. El objeto será capaz de identificarse de manera única  
- Nivel 2: Ubicación. Se podrá saber dónde está dicho objeto o dónde ha estado.  
- Nivel 3: Estado. Será capaz de comunicar el estado en que se encuentra, así como sus características.  
- Nivel 4: Contexto. El objeto será capaz de percibir el entorno en que se encuentra.

Si lo analizamos aquí nos parece muy infantil esta clasificación ya que está pensada bajo la premisa de dispositivos un poco "tontitos", y desde luego, lo que hoy posibilita el mercado hace más diversa la clasificación, y podríamos añadir niveles como:

- Nivel 5: Criterio. El objeto se comunica, se identifica, se ubica, analiza su entorno, decide y ejecuta en función de su criterio.

- Nivel n+1: ?¿?¿

**¿Qué protocolos de comunicación utilizará el IoT?**

A saber ,esto siempre es el dilema, da igual que hablemos de M2M, de domótica...o de automatización industrial, un sinfín de iniciativas se ponen en marcha para intentar conjugar un protocolo que sirva como estándar y de alguna manera tenga en cuenta la idiosincrasia de los sistemas que queremos meter en escena.  
Y si bien tenemos Zigbee (IEEE 802.15.4), Bluetooth LTE, 6LowPan, WiFi, GSM (con todas sus respectivas Gs), u otras esperanzadoras como SigFox...y desde luego un maravilloso mundo TCP/IP que sabemos que es capaz de desplegar redes mundiales, pero que no esta pensado para meter sus vetustas arquitecturas directamente en sensores que deberían funcionar, al menos algunos, durante décadas, es decir autosuficientes en el tema de carga (solar, viento..etc) o auto eficientes en el tema de consumo, bueno, esto sin hablar de ciento y una mil conjeturas propietarias lidiando el protagonismo para el gran negocio que se avecina.

En Domodesk vemos que iniciativas en grupos de trabajo como RPL Routing Protocol for Low-Power and Lossy Networks (http://tools.ietf.org/html/rfc6550 ) empiezan a pensar en arquitecturas que posibiliten los millones de escenarios posibles si queremos un Internet of Everything que funcione, o como este grupo define el OF (objective functions), porque no debería ser la misma prioridad un MEMS que intente decirle a nuestro médico y servicio asistencial que estamos sufriendo un infarto, que un sensor que se esta preocupando de vigilar por la eficiencia de nuestro sistema de climatización, y tampoco la jerarquización y los caminos que debe seguir laseñal hasta que encuentre un punto de reunión que controle su direccionamiento IPv6, como veis la "comedura de tarro" es directamente proporcional al objetivo de llenarlo todo de posibilidades de comunicación inteligente, y hay mucho que definir.  
Pero en Domodesk ya hace tiempo que apostamos por TCP/IP y Wireless con topología en rejilla (elemento clave...el MESH), y poco cuesta extrapolar esto a lo que será una casa más grande, la de todos, el planeta ;-)

**¿Qué es y de que partes se compone un dispositivo M2M?**

Como hemos hablado anteriormente de los dispositivos M2M ya que son una tecnología propicia a la hora de desarrollar el Internet de las cosas vamos a hacer una breve descripción de en qué consisten.   
Los dispositivos M2M (machine to machine) como su propio nombre indica se trata de dispositivos capaces de establecer una comunicación tanto con el servidor como con otros dispositivos M2M.

Las partes de que se compone son las siguientes:

- Dispositivos de gestión: Forman parte de este grupo todas aquellas máquinas o dispositivos cuya labor va a ser la de gestionar datos (alarmas en hogares, contadores, paneles de información, puntos de venta,etc)  
- Dispositivos M2M: serán aquellos dispositivos (módulos) que conectados de forma remota a cualquier máquina recoja información y mantenga una comunicación con el servidor. Eventualmente también tendrán capacidad para procesar información individualmente.  
-Servidor: Será aquel sistema que envié y reciba dicha información de las máquinas y a su vez haga una gestión eficiente de la misma.  
-Red de comunicación: se trata del medio físico mediante el cual viaje la información pudiendo de ser de dos clases: cableado e inalámbrico, siendo este último el método habitual puesto que en principio carece de lógica implementar el Internet de las cosas mediante cable a no ser que sea algún dispositivo muy especifico.

**¿Cuál ha sido la evolución del Internet de las cosas?**

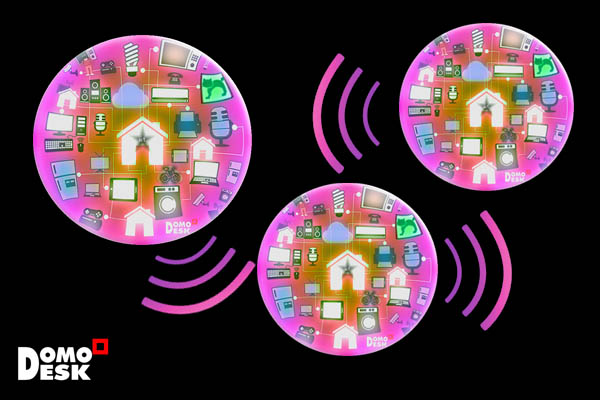
Se puede hablar de sus primeros pasos en el año 1990 cuando Jhon Romkey y Simon Hacket consiguieron diseñar una tostadora con conectividad a Internet, pudiendo desde cualquier ordenador determinar su encendido, su apagado y configurar el tiempo de tostado de la misma.   
A partir de este momento, se supo el potencial que tendría la posibilidad de conectar ciertos dispositivos a Internet, pero fue en 1999 cuando fueron introducidos los conceptos básicos de el Internet de las Cosas por el ingeniero Bill Joy, el cual se percato de la importancia que tendría este aspecto a la hora de automatizar y disponer de control sobre una multitud impensable de dispositivos, escenarios que también planteaban JINI y UPnP.  
Nos remontamos ya a 2009 donde fue bautizado el término gracias a un artículo publicado por Kevin Ashton el 12 de Julio de 2009, dicho artículo hablaba de la gran funcionalidad que podría aportar conectar todo a la red para poder contar los objetos, dispositivos, saber la posición en que se encuentran, su estado y que éstos pudiesen darnos información sobre el entorno en que se encuentran.

Unos años antes se realizó un estudio en el cual se determinaba que alrededor de 1000 millones de dispositivos estaban conectados a Internet entre consolas, ordenadores, móviles, etc.  
La empresa CISCO, formuló mediante un estudio que la cantidad de dispositivos electrónicos conectados a la red era más elevado que la población mundial.  
Por último, a partir del año 2011 se diseña el protocolo de direccionamiento de Internet IPv6 posibilitándola identificación de una infinidad de direcciones y haciendo posible el IoT ya que se estima que en menos de 10 años existan cerca de 50.000 millones de dispositivos conectados a la red.

**¿Para cuando se prevé que sea posible la implementación a gran escala de IoT?**

No hay una fecha exacta, pero lo que esta claro es que con la velocidad con la que avanza la tecnología, con circuitos cada vez más baratos y a su vez más pequeños, y la increíble evolución de las redes informáticas y las posibilidades que ésta ofrece, no falta mucho, serán 5, 10 o 15 años, pero lo que queda demostrado es que ya empieza a ser un hecho, esta ahí, y es posiblemente junto con la robótica el futuro más cercano que podemos observar, solo hay que echar un vistazo a las miles de campañas de crowdfunding (palabreja de moda para democratizar las inversiones..., resumiendo, que paguen los fans) con miles de artilugios pujando por un papel en este mundo.

Es 2014, demos la bienvenida a la nueva era de Internet, EL INTERNET DE LAS COSAS, y deja que en Domodesk te sigamos acompañando, al menos, 16 años más :-), no en vano, poner las electrónicas a trabajar en red para el disfrute y utilidad de las personas, es domótica, pura y dura.



**ACTUALIZAMOS IoT Arena.-**

A Julio de 2014 vemos como esta el panorama de iniciativas que persiguen un trozo de protagonismo en el mundo de la **domótica, Internet de las Cosas IoT**, o llámalo, si quieres, una utopia de un cuasi infinito mundo de objetos conectados, comunicándose entre ellos para, según todos, hacernos la vida más fácil y poniendo a las personas en el centro de aprovechamiento de los avances tecnológicos.

El juego de asociarse con el caballo ganador se convierte en una pesadillas para todos, desde fabricantes de hardware hasta los grandes del consumo electrónico, de ahí que a muchos los veamos flirteando con varios estándares, protocolos de comunicación o refritos de otros tiempos.

Nuestra experiencia en el mundo de la domótica, de 16 años, consigue que no acabemos por pretender seguir todas y cada una de las iniciativas, nosotros ya tenemos nuestras apuestas y el resto ya los hemos condenado al silencio. Sin pecar de prepotentes, en Domodesk descubrimos que el arte de todo este despropósito de “egos” es la integración, y esperar que surja un “esperanto” que se convierta en un lenguaje único para comunicar, fabricar y poner en marcha…., eso, es una ilusión, así que optamos por seguir aprendiendo a integrar mundos diferentes de la forma más sencilla para el usuario final.

Internet de las cosas (en inglés, Internet of things, abreviado IoT) es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet. Alternativamente, Internet de las cosas es el punto en el tiempo en el que se conectarían a internet más “cosas u objetos” que personas. También suele referirse como el internet de todas las cosas o internet en las cosas. Si los objetos de la vida cotidiana tuvieran incorporadas etiquetas de radio, podrían ser identificados y gestionados por otros equipos, de la misma manera que si lo fuesen por seres humanos.

El concepto de internet de las cosas lo propuso Kevin Ashton en el Auto-ID Center del MIT en 1999, donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores.

Por ejemplo, si los libros, termostatos, refrigeradores, la paquetería, lámparas, botiquines, partes automotrices, etc. estuvieran conectados a Internet y equipados con dispositivos de identificación, no existirían, en teoría, artículos fuera de stock o medicinas caducadas; sabríamos exactamente la ubicación, cómo se consumen y se compran productos en todo el mundo; el extravío sería cosa del pasado y sabríamos qué está encendido o apagado en todo momento.9 10

El internet de las cosas debería codificar de 50 a 100 000 billones de objetos y seguir el movimiento de éstos; se calcula que todo ser humano está rodeado de por lo menos 1000 a 5000 objetos.11 Según la empresa Gartner, en 202012 habrá en el mundo aproximadamente 26 mil millones de dispositivos con un sistema de adaptación al internet de las cosas.13 Abi Research, por otro lado, asegura que para el mismo año existirán 30 mil millones de dispositivos inalámbricos conectados al Internet.14 Con la próxima generación de aplicaciones de Internet (protocolo IPv6) se podrían identificar todos los objetos, algo que no se podía hacer con IPv4. Este sistema sería capaz de identificar instantáneamente por medio de un código a cualquier tipo de objeto.15

La empresa estadounidense Cisco, que está desarrollando en gran medida la iniciativa del internet de las cosas, ha creado un “contador de conexiones” dinámico que le permite estimar el número de “cosas” conectadas desde julio de 2013 hasta el 2020.16 El concepto de que los dispositivos se conectan a la red a través de señales de radio de baja potencia es el campo de estudio más activo del internet de las cosas. Este hecho se explica porque las señales de este tipo no necesitan ni Wi-Fi ni Bluetooth. Sin embargo, se están investigando distintas alternativas que necesitan menos energía y que resultan más baratas, bajo el nombre de “Chirp Networks”.17

**Historia**

Los ordenadores actuales —y, por tanto, internet— son prácticamente dependientes de los seres humanos para recabar información. Una mayoría de los casi 50 petabytes (un petabyte son 1024 terabytes) de datos disponibles en internet fueron inicialmente creados por humanos, a base de teclear, presionar un botón, tomar una imagen digital o escanear un código de barras. Los diagramas convencionales de internet, dejan fuera a los routers más importantes de todos: las personas.

Una visión alternativa, desde el mundo de la Web semántica, se centra más bien en hacer que todas las cosas (no sólo las electrónicas, inteligentes o RFID) tengan una dirección basada en alguno de los protocolos existentes, como el URI. Los objetos o las cosas no conversan, pero de esta forma podrían ser referenciados por otros agentes, tales como potentes servidores centralizados que actúen para sus propietarios humanos.

Se estima que el proyecto cuesta 19 billones de dólares estadounidenses, según el director ejecutivo de Cisco22 y, como eso, muchos dispositivos del internet de las cosas formarán parte del mercado internacional. Estos son algunos problemas que podrían surgir:

**Inteligencia**

El Internet de las cosas probablemente será "no determinista" y de red abierta (ciberespacio), en la que entidades inteligentes auto-organizadas (servicio Web, componentes SOA) u objetos virtuales (avatares) serán interoperables y capaces de actuar de forma independiente (que persiguen objetivos propios o compartidos), en función del contexto, las circunstancias o el ambiente. Se generará una Inteligencia Ambiental (construida en Computación ubicua).

La versión industrial del IoT se conoce como IIoT, Industrial Internet of Things, de sus siglas en inglés. Incluirá determinismo, fiabilidad y sincronismo.

**Arquitectura**

El sistema será probablemente un ejemplo de "arquitectura orientada a eventos, construida de abajo hacia arriba (basada en el contexto de procesos y operaciones, en tiempo real) y tendrá en consideración cualquier nivel adicional. Por lo tanto, el modelo orientado a eventos y el enfoque funcional coexistirán con nuevos modelos capaces de tratar excepciones y la evolución insólita de procesos (Sistema multi-agente, B-ADSC, etc.).

En una Internet de las Cosas, el significado de un evento no estará necesariamente basado en modelos determinísticos o sintácticos. Posiblemente se base en el contexto del propio evento: así, será también una Web Semántica. En consecuencia, no serán estrictamente necesarias normas comunes que no serían capaces de manejar todos los contextos o usos: algunos actores (servicios, componentes, avatares) estarán auto referenciados de forma coordinada y, si fuera necesario, se adaptarían a normas comunes (para predecir algo solo sería necesario definir una "finalidad global", algo que no es posible con ninguno de los actuales enfoques y normas).

**¿Sistema caótico o complejo?**

En semi-bucles abiertos o cerrados (es decir, las cadenas de valor, siempre que sean una finalidad global pueden ser resueltas), por lo tanto, serán consideradas y estudiadas como un Sistema complejo, debido a la gran cantidad de enlaces diferentes e interacciones entre agentes autónomos, y su capacidad para integrar a nuevos actores. En la etapa global (de bucle abierto completo), probablemente esto será visto como una caótica medioambiental (siempre que los sistemas tengan siempre finalidad).

**Seguridad**

La empresa Hewlett Packard realizó un estudio en 2015, reportando que entre otros hallazgos respecto a los dispositivos IoT, 70% de ellos tiene vulnerabilidades de seguridad en sus contraseñas, hay problema con el cifrado de los datos o los permisos de acceso, y el 50% de las aplicaciones de dispositivos móviles no encriptan las comunicaciones. La firma de seguridad Kaspersky Lab realizó pruebas en objetos conectados al IoT y encontró que una cámara monitor para bebé podía hackearse para interceptar el video y en una cafetera que transmitía información sin encriptar, se podía conocer la contraseña de la red WiFi en donde estuviera conectada.

Dado esto, la seguridad se ha vuelto una situación de mucha importancia, porque pareciera que estos dispositivos no tienen riesgo para los datos que transmiten y almacenan, parecier que no son vulnerables, pero la realidad es que éstos dispositivos junto con otros que no tienen una debida protección, hicieron posible varios ataques a estos dispositivos.

La proyección de crecimiento de dispositivos IoT ha sido exponencial, y se estima que para el año 2020 habrá 50,000 millones de dispositivos conectados en todo el mundo. Este crecimiento puede hacer que el tema se seguridad de los datos sea una situación más crítica ante la falta de procesos que aseguren la integridad y encriptación de los datos.

Los datos que guardan los dispositivos IoT son altamente codiciados debido a que son de uso cotidiano y almacenan información acerca de los hábitos de los usuarios, por lo que contar con esas bases de datos es valiosa para varias empresas, que pueden dirigir sus esfuerzos en productos y servicios enfocados en los hábitos y preferencias de las masas. Lo que podrá ayudar a aminorar el problema, será el cifrado y la encriptación de datos, para poder subir los datos a la nube.