Escuela Politécnica Superior de Jaén

Grado en Ingeniería Informática

UNIVERSIDAD DE JAÉN

Escuela politécnica Superior de Jaén

Trabajo Fin de Grado

INTERNET DE LAS COSAS. PRIVACIDAD Y SEGURIDAD

ALUMNO: MIGUEL CASTRO SOLA

Tutor: Dra. Dª. Macarena Espinilla Estévez
Dpto: INFORMÁTICA

SEPTIEMBRE, 2016

Internet de las Cosas. Privacidad y Seguridad

Miguel Castro Sola

Septiembre 2016

Universidad de Jaén

Escuela Politécnica Superior de Jaén

Departamento de Informática

Dra. Da. Macarena Espinilla Estévez, tutora

del Trabajo Fin de Grado titulado:

Internet de las Cosas. Privacidad y Seguridad,

que presenta D. Miguel Castro Sola,

autoriza su presentación para defensa y evaluación en la

Escuela Politécnica Superior de Jaén.

Jaén, septiembre de 2016

El alumno:

Miguel Castro Sola

La tutora:

Macarena Espinilla Estévez

A todos los que me ayudaron en esta etapa y compartieron horas de risas, nervios y alegrías.

A mi tutora Macarena Espinilla Estévez por su ayuda y paciencia.

Y a Carmen por su mano en mi espalda, sosteniéndome en esta última etapa y dándome el último empujón.

Gracias.

Índice de contenidos

1.Introducción a IoT

1.1. Motivación

Actualmente vivimos en un mundo de continuo cambio a nivel tecnológico. No hay más que encender el ordenador o dispositivo móvil y comprobar las cosas que podemos hacer con él: desde enviar a hacer la colada a una lavandería, reservar un billete de avión para un vuelo, coger nuestro teléfono móvil y pagar la cuenta del restaurante con solo pulsar un dedo. Incluso sentados en nuestro sofá en casa, podemos pedir a nuestra televisión que busque nuestra película favorita y la reproduzca solo con decirlo en voz alta.

La tecnología avanza con nosotros y para nosotros, para hacernos la vida más sencilla y cómoda, para tener interconectadas todas las cosas de nuestro día a día y permitirnos ser más productivos. Y para tener estas cosas conectadas entre sí hace falta un medio para ello: Internet.

Internet hace que unas cosas se comuniquen con otras. Que transfieran datos de su estado y reciban otros del entorno creando así una red de información que puede ser usada de diferentes formas y aprovechada para hacer funcionar todo en su conjunto, finalmente componiendo "El internet de las cosas" (Internet of things).

Como estudiante del Grado de Ingeniería Informática, el escenario en el que me muevo es amplio debido a la potencia que tiene la profesión que he escogido, pero sin duda una de las ramas más prometedoras y fascinantes es sobre la que trata este Trabajo fin de Grado. La interconexión de todas las cosas que nos rodean, no solo a nivel cotidiano, sino a nivel empresarial, urbano, energías renovables, etc., no es algo inimaginable, sino que es algo que está ya en nuestra sociedad actual.

Un aspecto clave en la informática y la tecnología en general es su rápido cambio y su impacto en el mundo, y por consecuencia, la adaptación también debe de ser rápida. Pero, ¿está preparada la sociedad para este cambio? Y lo más importante, ¿Estamos *protegidos* para lo que viene?

Al mismo tiempo que avanza la tecnología también debe de avanzar la seguridad para protegernos sobre los posibles ataques que se hagan hacia ella.

Es mi afán por la tecnología y la seguridad la que me ha llevado a elegir este proyecto que combina ambas cosas, y me resulta muy ilusionante poder dedicarme a desarrollar un proyecto de tal envergadura pudiendo ampliar mis conocimientos en esta rama y conocer más el sector sobre el que se moverá.

1.2. Propuesta

La propuesta de este Trabajo fin de Grado es realizar un estudio sobre las cuestiones de privacidad y seguridad de los datos en el paradigma de internet de las cosas.

1.3. Objetivos

¿Estamos preparados para el cambio tecnológico que se avecina con "El internet de las cosas"? ¿Estamos totalmente protegidos de *él*?
El objetivo de este trabajo es analizar en profundidad todos los cambios que va a suponer la implantación de esta nueva forma de entender la tecnología en general, y con ella la sociedad y la manera de hacer las cosas tanto cotidianas como laborales.

Una vez hecho esto, se analizarán y evaluarán los riesgos que conlleva vivir inmersos en esta tecnología, donde toda la información estará al alcance de "todo y todos" y finalmente se explorarán y se propondrán diferentes soluciones para estos problemas.

1.4. Estructura

La estructura del proyecto será la siguiente:

En la primera parte se hará una introducción y una revisión completa del Internet de las cosas, desde los inicios hasta lo que se espera pasando por la situación en la actualidad de esta tecnología.

En esta parte se abordará todo lo que nos ofrece IoT y también los problemas que puede causar en un futuro. Al finalizarla estaremos preparados para empezar a identificar cada una de las amenazas que plantea.

En el segundo punto se explicará y analizará en mayor detalle los diferentes grupos de amenazas a la seguridad, que serán: seguridad en el software, seguridad en la configuración y funcionalidad, seguridad en el hardware, seguridad en los usuarios.

El tercer punto será un pequeño apartado donde se comentarán algunos casos registrados sobre ataques a la seguridad tecnológica e informática.

En el cuarto punto se propondrán soluciones a las posibles amenazas.

En el quinto punto se analizarán los resultados obtenidos de las encuestas que se realizarán sobre Internet de las cosas a la gente.

Finalmente, el proyecto se terminará con una conclusión donde se expondrán y recopilarán los datos más significativos y daré nuestra opinión sobre los mismos.

Durante todo el proyecto se irán intercalando escenarios de ejemplo, mediante los cuales se intentará explicar con ejemplos prácticos, todo lo que se puede llegar a conseguir con esta nueva manera de entender el mundo. Aparecerán enumerados desde el número uno en adelante.

2. Internet of Things (Internet de las cosas)

2.1. Retrospectiva

El internet de las cosas (desde ahora y durante todo el proyecto: **IOT**) no es un concepto reciente y novedoso.

Tal vez tendríamos que remontarnos al año 1927, cuando Nikola Tesla conformó la base de las comunicaciones inalámbricas y de radio, pero avanzaremos un poco más adelante.

La primera conexión entre computadores se realizó allá por el año 1969 con la red ARPANET, creada por el departamento de Defensa de Estados Unidos, que, aunque por aquel entonces no se hablaba de Internet, supuso el primer nodo de lo que es ahora. Aquella red descentralizada fue creciendo e interconectando más computadores y paralelamente iban comenzando a existir nuevas redes (ALOHA, Ethernet…).

Estas redes ya conectaban cosas: computadoras. Aunque por sí solas no podían transferir información, es decir, necesitan de una persona que haga pasar la información de un lado a otro. Y en la otra parte, es necesaria otra persona que analice esa información y mande una respuesta.

Diez años después, se implantó el protocolo TCP/IP y en 1990 Tim Berners-Lee implementó con éxito la primera comunicación entre un cliente HTTP y un servidor en internet. Un año más tarde se crearía la primera página web y a partir de ahí la evolución de la informática y las comunicaciones ha sufrido un avance exponencial que llega hasta nuestros días y realmente nadie sabe dónde estará el límite.

Pero volvemos al año 1990, donde Mark Weiser obtuvo el reconocimiento mundial gracias a su trabajo *The Computer for the Twenty-First Century* donde, por primera vez alguien hablaba sobre interconectar elementos que no fueran computadores, Mark Weiser (1990) defendía que los ordenadores personales serían reemplazados por “ordenadores invisibles” introducidos en objetos de uso cotidiano. En su trabajo decía "La computadora es un punto de conexión demasiado enredado, su manejo requiere mucha atención exclusiva, quitando la atención al usuario de la tarea que debe hacer".

Y precisamente esa es la idea de **IOT**: Hacer que podamos concentrar toda nuestra atención en las actividades de la vida cotidiana y laboral sin preocuparnos de suministrar información a los aparatos electrónicos que nos rodean, estando esta tarea en manos de *ellos* mismos.

Escenario 1:

Un grupo de escolares llegan al aula por la mañana y su tableta electrónica automáticamente se conecta con la tableta del profesor que previamente ha definido los contenidos de la lección de hoy y se actualizan en los aparatos de todos los alumnos. Los teléfonos móviles automáticamente se desconectan al entrar a clase. El profesor da las notas de los exámenes y se mandan a los alumnos y a sus padres en ese momento, que podrán firmar el examen como recibido y mandarlo de vuelta.

Al terminar la clase los contenidos se actualizan con información de cada alumno y se almacenan hasta la siguiente clase de esa asignatura.

En este ejemplo se pretende esbozar mediante una situación cotidiana en el ámbito estudiantil, cómo puede ayudarnos en procesos tan básicos en los que nunca antes se había pensado cambiar.

Aunque Mark Weiser dio las primeras pinceladas en el 90 de lo que a la larga se convertiría en IOT, no fue hasta el 1999, cuando se utilizó se utilizó por primera vez el término IOT. Kevin Ashton impartió una conferencia en Procter and Gamble (1999) donde dijo “Necesitamos un internet de las cosas, una forma estandarizada para equipos para entender el mundo real.”

En ese mismo año, Neil Gershelfeld (1999) utilizó ese mismo término en su libro Cuando las cosas empiezan a pensar donde escribió*: "En retrospectiva parece que el rápido crecimiento de la World Wide Web puede haber sido sólo la acusación de la desencadenada explosión real que ahora está provocando que las cosas comiencen a utilizar la red."*

Desde entonces el término IOT se ha ido extendiendo cada vez más, cobrando más importancia a medida que científicos e investigadores demostraban la importancia que llegaría a cobrar esta nueva tecnología en conferencias, revistas científicas etc.

Por tanto, ¿qué es internet de las cosas? La definición más clara y sencilla es: Un concepto que se refiere a la interconexión digital de objetos cotidianos con internet, tanto entre ellos mismos como entre personas y objetos.

2.2. IoT en la actualidad

Figura 2.1: Interconexión de dispositivos en Internet de las cosas.

La firma EMC, empresa desarrolladora de software y sistemas para la administración y almacenamiento de información espera que en 2020 habrá unos 30.000 millones de dispositivos electrónicos conectados a internet. Aunque esta fecha queda aún muy lejana, Gartner, otra importante consultora y empresa de investigación de las tecnologías de la información, asegura que en 2016 habrá más de 6.400 millones de dispositivos conectados a la red.

Esta cifra está cerca de la población mundial, y aunque actualmente no se le dé demasiada importancia, ya que IoT avanza desde la sombra y la tecnología es casi invisible, en mi opinión, tiene (y tendrá) un impacto global en todo el mundo debido a la velocidad a la que avanza.

Para hacernos una idea más clara de la situación actual de esta tecnología se van a presentar algunos datos más:

1. **Usuarios activos en internet.**

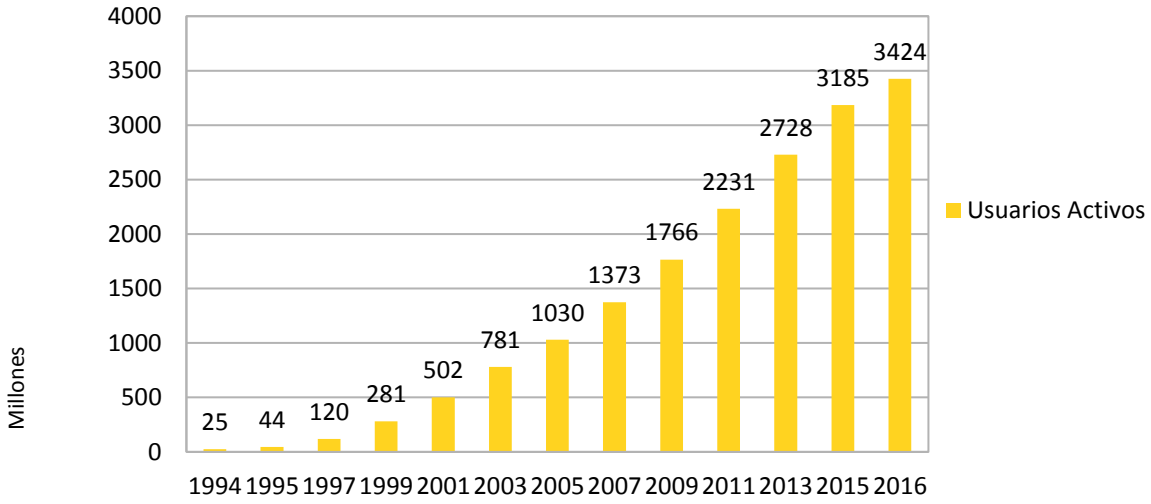

Gráfico 2.1: Usuarios activos en Internet

2. Usuarios usando sistemas de mensajería. En este ejemplo se han obtenido las estadísticas de Whatsapp.

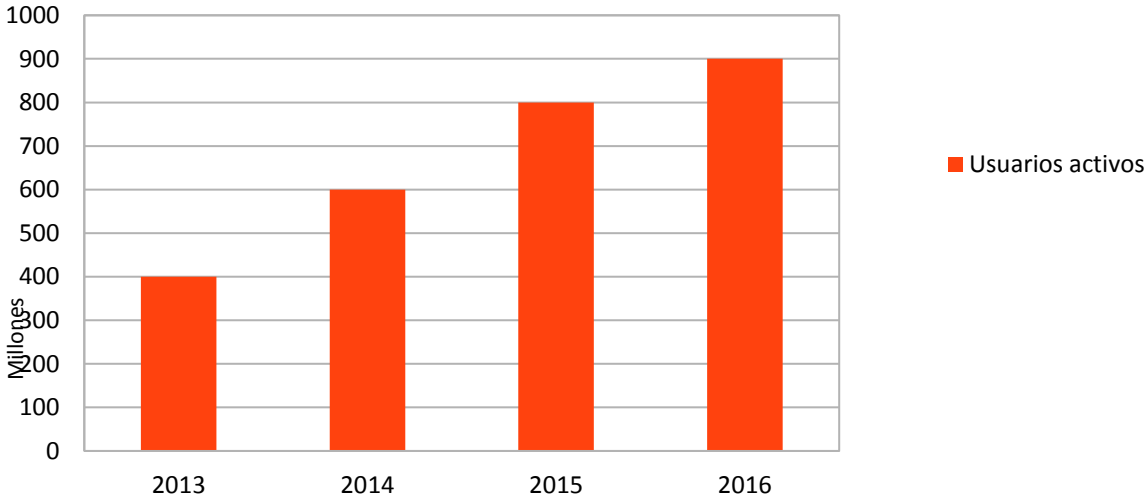

Gráfico 2.2 Usuarios activos en Whatsapp.

Por tanto, hablamos de que el total de dispositivos conectados a la red duplicará el de usuarios reales.

Steve Prentice (2014), vicepresidente de Gartner subraya: "***El número de dispositivos inteligentes conectados a internet seguirá creciendo de manera exponencial***, *otorgando a las cosas inteligentes la capacidad de sentir, interpretar, comunicar y negociar, y efectivamente tener una voz digital",*

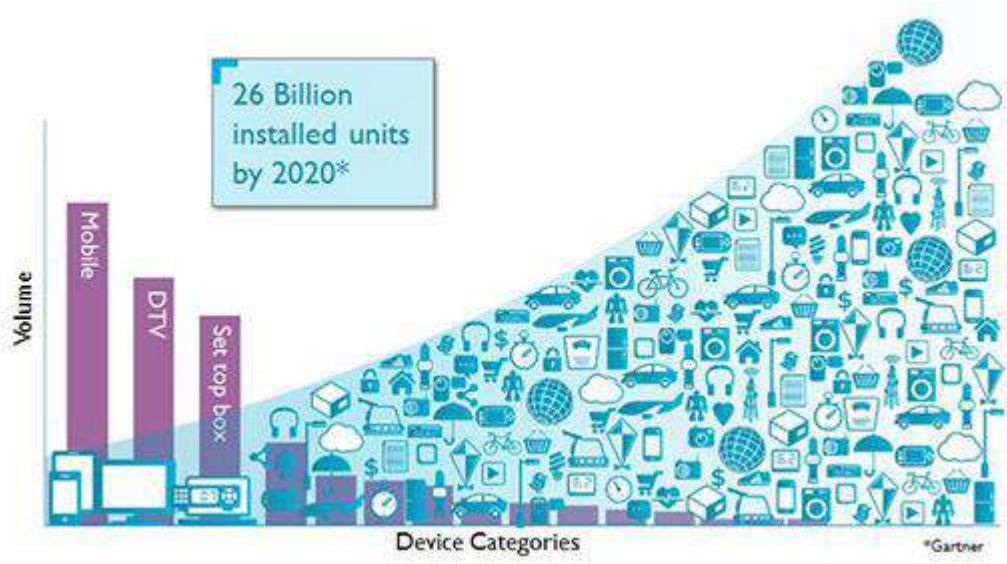

Figura 2.2: Unidades inteligentes instaladas en 2020.

Fuente: Gartner

Escenario 2:

Una persona sale de su casa para comprar el pan. Su móvil se conecta con un sensor medioambiental que le indica la temperatura actual y su armario le recomienda qué ropa sería la adecuada para ponerse ese día. Cuando llega a la panadería la puerta se abrirá desde el dispositivo móvil de la persona, y gracias a la compra que ha estado haciendo durante el año, la compra se hará automáticamente y cuando entre al establecimiento, ya estará lista la barra de pan que el cliente desea. Incluso estará pagada.

Al salir prefiere ir en Taxi a ver a un amigo y al acercarse a una parada, un taxi habrá recibido la llamada y le estará esperando.

Aquí se muestra otro ejemplo un poco más complejo pero que sigue haciendo referencia a un episodio de la vida cotidiana, incluyendo ejemplos como smartphones y sensores, que se conectan e intercambian información por si solos.

Steffen Sorrel, autor del estudio El Internet de las Cosas: Consumo, Industria y Servicios Públicos acerca del internet de las cosas en el consumo, industria y servicios indica:

*"El internet de las cosas aún se encuentra en una **etapa temprana de desarrollo.** Conocer qué tipo de información hay que recopilar y cómo integrarla en los dispositivos continúa siendo un **gran desafío** para la mayoría de las empresas".*

Y aunque parece contradictorio, IoT se encuentra en su primera fase a pesar de todos los datos expuestos, y es que es tan grande el escenario que abarca, que pienso que es complejo descubrir cuál será la mejor forma de hacer que todo se interconecte de la manera adecuada.

Lo que sí está claro es que, aunque actualmente no esté teniendo un gran impacto en la sociedad y sobre todo en la vida cotidiana de la gente, sí se está empezando a ver cambios en la industria, sanidad y el sector medioambiental, como se detallará a continuación.

Otra de las cosas que están claras, es que IoT está evolucionando más rápidamente de lo que estamos desarrollando nuestra protección hacia *él.*

Telefónica presentó un informe el 28 de enero de 2016, titulado "**Alcance, escala y riesgos sin precedentes: asegurar el Internet de las cosas**" indica y analiza que la ciberseguridad va a la zaga respecto al desarrollo de IoT, concluye que las innumerables ventajas del IoT en una sociedad interconectada tienen su lado negativo en la necesidad de un grado de preocupación y protección necesario para evitar sus posibles ataques derivados.

"Todo el mundo se centra en las oportunidades de innovación que ofrece el IoT, pero hasta este momento se ha hablado relativamente poco de su lado más siniestro", indica **John**

Moor, director de The Internet of Things Security Foundation, citado por Javier López Tazón (2016) *"Si no tenemos cuidado podemos meternos en problemas sin darnos cuenta. Y algunos de ellos, sin precedentes".*

El informe ha sido elaborado por las **divisiones de ciberseguridad e IoT de Telefónica**, en asociación con una serie de organizaciones que operan en el ámbito de la ciberseguridad, como el CICTE (Comité Interamericano contra el Terrorismo de la OEA), el NMI (National Microelectronics Institute), el Grupo de Ingeniería Telemática de la Universidad de Cantabria, Future Technologies Kapersky Lab, SIGFOX e Intel Corporation Iberia. Hace un hincapié en la necesidad de una normativa y regulación sólidas y robustas, junto con una mayor colaboración y diálogo entre todas las partes implicadas en el desarrollo para dar una mayor seguridad y confianza al usuario, creando una defensa robusta y consistente contra todas las amenazas.

"*No se trata solo de la privacidad de los datos o de la seguridad de nuestras identidades digitales*", explica **Chema Alonso, CEO de ElevenPaths**, citado por Javier López Tazón (2016) la filial de ciberseguridad de Telefónica. "*En los próximos años viviremos rodeados de dispositivos conectados a Internet que digitalizarán cada paso que demos, convertirán nuestra actividad diaria en información, distribuirán cualquier interacción por la red e interactuarán con nosotros en función de esta información. Nunca antes nuestro día a día había estado tan cerca del mundo digital. La difusa línea entre el mundo digital y el mundo real es precisamente el espacio donde se materializan los cambios introducidos por el IoT. Comprendamos el problema antes de que sea demasiado tarde y garanticemos que estamos en condiciones de ofrecer un plan de protección completo, aprovechando todos los conocimientos que se han generado en otros ámbitos*".

"*IoT está dejando rápidamente obsoletas las leyes necesarias para regular y normalizar las medidas de seguridad*", señala **Belisario Contreras, Gerente del Programa para el Comité Interamericano contra el Terrorismo en la Organización de los Estados Americanos (OEA)**, citado por Hilda Gomez (2016) "*Esta velocidad de desarrollo también está afectando*

a las cuestiones de compatibilidad, ya que las medidas de seguridad para algunos dispositivos y plataformas pueden no ser compatibles con otros al aparecer versiones más recientes".

"*El futuro de la IoT es incierto, pero solo por medio de la colaboración y de la experiencia acumulada podremos conseguir partir de una base segura*", concluye **Alonso**.

La contrapartida de todas las ventajas que se comienzan a apreciar en torno al Internet de las Cosas es la seguridad y la protección de los datos. Según John Moor, director de The Internet of Things Security Foundation.

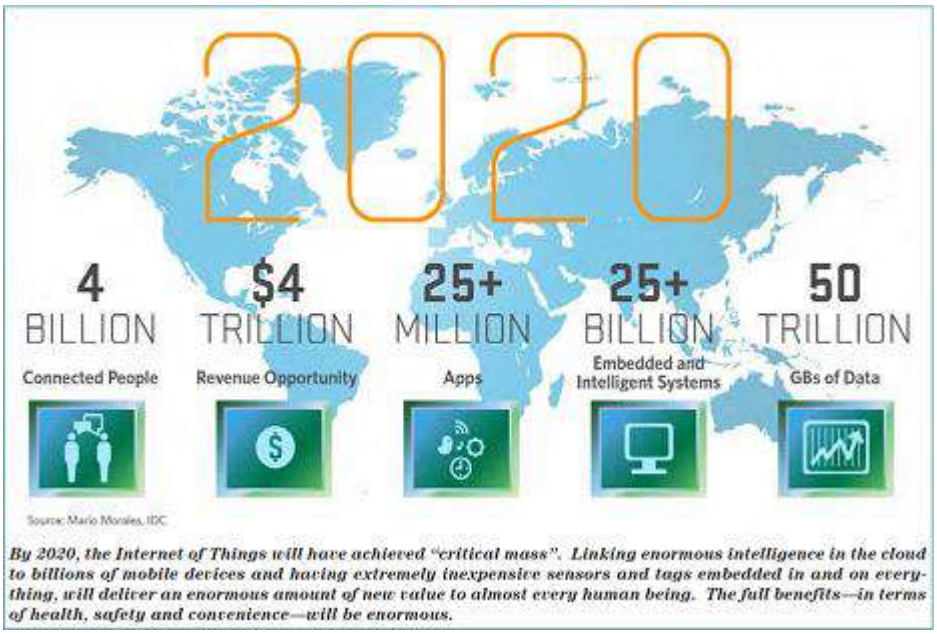

Figura 2.3: Elementos conectados estimados en 2020.

Fuente: Mario Morales

Es turno en este capítulo de centrarnos en profundidad en la situación actual a nivel legislativo y derechos legales tanto a nivel nacional como internacional en torno a IoT.

En los siguientes apartados de este proyecto se intentarán resolver problemas derivados a vacíos legales que existen actualmente con este tipo de tecnologías y se aportarán datos para conocer el estado actual de la legislación y si verdaderamente los usuarios estamos protegidos ante la llegada de IoT.

La cantidad de preguntas que se obtienen al pensar en las posibilidades que ofrece la implantación de IoT es abrumadora. ¿Debe poder denunciarse a una persona si su coche automático va demasiado rápido?, ¿Puede la policía detenerte si los sensores indican que, según tu estado de ánimo o nivel económico, es posible que vaya a cometer un delito? ¿Pueden los fabricantes introducir sensores en sus productos para ofrecerte un mejor servicio posventa? ¿Pueden fabricantes compartir tus datos personales para ofrecerte un mejor servicio? ¿Si tu coche conduce por ti, y se produce un accidente, de quién sería la culpa? ¿Qué información es segura de alojar en un wearable? ¿De quién son los datos almacenados en una pulsera inteligente que mide tu actividad física? ¿El fabricante puede vender estos datos? ¿Cuándo subimos una foto a Facebook con nuestra localización, ¿Facebook puede vender estos datos?

Para resolver todas estas preguntas es necesario antes hacer un recorrido por las leyes de protección de datos.

2.2.1. Aspectos legales

La mejor manera de empezar a hablar de los aspectos legales acerca de IoT es analizando el nuevo Reglamento de Protección de Datos europeo que ha entrado en vigor el 25 de mayo de 2016, y que obtenemos toda la información desde la web de la Agencia Española de Protección de Datos.

Algunos puntos de este nuevo reglamento que son interesantes para el presente proyecto y que afectan a la seguridad y privacidad de IoT son:

1. En este nuevo Reglamento de Protección de Datos, aparte de recoger los derechos de acceso, rectificación, cancelación y oposición, se regulan dos nuevos derechos, como son el llamado "Derecho al olvido". El derecho al olvido es el derecho del ciudadano de exigir que los datos personales sean suprimidos cuando, entre otros casos, ya no sean útiles para la finalidad en los que fueron obtenidos y recogidos. El segundo derecho añadido es el de la portabilidad de los datos.
2. La necesidad del consentimiento claro y afirmativo de la persona concernida al tratamiento de sus datos personales.
3. El derecho a ser informado si sus datos personales han sido pirateados.
4. Las aplicaciones, redes sociales y demás servicios tendrán que presentar determinados niveles por diseño o por defecto para proteger los datos personales de los usuarios.
5. Otro aspecto positivo que se ha mejorado en este nuevo reglamento es la obligación para las empresas designar para ciertos casos un delegado de protección de datos "DPO. Data Protection Officer", para garantizar el cumplimiento de la normativa. También las cuantías de las sanciones se elevan considerablemente, hasta el punto de alcanzar hasta 20.000.000 de euros, o el 4% del volumen de negocio total anual global del ejercicio financiero anterior.
6. La creación de una Unidad de Evaluación de las últimas novedades tecnológicas, prevista para la gestión de IoT.
7. Medidas de seguridad y un mantenimiento de un registro de tratamientos.
8. Realización de evaluaciones de impacto sobre la protección de datos.

La Agencia Española de Protección (2015, nota de prensa) de datos considera que "*es necesario realizar una* ***reflexión más profunda sobre los límites de estos sistemas*** *y la necesidad de conciliar los beneficios de la innovación y la economía digital con el respeto a los derechos fundamentales de las personas*".

La AEPD cree que es absolutamente necesario que entre los desarrolladores, ingenieros y expertos en privacidad y seguridad exista un diálogo acerca del mejor tratamiento de los datos "*teniendo siempre presente que el derecho a decidir sobre la propia información personal es un derecho fundamental y, como tal, es irrenunciable. En este terreno,* ***no todo lo tecnológicamente posible resulta aceptable***", en palabras del director de la agencia, José Luis Rodríguez Álvarez.

2.2.2. Vacíos legales

Para comenzar a hablar de este apartado sobre los diferentes vacíos legales en los que se adentra IoT, es necesario ponernos en situación centrándonos en esta tecnología, y para ello vamos a exponer un caso real sobre un incidente registrado en 2014.

En este año, un francés llamado Damien Vigoroux que vivía en Barcelona, desapareció en una zona montañosa cercana a Montserrat. Se fue de excursión él solo y por la tarde envió algunos mensajes a sus amigos a través de la aplicación de mensajería instantánea Whatsapp y algunas fotografías de cómo iba su excursión. Al día siguiente sin noticias de él, sus familiares denunciaron a la policía su desaparición.

En este momento el móvil de Damien ya estaba apagado, con lo que era imposible hablar con él y pedirle que enviase su localización a través del GPS de su móvil. Como las tareas de búsqueda resultaron infructuosas, los amigos y familiares de Damien pidieron a Google los datos de geolocalización de su terminal Android, ya que podría ser de gran ayuda para este caso el poder obtener la última información de localización registrada por su teléfono.

El problema residía en que los satélites que usa Google no son de su propiedad, al igual que ocurre con Apple o Microsoft, y el proceso de solicitar esa información podía tardar unos 30 días, haciendo inútiles los datos ya que el plazo es demasiado largo. Al final de este tiempo, que al final fueron 90 días, resultó que no se habían podido obtener ninguna información localizable enviada por su el teléfono de Damien.

La política de empresa de google hizo que el proceso fuera largo y repleto de trámites, haciendo imposible que la información que se pudiera haber obtenido hubiera servido para algo.

A parte de la geolocalización, existe otra manera de obtener la posición de un teléfono móvil, que es mediante triangulación telefónica. Consiste en medir la potencia procedente de las antenas hacia el terminal, y comparando las intensidades de las antenas se puede obtener una posición aproximada donde se encuentra el móvil.

Para obtener la localización por triangulación hay que iniciar una vía judicial y pedir permiso a un juez. Cuando se autorice, el proveedor de telefonía envía los datos. La resolución judicial es una vía más rápida, tardando entre horas y algunos días.

Pablo Castro (2015, citado por Pablo G. Bejarano), uno de los bomberos a cargo del caso de Damien informa: "*La probabilidad de que alguien con Android, con la geolocalización activada se pierda en la montaña es bastante alta*". Pese a esta información y alta probabilidad, no hay cauces legales para obtenerla rápidamente. En España, de momento solo hay legislaciones sectoriales. La Ley 25/2007, de conservación de datos, derivada de la directiva europea de retención de datos (que fue invalidada por el Tribunal de Justicia de la Unión Europea), obliga a las operadoras a almacenar una serie de información de cada usuario. Esta normativa no implica a Google, Apple o Microsoft, que no son operadoras.

"La ley de enjuiciamiento criminal no tiene ninguna previsión en este sentido, solo tiene un apartado dedicado a las escuchas telefónicas, que está desde 1988. En el ámbito penal está completamente huérfano de regulación. En el civil ni se contempla. La situación es de vacío normativo. No hay nada legal, por escrito, que pueda servir a un juez para ordenar este tipo de cosas. Ya ha habido una sentencia del Tribunal Supremo en la que advierte de la necesidad de que el legislador regule esto", indican fuentes jurídicas (2015, citadas por Pablo G. Bejarano),

Hoy en día, para casos de emergencia o intentos de suicidio, por poner algunos ejemplos, no hay ninguna norma que avale pedir los datos GPS a un juez. No hay actualmente ningún procedimiento establecido para poder llevar a cabo la cesión de este tipo de datos.

Esta información procede de **sistemas de satélites cuyos servicios Google o Apple arriendan**, pero cuya propiedad es del gobierno de Estados Unidos u otras instituciones de carácter internacional, pues se trata de tecnología de origen militar. Existen problemas de jurisdicción y de confidencialidad a la hora de pedir estos datos.

Por su parte, Castro (2015, citado por Pablo G. Bejarano), critica que **los protocolos no son abiertos**. "*No es ya que no se renueven, sino que no son flexibles a los avances de la tecnología*", recalca. Esto hace que los servicios de emergencia, en este caso, y en un futuro, otro tipo de servicios y situaciones no puedan beneficiarse de herramientas que proporciona la tecnología. No se contemplan aun estas acciones en un marco legal, y es necesario como indicamos en este apartado que desde todas las partes de haga un esfuerzo para que cambie.

Este ejemplo nos ha servido para explicar un problema actual que existe relacionada con el internet de las cosas, y que en un futuro puedan existir aún más debido a los vacíos legales y falta de leyes para tramitar estos problemas.

Pero sigamos con más ejemplos que se están produciendo actualmente a medida que avanza la tecnología. Esta vez nos centramos en un accidente ocurrido el 7 de mayo de este mismo año. Un coche Tesla, creado por la empresa Tesla, fundada por Elon Munsk con sede en la bahía de San Francisco, tuvo un accidente cuando estaba en piloto automático. El coche se metió debajo del remolque de un camión produciendo la muerte inmediata del conductor que iba en el vehículo.

Joshua Brown, había delegado la responsabilidad de la conducción en su vehículo, que a través de inteligencia artificial va aprendiendo de la conducción manual del conductor.

Según los informes oficiales, el coche de Brown iba a mucha velocidad y no frenó cuando debería de haber frenado.

A pesar de la cantidad de sensores que lleva el vehículo, no detectó el camión, ya que era blanco y la luz que había ese día pudo haber contribuido a la no detección del camión.

Al ser el primer accidente de este tipo, existe un vacío legal y no está claro de quién es la responsabilidad del accidente. Desde la compañía explican que en el momento que el piloto automático es puesto en marcha, es una condición imprescindible mantener las manos en el volante, y si el coche no detecta esto, se detiene inmediatamente. Así pues, ¿es culpa del conductor o de la empresa que ha fabricado el coche y el accidente es producido por la "inteligencia artificial" Tesla?

Existe un concepto en filosofía que se denomina "Moral utilitaria". Es una doctrina que se basa en que el resultado final es lo que importa. Podemos aplicar este concepto al ejemplo de los automóviles autónomos.

Si estos automóviles se programan según esta moral, en caso de accidente siempre se buscaría producir el menor número de muertos posibles, pudiendo darse el caso de que el coche decidiera matar a sus ocupantes si fuera menor que el número de muertos resultantes que produciría si no lo hiciera.

Este tipo de comportamiento del vehículo produce una serie de dilemas morales y legales que son difíciles de abordar.

Un estudio de la revista Science (Jean-François Bonnefon, Azim Shariff, Iyad Rahwan ,2016), realizó una encuesta en la que planteaba si un vehículo autónomo debería comportarse según

esta situación. La gran mayoría de personas creía conveniente que estos vehículos deberían de comportarse así, incluso si sus propios hijos fueran a bordo del vehículo.

La mayoría también respondieron que no se comprarían un coche que funcionase de esta manera.

Como seguimos viendo, no se está consiguiendo que a medida que avanza Internet de las Cosas, se estén tomando las correspondientes medidas en el ámbito legal para proteger a las personas adecuadamente.

Vamos a seguir viendo más peligros a los que se enfrentan los usuarios en la actualidad con el uso de las nuevas tecnologías. En este caso vamos a elegir la red social con mayor número de usuarios de Internet.

Cuando se entra por primera vez a esta red social y acepta todas las condiciones de uso y política de privacidad para poder registrarse como usuario en la red no piensa que está cediendo absolutamente todos los derechos que afectan a su imagen, mediante una renuncia clara a ellos.

Si se lee escrupulosamente todas las cláusulas que firma al registrarse podemos leer el punto número 2.5 del contrato de licencia:

"*Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello (del mismo modo que tú no tienes obligación de ofrecerlos)".*

Lo que indica claramente quien es el dueño de todo el contenido alojado en la red social.

Es por eso que el usuario de esta red social debe de ser muy consciente de todo lo que publique, ya que Facebook puede hacer todo lo que quiera con las imágenes: "*Copiarlos, publicarlos, almacenarlos, retenerlos, publicitarlos, transmitirlos, escanearlos, cambiarles el formato, modificarlos, editarlos, traducirlos o adaptarlos*"

El problema es que cualquier usuario que quiera pertenecer a la red social debe de aceptar todas las cláusulas del contrato de privacidad. Así que la recomendación es que, si finalmente el usuario ingresa en la web, debe de ser consciente de lo establecido en este contrato.

Un ejemplo de este caso de quien es el verdadero poseedor de lo que se sube a una red social, aunque en otra red como es Instagram, fue el que ocurrió en mayo del año 2015, cuando un fotógrafo y pintor llamado Richard Prince presentó en Nueva York en la feria de arte Frieze una exposición llamada "Nuevos Retratos". En esta feria, presentó capturas de pantalla de algunas fotografías que usuarios de esta red habían publicado. Prince presentó estas fotos sin el consentimiento real de los usuarios y vendió casi todas las instantáneas a un precio de 90.000 cada una. Esto creó un gran revuelo entre los usuarios al darse a conocer la noticia y fuentes de

la red social comentaron al diario estadounidense The Washintong Post: "*Los usuarios de Instagram son dueños de sus fotografías. Punto. Si alguien siente que sus derechos de autor han sido violados, pueden escribirnos y nosotros tomaremos las medidas oportunas*",

Realmente esto no es un vacío legal ya que claramente en las condiciones de privacidad se indica todo lo relativo a los derechos de las imágenes, y esto es más bien un problema relacionado con la cultura del usuario en internet.

Seguimos hablando de riesgos para la privacidad de los usuarios utilizando las nuevas tecnologías de Internet de las cosas.

En este caso nos centramos en una tecnología weareable como son las "SmartBand" o pulseras inteligentes. Estas pulseras registran todo tipo de información sobre los hábitos y estilo de vida de la persona que lleva la pulsera como distancias recorridas, calorías, niveles de azúcar y tensión. Esta tecnología presenta una de los mayores peligros para la privacidad. Con toda esta información recogida de estos dispositivos y almacenados por la empresa que los fabrican, pueden analizarla y conocer multitud de datos importantes de los usuarios, como la hora a la que se levantan, a qué hora se sale del trabajo, etc… pudiendo utilizarlo para vendérsela a otras empresas.

Según la consultora tecnológica IDC, sólo hasta mediados de este año las principales compañías que desarrollan estos dispositivos lograron poner en el mercado mundial 18,1 millones de unidades, lo que supuso un incremento interanual del 223%.

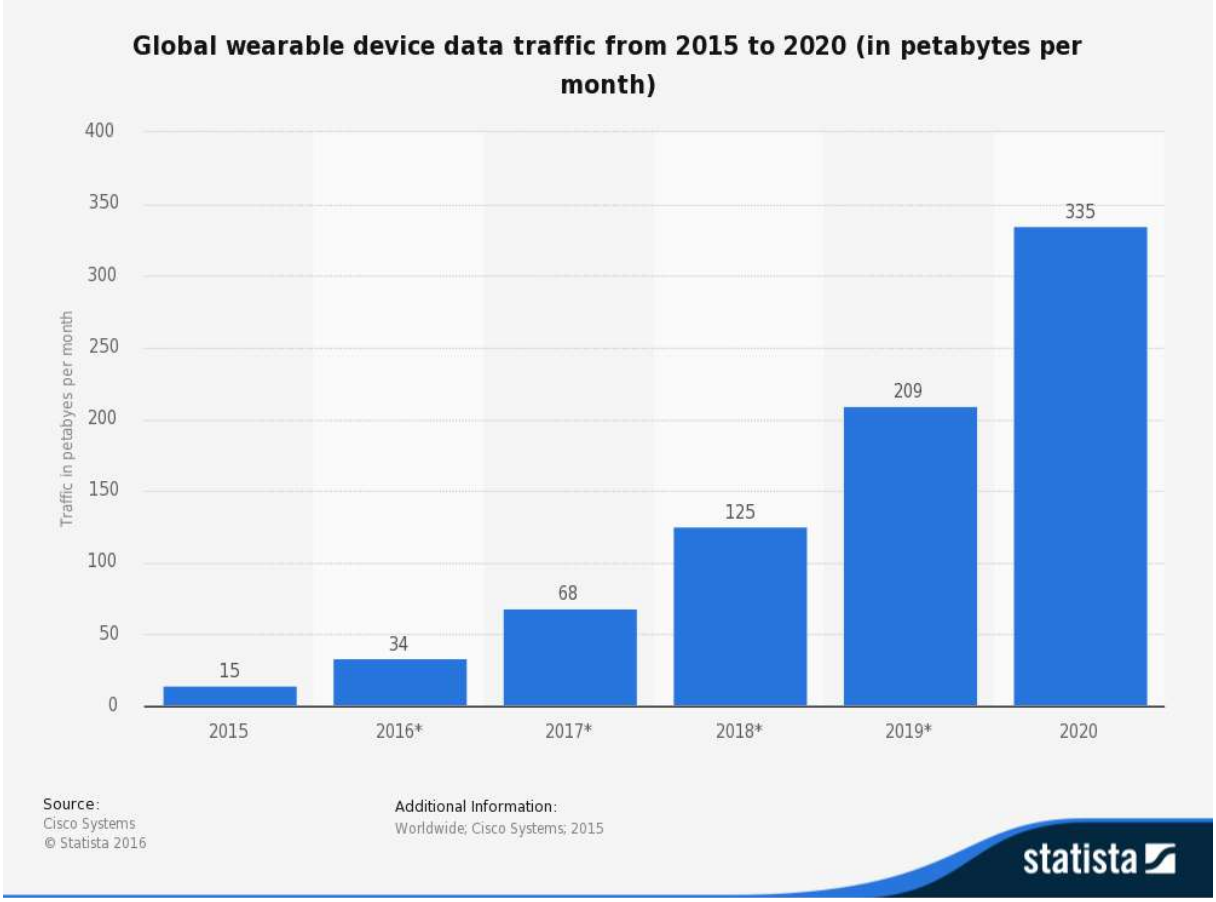

Gráfico 2.3. Tráfico de dispositivos weareable entre 2015 y 2020

SIST. OPERATIVOS DE PULSERAS INTELIGENTES	CUOTA MERCADO 2015 ▲	CUOTA MERCADO 2019
WatchOS (Apple)	58,30%	47,40%
Android/Android Wear	17,40%	38,40%
Pebble OS	8,70%	3,1%
RTOS	8,3%	9%
Tizen	6,7%	2,2%
Otros	0,60%	0%

— Previsiones sobre pulseras inteligentes

Las ventas de estos dispositivos alcanzarán las 76,1 millones de unidades en 2015, un 163,6% más frente a los 28,9 millones de unidades vendidas en 2014. En 2019, las ventas de todo el mundo llegarán a 173,4 millones de unidades.

Fuente: IDC Forecasts Worldwide Wearable Shipments EL ESPAÑOL

Gráfico 2.4: Previsiones sobre pulseras inteligentes

Todos los datos que están relacionado con la salud en España están considerados como de especial protección. En el artículo 7.3 de la Ley Orgánica de Protección de Datos establece que los datos de salud solo se pueden utilizar por dos causas: Consentimiento expreso del titular o habilitación legal por razones de interés general.
El jefe de área de la Agencia Española de Protección de datos, Emiliano Aced (2015, citado por Pablo Romero), considera que la única fuente de legitimación válida es el consentimiento: "*En general, todos los tratamientos de consumo están basados en que la persona acepte los términos concretos. Es importante destacar que quien acepta los términos es quien se pone el sensor*", indica Aced.
"*Nadie te obliga a comprarte la pulsera, a permitir que recabe determinados datos y a que se envíen a un servicio remoto*", afirma Aced, quien añade: "*Eres tú quien te compras el dispositivo, te lo pones y empiezas a transmitir esos* datos". "Normalmente todo el mundo te pide que aceptes sus términos y condiciones", apunta, "*otra cosa es que te los leas o no; aquí entraríamos ya en el terreno de si la información proporcionada es suficiente o no*".

Y es que la trasparencia en la gestión de datos es un asunto clave, tal y como recoge el dictamen de las autoridades de protección de datos europeas sobre IoT publicado el año pasado. Todos los datos deben de recogerse como hemos venido hablando en este trabajo, de forma clara, leal y legal y el usuario debería ser consciente de ello.

"*Si yo permito que se traten unos datos de salud tengo que saber en qué condiciones estoy aceptando ese tratamiento, para qué se van a utilizar, y luego ya decidiré si quiero o no compartirlos*", indica Aced. "*También tengo que saber si el gestor de todo esto va a hacer algo más con esos datos, como por ejemplo establecer perfiles para venderlos a compañías de seguros para estudios de tarificación y análisis de riesgos -evidentemente datos anónimos-, algo que ya está pasando. O ceder esos datos para investigaciones científicas con nombres y apellidos*". "*Todo eso lo tengo que saber claramente, de manera entendible, de modo que yo pueda aceptar esas condiciones de forma informada*", concluye.

Y volviendo a hacernos la misma pregunta que estamos intentando resolver durante todo este proyecto, ¿Estamos protegidos?

El experto y responsable de la empresa ePrivacidad, Samuel Parra (2015, citado por Pablo Romero) afirma rotundamente: "*Mi respuesta a si estamos protegidos es un absoluto no. Los usuarios utilizan estos dispositivos sin cuestionarse siquiera el uso que la empresa propietaria o terceros que tengan acceso a la información que genera el dispositivo van a hacer de ella* ".

En el momento en el que el dispositivo, en este caso la pulsera inteligente, toca la piel al ponernos la pulsera ya comienza a registrar datos, y se aplica la normativa española. Sergio Carrasco, ingeniero y abogado especializado en el tema de las nuevas tecnologías indica: No me preocupa el dispositivo concreto, lo que me importa es la naturaleza del dato y las medidas que se deben de aplicar al tratarlo. Por lo tanto, y dado que están relacionados con la salud, existen multitud de obligaciones que, casi seguro, se incumplen sistemáticamente".

Samuel Parra indica que si estamos en territorio español se aplicarían las leyes españolas "la empresa que recibe los datos del *wearable* utiliza medios (la pulsera, la camiseta, etc.) ubicados en territorio español", tal y como exige el artículo 2.1.c. de la LOPD. "Esto significa que, poniéndonos en el escenario en el que la pulsera la compramos a una tienda en China y la empresa que ofrece el servicio (la que recibe los datos) está en Estados Unidos, se seguirá aplicando nuestra normativa de protección de datos. En la práctica me temo que las empresas, si están fuera de la UE, no atenderán las peticiones de acceso o cancelación de datos."

Emilio Aced indica: "*Sería importante que, una vez aceptadas las condiciones del servicio, pudiéramos saber que no se hace nada que se salga fuera de ese parámetro que yo he aceptado*". El problema es que no hay manera de comprobar que esto no sucede.

Lamentablemente, actualmente en el mundo no podemos hablar de una ciberseguridad 100% fiable a día de hoy, ya que aún hay determinados vacíos legales que no son cubiertos a la misma velocidad con la que la tecnología avanza, ofreciendo novedosas aplicaciones antes de aplicar un marco legal claro.

Tenemos que tener en cuenta que el Internet de las Cosas forma parte de un grupo mucho más amplio que es el mundo tecnológico, que por ahora no está dividido por países ni continentes, un problema añadido ya que entran en juego las diferentes normativas de cada país –la protección de datos está regulada actualmente de manera diferente en Estados Unidos y en Europa, por ejemplo, y la normativa puede llegar a variar en función de la industria de la que hablemos-. Esto implica que la protección y gestión de datos varía según en qué país se aplique la regulación.

2.3. ¿Hacia dónde se dirige?

2.3.1. Impacto de IoT

Así pues, ¿cuál es el futuro de IoT?

Lo primero que se debe observar e imaginar es el gran impacto que se producirá en todos los sectores de actividad. Una red tan grande y con tantos objetos "inteligentes" conectados entre sí necesita unas condiciones necesarias para que se pueda implantar correctamente.

Unos sectores profesionales podrían desaparecer, otros en cambio, comenzarán gracias a la nueva era de la tecnología. En este escenario, quedarán los que sepan adaptarse más rápido a estos cambios, así como ocurrió con las tecnologías de la información.

Según la firma de analistas Gartner, en todos los sectores tendrá un gran impacto toda la red de dispositivos conectados, desde empresas, autoridades locales, hospitales y consumidores, llegando a unos gastos totales de 260.000 millones en 2020.

Estos datos suenan prometedores en cuanto a la economía, pero, ¿En qué sector se estima que será el que tenga más objetos conectados?

El estudio realizado por Gartner que se presentó en la "Gartner Symposium/ITxpo" del 9 de noviembre de 2014 en Barcelona, estima que las aplicaciones para los consumidores, principalmente en el sector de la automoción, serán las que más difusión en los próximos años. Calculan que aproximadamente 13.000 millones de dispositivos conectados pertenecerán al sector de consumo. Como indican en el estudio: "*El número de dispositivos inteligentes conectados seguirá creciendo de manera exponencial, ofreciendo a los objetos inteligentes la capacidad de sentir, interpretar, comunicar y negociar, y efectivamente tener una 'voz' digital*", según Steve Prentice, vicepresidente de la consultora. "*Los CEO deben buscar oportunidades para crear nuevos servicios, escenarios de uso y modelos de negocio basados en este crecimiento*".

Seguido del sector consumo, afectará también en gran medida al sector industrial: los servicios públicos, la fabricación y el transporte serán los mercados clave de esta tecnología.
Las empresas estarán obligadas a buscar un equilibrio entre los datos recogidos y almacenados en la red por los dispositivos y sensores conectados, y el análisis de toda esa cantidad de información con el riesgo de su pérdida o mal uso.

Todos los retos que plantea el IoT para la seguridad de toda esa información pondrá a las empresas en la obligación de invertir en seguridad tecnológica a unos niveles que nunca antes se habían pensado.

Terminando con el análisis de beneficios, IDC (2015) (International Data Corporation, especialistas en información tecnológica) calcula que el mercado mundial de IoT crecerá hasta llegar a 3.040 millones de dólares hasta el año 2020.

Category	**2013**	**2014**	**2015**	**2020**
Automotive	96	189	372	3.511
Consumer	1.842	2.440	2.874	13.172
Generic Business	395	479	623	5.158
Vertical Business	698	836	1.009	3.164
Grand Total	**3.032**	**3.750**	**4.880**	**25.006**

Tabla 2.1: Unidades de internet de las cosas por categoría (Millones)

Fuente: Gartner (November 2014)

Como hemos comentado al inicio de este proyecto, desde que apareció Internet en la vida de todas las personas se ha convertido en un factor imprescindible en la economía mundial. En todos los sectores de la sociedad es algo fundamental y se utiliza día a día por todo el mundo. Cuando apareció la tecnología inalámbrica, hizo que aumentasen las posibilidades de la red, pudiendo ser alcanzable desde cualquier parte del mundo. De esta forma las nuevas tecnologías que aparecen y derivan de esta tecnología tienen un enfoque innovador y están basados en la ubicuidad como hicimos mención en anteriores capítulos.

Internet de las cosas, sin duda tiene un potencial enorme y puede marcar un impacto muy significativo en la sociedad, como hizo Internet en su día.

Vamos a analizar el impacto a través de 3 puntos de vista: Impacto en las personas, modelos de negocio que plantea, y el impacto a la hora de consumir recursos.

2.3.1.1. Impacto de IoT en las personas

Interconexión de personas con personas, de personas con cosas y de cosas con otras cosas. En la misma definición de la tecnología ya se puede observar el impacto que tiene y tendrá en la sociedad IoT.

Todo estará interconectado con nosotros, basándose como referencia nuestro teléfono móvil que será la central con la que nos conectaremos al resto del mundo. Y es que todas las aplicaciones que se están desarrollando actualmente ya dan por hecho que el usuario tiene una conexión a internet y se podrá conectar a una red sin problema. Los desarrolladores de aplicaciones y hardware, solo tienen que reinventar lo que ya existe, dotándolo de conexión. Veremos más adelante todos los peligros que esto conlleva, porque existen muchos riesgos en todo el proceso de desarrollo-comercialización-usuario.

La conexión en todo momento en una red, sin importar dónde ni cuándo, permaneciendo intercambiando datos con todos los destinos muestra de por sí el peligro que puede ocasionar.

De la resolución de esos problemas dependerá que el impacto hacia las personas sea bueno y útil, o sea un verdadero problema y una violación de todos los derechos de la sociedad.

2.3.1.2. Modelos de negocio que plantea

Hablamos ahora del impacto de IoT en los negocios.

El hecho de que todo esté interconectado y las personas con ello, hace que las empresas sean capaces de adaptarse rápidamente a la nueva tecnología, sin que ello conlleve un cambio en su función principal a la que se dedique, ya que IoT cambiará por seguro la forma de trabajar y de prestar servicios a la sociedad.

La arquitectura orientada a servicios, o SOA, en el argot de una empresa, es la arquitectura que se encarga de aislar las funciones principales del negocio independientes que no cambian de los que sí.

Con la era del 2.0 y las redes sociales, todas las empresas tuvieron que adaptarse a esta nueva forma de prestar servicios y descubrir nuevas líneas de negocio, creando nuevos puestos de trabajo orientados a nuevos expertos en la nueva tecnología.

De igual forma va a ocurrir con IoT, se abrirán nuevas vías de negocio orientadas a la interconexión y aparecerán nuevas áreas de conocimiento y de trabajo.

2.3.1.2. Impacto en la consumición de recursos

La preocupación que existe hoy en día por el estado de salud de la tierra, las energías renovables, y el consumo de recursos a nivel en el que lo estamos haciendo, ayudado por el cambio climático y el aumento masivo de la población, ha hecho que los avances tecnológicos se centren en ayudar a frenar el proceso lo máximo posible.

La tecnología de Internet de las Cosas parece estar diseñada especialmente para esta tarea y es uno de los campos más prometedores. El uso de sensores puede controlar las diferentes variables necesarias para el mantenimiento de estos recursos.

En uno de los siguientes apartados comentaremos en más profundidad las diferentes aplicaciones derivadas del IoT en el ámbito de las energías renovables.

Escenario 3:

Una fuente en una plaza de una ciudad importante se atasca. La fuente tendrá un sensor que informará a los técnicos del ayuntamiento qué circuitos se han estropeado y cuál es la manera más rápida de solucionarlo, así como las herramientas que deberán llevar para su reparación.

Si no se hiciera de esta forma, los técnicos tendrían que haber parado el funcionamiento total de la fuente hasta que pudieran revisar todos los circuitos y ver cuál es el que se ha estropeado y una vez hecho esto, pedir los repuestos y esperar a que llegasen. La diferencia de eficacia y eficiencia que se aprecia en este escenario es considerable.

En este escenario se pasa a una situación cotidiana a una situación en el ámbito empresarial en la que se pone de manifiesto la gran importancia y peso que cobrará en la industria la introducción de los dispositivos IoT.

Según el informe Connected Life: The next five years in Asia (2013) de GSMA, organización de operadores móviles que se dedica al apoyo de la normalización, implementación y promoción de telefonía movil GSM, que ha estudiado el impacto de IoT, prevé que Asia será la región más interconectada y la que más beneficios obtendrá de una economía más productiva; China conseguirá llegar a 22.000 millones de dólares de ganancias al reducir la congestión del tráfico; India podrá llevar la electricidad a 10 millones de hogares en 2017 y evitar que el 24% de la electricidad que cada año genera se pierda; Japón ahorrará más de 10.000 millones de dólares en coses sanitarios y Corea del Sur reducirá el coste educativo por estudiante hasta 12.000 dólares.

2.3.2. Factores que decidirán el futuro de IoT

La población actual del mundo se encuentra en casi siete millones y medio de personas. Todas ellas con necesidades de comunicación de cualquier índole. Teniendo en cuenta esta estadística resulta muy atractivo el hecho de que las máquinas sean capaces de conectarse entre sí y con la población mundial. Estas cifras crecen día a día de manera exponencial.

imaginemos de nuevo por un segundo un mundo perfecto donde IoT se ha integrado perfectamente. Un mundo donde cualquier incidencia es resuelta en cuestión de segundos. Supongamos que ocurre un accidente de tráfico entre dos coches. Los sensores que tienen estos coches detectarán el accidente que hará que automáticamente se active el servicio médico. Por otra parte, el sistema de los semáforos y señalización recibirá un aviso y regulará el tráfico conforme al accidente para evitar posibles atascos. Finalmente, el accidente es avisado a la compañía de seguros para gestionar el accidente.

Es fácil ver que en ese mundo perfecto interconectado todo será muy eficiente, rápido y sobretodo seguro.

En este capítulo va a hablar sobre los factores que van a hacer que IoT pueda adaptarse al mundo, analizando los que pueden impulsarlo como los que pueden ralentizarlo.

2. 3. 2. 1. Obstáculos de IoT

Los problemas a los que se va a enfrentar IoT como dijimos en los primeros capítulos no van a ser sino similares a los que se enfrentan otros desarrollos tecnológicos que pueden afectar a la vida de las personas. Y profundizando en los que tienen mayor relación con este TFG, son: asegurar la privacidad y seguridad de los usuarios y las personas, y conseguir que se creen estándares aceptados globalmente. Otros de los obstáculos pueden ser las limitaciones actuales de infraestructuras, la gran necesidad de inversión en los actuales equipos, y las barreras de entrada psicológicas en las personas.

Hay que ser conscientes de que todavía nos cuesta dejar el mando a aparatos y procesos automáticos, ya sea por inseguridad que nos produce o porque somos conscientes de una máquina no va a poder realizar mejor el trabajo.

Para que una máquina pueda considerarse inteligente, debe de pasar el llamado “test de Turing”. Consiste en una prueba en la que la inteligencia artificial debe de convencer a un jurado de que están hablando con una persona real que está en otra habitación. Hasta el año 2014 ninguna máquina había superado esta prueba. Se trata de chatbot, un robot programado para mantener una conversación online pudo convencer al 33% de los jueces de que estaban ha-blando con un niño de 13 años.

Es por eso que nos es tan difícil confiar nuestra vida y seguridad a una máquina actualmente.
ya hemos hablado en este proyecto de todas las posibilidades que tiene IoT, y es por esto que la preocupación por la seguridad de los usuarios por sus datos es muy alta.
Hay gente que está totalmente en contra de esta tecnología ya que piensa que va a suponer una total violación de su persona y su información.
Otro de los problemas que van a suponer un problema a superar va a ser la capacidad de creación de estándares. Cada sensor que está en las ciudades, automóviles, campos agrícolas, funcionan de manera independiente e incompatible. Esto dificulta que entre dos sensores diferentes puedan comunicarse entre sí y operar en conjunto.
Poniendo un ejemplo sobre los sensores adaptados en un campo agrícola, midiendo las variables del cultivo y obteniendo información del mismo. Al lado hay un sistema de control del clima que obtiene datos en tiempo real del tiempo. En el momento que empiece a llover el sistema medioambiental debe de poder cooperar con el sistema de control del cultivo. Al estar tan dividido el mercado de fabricantes, actualmente no existe ningún estándar que pueda que todos los dispositivos funcionen correctamente en conjunto.
Todo apunta a que existirá un sistema operativo que podrá gestionar todos los mecanismos y sensores.
Como hemos estado hablando en anteriores puntos, recordamos que los sensores son dispositivos que se conectan con objetos cotidianos para medir variables como la temperatura, movimiento, etc., y enviar esa información a través de internet. Es cierto que actualmente los sensores son cada vez más baratos, pero muchos de los dispositivos y herramientas necesarias que son complementarios a los sensores como las estructuras de red o plataformas de análisis de datos son muy costosas y que realmente no son rentables a nivel personal o particular.
El motivo del elevado precio de estos dispositivos es el no haber una normativa clara y el actual estado de esta tecnología. Este hecho provoca que los fabricantes tengan miedo a un cambio de normativa.
Hablamos ahora de otro de los factores importantes que debe de superar IoT. Y no es más que el cuello de botella al que está destinado debido a las direcciones IP. Recordemos que actualmente se está trabajando con el protocolo IPv4 y mediante este protocolo, solo hay cabida para unos 4300 millones de direcciones. Actualmente el tercio de la población mundial ya está conectada, unos 2000 aproximadamente de personas, por tanto, no queda mucho margen para seguir conectando todas las “things” de esta tecnología. Con el cambio de protocolo a la versión IPv6 se permitiría conectar unos 340 billones de billones de billones de direcciones IP. Prácticamente cualquier dispositivo podrá conectarse a internet con una IP única.

De igual modo, aunque se consiga solventar los problemas de conectividad, se irá creando una red cada vez más compleja de objetos interconectados que puede suponer un gran problema. El llamado efecto dominó puede producir que la caída del sistema pueda crear grandes problemas en los dispositivos conectados. ¿Qué pasaría si un dispositivo médico interrumpiera y comenzase a ir de un modo erróneo produciendo daños a alguna persona? O que ocurra algún desastre natural que estropeara los servicios, o un ataque cibernético que pusiera en jaque a los aparatos conectados. Los daños que pueden ocasionar son incalculables.

Otro de los problemas será el de la gran cantidad de datos que van a generar estos sensores. ¿Es realmente necesaria toda esa información?, ¿Cómo podremos saber la información que necesitamos y la que no?

Realmente será complicado manejar la cantidad ingente de datos que habrá en las plataformas de datos que estará a disposición de todo el mundo. Es por ello que se está creando un nuevo modelo de negocio que consiste en la estructuración de datos y contenidos en internet.

Finalmente, IoT con el tiempo deberá responder la siguiente pregunta: ¿Realmente es necesaria la solución que puede aportar a los problemas cotidianos?

Pensemos un momento en los siguientes dispositivos que pueden aparecer: Un dispositivo que avise de cuando echar de comer a los peces, un paraguas que cambie de color según la previsión del tiempo, o un dispositivo que avise de cuando cambiar la cerradura de la puerta. Sin duda son avances importantes, pero todos estos problemas tienen soluciones más sencillas y seguramente más económicas sin poner en riesgo nuestros datos y nuestra privacidad.

Sin duda otros campos se beneficiarán de esta tecnología en mayor medida como veremos en el siguiente apartado donde analizaremos los 10 sectores en los que IoT tendrá mayor impacto. Pero aun es una incógnita saber si la población mundial aceptara que todos estos dispositivos ingresen en la vida de las personas haciéndole la vida más fácil, o todo lo contrario.

2.3.2.2. ¿Quién y dónde se dará el primer paso?

En este capítulo intentaremos dar respuesta a tres preguntas que nos quedan por responder acerca del futuro de IoT.

Primero, aún queda por saber quién será el que guiará en el camino del cambio hacia esta nueva tecnología. ¿Los gobiernos?, ¿Las grandes empresas? ¿Los consumidores o los fabricantes?

En segundo lugar, veremos en qué zonas es posible que se desarrolle con más fuerza esta tecnología. ¿Serán Estados Unidos y Europa, o los países asiáticos?

En último lugar, analizaremos el debate sobre si Internet de las cosas debe tener una mentalidad colaborativa o "Open Source" o será una mentalidad privativa.

Para responder a la primera pregunta tenemos que hablar primero del poder de los usuarios de internet actualmente. Los usuarios de las redes sociales tienen un gran peso y pueden definir el rumbo que puede seguir cualquier tecnología.

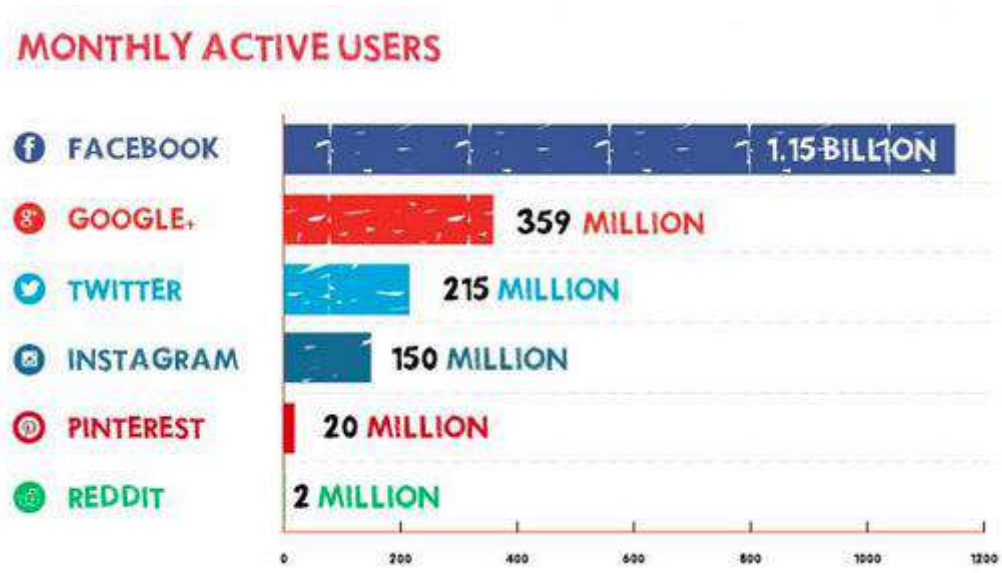

Gráfico 2.5: Usuarios activos mensuales en las redes sociales

Pero, aunque el escenario donde los usuarios puedan decidir todo lo relacionado con IoT, no es muy lógico pensar que el grupo que sea el que dé comienzo y lleve la voz cantante sean los usuarios de internet.

Si pensamos en los gobiernos, no tardamos mucho en darnos cuenta que la rapidez en la que los gobiernos cambian y los largos plazos que existen en la burocracia, parece complicado que una tarea ardua la creación de unos estándares que rijan IoT.

Por supuesto los gobiernos serán piezas clave en la innovación, pero se podría tratar más de un papel de liderazgo. Creación de estándares y leyes y derechos individuales de los usuarios son sus principales funciones en el comienzo y desarrollo de IoT.

Pienso que las empresas y los emprendedores emergentes que se dediquen a fabricar dispositivos de IoT serán los que, entre ellos, consigan marcar el rumbo que va a seguir esta tecnología, y gracias a la ayuda de los usuarios y los gobiernos puedan formar y comenzar a dar un sentido y una forma más homogénea para que en todos los lugares del mundo se usen los mismos protocolos, y pueda ser más fácil y seguro el poder hacer uso de todos los dispositivos.

La segunda respuesta parece a apuntar a los países como Estados Unidos, China y Europa. Aunque es China el país que está posicionado en cabeza al ser el mayor fabricante de dispositivos IoT actualmente, y uno de los países más consumistas del mundo. También es el país más avanzado tecnológicamente y con una cultura respecto a las nuevas tecnologías que viene promovida por su gobierno.

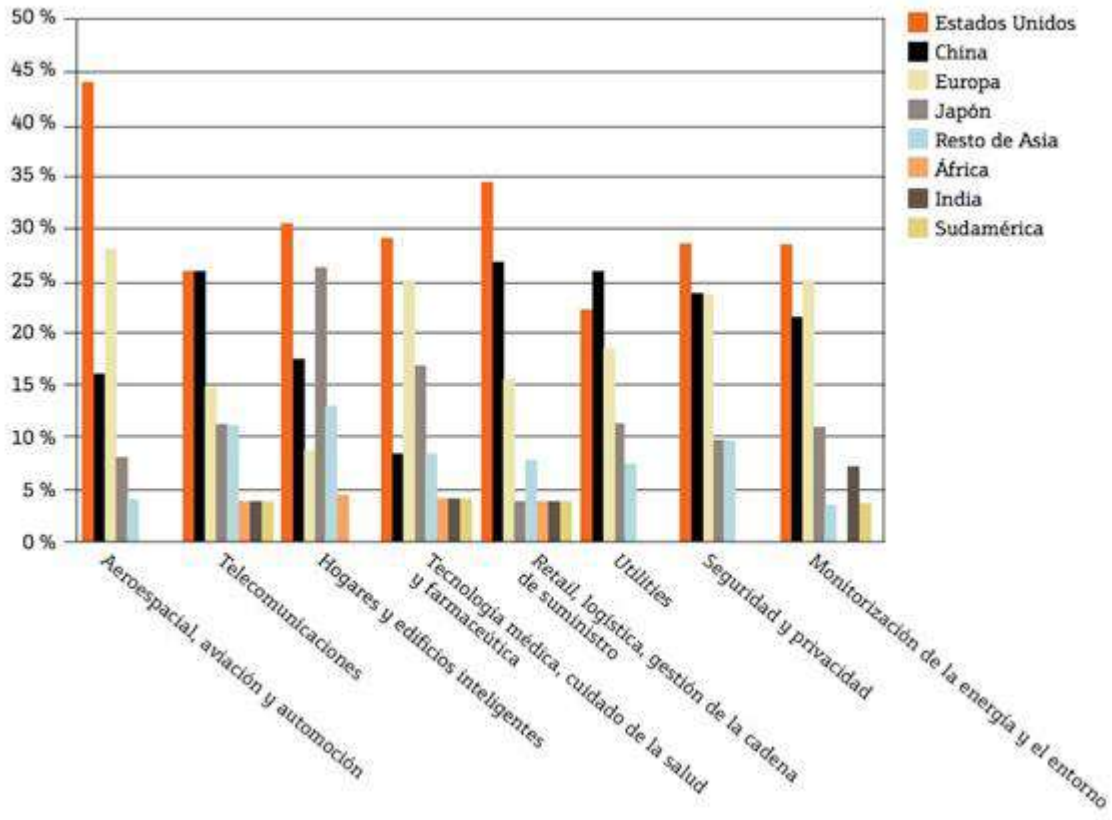

Gráfico 2.6: Distribución por países del impacto en los sectores de IoT.

Fuente: Fundación de innovación Bankinter

Por último, todo indica que la mentalidad de desarrollo "Open Source" va a predominar estos desarrollos, pero con matices. En los sectores donde es necesaria una gran inversión de dinero y con procesos costosos y complejos, como en los sectores de medicina, aeronáutica y automoción, serán las grandes industrias y empresas las que dirijan estos desarrollos.

El reto para fabricantes y gobiernos de todo el mundo, será el de crear dispositivos y sensores que sean eficientes energéticamente, robustos y que aguanten el paso del tiempo en ambientes de todo tipo.

Pero, sobre todo, deberán crear dispositivos seguros. Y sobre este aspecto nos centraremos a partir de este momento.

¿Con qué amenazas nos vamos a encontrar y cómo podemos protegernos?

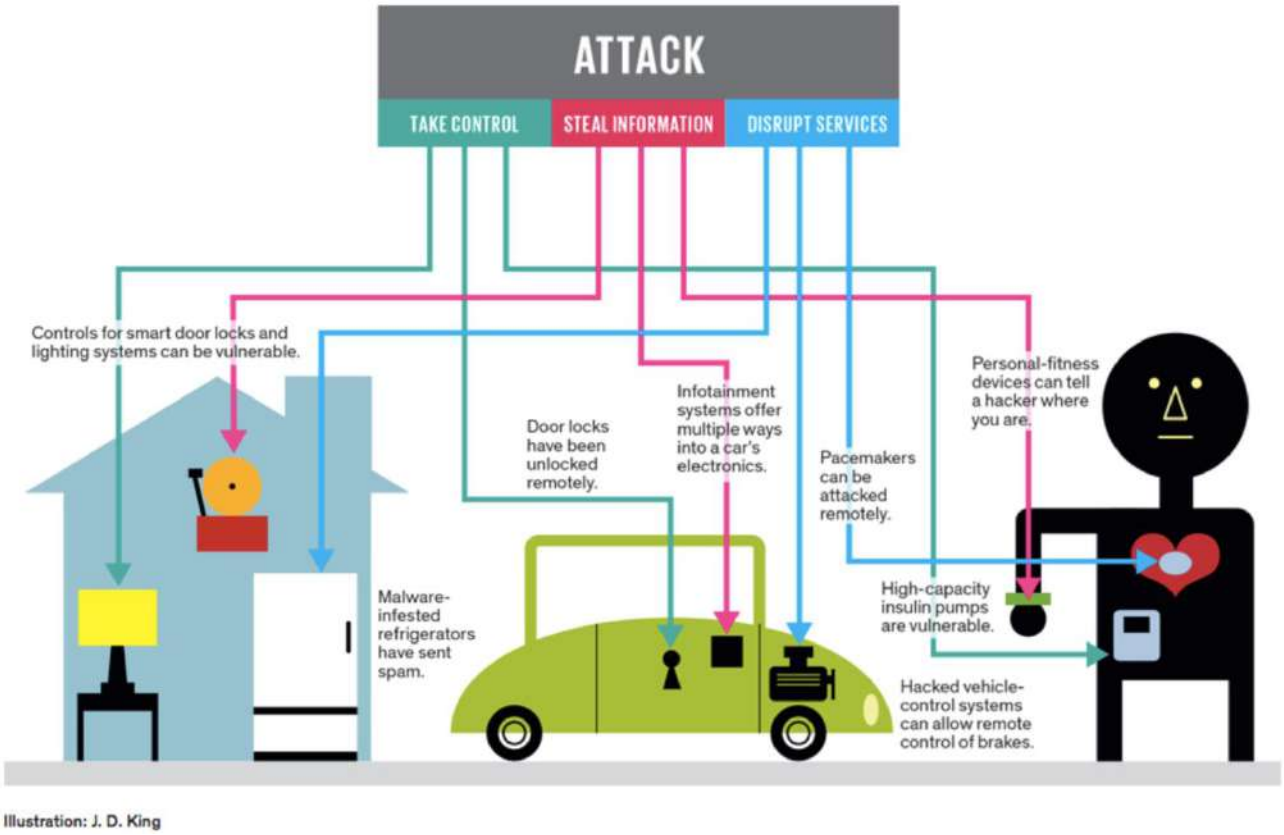

Figura 2.4: Ataques a la tecnología de IoT

Escenario 4:

Un sistema inteligente con multitud de sensores conectados en la totalidad de una ciudad como puede ser Jaén, podría ser capaz de analizar los datos atmosféricos, climáticos, y otros datos relacionados con el estado actual del clima para predecir con antelación, cómo varía la contaminación en la ciudad debido a las fábricas, transporte, etc… y ayudar a tomar medidas preventivas contra las subidas del nivel de polución, como parar temporalmente las fábricas, o reducir la velocidad máxima en las vías.

Esto ya es una realidad, y el proyecto Green Horizont de IBM, se está centrando en el desarrollo de una tecnología para controlar la contaminación y proteger el medio ambiente.

Aplicada a Pekin, esta tecnología ya es capaz de prever la evolución en el aire en la ciudad con 72 horas de antelación.

2.4. Aplicaciones de IoT con análisis en la seguridad

En este apartado se van a desglosar de una manera más amplia y diferenciada cada uno de los campos en los que IoT aportará aplicaciones y ayudará en el desarrollo de las actividades de los mismos.

Este recorrido por los diferentes ámbitos se va a realizar desde el punto de vista de la seguridad sobre los usuarios.

2.4.1. Aviación

En este sector como es el de la aviación los efectos que podría tener la inclusión de iot son variadas, como reducir los tiempos de viaje, aumentar la seguridad y comodidad de los pasajeros, reducir costes a las compañías y aeropuertos, hacer más eficiente el viaje y abaratar costes.

Rutas optimizadas: aviones interconectados entre sí y con el centro de control. De esta manera las rutas podrían calcularse exactamente al momento, pudiendo salir de las rutas establecidas y poder evitar accidentes, aterrizajes de emergencia, etc. De esta forma se ahorraría combustible al tener cada avión su ruta exacta.

Aeropuertos inteligentes: los aeropuertos serán capaces de gestionar todo el proceso de embarque, salida, entrada, controles de todo tipo de forma automática y segura, haciendo todo más fácil para el usuario y más eficaz y eficiente.

actualmente el aeropuerto de Dubai se encuentra en proceso de cambio para integrar tecnología IoT incluyendo servicio de limpieza inteligente, portamaletas automáticos, escáner facial para controles, etc.

Dr. Ian Bache, director de pre-venta técnica, ARINC aeropuertos de información de gestión de servicios, Rockwell Collins, dijo: *"los aeropuertos están siempre en busca de automatizar el procesamiento de pasajeros, manteniendo los más altos niveles de seguridad ofrecemos soluciones a medida que se pueden configurar con el aeropuerto. Las soluciones de gestión de identidad. Muchos aeropuertos en esta región están mostrando interés en estas tecnologías* ".

Pero aún queda mucho por hacer en este sector ya que siendo un transporte tan importante y usado en el mundo debe de asegurarse al máximo nivel que la seguridad de usar esta tecnología, como vuelos automáticos y customizables, aeropuertos sin personal de control, etc…

2.4.2. Automoción

Al igual que en el sector de la aviación, este sector también va a ser uno de los que más se beneficiarán de las nuevas tecnologías, y con él, los millones de usuarios que utilizan el coche, transporte público, etc.

Las empresas más importantes del mundo de la automoción como General Motors van a invertir una gran suma de dinero para desarrollar taxis inteligentes. Ford y Google siguen trabajando en coches automáticos sin conductor.

En este sector vuelve a ser el protagonista la seguridad del usuario al viajar, por ejemplo, en un coche sin conductor, y con ello, las leyes que se deben de aplicar en caso de que se produzca alguna incidencia. Todo para que el usuario esté protegido y sienta la necesidad y seguridad de utilizar esta tecnología en su día a día.

2.4.3. Telecomunicaciones

La capacidad más importante de IoT está precisamente en su definición: Interconexión y comunicación.

En el sector de la comunicación, vemos que las empresas operadores de telecomunicaciones van a tener un gran protagonismo respecto al uso de IoT ya que en su poder están todas las infraestructuras actuales que recogen los datos y tienen las capacidades comunicativas que comentábamos anteriormente

El servicio más básico que deberán cumplir todas las operadoras será el de proporcionar la conectividad necesaria para que los dispositivos puedan conectarse a internet. Pero conforme avanza la tecnología, se espera que estas compañías generen nuevas líneas de negocio y servicios añadan los posibles como nuevos sistemas de facturación y tramitación inteligentes o diseño de nuevos tipos de redes que se adapten a los nuevos sistemas inteligentes interconectados, etc.

2.4.4. Edificios Inteligentes

El sector que más rápido ha crecido con respecto a esta tecnología y que es sin duda una realidad presente. Las casas se convertirán en un sistema inteligente capaz de adaptarse al usuario y a su forma de vida, de modo que el usuario pueda dejar de prestar atención a las tareas domésticas, hacer la comida o apagar las luces cuando vaya a dormir.

Sin duda la seguridad también tendrá un factor importante ya que la cada puede funcionar como no debiera y producir algún accidente doméstico.

2.4.5. Salud

IoT tendrá muchas aplicaciones en el sector de la salud. La posibilidad de poder usar el teléfono móvil con sensores para poder medir las variables corporales y estar conectado con nuestro médico en todo momento. Poder realizar un diagnóstico rápido de un paciente, prevención de enfermedades o monitorear accidentes son las funciones principales que se esperan en este sector.

2.4.6. Agricultura y alimentación

Anteriormente hemos hablado de la explotación de recursos y cómo IoT puede ayudar a esta tarea que se antoja muy complicada.

Según la FAO (Organización de las Naciones Unidas para la alimentación y la agricultura) predice que el sector agrícola deberá enfrentarse al reto de tener que alimentar a 9,6 millones de personas que predicen para el año 2050. La producción del alimento deberá aumentar en 70% a pesar de los muchos de inconvenientes que debe de superar como la escasez de tierras de cultivo, el impacto del cambio climático en la agricultura, etc.

Aquí entra en juego la investigación de diferentes aplicaciones de IoT para este sector. Es necesario aumentar la calidad y cantidad de producción agrícola, y los sensores y la interconexión de los mismos producirá una agricultura inteligente.

Está ocurriendo ya, aunque en menor medida. Instituciones y corporaciones ya están reconectando grandes cantidades de información sobre cultivos, suelos, fertilizantes, información climática, maquinaria, etc.

Por ejemplo, en el sector de la ganadería, ya se están utilizando sensores para monitorear y detectar las posibles enfermedades y trastornos en la salud de los animales, la temperatura corporal, o incluso el pulso, incluso la posición mediante GPS.

Varias empresas privadas también están comenzando a moverse y ser activas en este sector, algunas como Anemon (Suiza), eCow (Reino Unido), Connected Cow (Alemania). Incluso la pesca inteligente está también en sus etapas iniciales con algunos proyectos en Europa, Corea del sur, Norteamérica, y Japón.

"*La agricultura de precisión no es nueva. Los fabricantes de vehículos agrícolas (John Deere, CNH Global, Class y otros) han estado involucrados en este segmento durante un tiempo. Inicialmente, comenzaron principalmente con tecnologías de posición (GNSS)*", señala Saverio Romeo (2015, citado por Federico Guerrini), analista principal de Beecham Research.

Romeo es el coautor de un informe llamado "Hacia la agricultura inteligente – La adopción de la agricultura de la visión IoT" (2015) publicada en enero por Beecham, centrado en explorar cómo las operaciones agrícolas están cambiando a través del IoT.

"*Me gustaría destacar el hecho*", dice Romeo, "*de que el objetivo no debería ser el 'industrializar' la agricultura, sino hacer la agricultura más eficiente, sostenible y de alta calidad. No debemos buscar revoluciones. Debemos buscar una reinterpretación de las prácticas agrícolas por medio del uso de tecnologías de manejo de información. Y esta reinterpretación debería tomar lugar junto con una nueva visión de las áreas rurales*".

Esto significa que el sector de la agricultura deberá estar interconectado a su vez con la industria inteligente, turismo inteligente, y demás actividades que giran en torno a la agricultura

El problema en este sector, es el mismo que en los demás, el alto costo de implementación y puesta en marcha de esta tecnología. Pero es no significa que no pueda empezar a implementarse en menor escala. En viñas, por ejemplo, *"hay sensores instalados en varias ubicaciones en el campo, para recolectar datos sobre el suelo y las plantas, para luego ser usados en la prevención de enfermedades como la peronospera*", señala Romeo.

Sin duda uno de los sectores más importantes y que hay que tener en cuenta cómo se irá desarrollando ya que su impacto en el resto de sectores y en el mundo es muy elevado.

2.4.7. Farmacéutica

Este sector va de la mano con el sector de la salud y por lo tanto también se va a ver afectado por esta tecnología.

Aunque en la industria farmacéutica la tecnología de IoT está todavía llegando, el potencial que se puede prever es enorme, sobretodo en la transmisión de datos de pacientes y seguimiento de medicamentos. Esta tecnología va a cambiar la manera de recoger los datos clínicos durante todo el proceso.

Algunos ejemplos de lo que se está empezando a desarrollar son el proyecto llevado a cabo por Novartis, que con la ayuda de la compañía Qualcomm están desarrollando un inhalador conectado a internet para enviar información de su uso y datos que los sensores puedan proporcionar. Así podrán monitorear cada inhalación y pueden hacer un seguimiento a sus pacientes.

En el futuro veremos muchos más acuerdos de este tipo entre farmacéuticas y tecnológicas. La llegada del IoT a la industria farmacéutica junto con otra tecnología importante como es Big

Data, supondrá una revolución, tanto a la hora de realizar los ensayos clínicos como la comercialización de medicamentos, hacer seguimiento a los pacientes, etc.

2.4.8. Vida independiente

En la vida de las personas mayores y su independencia también se prevé un impacto gracias a las nuevas tecnologías. De nuevo entran en juego multitud de sensores que podrían hacer un seguimiento completo de la persona, para monitorear a la persona. Las aplicaciones y las "things" pueden aprender rutinas de la persona a la que están conectadas, generar alertas, mandar notificaciones, etc.

2.4.9. Transporte de personas y mercancías

IoT puede ofrecer soluciones para sistemas de peaje y tarificación, control de pasajeros, control de cargas y mercancías, y así poder satisfacer la demanda de seguridad necesaria para este tipo de actividad.

También se podrá monitorear el tráfico al instante, que junto a sistemas de transporte inteligentes harán los transportes de personas y mercancías más eficiente. Las empresas de transporte se convertirán en más eficientes con contenedores de embalaje que puedan pesarse y escanearse por sí solos y optimizando los flujos de transporte.

2.4.10. Medio ambiente

Como hemos hablado anteriormente, uno de los mayores impactos y más importantes que se prevee es en el sector medioambiental, donde se estima que será el sector que más crezca en la utilización de dispositivos inalámbricos.

La integración de estos sensores y dispositivos abrirá las puertas a nuevas aplicaciones con impactos positivos sobre la sociedad como pueden ser el estado actual de los bosques, el nivel de contaminación, mediciones sobre el reciclaje, consumos de energía, etc.

2.5. Tecnologías con las que trabaja IoT

La arquitectura de IoT se basa en la comunicación entre dispositivos conectados unos con otros, produciéndose la comunicación máquina a máquina (M2M), que, aunque es un concepto general se aplica a la arquitectura de IoT.

En este apartado final, se explicará más a fondo la tecnología con la que trabaja IoT que se ha dividido en cuatro grupos.

2.5.1. Tecnologías de recolección de datos

En todos los puntos anteriores hemos hablado de la importancia de los sensores en la tecnología de IoT. En este apartado recopilaremos y describiremos algunos de los sensores más usuales y sus características.

Los sensores recogen por lo general variables físicas del entorno. Un sensor puede estar conectado a una calle, a una persona o a un automóvil, y se encargará de recoger datos característicos de lo que están conectados.

Según la RAE, un sensor es: "Dispositivo que detecta una determinada acción externa, temperatura, precisión, etc…, y la transmite adecuadamente".

En base a esta definición, un sensor es un dispositivo eléctrico. Un sensor también podría ser un componente M2M, como un lector RFID (Radio Frecuency IDentification), o un medidor de SCADA (Supervisory Control And Data Adquisition).

A parte de estos sensores, tenemos otros dispositivos que actúan como sensores ya sean porque tienen sensores incrustados, como por ejemplo los teléfonos móviles, dispositivos del hogar, vehículos etc…

Debido a las grandes diferencias existentes entre los sensores que recogen datos, debe de existir una plataforma que gestione las diferencias de datos.

Como comentamos, los actuales smartphones, recolectan infinidad de datos precisos en tiempo real, lo que se convierten en el dispositivo número uno en la integración de IoT. Los fabricantes de dispositivos móviles deberán de comenzar a crear sensores más sofisticados para aumentar aún más la potencia y capacidad de recolección de datos.

Los lectores RFID, NFIC, lectores NFIC, e incluso los códigos QR pueden ser leídos por los smartphones.

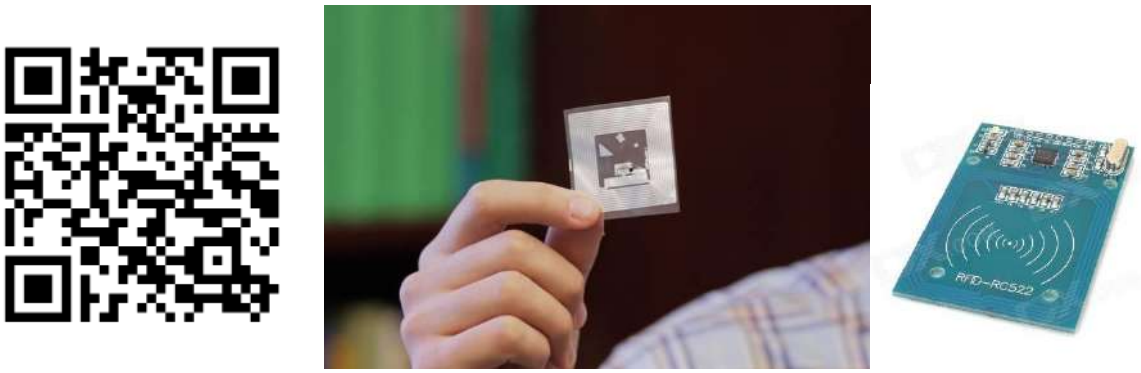

Figura 2.5: Código QR, sensor NFIC y sensor RFID.

2.5.2. Tecnologías de comunicación de datos

Igual de importante que los sensores es la infraestructura de comunicación. Las redes inalámbricas son las que van a permitir la conexión entre todos las "things" y las personas.

Las redes inalámbricas permiten crear y desarrollar aplicaciones basados en la ubicuidad y la innovación. Actualmente cualquier usuario asume que en cualquier lugar a dónde va, va a disponer de una conexión a internet y va a poder utilizar todos los servicios disponibles.

	Radio de acción	Tasa de bits	Consumo	Normas
ZigBee	10-100m interior, 1km exterior	2.4ghz, 868Mhz,915Mhz	50mW	Estándar de facto
Wavenis	200m interior,1km exterior	10kb/s – 100kb/s	18mA	Propietario
Mbus	80m interior -5000 exterior	16-66kbps	37mA	Estándar EN
Z-Wave	30m interior, 100 exterior	40-100kbps	20mA	Propietario
Wifi Low Power	70m interior- 300m exterior	11mb	60mW	Estándar
WIMAX	Hasta 75km	Hasta 75MBps	230mW	Estándar
PLC Watteco	50m	10kbps	Inferior a ZigBee	Propietario
PLC NEC		30kbps	25mW	Propietario
GMS/GPRS		85kbps	2,6 mA	Estándar

Tabla 2.2: Redes Inalámbricas.

El cambio necesario que se va a producir en el cambio de IPV4 a IPV6 va a permitir que todos los objetos del planeta conectados tengan una IP propia.

Las redes inalámbricas para la IoT se pueden clasificar en redes de corto alcance como son PAN, LAN, MAN, RFID, WIFI, WiMax y redes de largo alcance como WAN, GSM, CDMA, WCDMA y otras redes como vía satélite.

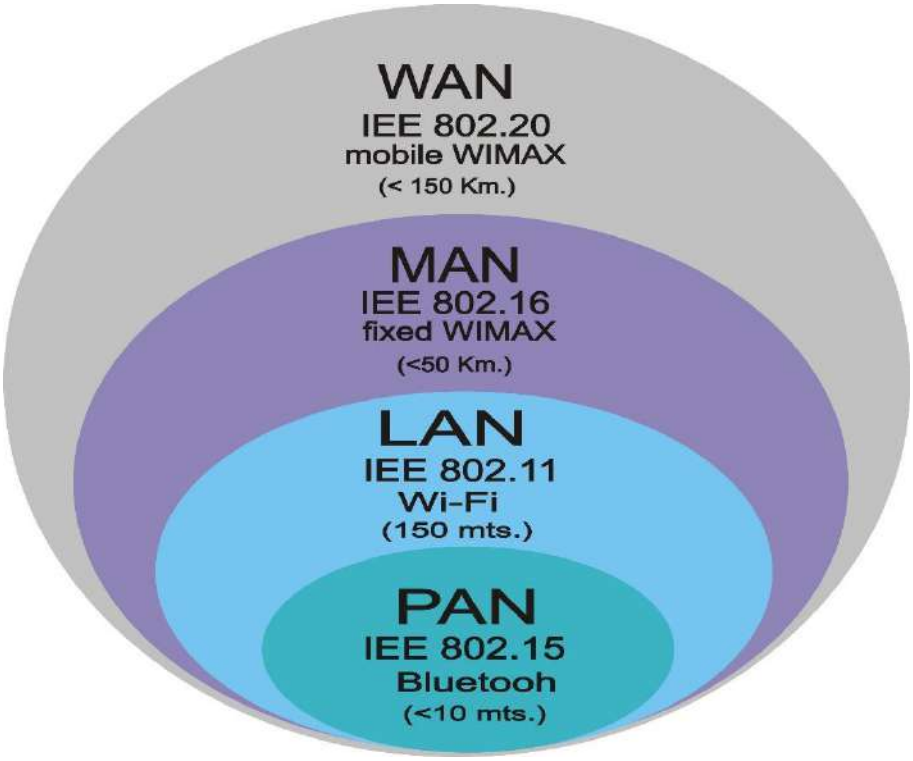

Figura 2.6: Cobertura geográfica de las redes.

Algunos de los estándares de las redes inalámbricas son:

Estándares Inalámbricos Ethernet

	Ancho de Banda	Frecuencia	Alcance	Interoperabilidad
802.11a	Hasta 54 Mbps	5 GHz band	100 pies (30 metros)	Banda no interoperable con 802.11b, 802.11g, 802.11n
802.11b	Hasta 11 Mbps	2.4 GHz band	100 pies (30 metros)	Interoperable con 802.11g
802.11g	Hasta 54 Mbps	2.4 GHz band	100 pies (30 metros)	Interoperable con 802.11b
802.11n (Pre-standar)	Hasta 540 Mbps	2.4 GHz band	164 pies (50 metros)	Interoperable con 802.11b and 802.11g
802.15.1 Bluetooth	Hasta 2 Mbps	2.4 GHz band or 5 GHz band	30 pies (10 metros)	No interoperable con cualquier otro 802.11

Tabla 2.3: Estándares de redes inalámbricas.

Por último, hablamos de otra tecnología de comunicación como son los satélites COMSAT. Son satélites de comunicaciones en una localización determinada que recibe ondas procedentes de una posición y las transmite a otra. Estos satélites funcionan actualmente trabajando para las comunicaciones de buques, aviones, telefonía, televisión, radio o GPS. Estos satélites se pueden utilizar para la tecnología M2M, produciendo una mejor cobertura en zonas remotas.

2.5.3. Tecnologías de almacenamiento y análisis

Por último, para completar el trío de tecnologías necesarias para el desarrollo de IoT, tenemos que hablar de plataformas donde se almacena la gran cantidad de datos que provienen de todos los sensores y transportadas por las redes inalámbricas.

Estas plataformas deben de permitir la gestión y el análisis de los datos en tiempo real y poder relacionar tecnologías como Big data, data mining o fusión de datos.

3. Amenazas

3.1. Seguridad

En este momento que se encuentra el TFG, es donde se tienen que identificar los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT, se tiene que tener en cuenta las diferentes vías de ataque de estos dispositivos, así como los ordenadores personales. Hay que tener claro entonces las diferencias de estos dispositivos con respecto a los demás.

Estos dispositivos empotrados son menos complejos que un ordenador personal ya que están diseñados para ejecutar una tarea o funcionalidad en específico y no algo general. Esto hace que estos sistemas sean muy variables ya que cada fabricante lo realice de una forma diferente a los demás, siguiendo su propio diseño. Esto dificulta que se pueda seguir un operativo común como ocurre con los ordenadores personales o smarthphones.

Así, los ordenadores personales utilizan un sistema operativo común (Windows, Linux, …), y los smartphones (android, iOS,). De este modo se pueden mantener actualizaciones de seguridad comunes a cada sistema operativo porque es el fabricante de software quien las crea y despliega en los diferentes dispositivos.

En el caso de los dispositivos de IoT, es el fabricante del propio hardware quien se encarga de la creación y mantenimiento del software. De esta forma, puede que no se tenga la experiencia ni recursos para poder generar un buen sistema de seguridad y protegerse ante posibles amenazas.

A esto hay que añadirle que estos sistemas no se fabricaron ni se diseñaron para estar conectados a la red, lo que conlleva que sean todavía más vulnerables y tengan un riesgo más alto.

Existe un concepto que se denomina “Security by Default”, que no es más que el establecimiento de una configuración por defecto que sea segura en el momento de la fabricación y distribución de un dispositivo.

Con este concepto se pretende solucionar el problema que tienen estos dispositivos, que no vienen dados por las capacidades o calidad de los mismos, sino por la ausencia de interfaces amigables que permitan administrarlos como en el caso de los PC o smartphones.

Lamentablemente el problema es que estas configuraciones no se tienen demasiado en cuenta, y los dispositivos salen al mercado y se comercializan con un nivel de seguridad medio o bajo.

Finalmente, otro de los puntos débiles de los dispositivos de IoT es su ubicación física, ya que pueden ser desde frigoríficos, sensores en semáforos, casas inteligentes, actuadores

medioambientales, etc, haciendo más difíciles de proteger por el hecho de que son accesibles a todo el mundo. Tal vez este sea uno de los problemas más graves.
Todo esto, añadido a los problemas de seguridad por defecto sobre la confidencialidad, integridad y disponibilidad, y que estos dispositivos tienen la capacidad de hacer cambios y actuar sobre el mundo real, puede ser un verdadero problema si no se consigue crear un sistema de seguridad fuerte y robusto que los proteja de todas las amenazas.

3.1.1. Seguridad en la transmisión de datos

Se procederá entonces a analizar detalladamente los posibles agujeros (o canales) de los que se puede sacar información en la vida útil de los dispositivos de IoT.

Se empezará con la que parece la vía más obvia en cuanto a posibles ataques se refiere. La transmisión de datos entre los dispositivos conectados a IoT, puesto que estos dispositivos están enfocados a estar continuamente transmitiendo información entre ellos o hacia la nube.

Es fácil reconocer que es en este aspecto donde debemos centrarnos en defendernos respecto a posibles ataques ya que los sistemas distribuidos emplean numerosos canales de distribución, ya sea inalámbricos, por cable, etc. Todas estas vías de información, sobre todo las que son inalámbricas y públicas, son susceptibles de sufrir ataques.

Es por eso que estos dispositivos necesitan garantizar un nivel de seguridad mínimo en cuanto a la integridad, protección y encriptación de sus comunicaciones ya que, si no se proporcionan estos niveles de seguridad, no será complicado que un atacante pueda acceder a esa información intercambiada.

La información puede contener tanto datos privados como datos personales, incluso información acerca de los dispositivos que puedan permitir el control del mismo.

Es necesario por tanto un buen sistema de cifrado de datos para evitar los ataques de tipo *Man in The Middle*, en el que el atacante se encuentra en el medio de los dos extremos de la comunicación y simplemente interfiere todos los mensajes de la misma sin que los comunicadores se den cuenta de que están siendo interceptados y posiblemente alterados. Siendo esto último altamente peligroso debido a que, si la información que se modifica actúa directamente sobre el dispositivo y su actividad, puede causar un gran problema, siendo incluso peligroso para la vida de las personas.

Vamos a poner un escenario en el que se va a poder apreciar las consecuencias de un posible ataque en la comunicación entre un dispositivo y su conexión con los datos a la nube.

Supongamos que hemos comprado una moto de último modelo, que incorpora entre otras cosas un sistema inteligente conectado a la red que ofrece servicios ofrecidos por el fabricante, facilitándonos información como la velocidad, posición, tiempo medio, estado general de la moto, etc. Supongamos también que la comunicación entre nuestro vehículo e internet es poco segura y tiene un nivel bajo de encriptación. Un atacante podría acceder a la comunicación y obtener valores como la posición del vehículo, sabiendo en todo momento la ruta que seguimos, dónde vivimos, donde trabajamos etc. También podría conocer el estado del motor, nivel de líquidos.

El otro factor importante, es que, si este atacante puede modificar la información en la comunicación y pudiera dar las mismas órdenes que damos nosotros, podría hacer que se encendieran las luces, cambiar de marcha, acelerar, frenar, dependiendo de las funcionalidades que permita hacer el dispositivo de IoT.

3.1.2. Seguridad en el software

Se pasará ahora a otro de los canales sobre los que se pueden realizar más ataques. Es el aprovechamiento de las debilidades en el software en los dispositivos IoT.

Cuando se crea un dispositivo y se le añade un sistema operativo, normalmente se utilizan versiones simplificadas de los sistemas operativos de uso común como pueden ser Windows, Linux, etc. De esta forma los costes de fabricación de estos dispositivos se reducen considerablemente. Esta práctica, evidentemente supone un riesgo a la seguridad ya que cuando se detecta una vulnerabilidad en estos sistemas operativos se explotan en todos los dispositivos que lo tengan instalado.

Otra característica que se obtiene al desarrollar el dispositivo abaratando costes en su desarrollo, es la interfaz web. Estos, al ser de pequeño tamaño, y no disponer la mayoría de una pantalla, tienen que ser controlados a través de internet. Si estas interfaces para acceder a los dispositivos y configurarlos, manipularlos, etc, no se protegen debidamente, cuando se produzca algún ataque y accedan intrusos, podrán acceder a todos los dispositivos que usen esa interfaz.

Una última característica que tienen en común la mayoría de dispositivos de IoT es su acceso a los servicios en la nube. Si en estas plataformas de servicio no se llevan a cabo tareas de mantenimiento, actualización y protección, puede ser una vía muy peligrosa para poder acceder a toda la información y poder tomar el control de los dispositivos.

Algunos dispositivos como smartphones o televisiones inteligentes, pueden acceder a repositorios de aplicaciones para añadir nuevas funcionalidades. Ésta puede ser la puerta de

entrada a aplicaciones maliciosas que puedan tomar el control de los dispositivos, explotar vulnerabilidades, obtener información confidencial, o incluso descargando más aplicaciones maliciosas sin nuestro consentimiento.

Por tanto, de igual manera, los responsables de estos servicios en la nube y repositorios tienen la misma responsabilidad de mantener correctamente sus servicios para permitir que los dispositivos accedan a ellos sin ningún problema para su seguridad.

3.1.3. Seguridad en la configuración y funcionalidad

Muchas veces, el principal problema en cuanto a seguridad se refiere, radica principalmente en la configuración (por defecto, y posibles opciones configurables) y la funcionalidad del propio dispositivo.

Muchos fabricantes, a la hora de establecer la configuración por defecto del dispositivo, eligen unas opciones que posiblemente el usuario no va a utilizar nunca, o bien, que por estar activadas y permitir el uso de esa funcionalidad avanzada, el usuario no tenga suficientes conocimientos y la emplee mal, produciendo una brecha de seguridad y posible acceso para intrusos.

De nuevo, entra en juego el papel de fabricantes, que son los responsables directos de esta posible vía de acceso de intrusos. Los distribuidores deben de ser conscientes, y adoptar una política de configuración segura, permitiendo además a los usuarios poder configurar el dispositivo acorde a sus necesidades, sin ser un sistema rígido, marcado con las opciones de fábrica.

Se pondrá un ejemplo para poder entender mejor este problema.

Cuando adquirimos un smartphone, éste viene con unas configuraciones por defecto generales del dispositivo, y además viene con un apartado de configuración para redes. Esta configuración por defecto puede ser peligrosa. Si viene activado para que el dispositivo esté conectado permanentemente a internet, y un usuario inexperto no es consciente de esto, puede ser un problema ya que el dispositivo estará continuamente conectado a internet, descargando y transfiriendo datos, posiblemente sin el conocimiento del usuario.

3.1.4. Seguridad en el Hardware

Para este caso, esta posible brecha de seguridad ya existe antes de IoT. Los problemas debidos a la mala política de seguridad para el hardware son las menos frecuentes, pero lamentablemente son las que producen problemas más difíciles de solucionar.

Obviamente, los problemas de seguridad en el hardware se producen sin la necesidad de estar conectados a internet, pero puesto que los dispositivos de IoT también cuentan con este problema, se ha incluido en esta lista de posibles brechas de seguridad.

Los ataques contra el hardware se producen, sobre todo, cuando el dispositivo tiene una gran seguridad a nivel de software, cuando se encuentran en puntos aislados de la red, o cuando están bien protegidas para un acceso a través de internet.

Es entonces cuando se producen estos ataques, que suelen estar dirigidos a los componentes conectados a la red eléctrica.

La diferencia de estos ataques es que para realizarlos es necesario un equipamiento especializado para producirlos. Según el equipo que del que se disponga se podrán realizar diferentes tipos de ataques, desde ingeniería inversa a monitorización de interfaces.

Los ataques más habituales son los accesos a la información tanto volátil y no volátil como memoria RAM y discos duros. Si podemos acceder a la memoria no volátil, es posible acceder a claves, información de acceso, etc. Si podemos acceder a la memoria no volátil, se puede acceder a toda la información guardada.

Hay dos posibles protecciones para este tipo de ataques:

El primero de ellos es garantizar que, si el dispositivo es manipulado, automáticamente se destruya la información que contenta. La segunda es un buen sistema de cifrado de información, de modo que, si finalmente acceden a los datos, les sea imposible descifrarlos.

Un punto a tener en cuenta en este apartado es el borrado de información.

Cuando un dato se borra de un dispositivo no volátil, se modifican las tablas de asignación de archivos en el sistema de ficheros, haciendo que el espacio que ocupaba el dato está disponible para otro nuevo dato, pero sin realizar un borrado efectivo.

Existen herramientas que, sin un mínimo de pasadas de borrado, es posible recuperar la información que se encontraba en el disco.

3.1.5. Seguridad en los usuarios

Se va a terminar con una vía de acceso que no está relacionada directamente con los dispositivos IoT, sino con los usuarios. En muchos casos, si todos los puntos anteriores como el software,

hardware, comunicaciones y configuraciones están perfectamente protegidos y construidos, un mal uso del usuario puede poner en serio peligro toda la información del dispositivo.

Es probablemente el principal motivo por el que se producen ataques sobre los dispositivos ya que, como parte de la cadena, los usuarios somos el eslabón más débil y podemos cometer errores.

El principal ataque se basa en la llamada ingeniería social. Básicamente se centra en aprovechar los errores humanos para comprometer la seguridad de los dispositivos mediante la confusión y el engaño.

Debido a que la mayoría de los accesos a las plataformas privadas en internet son a través de unas credenciales, la ingeniería social intenta acceder a ellas mediante estafas a través de correos electrónicos, sitios web falsos, o suplantación de identidad.

Estos ataques están dirigidos a grandes empresas y clientes potenciales para poder obtener un mayor beneficio.

Es necesario crear una cultura de seguridad para los usuarios y concienciarlos sobre los problemas que pueden producir si no ponen atención a sus actividades mientras utilizan los dispositivos ya que como hemos comentado anteriormente, no sirve de nada que un dispositivo esté perfectamente protegido, si nuestra clave de seguridad la apuntamos en nuestra red social preferida. De esto se hablará más adelante en el punto 4.6 del TFG.

3.2. Protección y privacidad. Recomendaciones

Como se viene contando en todo este TFG, de todos los desafíos con los que se encuentra el desarrollo de IOT, la protección sobre la privacidad de los usuarios es el que genera mayor preocupación en los consumidores. Por ello, las autoridades europeas de protección de datos, destacando entre ellas la francesa (CNIL) y la española (AEPD) realizaron el primer dictamen en 2014 sobre las recomendaciones que debemos de seguir.

El grupo de trabajo de la Unión Europea del artículo 29 de protección de datos (G29) ha dado una serie de recomendaciones sobre tres tipos de sistemas de IOT: Los *weareables computing* (tecnología para llevar puesta), los dispositivos que registran actividades de las personas y su estilo de vida y la domótica.

Entre las recomendaciones más importantes destacamos: “para que esta tecnología tenga éxito y de frutos es necesario, en palabras del G29, que los usuarios del Internet de las Cosas puedan permanecer siempre en control de sus datos y deben saber claramente cómo y para qué se van

a utilizar los mismos. Deben dar su consentimiento expreso tras recibir la información de forma clara y transparente. Esta claridad es otra de las bases del éxito de estas tecnologías".

Los retos que según el G29 resaltan para superar son: Controlar que los datos y la información que cae en manos de terceros. Es importante que el consumidor sepa en todo momento quien obtiene esos datos y qué hace con ellos, por tanto, el consentimiento es libre por parte del usuario el que se usen o no sus datos. Otro aspecto importante que controlar es que los datos se usen para el fin que fueron recogidos. El G29 también cree que es importante que las aplicaciones y dispositivos se puedan usar de forma anónima.

La Agencia Española de Protección de Datos habla al respecto del dictamen del G29:

"*La información personal sólo puede ser recogida para unos fines determinados, explícitos y legítimos. Este principio permite a* ***los usuarios conocer cómo y con qué fines se están utilizando sus datos*** *y decidir en consecuencia. Además, los datos recogidos deben limitarse a los estrictamente necesarios para la finalidad definida previamente. Los datos que son innecesarios para tal fin no deben ser recogidos y almacenados por si acaso o porque podrían ser útiles más adelante*".

Igual de importantes que las recomendaciones generales sobre la privacidad y seguridad del G29, son las recomendaciones dirigidas a otros sectores específicos.

- Fabricantes de dispositivos.
- Desarrolladores de APP.
- Propietarios y/o usuarios de dispositivos.

Recomendaciones para Fabricantes de dispositivos:

1. Informar claramente de todos los sensores que contiene el dispositivo, qué datos recogen y en qué se emplearán esos datos.
2. Gestionar la retirada del consentimiento y la oposición al tratamiento.
3. Dificultar la trazabilidad pasiva.
4. Utilizar datos agregados en lugar de datos brutos.

Recomendaciones para Desarrolladores de App:

1. Avisar en todo momento y recordar cuando los sensores están activados y recogiendo datos.
2. Deben de facilitar al usuario en todo momento la tarea de borrado y acceso a sus datos.
3. Deben de aplicar el principio de minificación de datos.

Recomendaciones para propietarios y/o usuarios de dispositivos:

1. El consentimiento de los usos de datos debe de ser obtenido de forma libre e informada. Es importante que el usuario no fuera penalizado en calidad de servicio ni económicamente por no facilitar datos.
2. Deben de poder administrarse los datos en cualquier momento.

A pesar de que la preocupación de la privacidad está siendo un aspecto clave en el desarrollo de esta tecnología, que incluso está convirtiendo en una carga muy grande para superar, no debe de ser una barrera que no pueda sobrepasarse, ya que son tantas las posibilidades que nos ofrece y cómo nos puede cambiar la forma de vivir a las personas que merece la pena que desde todos los sectores se ponga especial interés en seguir las recomendaciones y trabajar en conseguir una gestión de la privacidad del consumidor esperada.

Escenario 4:

Llevamos unos días encontrándonos mal y en vez de pedir cita con nuestro médico que de cabecera para que nos examine para detectar alguna dolencia, vamos a nuestra habitación donde tenemos un espejo inteligente que, con únicamente reflejarnos en él, analiza nuestro cuerpo mediante sensores, en busca de alguna enfermedad.

Como podemos ver, el sector de la salud es el que más se está beneficiando (y seguirá haciéndolo) de los avances de esta tecnología.

En la actualidad se está desarrollando este tipo de espejo, Wize Mirror es el nombre de este aparato tecnológico que podría suponer un avance impensable hace años, donde el diagnóstico está en la casa de cada uno.

4. Soluciones

Llegados a este punto del TFG en el que ya se han repasado las posibles vías de ataque y analizado una serie de casos reales sobre ataques, toca al fin, recorrer una serie de puntos en los que se dividirán las posibles soluciones y tipos de estrategia para hacer frente a las vías de ataque comentadas anteriormente.

Por supuesto, estas soluciones no representan una guía infalible contra todo tipo de ataques. Dentro de nuestras posibilidades tenemos que aplicar todas las técnicas para garantizar un uso seguro de nuestro dispositivo de IoT.

4.1. Control en las interfaces de acceso

Cuando hablamos de los posibles riesgos en una mala configuración y diseño del software en el apartado 3.1.2 de este TFG, indicamos que una de las partes más vulnerables recae en la interfaz de los dispositivos. La mayoría de los dispositivos que se conectan a la red necesitan de una serie de parámetros y opciones que pueden o deben ser configuradas según el escenario en el que convivan. Para eso las interfaces son muy importantes tanto para el usuario como para el fabricante.

El problema nace en el momento que las interfaces presentan sistemas de seguridad y autenticación obsoletos, inestables o incluso, inexistentes.

La solución de este problema es realizar una interfaz capaz de poder ser controlada mediante dispositivos remotos como pueden ser tabletas, smartphones o incluso desde otro dispositivo IoT conectado. Esta interfaz debe de ser robusta y seguir una serie de *buenas prácticas* para que el acceso sea controlado y la seguridad, por tanto, completa.

En primer lugar, se debe de poder definir qué dispositivo o dispositivos son los que van a poder conectarse a esa interfaz si el acceso es abierto mediante internet. Si controlamos de esta forma los dispositivos, sería muy complicado que pudieran atacar nuestra interfaz de control del dispositivo y generar cualquier perjuicio.

En muchos casos, estas interfaces no presentan ningún tipo de autenticación ni validación, y cuando vienen implementadas, las credenciales no se han cambiado y siguen las que el fabricante suministró.

Hay que hacer una mención especial en este apartado de autenticación la importancia de generación de las contraseñas, cuyas recomendaciones desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO) se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

Emplear un mínimo de 7 caracteres, mayúsculas y minúsculas, algún número y algún símbolo especial.

Otro de los puntos clave para el acceso a la interfaz del dispositivo se centra en el cifrado web. Cuando un sitio web implementa un sistema de cifrado hace uso del protocolo HTTPS. De este modo sería muy complicado que alguien pudiera interceptar nuestras credenciales de acceso ya que no estaríamos navegando por una Internet *abierta*.

Otra de las opciones consistiría en utilizar un Virtual Private Network, o VPN. Esto nos permitiría crear una extensión de red segura sobre la red abierta Iternet, de modo que estaríamos en una red privada con todas las funcionalidades existentes en Internet.

4.2. Actualización de dispositivos

Cuando un dispositivo aparece en el mercado, como, por ejemplo, un smartphone, aparece con unas funcionalidades definidas y un software diseñado que aprovecha las capacidades de hardware. En muchos casos, aunque el usuario gestione correctamente el dispositivo y defina en la interfaz de control los parámetros adecuados para una correcta seguridad, es el propio software el que presenta el problema ya que de base está mal implementado o configurado.

En este caso los esfuerzos del usuario resultan en vano ya que quien tiene que corregir este problema es el fabricante de software o hardware.

La mejor solución para este tipo de problema es mantener constantemente el dispositivo actualizado a la última versión que presente el fabricante ya que las constantes actualizaciones presentan mejoras de seguridad, rendimiento, durabilidad, etc.

Por desgracia hay fabricantes que no presentan estas actualizaciones para solucionar los diversos problemas de seguridad. Una buena práctica consiste en analizar, a la hora de la adquisición de un dispositivo, los diferentes fabricantes para conocer quién da un mejor soporte de actualización del dispositivo y así saber que tenemos un respaldo del fabricante que resultará a la larga muy importante.

4.3. Configuraciones seguras de la red

Este punto no está enfocado únicamente para la seguridad en IoT, sino en general todos los dispositivos conectados a las redes. Pero uno de las mejores tareas que podemos poner en marcha a la hora de defendernos sobre cualquier ataque, es sin duda seguir las recomendaciones y buenas prácticas a la hora de configurar la red con la que trabajemos.

En primer lugar, lo más importante es la configuración del Firewall de la red o *Cortafuegos*.

El cortafuegos es la primera parte de nuestro sistema de seguridad de la red que toma contacto con el exterior, y es quien va a controlar los accesos. Es por tanto una pieza clave a la hora de proteger nuestros dispositivos, aunque también puede ser el motivo por el que nuestro sistema sea totalmente vulnerable si su configuración está mal realizada.

Es por ello por lo que además entra en juego un IDS o *Sistema de Detección de Intrusos*, que no es más que un programa que se encarga de detectar algún acceso no autorizado en nuestro sistema. En el caso de que nuestro Firewall sea defectuoso y provoque accesos no deseados, es nuestro IDS quien se encargará, gracias a los sensores virtuales, anomalías en la red que puedan ser indicio de ataques.

En el caso en el que un intruso accediera a nuestra red sin permiso y nuestro IDS lo detectase, un firewall bien configurado bloquearía los puertos y protocolos de comunicaciones para proceder a contrarrestar el ataque.

4.4. Control de aplicaciones en la nube (cloud services)

Como se ha estado comentando en todo el desarrollo de este TFG, una de las características y funcionalidades más importantes y atractivas de los dispositivos de IoT, es el acceso y suministro de datos a la nube para controlar aplicaciones en la nube o Cloud Services.

El inconveniente de esta funcionalidad es su propia definición de servicio en la nube. Al estar abierta sin ningún tipo de restricción a todos los usuarios de la red, es necesario tomar una serie de medidas más estrictas. Hay que tener en cuenta que debemos de saber en todo momento como va a ser el traspaso de datos desde nuestro dispositivo al servicio, y viceversa.

Por tanto, la seguridad de este canal de comunicación es crucial, y se deben de seguir las recomendaciones de privacidad y acceso para evitar los problemas que se han expuesto en el punto de seguridad en la transmisión de datos 3.1.1.

Además, si el servicio que está en la nube es el que gestiona nuestro dispositivo, así como la gestión de los datos que proporciona, deberemos seguir las recomendaciones del anterior punto 5.1 sobre control de interfaces de acceso acerca de contraseñas y conexiones cifradas.

4.5. Uso de aplicaciones móviles

En la actualidad, en el nivel de desarrollo de la tecnología de IoT, la mayoría de las aplicaciones destinadas a IoT están orientadas a los smartphones. Esto es debido al gran auge que actualmente tienen los smartphones en nuestra vida cotidiana.

Mediante el smartphone es muy sencillo e intuitivo, debido a la cultura tecnológica que existe actualmente, poder gestionar nuestro dispositivo de IoT, acceder a nuestros datos, y monitorizar el estado actual del dispositivo.

Sin embargo, para que la aplicación no se convierta en una vía de ataque, es necesario seguir una serie de requerimientos a la hora de utilizar estas aplicaciones.

Empezaremos por el primer eslabón en el proceso desde que descargamos la aplicación. Es crucial que la aplicación tenga un fabricante de confianza y una zona de descarga segura y confiable, así evitamos que desde el sitio de descarga se pueda introducir algún software malicioso. Se debe de descargar por tanto de la página oficial de aplicaciones.

En siguiente paso es instalar la aplicación. Se debe de prestar mucha atención a los permisos que solicita la aplicación para poder ejecutarse. Por ejemplo, si instalamos una aplicación para poder controlar la temperatura de nuestro frigorífico, es lógico que requiera permisos de conexión a la red, pero no lo es que solicite permisos de lectura de nuestros mensajes.

Finalmente, debido a que nuestro smartphone lo usamos diariamente para más utilidades y no solo para el uso y control del dispositivo de IoT, debemos seguir las indicaciones que se ha expuesto en el apartado de Actualización del dispositivo 5.2.

4.6. Cultura de seguridad de los usuarios

Se va a terminar este recorrido sobre los consejos y recomendaciones de las buenas prácticas para enfrentarnos a los diferentes ataques a nuestros dispositivos de IoT, centrándonos en los seres humanos.

Como ya se ha hablado en el punto 3.1.5 *Seguridad en los usuarios* de este TFG acerca de los posibles ataques que pueden acechar a esta vía, es en este apartado donde presentaremos las soluciones y buenas prácticas para mitigar todos los posibles problemas causados por la falta de cultura de seguridad que existe entre los usuarios de internet.

Se van a dividir las soluciones en un decálogo donde se recogen las buenas prácticas más importantes que son:

1. Contraseñas de acceso seguras:

Como ya se ha hablado en este TFG en anteriores puntos, una de las mejores prevenciones para mantener una correcta seguridad en nuestra experiencia como usuario en internet es mantener un completo control de nuestras contraseñas manteniéndolas seguras según se indica en el punto 5.1.

2. Realizar copias de seguridad:

En el caso de que por algún motivo hayamos recibido un ataque a nuestro dispositivo, sería un problema muy grave que pudiera haber borrado todos nuestros datos que nuestra aplicación ha ido guardando a lo largo del tiempo. Aunque el perjuicio se ha producido, una buena práctica para poder reducir el daño, es realizar copias de seguridad periódicas de los datos que nos gustaría conservar en el caso de que pudiésemos perderlos. Estas copias de seguridad deberán guardarse en otro dispositivo.

3. Proteger físicamente los dispositivos:

Si disponemos de un dispositivo que realiza un escáner diario mediante sensores, sería crucial que por algún motivo (sea un atacante o causa natural), nuestro dispositivo se bloquease o se apagase y dejase de realizar su función. Es por ello que, para prevenir este tipo de incidentes, es necesario proteger nuestro dispositivo con herramientas como SAI (sistema de alienación ininterrumpida), y otros aparatos que nos ayuden a relanzar el dispositivo en caso de que deje de funcionar.

4. Uso de Firewall:

De el correcto uso del Firewall ya se ha hablado en el punto 5.3.

5. Redes sencillas:

Si nuestro dispositivo no necesita una compleja red para poder funcionar, es recomendable que la red que configuremos no sea mayor que la que necesita, ya que una red pequeña, es más administrable y, por tanto, es más segura.

6. Redes complejas:

En el caso en el que nuestro dispositivo necesite de una red más amplia para funcionar, se deben de establecer políticas de acceso de usuarios para gestionar totalmente quien puede acceder a la red.

7. Antivirus y antiespías:

Desde cualquier sitio en el que controlemos nuestro dispositivo de IoT es necesario que dispongamos de algún software diseñado exclusivamente para poder proteger nuestro sistema operativo de posibles malware y espías que puedan acceder a nuestro equipo y con ello poder suplantar nuestra identidad y acceder a el control total de nuestro dispositivo.

8. Actualizar sistemas operativos y aplicaciones:

Del mismo modo en el que hablábamos en el punto 5.2 sobre las actualizaciones de dispositivos, la misma solución se aplica a la actualización de aplicaciones que nos permitan controlar los dispositivos inteligentes. Estas actualizaciones de las aplicaciones también corrigen problemas de seguridad.

9. Usar con precaución el correo electrónico y mensajería:

Es necesario concienciar a los usuarios para el correcto uso del correo electrónico y servicios de mensajería, ya que es la principal vía de ataques de ingeniería social (ver índice 3.1.5). Lo más seguro es no transmitir datos confidenciales ni sensibles si no se tienen elementos de autenticación y no aceptar programas o datos que provengan de fuentes desconocidas. Por tanto, hay que confirmar la fuente previamente.

10. Precaución en el uso de internet:

No acceder a sitios web que tengan direcciones extrañas, ni que estén contenidos en correos electrónicos mencionados en el punto anterior. Tampoco es recomendable introducir ningún dato confidencial que no tenga los elementos de seguridad adecuados.

5. Análisis de la encuesta “Qué opina de IoT”

Una de las finalidades secundarias con las que se ha afrontado este proyecto es conocer la opinión de los usuarios que día a día utilizan internet y los primeros pasos de la tecnología de IoT. Es muy interesante conocer si los usuarios normales saben acerca de Internet de las cosas, si les preocupa realmente la seguridad de su información, o si realmente son conscientes de todo lo que se avecina con esta tecnología.

Se han realizado dos encuestas:

Una a través de internet en la que había que responder a una serie de cuestiones con “SI” o “NO”, en la que han respondido un total de 374 personas, y en la que he sacar varias conclusiones bastante interesantes que a continuación se detallarán.

La otra en cuesta se realizó a 10 personas en la calle en la que se preguntaban las mismas preguntas, pero se recogía información más precisa pudiendo analizar mejor lo que piensa la gente.

5.1. Análisis primera encuesta

En este apartado se van a analizar los resultados obtenidos por la primera encuesta analizando cada pregunta y sacando las conclusiones propias.

Pregunta 1: ¿Sabe qué es Internet de las cosas?

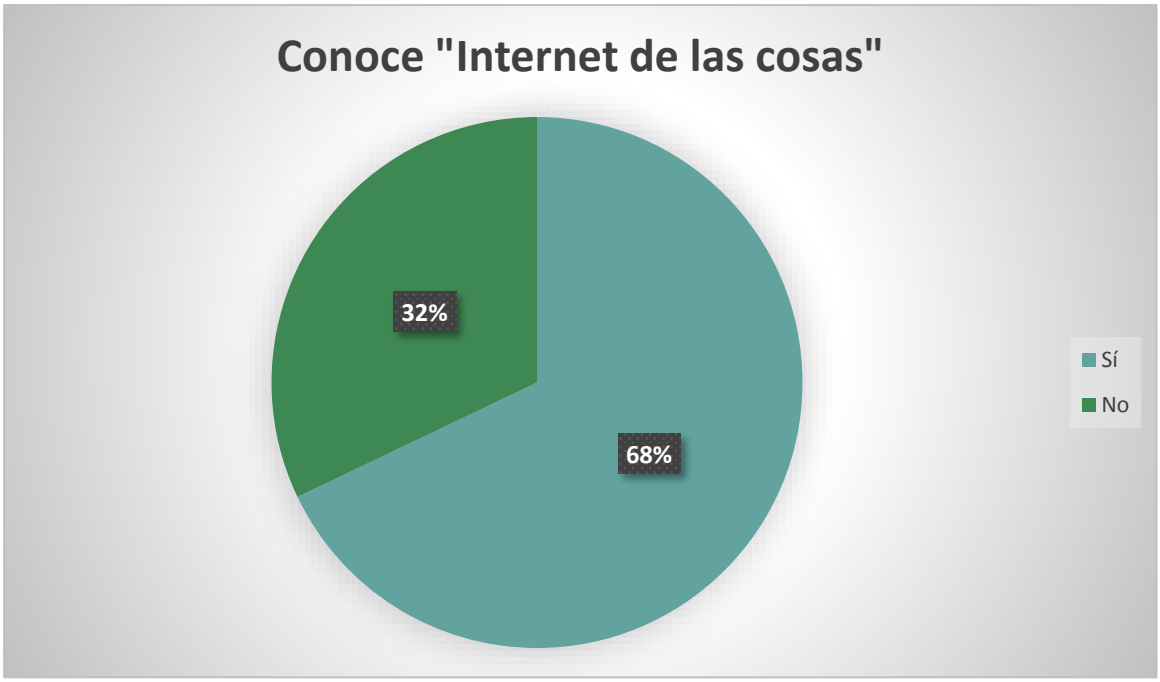

Gráfico 5.1: Pregunta 1 Encuesta

Los resultados de esta primera pregunta son bastante curiosos y no me los esperaba. Realmente casi un 70% de los encuestados conoce Internet de las cosas. En la realización de este proyecto he descubierto que los medios de comunicación, sobre todo los medios digitales están siguiendo con bastante rigurosidad e interés todo el avance que se está produciendo en IoT. Gracias a esto, los usuarios medios están al día de lo que ocurre en IoT. Además, al ser los avances tecnológicos un tema de interés general, es más probable que aparezca en los medios de comunicación o la gente busque más información.

Pregunta 2: ¿Está preocupado por la seguridad de sus datos y su privacidad en Internet?

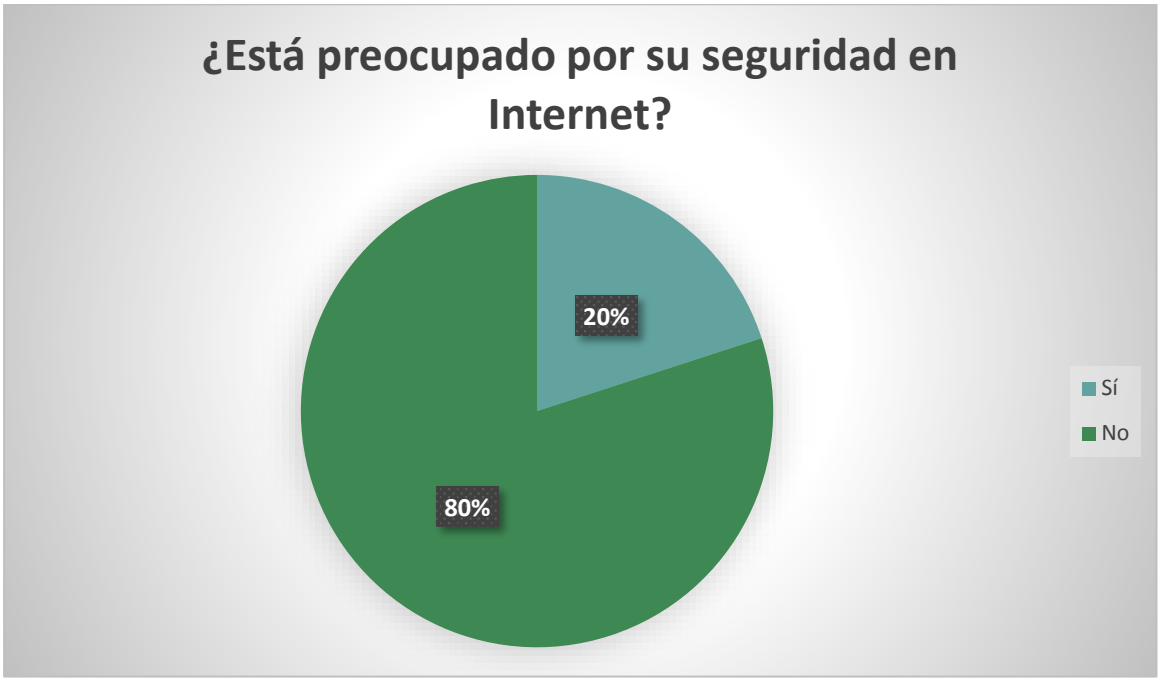

Gráfico 5.2: Pregunta 2 Encuesta

Esta pregunta también era importante conocer la respuesta ya que en este proyecto se ha intentado conocer el estado de la seguridad en Internet de las Cosas en concreto, y como consecuencia la seguridad en Internet. A la vista de los resultados, solamente a un 20% le preocupa la seguridad de los datos o de su información en internet. Esto es interesante, pero con un significado que he podido obtener gracias a la segunda encuesta. A la mayoría de la gente no le preocupa la seguridad en internet por alguno de estos dos motivos:

- Porque tiene una cultura de la seguridad en internet importante y es completamente consciente de lo que puede compartir en internet y toma las medidas adecuadas para su protección.
- Porque no es consciente del verdadero peligro que conlleva compartir información importante en redes sociales y otros medios y piensa que realmente es imposible que le pase nada.

Sería interesante saber de ese 80%, cuántos de ellos conocen realmente la importancia de la seguridad y de una buena cultura.

Pregunta 3: ¿Cree que internet de las cosas va a suponer un cambio positivo o negativo?

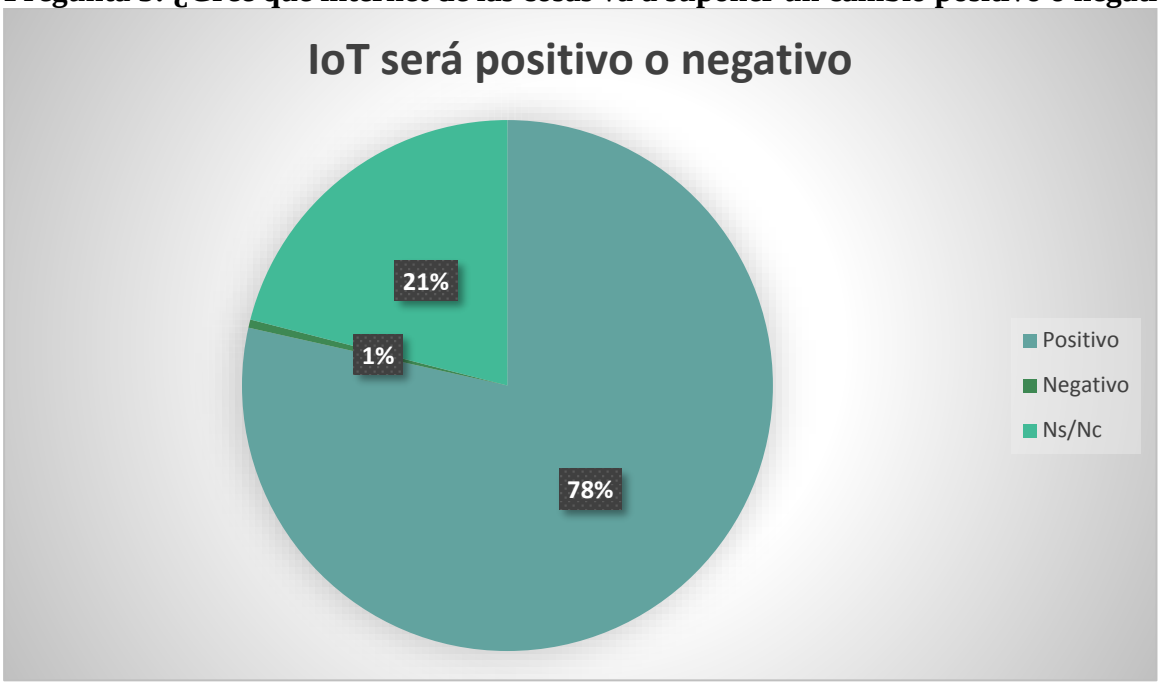

Gráfico 5.3: Pregunta 3 Encuesta

También era importante saber qué opina la gente acerca de la tecnología que está por venir. ¿Los usuarios la ven con potencial de tener un gran impacto en el mundo y en la forma de vivir de las personas? O en piensan en cambio que no va a suponer un gran cambio, o incluso será algo negativo y perjudicial.

Pues bien, los resultados han sido muy interesantes. Si quitamos el 21% que no conoce qué es internet de las cosas y no ha respondido ni positivo ni negativo, prácticamente la mayoría de las personas que han respondido piensan que es positivo, mientras que sólo el 1% es negativo. Este resultado indica lo bien que se está promoviendo y hablando de las virtudes de IoT.

Es tanto lo que parece que puede ofrecernos IoT que parece difícil que alguien piense que no es necesario que la tecnología de IoT llegue hasta nuestra sociedad hoy en día.

Como hemos analizado en todo el proyecto, será un cambio muy importante en todos los aspectos y sectores de la vida, pero es bueno saber que la mayoría de la gente encuestada opina que, aunque el cambio sea importante, va a ser muy beneficioso para el mundo.

Pregunta 4: ¿Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

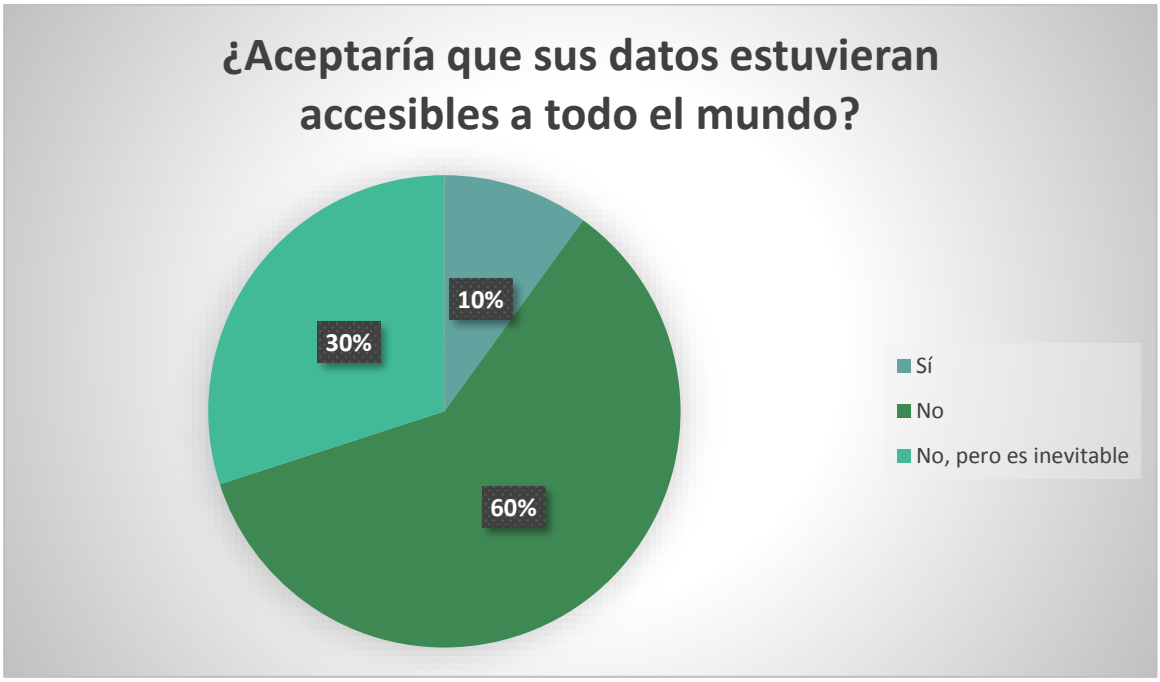

Gráfico 5.4: Pregunta 4 Encuesta

Como hemos comentado en el proyecto, una de las características más importantes de IoT es la accesibilidad de los datos desde cualquier parte del mundo y el continuo traspaso de información de un dispositivo a otro.

Con esta pregunta quería conocer si los usuarios aceptarían el hecho de que sus datos puedan ser accesibles por todo el mundo pudiendo causar daños y perjuicios en caso de robo de esa información, o si en cambio están seguros de que sus datos no van a sufrir ningún altercado.

El 60% piensan que este va a ser un gran problema ya que no se van a sentir muy seguros sabiendo que toda su información va a estar en plataformas a las que todo el mundo y cualquier dispositivo pudiera tener acceso.

Esto demuestra que IoT tiene que demostrar que va a proporcionar una verdadera seguridad y protección a los usuarios si de verdad quiere triunfar y asentarse.

El 30% piensa que, aunque les preocupa la seguridad de sus datos, va a ser inevitable en esta tecnología proporcionar el control y seguridad absolutas.

El 10% no les preocupa.

Pregunta 5: ¿Aceptaría viajar en un coche automático sin conductor?

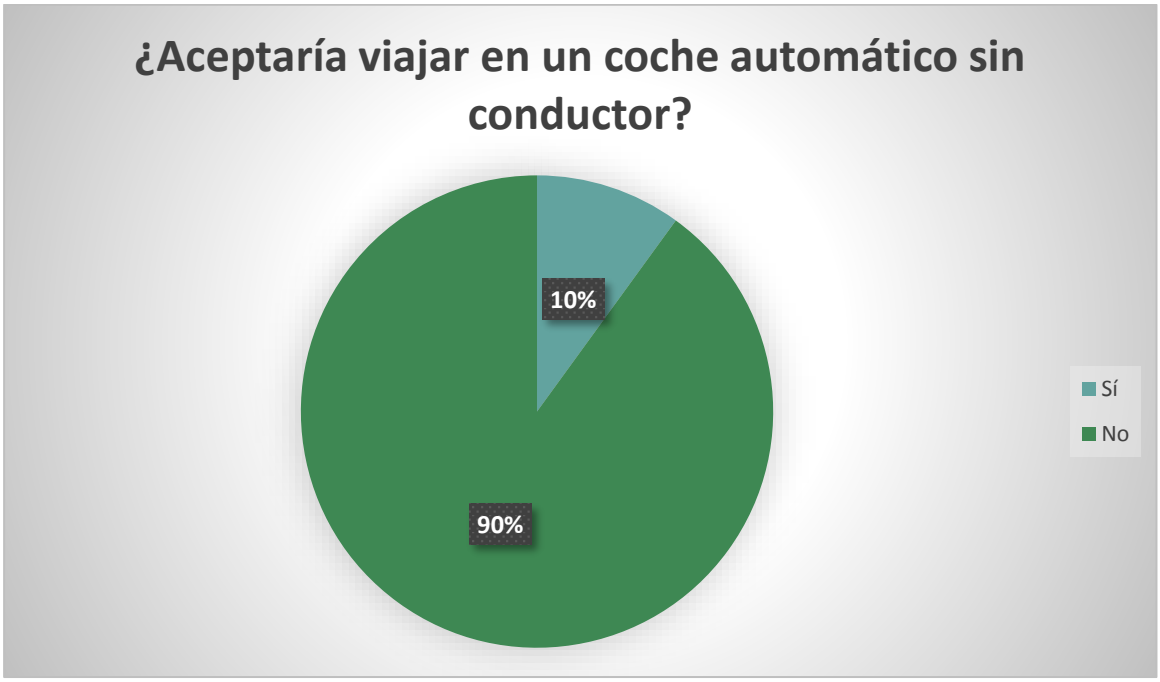

Gráfico 5.5: Pregunta 5 Encuesta

Se eligió esta aplicación de IoT para la pegunta ya que es el sector de la automoción donde más avances se están produciendo en la actualidad. Los coches automáticos son ya una realidad. El problema es que no están funcionando todo lo bien que desearían sus fabricantes y se han producido varios incidentes que se han propagado por los medios de comunicación, haciendo que los usuarios vean que aun la tecnología aún no está lista.

Es por eso que el 90% de la gente ha dicho que no. Creo que no es porque desconfíen de que algún día se pueda viajar en coches automáticos, sino que actualmente no se ven seguros debido al nivel en el que está IoT.

Pregunta 6: ¿Cree que el mundo está preparado para IoT?

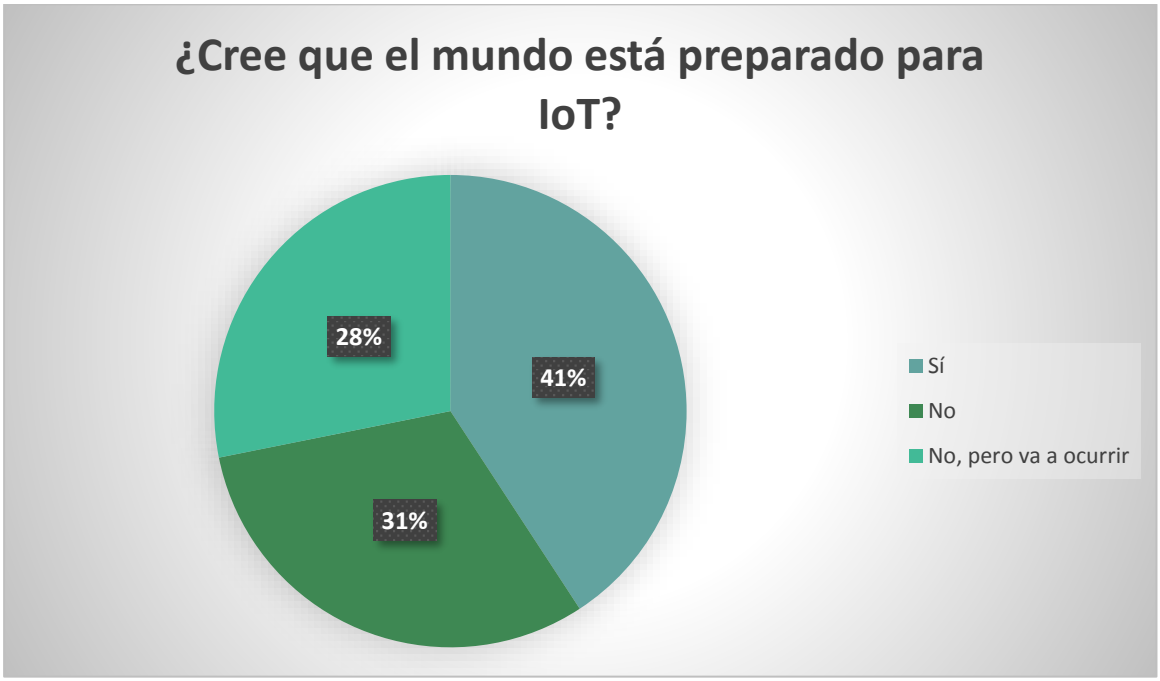

Gráfico 5.6: Pregunta 6 Encuesta

La última pregunta es para conocer si la gente cree que el mundo está preparado para la llegada de IoT. A lo largo de las páginas de este trabajo, se han ido desgranando todo lo que va a suponer la llegada a nuestras vidas la tecnología de IoT, y hemos comprobado que el cambio va a ser grande. Muy grande. En mi opinión, la equiparo, aunque en este caso en una proporción mucho mayor a la llegada de Internet. ¿El mundo estaba preparado de su llegada? Tal vez no, la gente no era consciente del cambio que suponía y no estaba “entrenada” ni tenía la cultura necesaria para poder explotar al máximo esa tecnología. En estos momentos, la gente tiene un nivel de cultura tecnológica más avanzada, pero tal vez no la necesaria.

Pienso que ocurrirá lo mismo que entonces ocurrió con Internet. Va a pasar un tiempo hasta que se pueda sacar todo el partido a esta tecnología, y estemos o no estemos preparados, va a ser inevitable que ocurra.

Un 41% ha indicado que sí está el mundo preparado, y 59% ha respondido que no. Aunque un 28% afirma que va a llegar IoT a nuestras vidas a pesar de esto.

5.2. Análisis segunda encuesta

A raíz de la primera encuesta realizada y los resultados obtenidos me vi obligado a realizar una segunda encuesta más extensa en la que preguntar directamente en la calle a algunas personas y hablar con ellas sobre IoT, volviendo a preguntarles en persona las mismas preguntas que la primera encuesta.

Los resultados de la encuesta están en el Anexo 1.

Las respuestas obtenidas han sido similares a las obtenidas a las de la primera encuesta, lo que indica que el conocimiento y la cultura de los usuarios respecto a internet en general y de internet de las cosas están muy asentadas en la sociedad en este momento actual.

Una de las respuestas interesantes ha sido los de la pregunta número 2: **Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?**

La mayoría de la gente no está demasiado preocupada por la seguridad de sus datos, pero a raíz de las respuestas obtenidas, parece que esa confianza sea infundada por el desconocimiento. Es decir, la gente cree que están totalmente protegidos por las leyes y por la propia seguridad de la tecnología y que es imposible que les ocurra nada.

En la pregunta número 5: **¿Aceptaría viajar en un coche automático sin conductor?** Se han constatado los resultados de la primera encuesta. La mayoría de la gente encuestada ha respondido negativamente debido al actual estado de la tecnología, pero casi todos insisten en que la tecnología llegará para quedarse y será muy positivo para todo el mundo.

6.Conclusión

Como se ha venido hablando durante todo este TFG, se ha querido dar a conocer el estado del arte de "el Internet de las cosas". IoT es ya una realidad que está en la vida de cada individuo. Esta manera de pensar no es nueva y se viene dando desde las primeras interconexiones con computadores, pero que cada vez más se han ido añadiendo a esta red más y más dispositivos que hasta ahora era impensable que pudieran estar conectados con otros intercambiando información.

Este TFG se ha ido centrando en la importancia de que a la par de esta evolución, debe tenerse en cuenta una evolución en la seguridad, tanto a nivel de producción como a nivel de usuario. La seguridad y privacidad de nuestros datos e información es uno de los aspectos que más preocupan a la población, así como nuestra integridad física.

En términos generales, la seguridad debe de estar centrada tanto en nuestro dispositivo (configuración, acceso, información cifrada, localización) y seguridad de la red.

A nivel empresarial, esta evolución de la tecnología también supone un importante reto debido a que el nivel de aportación en los distintos ámbitos de trabajo es incalculable, pero también, el reto consiste en controlar todas amenazas a la seguridad que conlleva.

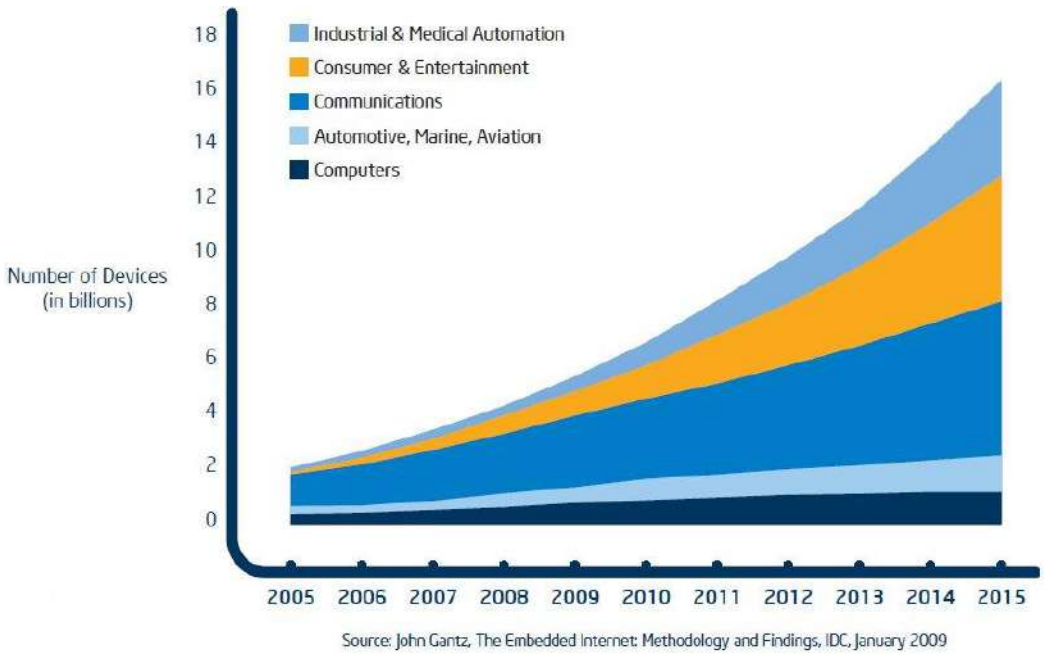

Gráfico 6.1: Evolución de dispositivos conectados

Como podemos ver en la ilustración X, hay sectores en los que esta tecnología ya está suponiendo un cambio y se está afianzando indudablemente.

Con la realización de este TFG he llegado a la conclusión de que para que esta tecnología tenga éxito en la sociedad debe de ser totalmente segura para el usuario. Y para que esto sea posible deben de participar todas las partes implicadas en el proceso desde el inicio en la fabricación como en el final y mantenimiento y uso.

Esta tecnología debe de suponer un avance no solo en el acceso y rapidez de datos, sino también un avance en la seguridad.

Partiendo de esta base, aportaré una serie de conclusiones propias:

1. Los riesgos y problemas que surgen en la seguridad relacionados con el uso y expansión de IoT no son nuevos, sino que existen desde las primeras interconexiones con computadoras. Lo que cambia es la escala en la que estos problemas y amenazas ocurren.
2. El hecho de que la interconexión de dispositivos aumente exponencialmente a medida que la tecnología se afianza en el uso cotidiano supondrá un gran tráfico de internet que afectará en gran medida a las infraestructuras que existen actualmente. Será un reto conseguir que esta tecnología se pueda afianzar en todo el mundo, incluso en países en los que aún las estructuras de acceso a internet son precarias y poco avanzadas.
3. La sociedad interconectada hasta el último extremo de la palabra no solo supondrá un cambio a nivel tecnológico sino a nivel personal de individuo, donde la mentalidad y forma de vida cambiará totalmente para adaptarse a la nueva forma de pensar, trabajar, y realizar tareas cotidianas.

Volvemos a la pregunta con la que empezamos este TFG: ¿Estamos preparados para IoT?

Tras investigar y recopilar todos los datos necesarios para la elaboración de este trabajo, mi opinión personal es un rotundo **sí**.

Un sí porque ya nos hemos enfrentado a esto antes. Es cierto que en otra medida ya que las capacidades tecnológicas en el momento que apareció Internet no eran las mismas que las actuales, pero en ese momento del tiempo, el impacto que supuso la llegada de Internet, o los ordenadores personales fue igual.

Ahora somos más conscientes de todo lo que podemos llegar a alcanzar y eso es un arma de doble filo que si somos capaces de gestionar y poner de acuerdo a todos los sectores involucrados en el proceso, conseguiremos explotar todo lo que nos puede aportar (y es mucho) Internet de las cosas en nuestra vida.

Por otra parte, como hemos visto a lo largo de todo el proyecto, IoT es una realidad, pero que avanza poco a poco y despacio, y no parece que vayan a ponerle freno las preocupaciones por la seguridad, limitaciones tecnológicas o costes.

Actualmente tal vez no sea necesario comprar un dispositivo con sensores para que abra las puertas de la casa cada vez que lleguemos, pero como todo, es un proceso, y empieza por este tipo de aplicaciones hasta llegar a dispositivos y funciones inimaginables.

Y la humanidad estará preparada cuando llegue ese momento.

7.Anexos

7.1. Anexo 1: Encuesta realizada.

En este anexo se mostrará la encuesta número 1: ¿Qué opina de Internet de las cosas?

Se ha realizado a 10 sujetos aleatorios y anónimos en la calle.

1.

Sexo: Hombre.

Edad: 23 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

No, pero imagino que será un concepto algo así como que el día de mañana todo estará en Internet y será manejable desde cualquier ordenador con acceso a Internet.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No, a día de hoy cualquiera que sepa te puede sacar lo que quiera, aunque no estén tus cosas propias en Internet, ya sea por otros contactos, por hackeo, etc. Es inevitable.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

Es la evolución normal a la que tiende el mundo, y será un cambio superpositivo para la evolución de la tecnología.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

Creo que importaría bien poco. ¿Seguridad? Pues no. ¿Beneficioso? Pues sí. Creo que, si aceptaría este concepto, más que nada por el hecho de las utilidades que se le puede sacar.

5: ¿Aceptaría viajar en un coche automático sin conductor?

Quizás con un poco más de testing... Mira el ejemplo del coche Tesla que acabo debajo de un camión.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

A día de hoy, no. Mucha mala gente con malas intenciones. Pienso que a este concepto habría que darle una vuelta para hacer que sea a la vez útil y seguro.

2.

Sexo: Hombre.

Edad: 45 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

Si. Es un conecto tecnológico en el que los objetos estarán interconectados.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No, pero porque yo sé lo que comparto y lo que no. Estoy preocupado por la poca consciencia de la gente.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

Creo que será un cambio positivo y necesario. Como la llegada de Internet.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

Sí, con mi consentimiento.

5: ¿Aceptaría viajar en un coche automático sin conductor?

Sí, cuanto antes mejor.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

No creo que el mundo esté preparado para este cambio.

3.

Sexo: Hombre.

Edad: 35 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

Sí, se trata de la interconectividad de todo tipo de dispositivos para buscar la eficiencia del uso de los mismos y elevar nuestra calidad de vida

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No, pero si soy consciente que cuantos más dispositivos se conecten a la red, más alto el riesgo de vulnerabilidad de los datos

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

Sin duda es positivo e inevitable

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

Sí, con las medidas de seguridad bien establecidas

5: ¿Aceptaría viajar en un coche automático sin conductor?

Sí, es el futuro de cómo los humanos vamos a trasladarnos en un futuro cercano.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Preparado o no va a pasar, se trata de tener la capacidad de comenzar a aceptar el cambio.

4.

Sexo: Mujer.

Edad: 34 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

Sí, aunque no estoy muy puesta en el tema.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

Sí, estoy preocupada del futuro de la privacidad

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

Es positivo, pero creo que los usuarios normales no lo vamos a poder usar ahora mismo.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

No lo acepto, pero es inevitable.

5: ¿Aceptaría viajar en un coche automático sin conductor?

Sí, siempre que tenga la opción de manejarlo automáticamente.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Creo que sí, sobre todo para temas domésticos que parece que es el sector más interesante. Aunque mucha población se va a quedar fuera de esta tecnología: Personas mayores o con menos recursos.

5.

Sexo: Mujer.

Edad: 25 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

Sí. Es la Interconexión con el mundo tecnológico.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No me preocupa mucho.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

Es un cambio positivo.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

No lo acepto.

5: ¿Aceptaría viajar en un coche automático sin conductor?

No, no me sentiría segura.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Creo que sí está preparado para el cambio, aunque queda mucho.

6.

Sexo: Mujer.

Edad: 56 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

No.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No, no uso mucho internet.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

(Después de explicarle el tema).

Supongo que sí, mientras más avances tecnológicos mejor.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

No lo acepto.

5: ¿Aceptaría viajar en un coche automático sin conductor?

No, de ninguna manera.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

El mundo se adaptará a todo.

6.

Sexo: Hombe.

Edad: 18 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

No.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No, pienso que internet es muy seguro. Tenemos muchas leyes que lo regulan.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

(Después de explicarle el tema).

Sí, el mundo evoluciona rápido y hay que adaptarse.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

No lo acepto.

5: ¿Aceptaría viajar en un coche automático sin conductor?

No. ¿Si tuviera un accidente por mal funcionamiento?

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Sí.

7.

Sexo: Hombe.

Edad: 30 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

Sí. Ahora se habla de ello prácticamente todos los días en los medios de comunicación.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

Sí, hay mucha delincuencia cibernética. Nadie está a salvo.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

Por supuesto, cualquier avance tanto científico como tecnológico es positivo siempre.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

No lo acepto.

5: ¿Aceptaría viajar en un coche automático sin conductor?

No.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Sí. Creo que es un cambio importante pero que va a tardar en ser útil creo.

8.

Sexo: Mujer.

Edad: 24 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

No.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No, uso internet a diario y nunca me ha pasado nada. Está todo muy bien regulado creo.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

(Después de explicarle el tema).

Sí, con esa tecnología podremos conseguir muchos avances en salud y ciencia.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

No lo acepto.

5: ¿Aceptaría viajar en un coche automático sin conductor?

No. Nunca confiaría en un robot creo.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Supongo. Nunca ha habido ninguna catástrofe por avanzar tecnológicamente.

9.

Sexo: Hombe.

Edad: 40 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

Sí. Es la conexión de todos los objetos con sensores que recopilan información.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

Claro que sí, si hay tanto dinero de por medio, es porque tendrá sus beneficios.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

No lo acepto.

5: ¿Aceptaría viajar en un coche automático sin conductor?

Sí, siempre que haya sido probado.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Sí. Ya ha habido otros avances importantes.

10.

Sexo: Hombe.

Edad: 23 años.

1: ¿Sabe usted qué es el "Internet de las cosas"?

Sí, sé lo que es.

2: Está preocupado actualmente por la seguridad de sus datos y su privacidad en internet?

No. Nunca me ha preocupado.

3: ¿Cree que Internet de las cosas puede suponer un cambio positivo en su vida o cree que no es necesario?

No creo que sea un cambio grande y no lo veo necesario.

4: Aceptaría y se sentiría seguro de que sus datos estuvieran al alcance de todo el mundo?

Lo acepto, pero no me sentiría seguro al 100%.

5: ¿Aceptaría viajar en un coche automático sin conductor?

No.

6: Cree que el mundo está preparado para un cambio como el que puede suponer Internet de las cosas?

Sí, como ya he dicho no creo que suponga un gran cambio.

7.2. Anexo 2: Guías para Internet de las cosas

En esta sección vamos a investigar algunas páginas que contienen guías sobre Internet de las cosas y ver qué ofrecen.

Página 1:

GSMA (http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/)

Figura: 7.1: Página inicial GSMA.

En esta sección de la página web de GSMA encontramos toda una guía para IoT. Es interesante ya que podemos descargar una guía diferente para según el ámbito en el que nos trabajemos.

Figura: 7.2: Página inicial GSMA.

Una vez hemos descargado la guía obtenemos un extenso PDF con un gran índice en el que nos habla de dispositivos móviles, dispositivos wereables, la tecnología IoT, una amplia introducción, incluso con un ejemplo sobre un dron.

En la web también podemos encontrar un blog con las últimas noticias y recursos interesantes.

Una excelente página web donde nos acercan, aunque de una forma muy técnica y no habilitada al usuario básico, pero muy completa. Solamente se encuentra en inglés.

Figura: 7.3: Página inicial GSMA.

Página 2:

Nccgroup (https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/april/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/)

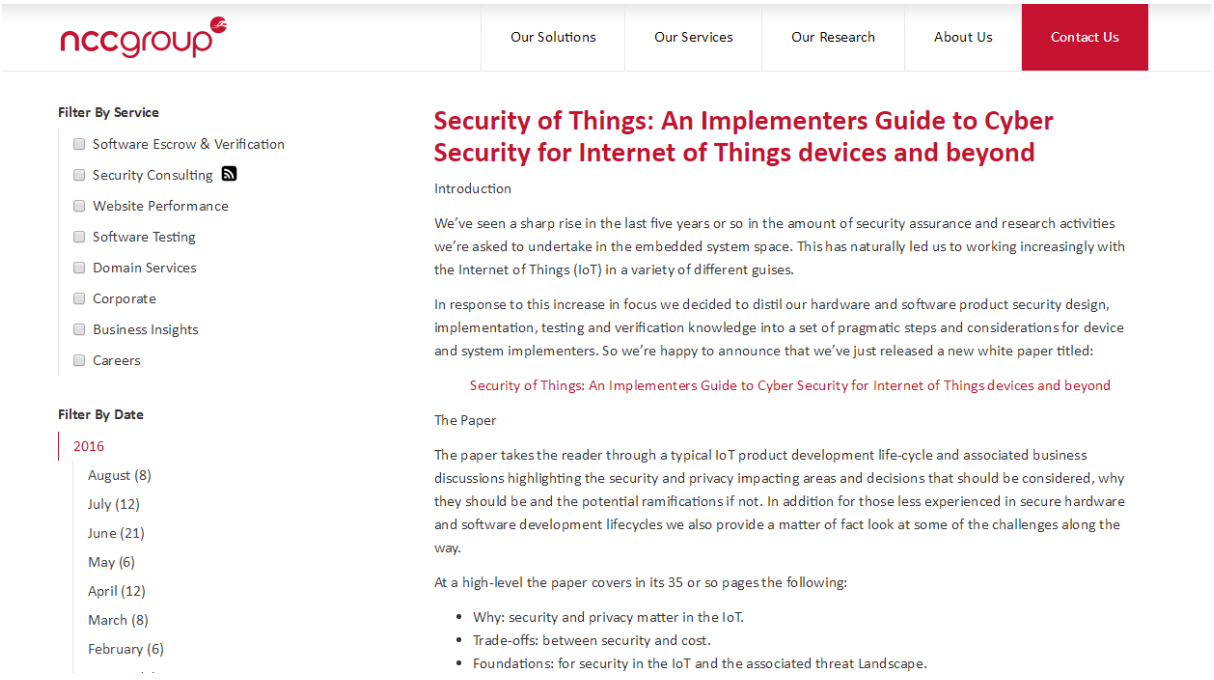

Figura: 7.4: Página inicial NCCGroup.

En esta página de NccGroup encontramos una web menos completa que la anterior sin prácticamente ninguna información adicional, con un acceso a un documento PDF con una guía de Internet de las cosas.

Lo bueno de esta página web es que la guía que nos descargamos es más específica, en concreto trata acerca de la seguridad en la ciberseguridad.

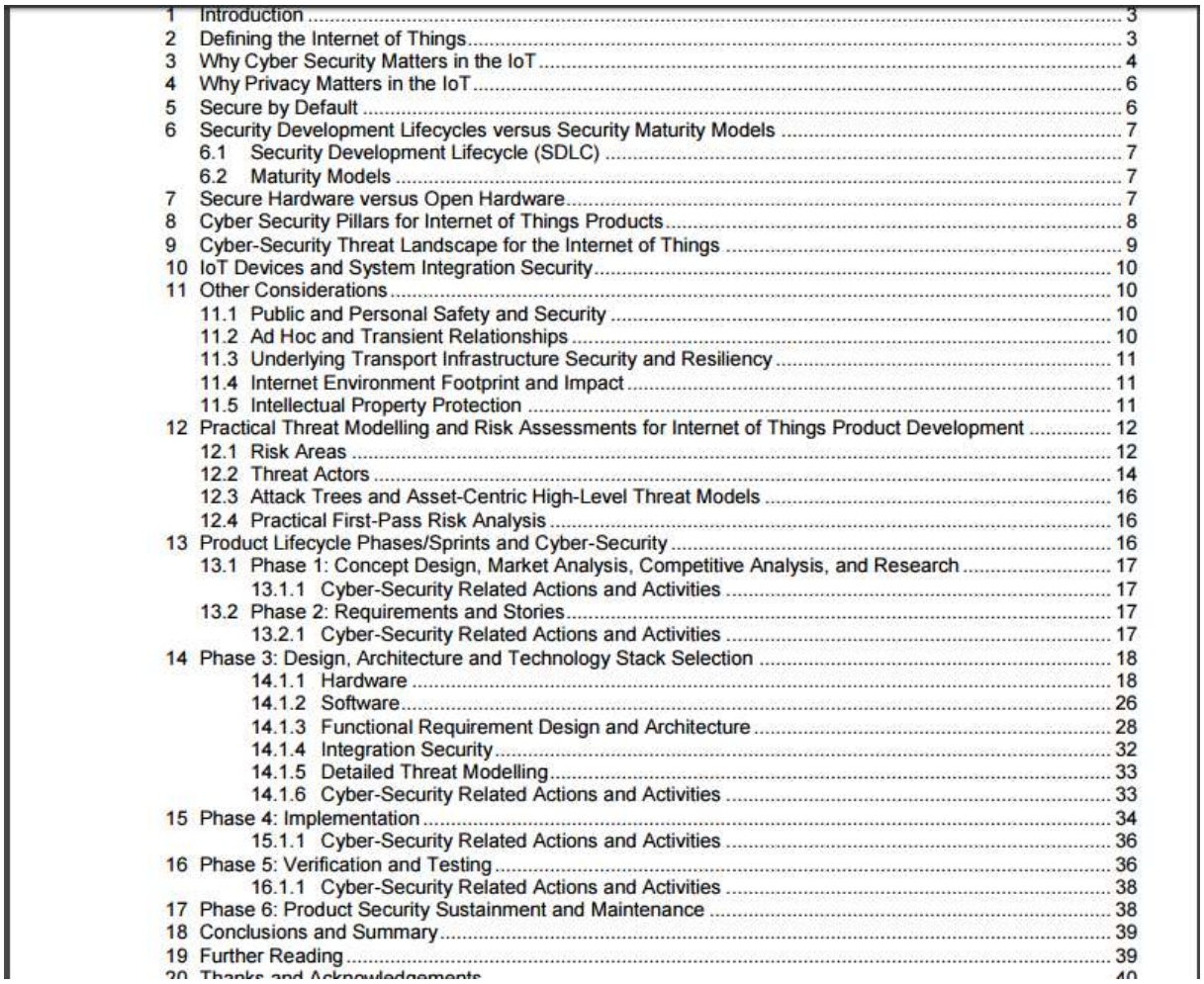

Figura: 7.5: PDF NCCGroup.

Página 3:

Recode (http://www.recode.net/2015/1/15/11557782/a-beginners-guide-to-understanding-the-internet-of-things)

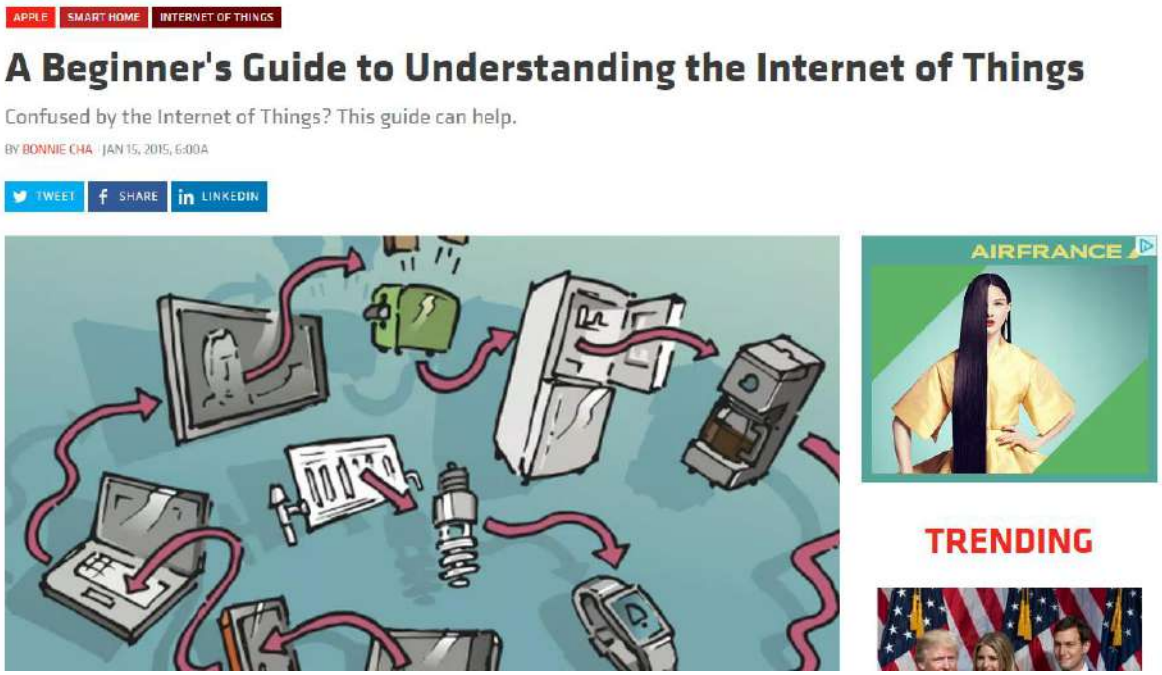

Figura: 7.6: Página inicial Recode.

Lo interesante de esta guía es que está orientada a principiantes. Aunque no está tan centrada en seguridad, explica de una forma muy sencilla entendible para todos, todo lo que significa Internet de las cosas, cómo funciona el sistema de sensores y recolección de datos, y dando consejos y conclusiones.

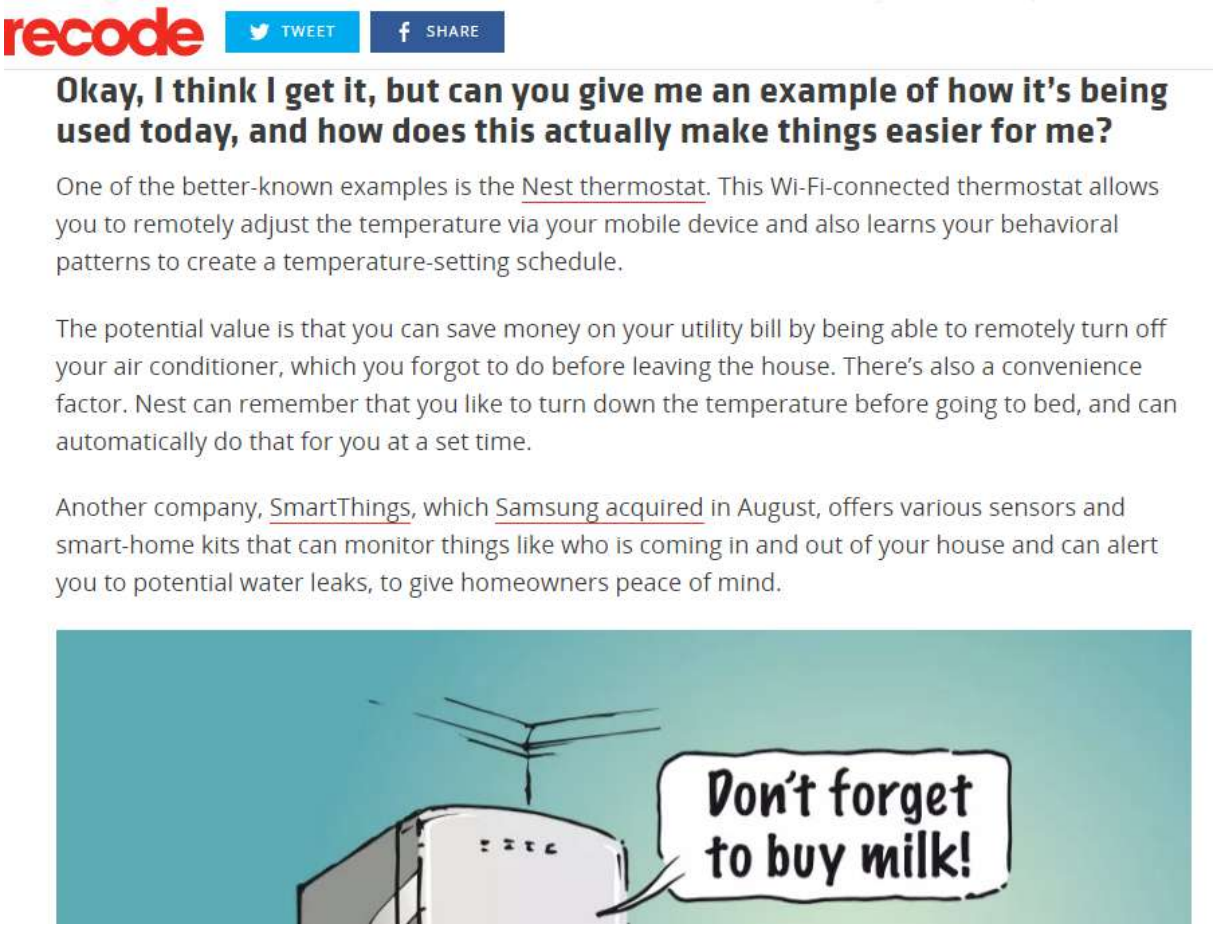

Figura: 7.7: Página inicial Recode.

Página 4:

Intel (http://www.intel.es/content/www/es/es/internet-of-things/overview.html)

En esta página de Intel, se puede leer en español una guía sobre internet de las cosas, orientado a las industrias, y usuarios habituales de tecnología.

Figura: 7.7: Página inicial Intel.

Lo interesante de estas guías es que la completan con videos explicativos. El punto negativo es que lo enfocan todo a la tecnología Intel, pero aun así es una guía muy completa respecto a Internet de las cosas y su seguridad.

Figura: 7.8: Página inicial Intel.

7: Bibliografía

[1] Internet of Things :https://club.globallogic.com.ar/la-internet-de-las-cosas-parte-1/

[2] ARPANET : https://es.wikipedia.org/wiki/ARPANET

[3] D. Mart´ınez, F. Blanes, J. Simo, and A. Crespo, "Redes de sensores y actuadores inaámbricas: Una caracterización y caso de estudio para aplicaciones médicas en espacios cerrados," Pendiente de publicación: XXIX Jornadas de Automática. Universidad Rovira i Virgili de Tarragona, España, 2008.

[4] History of Internet of things: http://www.sorayapaniagua.com/2012/04/15/un-poco-de-historia-sobre-internet-de-las-cosas/

[5] IOT: "Desde la Internet de los equipos hacia la Internet de las cosas" Friedemann Mattern y Christian Floerkemeier

[6] "Making your home 'smart', the Indian way". The *Times of India. Retrieved26 June 2015.*

[7] EMC Corporation: https://es.wikipedia.org/wiki/EMC_Corporation

[8] Mark Weiser: https://es.wikipedia.org/wiki/Mark_Weiser

[9] Jiniper Research: "El Internet de las Cosas: Consumo, Industria y Servicios Públicos" http://www.juniperresearch.com/researchstore/key-vertical-markets/internet-of-things/consumer-industrial-public-services

[10] Dispositivos conectados: http://hipertextual.com/2015/11/internet-de-las-cosas-dispositivos

[11] Moss, Jamie. "The internet of things: unlocking the marketing potential".theguardian.com. The Guardian. Retrieved 31 March 2015.

[12] Estadísticas IOT: http://www.marketingdirecto.com/actualidad/digital/2020-sera-ano-del-internet-las-cosas-numero-dispositivos-conectados-superara-los-38-millones/

[13] Estudio de previsión: http://www.ticbeat.com/tecnologias/previsiones-de-futuro-dominado-por-el-internet-de-las-cosas/

[14] "Internet of Things: The "Basket of Remotes" Problem". Monday Note. Retrieved 26 June 2015.

[15] "IoT Security Foundation – Executive Steering Board". IoT Security Foundation.

[16] Estudio previsión Gartner Symposium/ITxpo 2014 :http://www.gartner.com/newsroom/id/2905717

[17] GSMA http://www.gsma.com/aboutus/

[18] Estudio previsión beneficio Asia: http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/GSMA_PwC_Connected-life_260613.pdf

[19] Seguridad por defecto https://en.wikipedia.org/wiki/Secure_by_default

[20] Man in the middle: https://es.wikipedia.org/wiki/Ataque_Man-in-the-middle

[21] Ingeniería Social http://hipertextual.com/archivo/2012/04/que-es-la-ingenieria-social-y-como-estar-prevenidos/

[22] Recomendaciones G29 sobre IoT http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[23] INTECO recomendaciones contraseñas http://www.egov.ufsc.br/portal/sites/default/files/recomendaciones_creacion_y_uso_contrasenas.pdf

[24] VPN https://es.wikipedia.org/wiki/Red_privada_virtual

[25] Firewall https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

[26] Sistema de Detección de intrusos (IDS) https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

[27] Cloud Services https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

[28] Wize Mirror : http://www.semeoticons.eu/

[29] Green Horizont https://robotsia.com/2015/08/31/inteligencia-artificial-contaminacion-polucion-green-horizon/

[30] Alcance, escala y riesgo sin precedentes: Asegurar el Internet de las cosas_: https://www.telefonica.com/documents/23283/5538439/Telef%C3%B3nica_Security_IoT_Spanish.pdf/5137cc8e-e572-44c8-aecd-2f29f3f236be

[31] Triangulación por antenas: https://www.google.es/search?q=triangulaci%C3%B3n+telef%C3%B3nica&oq=triangulaci%C3%B3n+telef%C3%B3nica&aqs=chrome..69i57.4925j0j7&sourceid=chrome&ie=UTF-8

[32] Coche Tesla: http://www.xataka.com/automovil/asi-sera-el-tesla-para-el-gran-publico-el-model-e

[33] Moral Utilitaria: https://es.wikipedia.org/wiki/Utilitarismo

[34] Política de privacidad de Facebook https://www.facebook.com/privacy/explanation
Richard Prince https://es.wikipedia.org/wiki/Richard_Prince

[35] Eprivacidad http://www.eprivacidad.es/

[36] Arquitectura orientada a servicios: https://es.wikipedia.org/wiki/Arquitectura_orientada_a_servicios

[37] Aeropuertos inteligentes: http://tecniciencia.net/tecnologia-inteligente-revolucionara-aeropuerto-de-dubai/

[38] Satélites COMSAT http://www.astromia.com/glosario/comsat.htm

[39] Prueba de Turing http://www.elmundo.es/ciencia/2014/06/09/539589ee268e3e096c8b4584.html

[40] Adrian McEween (2013). Designing the internet of Things.

[41] Ian G Smith, The Internet of Things 2012 New Horizons, IERC - Internet of Things European Research Cluster, 2012.

[42] Internet Protocol, Version 6 (IPv6) Specification, https://www.ietf.org/rfc/rfc2460.txt, obtenido 2014.

[43] M. Karpiriski, A. Senart, V. Cahill (2006), Sensor networks for smart roads, PerCom Workshops.

[44] Changki Mo, J. Davidson (2013), Energy harvesting technologies for structural health monitoring applications IEEE Conference on Technologies for Sustainability (SusTech)

[45] S. Dey, A. Chakraborty (2012), S. Naskar, P. Misra, Smart city surveillance: Leveraging benefits of cloud data stores IEEE 37th Conference on Local Computer Networks Workshops

[46] J. Lee ; J.E. Kim ; D. Kim ; P.K. Chong ; J. Kim ; P. Jang (,2008) RFMS: Real-time Flood Monitoring System with wireless sensor networks, MASS

[48] Amazon Web Services, http://aws.amazon.com,

[49] Dave Evans (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (PDF). Cisco.

[50] Wood, Alex. "The internet of things is revolutionizing our lives, but standards are a must". theguardian.com. The Guardian.

[51] Swan, Melanie (8 November 2012). "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0". Sensor and Actuator Networks. 1 (3): 217–253.

[52] Porup, J.M. ""Internet of Things" security is hilariously broken and getting worse". Ars Technica. Condé Nast.

[53] Vongsingthong, S.; Smanchat, S. (2014). "Internet of Things: A review of applications & technologies" (PDF). Suranaree Journal of Science and Technology.

[54] E. Polycarpou, L. Lambrinos, E. Protopapadakis (2013.), Smart parking solutions for urban areas, WoWMoM,