UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM TEXCOCO

INTERNET DE LAS COSAS EMPRESARIAL; ORIGENES, EVOLUCIÓN Y TENDENCIAS.

E N S A Y O

QUE PARA OBTENER EL TÍTULO DE

LICENCIADA EN INFORMÁTICA ADMINISTRATIVA

PRESENTA

ALEJANDRA VANESSA SOTO HUERTA

DIRECTOR

M. en C. JOSUÉ VICENTE CERVANTES BAZÁN

REVISORES

Dra. MINERVA REYNA IZAGUIRRE

M. en C. YEDID ERANDINI NIÑO MEMBRILLO

TEXCOCO, ESTADO DE MÉXICO, MAYO DE 2018.

Índice

Índice de figuras

Introducción

Este ensayo habla sobre el internet de las cosas o mejor conocido como *Internet of Things* por sus siglas IoT.

En este ensayo abarque el IoT tomando en cuenta sus inicios dando a conocer quien fue el primero en mencionar al IoT como tal, mostrando una línea del tiempo, hasta lo que es ahora.

Las interrigantes que tiene este tema son: ¿cómo es el IoT en la actualidad?, ¿Qué es? ¿Cómo surge? ¿Cuáles son los beneficios que tiene el IoT? Y ¿cómo ha ayudado a facilitar actividades a las empresas? ¿Qué ventajas tiene?

Este ensayo tiene como objetivo principal presentar en términos sencillos y claros una compilación de los datos más relevantes acerca del internet de las cosas, considerada como la nueva tendencia del siglo XXI, para lo cual primeramente se abordarán los antecedentes del término, la primera persona que lo planteó, su desarrollo y evolución hasta la actualidad.

El concepto que tengo sobre el IoT es, red de objetos físicos –vehículos, máquinas, electrodomésticos y más– que utiliza sensores y API para conectarse e intercambiar datos por internet.

Capítulo I: Fundamentos que dan origen a la tecnología Internet de las Cosas

El internet de las cosas tiene sus inicios en el año de 1991, con Mark Weiser, quien escribió un artículo para la revista Scientific American titulado “El computador del siglo XXI”, donde se destaca una imagen que muestra en aquel entonces el desarrollo de ya tres dispositivos que posteriormente se tecnificarían para ser de uso mucho más común, como lo son una pantalla o televisor gigante, una tableta monocromática- en verde y negro- y un monitor individual observado por Weiser.

Sin embargo la idea de Weiser no era la creación de este nuevo concepto, sino más bien era la predicción que se utilizaría en el próximo siglo en las oficinas o puestos de trabajo del futuro dentro de las organizaciones, con el fin de economizar recursos y emplear los nuevos de una manera mucho más eficiente, sobre todo considerando que este grupo de científicos de Xerox en Palo Alto en 1991 ya eran responsables de los tabs (reemplazo al post-it) y de los pads (reemplazando a una libreta u hoja de papel) para uso comunitario. Mark Weiser bautizó a la relación entre el entorno humano y las máquinas como computación ubicua que representaba un concepto completamente diferente a la inteligencia artificial o a la realidad virtual, ya que lo que se quería conceptualizar a través del término era la incrustación de la computación en el diario vivir de las personas. Weiser murió en 1999 sin tener conciencia del aporte que realizó dentro del campo del internet, ya que gracias a dicha fotografía y a la consolidación de sus invenciones en el mismo año Kevin Ashton, investigador del Instituto Tecnológico de Massachusetts, acuña por primera vez y de manera formal el término de internet de las cosas, utilizándolo dentro del contexto del manejo de la cadena de suministros. Ashton también trabajaba en la realización de investigaciones relacionadas con la radio frecuencia o por su nombre en inglés conocido como radio frecuency identification.

El origen de los objetos conectados no es algo de hace pocas décadas, en realidad se remonta hasta los albores tecnológicos del siglo XIX, en lo que se consideran los primeros experimentos de telemetría de la historia. El primero del que se tiene constancia fue el llevado a cabo en 1874 por científicos franceses. Estos instalaron dispositivos de información meteorológica y de profundidad de nieve en la cima del *Mont Blanc*. A través de un enlace de radio de onda corta, los datos eran transmitidos a París. Otros experimentos, ya en el siglo XX, se realizaron desde iniciativas originadas en países como Rusia o Estados Unidos, ayudando al crecimiento de la telemetría y llevándola a un uso extensivo impulsado por la evolución de distintas tecnologías de telecomunicación.

La idea de poder conectar los objetos y de que éstos fuesen inteligentes ya se plasmó en aquella época en los pensamientos y escritos de científicos tan notables como Nikola Tesla o Alan Turing. Sus palabras, leídas desde una perspectiva histórica, cobran ahora sentido y demuestran cuan adelantados a su tiempo fueron. (Cendón, 2017)

El internet de las cosas surgió entre 2008 y 2009 como un simple momento en el tiempo en el que eran más las cosas conectadas a internet que las personas, según *Cisco Internet Business Solutions Group* (IBSG). (SorayaPaniagua, 2012)

En 2008 un grupo de empresas se unieron para crear la *IPSO Alliance*[1] con el objetivo de promover el uso del protocolo de internet en redes de objetos inteligentes y hacer posible el IoT. (SorayaPaniagua, 2012)

En 2011 se crea la iniciativa IoT-GSI *Global Standards* [2]para promover la adopción de estándares para IoT a escala global. China continúa invirtiendo e impulsando el

[1] IPSO Alliance es un foro global que abarca una membresía internacional diversificada, centrada

[2] IoT-GSI tenía como objetivo promover un enfoque unificado en el UIT-T para el desarrollo de normas técnicas (Recomendaciones) que permitan la Internet de las cosas a escala mundial.

desarrollo y la investigación en Internet de las Cosas con instituciones como *Shanghai Institute* o la *Chinese Academy of Sciences* (SorayaPaniagua, 2012).

En 2012 ya había 8.700 millones de dispositivos conectados. Durante este año se espera la verdadera explosión de *Internet of Things*. De ahí a los 26.000 millones -50.000 millones prevén en la imagen- que se esperan para 2020, hay un paso de futuro.

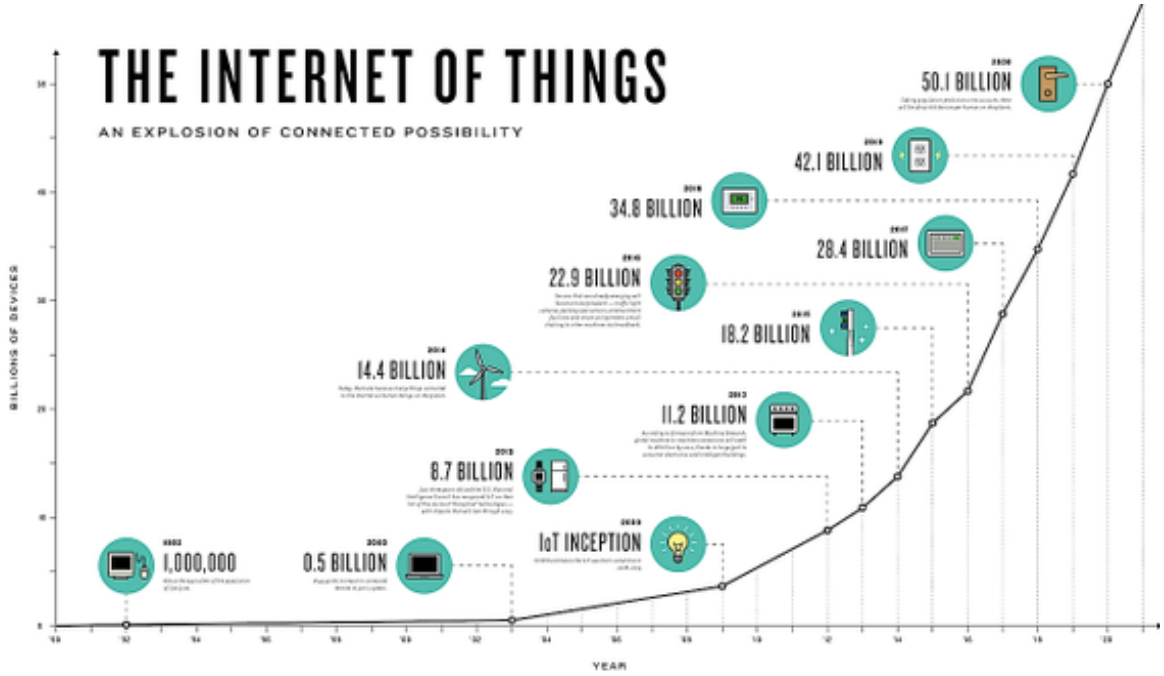

Figura 1 Cisco predice 50 mil millones de cosas conectadas al Internet de las cosas (IoT) para 2020 (Grail, 2017)

Historia cronológica del IoT

- **1949**: Se inventa el código de barras (que posteriormente evolucionaría para su uso en supermercados).
- **1960**: Morton Heilig recibe la patente para el primer dispositivo montado en la cabeza (*head-up wearable*).
- **1969**: El primer gran momento, se envía el primer mensaje a través de ARPANET (el precursor de internet).
- **1973**: Se otorga la primera patente para un lector/escritor RFID pasivo.
- **1980**: Miembros del departamento de Ciencias de Computación de CarnegieMellon consiguen instalar *micro-switches* en una máquina de venta de refrescos y conectarla al ordenador del departamento para poder comprobar desde la terminal el número de botellas que quedan y si están frías o no.
- **1990**: Olivetti desarrolla un sistema de localización mediante etiquetas e infrarojos que permite comunicar la posición de una persona dentro de un edificio a un centro de control.
- **1993**: Un proyecto de la universidad de Columbia denominado KARMA diseña un head-up de realidad aumentada con capacidad de sobreponer los planos y las instrucciones de mantenimiento a los objetos.
- **1994**: Steve Mann desarrolla la primera webcam inalámbrica y equipable.

- **1995**: Siemens establece un departamento dedicado dentro de su negocio de teléfonos móviles para desarrollar y lanzar un módulo *Global System for Mobile comunications* (GSM)[3] para aplicaciones máquina a máquina (*machine-to-machine* M2M).
- **1997**: Tiene lugar en Cambridge (USA) el primer simposio internacional del IEEE sobre "*wearable computers*".
- **1999**: Kevin Ashton hace referencia por primera vez al término "IoT"en una presentación para *P&G*.
- **2000**: LG anuncia su primera nevera conectada a Internet.
- **2003-2004**: El termino IoT es ampliamente usado en publicaciones de primer orden.
- **2005**: La Unión Internacional de Telecomunicaciones (UIT) publica su primer informe sobre IoT.
- **2005**: Nace Arduino, una plataforma fácil de usar y de bajo coste para desarrollo de aplicaciones.
- **2006-2008**: IoT recibe reconocimiento por parte de EU.
- **2008-2009**: Nace finalmente IoT al superar el número de dispositivos conectados al número de seres humanos. (Valle, 2014)

[3] Es un estándar de comunicación para la telefonía móvil, implementado mediante la combinación de satélites y antenas terrestres

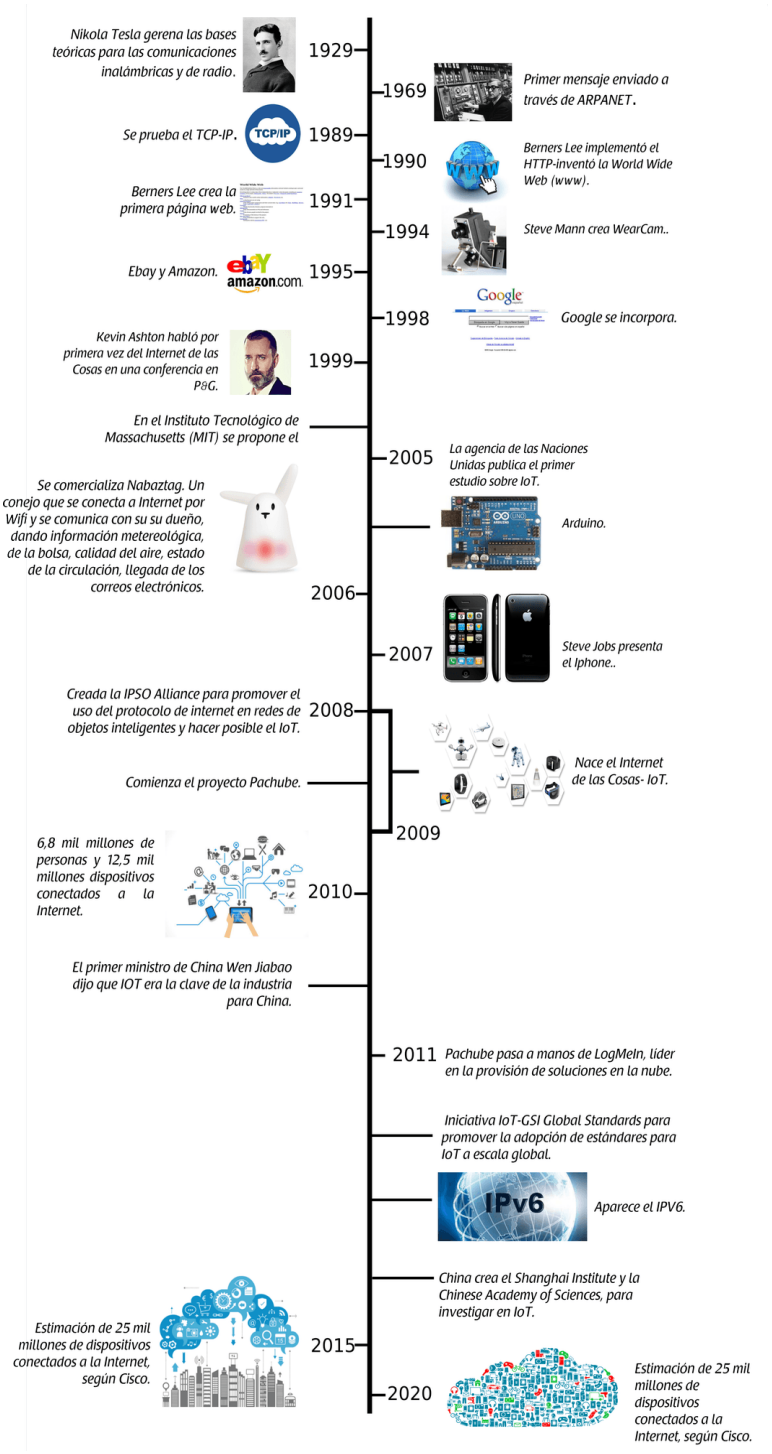

Figura 2 Infografía donde se observa los desarrollos que permitieron llegar al IoT y hacia donde apunta la creación de objetos del IoT (López N. , 2014)

Capítulo II: El internet de las cosas en la actualidad

Antes de analizar el estado actual de IoT, es importante ponerse de acuerdo en una definición. Según el Grupo de soluciones empresariales basadas en Internet (IBSG, *Internet Business Solutions Group*) de Cisco, IoT es sencillamente el punto en el tiempo en el que se conectaron a Internet más “cosas u objetos” que personas.

En 2003, había aproximadamente 6,3 mil millones de personas en el planeta, y había 500 millones de dispositivos conectados a Internet. Si dividimos la cantidad de dispositivos conectados por la población mundial, el resultado indica que había menos de un dispositivo (0,08) por persona. De acuerdo con la definición de Cisco IBSG, IoT aún no existía en 2003 porque la cantidad de cosas conectadas era relativamente escasa, dado que apenas comenzada la invasión de los dispositivos omnipresentes, como los *smartphones*. Por ejemplo, el Director General de Apple, Steve Jobs, no presentó el iPhone sino hasta el 9 de enero de 2007 en la conferencia *Macworld*. El crecimiento explosivo de los *smartphones* y las *tablet* PC elevó a 12,5 mil millones en 2010 la cantidad de dispositivos conectados a Internet, en tanto que la población mundial aumentó a 6,8 mil millones, por lo que el número de dispositivos conectados por persona es superior a 1 (1,84 para ser exactos) por primera vez en la historia. (Evans, 2011)

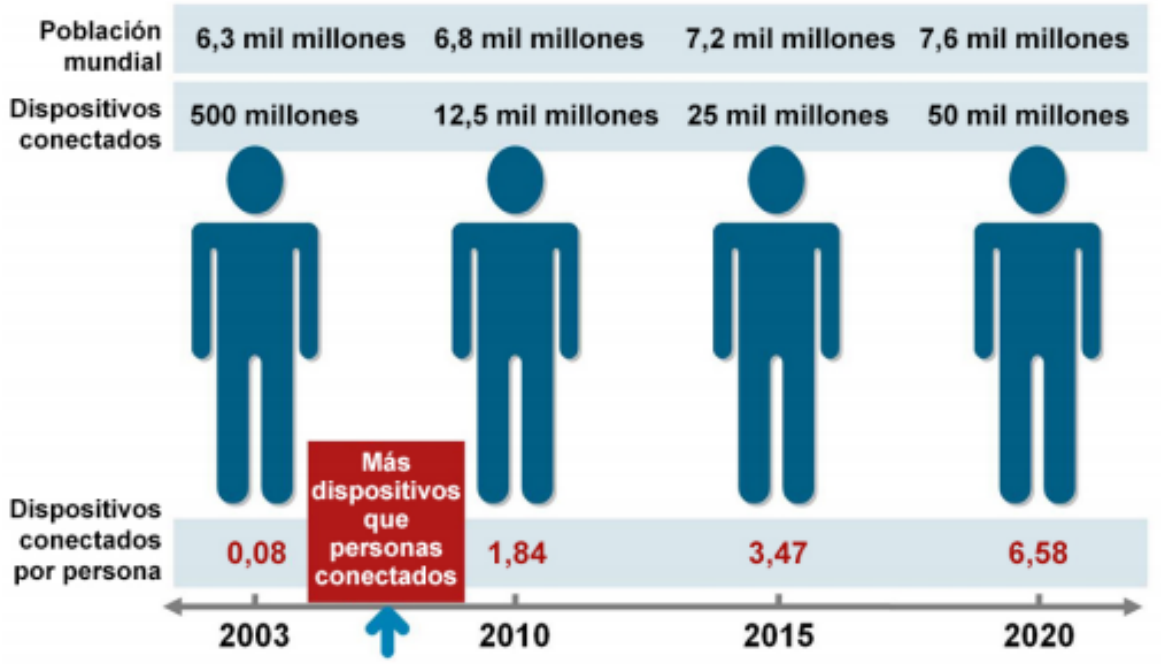

Figura 3 Internet de las cosas "nació" entre los años 2008 y 2009 (Evans, 2011)

En la actualidad, el internet de las cosas ha tenido un gran avance, a tal grado de volverse una necesidad. Como, por ejemplo: unos tenis para correr los cuales se sincronicen con el dispositivo móvil y te da la distancia que recorres, las calorías que quemaste, etc.

Tomando en cuenta esto, las grandes empresas, así como las micro, pequeñas y medianas empresas (PYMES), apuntan para ser favorecidas por el IoT de tal forma que durante este año será uno de los ejes en los que se trabajará por parte de compañías. Sin ir muy lejos, recientemente en el CES 2016 (*Consumer Technology Association*) celebrado en Las Vegas (EEUU) se presentaron todo tipo de aparatos relacionados con IoT, desde autos y motos, sistemas de audio, televisores y heladeras que manejan la casa, closets y cerraduras inteligentes, además los precursores *wearables*. (Genexus, 2016)

Por lo cual las empresas tomaron el desafío de llevar aquellas tecnologías con las que cuentan al siguiente nivel, evolucionarlas y adaptarlas con software o programas óptimos para ser parte de este proceso; pues uno de los principales retos que se espera a partir de este año será la competición de las empresas para moldearse al nuevo mercado que se está formado a través del IoT.

La arquitectura del IoT

La arquitectura debe permitir que la tecnología sea distribuida, donde los objetos puedan interactuar entre ellos, escalable, eficiente y segura, también tiene que ser capaz de mostrar todos los componentes como un único sistema a los ojos de los usuarios y desarrolladores**.**

Están basadas en la nube conectan los mundos reales y virtuales. Ayudan a las empresas a gestionar la seguridad y la conectividad de los dispositivos IoT, así como a recolectar datos de dispositivos, vincular dispositivos con sistemas backend, asegurar la interoperabilidad IoT y construir y operar aplicaciones IoT.

Los dispositivos del IoT siguen un proceso por el cual la información fluye del medio físico a un medio virtual. Este proceso lo podemos dividir en cuatro fases según la arquitectura propuesta por Sumit Sharma de MuleSoft, empresa creada en el 2006 y centrada en la creación de software para conectar aplicaciones, fuentes de datos y APIs.

Figura 4 Proceso por el cual la información fluye del medio físico a un medio virtual (Hernández, 2018)

Arquitectura escalable: El IoT necesita de una arquitectura que permita la escalabilidad, es decir, que de lo mismo que hoy se conecten 10.000 mañana 1.000.000 de dispositivos.

Arquitectura de referencia

Los proveedores de plataformas de IoT y los asociados de investigación colaboran a través de estas iniciativas para definir arquitecturas de referencia de IoT. Las arquitecturas de referencia actúan como cimientos arquitectónicos, describiendo los bloques de construcción de alto nivel que se utilizan dentro de las soluciones de IoT y estableciendo una terminología compartida para los principales conceptos arquitectónicos. Estas iniciativas aprovechan una amplia variedad de soluciones existentes para destacar patrones de diseños efectivos y mejores prácticas.
Algunas arquitecturas de referencia de IoT con extensas referencias incluyen:

- Internet de las Cosas – Architectura (IoT-A): El modelo y la arquitectura de preferencias de IoT-A se desarrollaron en 2013 a través de un proyecto insignia de la UE. El IoT-A se diseñó para ser construido con la finalidad de desarrollar arquitecturas concretas que son aplicables en variedad de dominios.
- IEEE P2413 - Estándar para una Infraestructura Arquitectónica para el Internet de las Cosas (IoT): Este proyecto de estandarización continua de IEEE tiene el objetivo de identificar semejanzas entre los dominios de IoT, inclusos la fabricación, los edificios inteligentes, las ciudades inteligentes, los sistemas de transporte inteligentes, la red eléctrica inteligente y el cuidado de la salud.
- Arquitectura de Referencia de Internet Industrial (IIRA): Industrial Internet Consortium, que fue fundado en marzo de 2014 por AT&T, Cisco, General Electric, IBM e Intel, desarrolló específicamente el IIRA para aplicaciones de IoT industriales

  Para desarrollar soluciones de IoT se pueden utilizar arquitecturas de referencia como plantillas. Las arquitecturas enumeradas anteriormente describen los componentes de la arquitectura de IoT y sus funciones en términos de alto nivel, pero se pueden concretar aún más correlacionando requisitos abstractos con tecnologías específicas o con pilas tecnológicas.

Integración, automatización y análisis de datos de IoT

Para aprovechar la amplia gama de datos generados por IoT, las organizaciones deben superar los tres retos clave que resaltan nuestros encuestados:

- Integración de datos de varias fuentes
- Automatización de la recopilación de datos
- Análisis de datos para detectar eficazmente la información práctica

El único modo que tienen las organizaciones para transformar datos sin procesar en información práctica es responder a estos tres desafíos.

Integración de datos de varias fuentes

En la mayoría de los casos prácticos de IoT, los datos deben recopilarse e integrarse antes de su proceso y análisis. La dispersión y la variedad sin precedentes de los dispositivos y datos actuales implica que la integración de datos es un obstáculo mayor que nunca. Las organizaciones deben tener en cuenta varios factores, incluida la instalación física de los dispositivos, mejores estándares de comunicación, el modo de administrar diversos tipos de datos (p. ej., vídeo y datos de geolocalización) y cómo integrar eficazmente los datos de IoT con datos de otras fuentes, como proveedores de datos de terceros de la nube, así como almacenes de datos internos históricos.

Las organizaciones empiezan a depender de la virtualización para integrar datos muy dispersos. La virtualización de datos logra que un conjunto heterogéneo de fuentes de datos se asemeje a una red troncal de gestión para usuarios y aplicaciones. Estas fuentes de datos no tienen por qué almacenarse localmente: pueden estar en cualquier lugar. Esto es especialmente valioso para una aplicación de IoT que dependa de datos de numerosas fuentes dispersas, como sensores integrados, cámaras de vídeo y fuentes de datos de terceros.

Automatización de la recopilación de datos

Después de recopilar e integrar datos de IoT, las organizaciones se enfrentan al reto de llevar los datos al lugar adecuado en el momento justo para su análisis. Esto incluye evaluar los datos para determinar si deben moverse o analizarse donde se encuentren, en el “perímetro” de la red (“mover los análisis a los datos”).

En la “informática perimetral”, por tanto, las aplicaciones, datos y servicios se insertan en el perímetro lógico de una red (alejados del centro) para propiciar el análisis y la generación de conocimiento en la fuente de los datos.

Es importante tener en cuenta lo siguiente cuando se trata de automatización de datos e IoT:

- Requisitos de rendimiento de la aplicación de IoT: ¿Hay algún requisito de baja latencia que afecte a los datos que deben procesarse? En determinados casos prácticos de IoT donde la baja latencia puede ser un requisito (p. ej., juegos o seguridad).
- Oportunidades de preprocesamiento de datos: En muchos casos, no sería apropiado transmitir todos los datos generados por una solución de IoT a la nube para su procesamiento. Puede tener sentido procesar o comprimir los datos de IoT antes de transmitirlos a la nube, o transmitir únicamente algunos datos seleccionados (p. ej., anomalías, excepciones o promedios).
- Aplicaciones de IoT muy dispersas: Algunas aplicaciones de IoT (p. ej., supervisión de flujos de trabajo, plataformas petrolíferas conectadas o redes inteligentes) pueden conllevar un alto grado de dispersión, de modo que el procesamiento perimetral se vuelve más interesante

Anatomía de un dispositivo IoT

Los objetos conectados que forman y formarán parte de la inmensa red de comunicación en la que se convertirá Internet de las Cosas, tienen una serie de características técnicas comunes entre todos ellos.

Básicamente, cualquier objeto conectado debe de integrar un pequeño sistema (aquí el tamaño es importante), formado por un sensor y/o actuador, un dispositivo de comunicación, alguna fuente de energía y además, debe de estar dotado con cierta inteligencia computacional, para lo cual se suele utilizar algún microcontrolador en la mayoría de los casos.

Antes de nada, conviene aclarar que el concepto de objeto en el mundillo de Internet de las Cosas está un poco difuso aún, y por tanto se debe utilizar en toda su amplitud. Puede tratarse tanto de tu futura cafetera conectada a la red, que

empezará hacerte el desayuno en cuanto suene tu despertador, hasta el reloj inteligente desde el que podrás controlar todas tus constantes vitales y enviárselas al médico de forma remota. Pero también se habla de objetos para definir todo dispositivo que forma parte de una aplicación de Internet de las Cosas pero que no tiene la apariencia de un objeto cotidiano y de uso reconocible.

Hardware del dispositivo de IoT

Para entender lo que está en el corazón de un dispositivo de IoT tenemos que entender las principales características del hardware concerniente que hace que los dispositivos de IoT funcionen:

- Adquisición y control de datos
- Procesamiento y almacenamiento de datos

Esencialmente, los dispositivos de IoT contienen*sensores*, *accionadores*, o ambos. Los sensores adquieren datos y los accionadores controlan los datos o actúan con base a ellos.

- **Los sensores** supervisan Cosas y brindan datos acerca de la Cosa, puede ser la temperatura, la intensidad de la luz o el nivel de batería.
- **Los accionadores** controlan la Cosa a través del hardware del dispositivo, como los controles de un termostato inteligente, el interruptor de regulación de intensidad de una bombilla inteligente o los motores reductores de una aspiradora robótica. Los accionadores representan la interfaz física hacia la Cosa que la hacen "funcionar", ya sea encender la calefacción, atenuar las luces o enviar la aspiradora robótica a su estación de carga.

Todos los dispositivos de IoT tienen una forma de procesar los datos, de almacenar esos datos localmente (si es necesario) y de brindar potencia de computación que haga que el dispositivo funcione.

Si es necesario que se coordinen los datos de varios sensores, o si los datos tienen que almacenarse en una memoria flash (por cualquier razón), esto lo realiza el componente que procesa datos del dispositivo de IoT.

Capítulo III: La evolución del internet de las cosas en las empresas

Por comparación, Internet ha seguido una ruta sostenida de desarrollo y mejora, pero podría decirse que no ha cambiado mucho. Básicamente sigue conservando el propósito para el que fue diseñada durante la era de ARPANET. Por ejemplo, en los comienzos había varios protocolos de comunicación como *AppleTalk*, *Token Ring* e IP. En la actualidad, Internet está estandarizada en gran medida con IP.

En este contexto, IoT adquiere gran importancia porque se trata de la primera evolución real de Internet (un salto que conducirá a aplicaciones revolucionarias con el potencial de mejorar drásticamente la manera en que las personas viven, aprenden, trabajan y se entretienen). IoT ya ha logrado que Internet sea sensorial (temperatura, presión, vibración, luz, humedad, estrés), lo que nos permite ser más proactivos y menos reactivos.

Además, Internet se expande hacia lugares que, hasta el momento, eran inalcanzables. Los pacientes ingieren dispositivos de Internet que ingresan a su cuerpo para ayudar a los médicos a diagnosticar y determinar las causas de ciertas enfermedades. Es posible colocar sensores pequeñísimos en plantas, animales y fenómenos geológicos y conectarlos a Internet.

En el otro extremo del espectro, Internet viaja al espacio por medio del programa *Internet Routing in Space* (IRIS) de Cisco.

En el 2015 alrededor de 10 mil millones de dispositivos se conectaron a Internet, mientras que para el 2020 se espera que habrá 34 mil millones de dispositivos, de los cuales se estima 24 mil millones representarán al ecosistema IoT. (Genexus, 2016)

Se espera que en los próximos cinco años se invierta a nivel mundial 6 billones de dólares destinados para dar soluciones para el IoT, principalmente para el desarrollo de aplicaciones, hardware para los dispositivos, integración de

sistemas, almacenamiento de datos, seguridad y conectividad. Las empresas serán quienes adopten mayoritariamente esta tecnología, seguido de los gobiernos y de los mismos consumidores, rescata el informe de *Business Insider*.

En este rubro, las compañías contemplarán tres formas para mejorar los negocios: a través de la reducción de los costos de operación, el aumento de la productividad y con la expansión a nuevos mercados o el desarrollo de nuevas ofertas de productos.

Según Cisco, ya hay cuatro mil millones de dispositivos conectados y en 2020 se alcanzarán los 200 mil millones, llegando a tener más de 26 dispositivos conectados por individuo (según Intel). (The Digital Business News, 2016)

En este entorno cambiante pero cada vez más conectado, el internet de las cosas se revela como la tendencia que no sólo fomentará las integraciones, sino que descubrirá las aplicaciones que los dispositivos conectados tendrán en el mundo de la empresa y los negocios. En el mismo sentido, el conocimiento requerido dará lugar a la creación de nuevos puestos de trabajo e inevitablemente al fin de otros. (The Digital Business News, 2016)

La principal virtud de los dispositivos conectados es que generan un gran conocimiento del individuo en función de sus hábitos, son capaces de registrar sus rutinas para personalizar cada función y herramienta e incluso predecir su futuro comportamiento. (The Digital Business News, 2016)

Con las nuevas posibilidades de conocimiento del usuario, las marcas modificarán muchos de sus procesos. Por ejemplo, los servicios de atención al cliente serán, gracias a la información que acumulen de cada cliente, totalmente dirigidos, de tal forma que estarán informados de cualquier problema en un servicio antes incluso de que se les comunique. (The Digital Business News, 2016)

Todos estos cambios van a modificar la forma de relacionarnos, de consumir y de trabajar. El IoT tendrá una implementación en todos los sectores de negocio, pero será más llamativa y probablemente más novedosa en *smart cities, health & fitness*, logística y distribución, *retail* y banca, automoción, hogar conectado y *work space*. Las oportunidades de negocio que el IoT generará en estos sectores, conformarán el panorama económico futuro. (The Digital Business News, 2016)

"Con mil billones de sensores incorporados en el entorno, todo conectado por sistemas de computación, software y servicios, será posible escuchar el latido de la Tierra al producirse el impacto entre la humanidad y el planeta tan profundo como cuando la aparición de Internet revolucionó la comunicación". (Hartwell, 2014)

Según indica el último *Mobility Report*[4] de la multinacional sueca, durante 2018 el número de dispositivos conectados superará al de teléfonos móviles; además, en 2021 habrá algo más de un teléfono móvil por persona. De modo que, con una población mundial estimada de 7,7 millones, los teléfonos móviles serán unos 8,6 millones. (Datagora, 2016)

En opinión de la multinacional sueca, entre 2015 y 2021, los dispositivos conectados crecerán un 23% anual, y la mayor tasa de incremento será para el Internet de las Cosas (IoT): del total de 28.000 millones de dispositivos en 2021, cerca de 16.000 millones serán IoT. Europa Occidental quien liderará las nuevas conexiones IoT en este mercado, donde se estima que los dispositivos crecerán hasta un 400% en 2021, sobre todo por las nuevas disposiciones regulatorias

[4] Es uno de los principales análisis sobre datos de previsiones, análisis y perspectivas sobre tráfico móvil, suscripciones y comportamiento de usuarios, lo que le permite aportar una visión global sobre tráfico actual y tendencias de mercado en la actual Sociedad Conectada.

relativas a contadores inteligentes y la creciente demanda de coches conectados, incluyendo la directiva *e-call* de la UE, prevista para 2018. (Datagora, 2016)

Conectividad y comunicación

La gestión de la conectividad y de la comunicación bidireccional entre los dispositivos, entre dispositivos y *gateways*, y entre *gateways* y servicios en la nube y aplicaciones es otra de las principales capacidades que a menudo se describen dentro de las arquitecturas de referencia de IoT. Las arquitecturas basadas en eventos son una buena elección para *edge computing*, ya que la comunicación entre dispositivos y servicios utiliza protocolos de comunicación/suscripción e intermediarios de mensajes.

Como bien sabemos los seres humanos evolucionan han evolucionado gracias a la comunicación, por ejemplo, después de descubrir, aprender o conocer algo que los seres humanos desconocen, es compartido, por lo que ya no hacía falta redescubrirlo: solo había que comunicarlo. Un ejemplo más moderno sería el descubrimiento de la estructura helicoidal del ADN, moléculas que transportan información genética de una generación a la siguiente.

Una vez que el artículo de James Watson y Francis Crick apareció en una publicación científica en abril de 1953, las disciplinas de la medicina y la genética pudieron tomar esta información y avanzar desde allí a pasos agigantados. Este principio de compartir información y aprovechar los descubrimientos se puede comprender mejor si se analiza la manera en que los seres humanos procesan los datos. Desde la base hasta la cúspide, las capas de la pirámide incluyen datos, información, conocimiento y sabiduría. Los datos representan la materia prima que se procesa para obtener información. Los datos individuales por sí mismos no son muy útiles, pero en volúmenes permiten identificar tendencias y patrones. Esta y otras fuentes de información se unen para conformar el conocimiento. En su sentido más básico, el conocimiento es la información de la que alguien es

consciente. Luego, la sabiduría nace de la combinación de conocimiento y experiencia. En tanto que el conocimiento cambia con el tiempo, la sabiduría es atemporal, y todo comienza con la adquisición de datos. (Evans, 2011)

Figura 5 Los seres humanos convierten los datos en sabiduría (Evans, 2011)

También resulta importante destacar que existe una correlación directa entre la entrada (datos) y la salida (sabiduría). Cuántos más datos se generan, más conocimiento y sabiduría pueden obtener las personas. IoT aumenta drásticamente la cantidad de datos que están disponibles para que los procesemos. Este aumento, combinado con la capacidad de Internet de comunicar estos datos, hará posible que las personas avancen aún más. (Evans, 2011)

IoT: imprescindible para el progreso de los seres humanos

A medida que sigue aumentando la población del planeta, se torna cada vez más importante que las personas se conviertan en guardianes de la Tierra y sus recursos. Además, las personas desean vidas saludables, plenas y confortables para sí mismas, sus familias y las personas que quieren. Si se combina la capacidad de la próxima evolución de Internet (IoT) para percibir, recolectar, transmitir, analizar y distribuir datos a escala masiva con la manera en que las

personas procesan la información, la humanidad tendrá el conocimiento y la sabiduría necesarios no solo para sobrevivir sino para mejorar y prosperar en los próximos meses, años, décadas y siglos. (Evans, 2011)

Tomando en cuenta el auge que el IoT está teniendo en el mercado global, se mostrará una infografía del crecimiento del IoT y sus proyecciones para los próximos años.

Por lo que podemos ver el IoT nos hará la vida más sencilla, por ejemplo, al haber casas inteligentes, con las que por medio de tu dispositivo móvil podrás prender la luz, o la estufa y al tener conexión con estos estos te podrán avisar si dejaste algo encendido o también estar programados para apagarse en determinado tiempo.

Capítulo IV: El IoT como la red de redes y su importancia

Actualmente, IoT está compuesta por una colección dispersa de redes diferentes y con distintos fines. Por ejemplo, los automóviles actuales tienen múltiples redes para controlar el funcionamiento del motor, las medidas de seguridad, los sistemas de comunicación y así sucesivamente. De forma similar, los edificios comerciales y residenciales tienen distintos sistemas de control para la calefacción, la ventilación y el aire acondicionado, la telefonía, la seguridad y la iluminación. A medida que IoT evoluciona, estas redes y muchas otras estarán conectadas con la incorporación de capacidades de seguridad, análisis y administración. (Evans, 2011)

Esta inclusión permitirá que IoT sea una herramienta aún más poderosa.

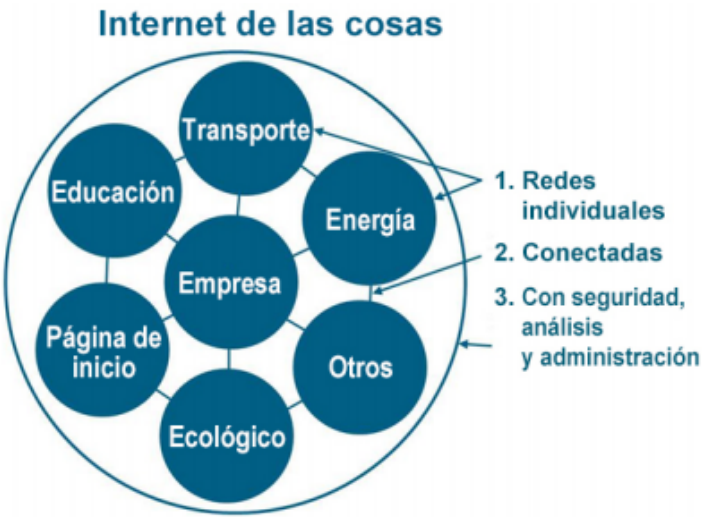

Figura 6 Los seres humanos convierten los datos en sabiduría (Evans, 2011)

Como vemos en la imagen anterior el IoT funciona como herramienta en diversas áreas como en el transporte por medio del GPS podrá tomar rutas alternas para evitar tráfico, etc.

Resulta interesante señalar que esta situación refleja lo que el sector de la tecnología experimentó en los primeros días de la red. Por ejemplo, a fines de la década de 1980 y a comienzos de la década de 1990, Cisco entró en el mercado aunando redes dispares con *routing* multiprotocolo, lo que luego condujo al establecimiento de IP como la norma de redes común. Con IoT, la historia se repite, aunque en una escala drásticamente más grande. (Evans, 2011)

Antes de que podamos ver la importancia de IoT, es necesario comprender las diferencias que existen entre Internet y *World Wide Web* (o web), términos que suelen utilizarse indistintamente. Internet es la capa física o la red compuesta de *switches, routers* y otros equipos. Su función principal es transportar información de un punto a otro, de manera veloz, confiable y segura. La web, por otro lado, es una capa de aplicaciones que opera sobre la superficie de Internet. Su rol principal

es proporcionar una interfaz que permite utilizar la información que fluye a través de Internet. (Evans, 2011)

Comparación entre la evolución de la web y la evolución de Internet

La web ha atravesado varias etapas evolutivas diferentes:

Primero fue la fase de investigación, cuando la web se denominaba Red de la Agencia de Proyectos de Investigación Avanzados (ARPANET). Durante este período, la web era utilizada principalmente por el área académica para fines de investigación. (Evans, 2011)

La segunda fase de la web fue la explosión de los sitios web publicitarios. Esta etapa se caracterizó por la "fiebre del oro" por los nombres de dominio y se concentró en la necesidad de que casi todas las empresas compartieran información en Internet para que los consumidores pudieran conocer sus productos y servicios. (Evans, 2011)

La tercera evolución fue el paso de la web de los datos estáticos a la información transaccional, que permitió la compra y venta de productos y servicios y la prestación de servicios. Durante esta fase, irrumpieron en escena empresas como eBay y Amazon.com. Esta etapa también será injustamente recordada como el auge y la caída de las "punto com". (Evans, 2011)

La cuarta fase, en la que actualmente nos encontramos, es la web "social" o de "experiencia", en la que las empresas como Facebook, Twitter y Groupon se han hecho inmensamente famosas y rentables (una notoria diferencia respecto de la tercera fase de la web) por permitir a las personas comunicarse, conectarse y compartir información (texto, fotos y video) personal con amigos, parientes y colegas. (Evans, 2011)

Capítulo V: Efectos estimados en el uso de la tecnología IoT en los consumidores

Debido al avance masivo del IoT, se dieron a conocer las diferentes áreas de aplicación en las que se encuentran:

- Medioambiente
- Industrias
- Ciudades
- Hogar
- Personal

Figura 7 Ámbitos de Aplicación del IoT (IW122grupo3)

En el ámbito del **medioambiente** se pretenden incluir aplicaciones centradas en redes de sensores destinadas a la protección y la salud, no solo del ser humano sino también de nuestro planeta. (Valle, 2014)

Algunos ejemplos de estas aplicaciones pueden ser las siguientes:

- **Control de polución en ríos/mares**: una res de sensores autónomos podrá comprobar el estado del agua y medir su pH, salinidad, temperatura, iones disueltos, etc.
- **Protección de fauna salvaje**: El uso de collares localizadores hace posible conocer la ubicación de ciertos animales, también ayudando a pastores a proteger sus rebaños.
- **Prevención de catástrofes**: una aplicación que de manera temprana alerte a los seres humanos sobre catástrofes naturales.
- **Sensores para ganado**: los cuales monitorean la salud, la fecundidad, y el estado de embarazo de sus vacas, así como el control de la producción. (Noriega & Jiménez)
- **Condiciones climáticas del cultivo**: permite generar análisis predictivos y aplicar acciones a tiempo. (Noriega & Jiménez)
- **Plantaciones**: los sensores monitorean permanentemente los niveles de humedad y radiación, enviando una señal que activa el riego. (Noriega & Jiménez)

En el ámbito de **industrias**, consideramos a los autómatas industriales como los precursores de IoT ya que es el área que más aplicaciones tiene hoy en día, ya que aporta en seguridad, monitorización, mejora de procesos productivos en general. (Valle, 2014)

- **Monitorización de estructuras**: el sistema *SmartPile*, el cual está basado en la instalación de un sensor *wireless* integrado en el cemento mientras fragua, de tal manera que queda unido a la estructura proporcionando datos a tiempo real de las tensiones de la columna.

- **Seguridad**: el sistema *enGauge*[5] que permite controlar el estado de los extintores, mandando alertas vía Wireless en caso de fallo/avería.
- **Analytics**: uno de los campos que más se está desarrollando, gracias al auge de los sistemas *BigData*[6] se están instalando sensores en los supermercados que analizan en tiempo real el comportamiento de los consumidores, de manera que son capaces de predecir los productos que tienen más éxito.
- **Manufactura inteligente:** El servicio o función de una máquina o una parte de ella pueden mejorar antes de que se presente una falla, eliminando así los costosos tiempos de inactividad y eventualidades no previstas.
- **Cadenas inteligentes de suministro:** Proporcionando información en tiempo real de la oferta, demanda y envíos a los clientes. Las entregas pueden ser rastreadas y recuperadas si son extraviadas o robadas.
- **Infraestructuras inteligentes**: Las oficinas inteligentes contribuyen a generar ahorros de energía, mejorar la auto sustentabilidad y potenciar la colaboración entre los empleados.

En el ámbito de **ciudades** se consideran todos aquellos usos que estén relacionados con "cosas" inteligentes en las ciudades. (Valle, 2014)

- **Ayuda al estacionamiento:** actualmente ya existe una guía que los automóviles actuales tienen y que ayuda a guiar al usuario para estacionarse

[5] Es tecnología de monitoreo electrónico para extintores de incendios asegura que los fundamentos están listos cuando los necesitamos y alerta a las autoridades cuando los extintores están activados para su uso.

[6] almacenamiento y tratamiento de grandes volúmenes de datos que poseen unas características muy concretas definidas como las tres V's (Volumen, velocidad y variedad).

utilizando una red de sensores autónoma Wireless que inyecta los datos en una aplicación web en tiempo real.

- **Contenedores inteligentes:** una alternativa que consiste en dotar a los contenedores de sensores que comunican a la central su estado en tiempo real, facilitando la recogida y optimizando los recursos.
- **Control eléctrico:** son sensores alimentados con baterías detectan caídas de tensión, fallos de suministro bypass en tiempo real notificándolo a la central.
- **Sensores en vehículos:** detectan objetos en la vía o cerca de ella con posibilidad de colisión. (Noriega & Jiménez)
- **Monitoreo de ciudades:** por medio de sensores y cámaras con algoritmos predictivos permite mayor control y la anticipación de eventos. Donde un chip permitirá el seguimiento de las armas de la policía. (Noriega & Jiménez)

En el ámbito del **hogar**, se engloba toda aquella domótica que es capaz de actuar y comunicarse de manera autónoma, este campo está orientado a la comodidad y seguridad.

- **Sistema de riego autónomo:** es un sistema para monitorización y automatización para plantas que permite controlar el crecimiento y regar de manera autónoma, siendo fácilmente adaptable desde 1 planta hasta 26.

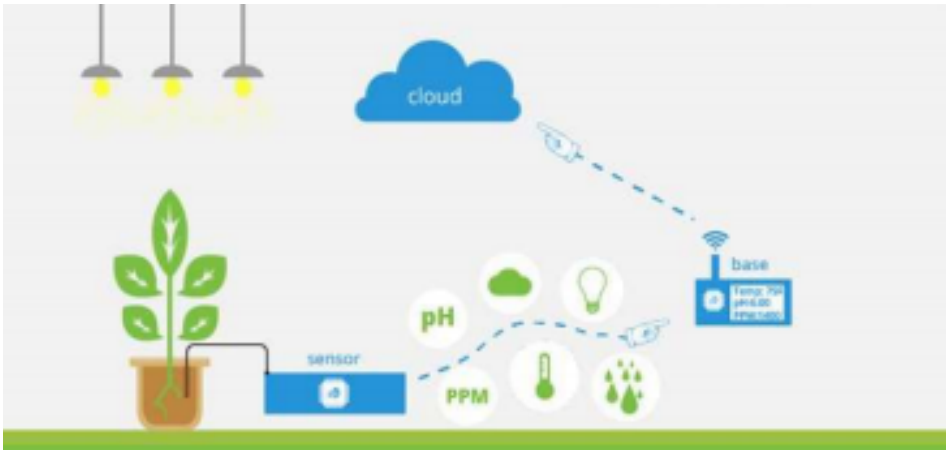

Figura 8 Ciclo de funcionamiento del Proyecto HarvestGeek. (Valle, 2014)

Entre otros sistemas que se utilizan es la iluminación, la apertura del garaje, control de termostatos y sistemas de seguridad, también dar a conocer al usuario lo que gastan o lo que necesitan; los cuales son controlados de forma remota, a través de apps de dispositivos móviles y computadoras.

En el ámbito **personal** se consideran todos aquellos objetos denominados "*wearables*[7]" y relacionados con el control/ayuda del ser humano, así como el industrial este campo también es de los que más está evolucionando.

- **Píldoras inteligentes:** es un sistema que se compone de un sensor fabricado completamente a base de nutrientes sin antena ni baterías y la cual es activada con los fluidos del estómago, este puede capturar el pulo cardiaco, actividad y horas de ingesta de medicación al tiempo el cual es emitido por bluetooth.
- **Salud:** promueve el abandono de fumar, reducción de peso, ejercicio para disminuir riesgos de problemas cardíacos, disminución del estrés. Esto es

[7] Wearable hace referencia al conjunto de aparatos y dispositivos electrónicos que se incorporan en alguna parte de nuestro cuerpo interactuando de forma continua con el usuario y con otros dispositivos con la finalidad de realizar alguna función concreta.

posible gracias a los sensores para la salud, que incluyen electrocardiogramas, presión sanguínea, oxímetros y una gran variedad de sensores especializados. (IW122grupo3)

- **Sensores en empaques de productos:** estos alertan a la nevera su caducidad para ser desechados. Donde las neveras llevan un inventario actualizado de lo que se tiene y recordar lo que falta. (Noriega & Jiménez)
- **Sensores en consolas de juegos:** detectan si se está cansado y/o aburrido. (Noriega & Jiménez)

Capítulo VI: El IoT como elemento de desarrollo productivo empresarial

Para las empresas, el IoT puede representar nuevas oportunidades para conectarse con sus clientes y socios, así como reunir, almacenar y analizar grandes volúmenes de datos. La gama de posibilidades que el IoT ofrece va en aumento y ahora las empresas de todo el mundo comienzan a andar los caminos destinados a aprovecharlo. Su impacto, sin duda, revolucionará la manera en que las empresas están haciendo negocio y elevará la productividad y eficiencia, similar a lo que sucedió con la llegada de las computadoras. (Alvarado, 2006)

En su reporte *TechRadar*[8], Forrester[9] revela que 23% de las empresas ya utilizan el IoT, mientras que 29% planean hacerlo en los próximos 12 meses. Aprovechan el IoT para transformar sus modelos de negocio, optimizar la utilización de activos físicos y financieros, y crear nuevas formas de relacionarse con sus clientes. De igual modo, Forrester prevé que el IoT creará grandes volúmenes de datos, por lo que la analítica de IoT se convertirá en una categoría y disciplina especializada.

[8] TechRadar es una publicación en línea centrada en la tecnología, con noticias y revisiones de productos de tecnología, especialmente gadgets.

[9] Es una empresa independiente de investigación de mercados que brinda asesoramiento sobre el impacto existente y potencial de la tecnología a sus clientes y al público en general.

Por su parte, Gartner calcula que para cuando finalice 2016 el gasto en servicios de IoT alcanzará los $235 mil millones de dólares, y que más de la mitad de los nuevos procesos de negocio y sistemas incorporarán algún elemento del IoT para el año 2020. (Alvarado, 2006)

Mientras los teléfonos móviles, los *smart TVs*, electrodomésticos y autos inteligentes pueden seguir captando la imaginación de los consumidores, es posible ver que hay mucho que ganar con las implementaciones empresariales. A diferencia de los sensores integrados en los dispositivos de consumo, aquellos integrados en maquinaria, contenedores, trenes, plantas de producción o puntos de venta, por ejemplo, están generando la información para crear aplicaciones en logística, redes inteligentes, servicios públicos, transportación, manufactura y *retail*. (Alvarado, 2006)

Pero más allá de los sensores y dispositivos, el valor real del IoT es determinado por los datos y las nuevas aplicaciones que los aprovechan. La inteligencia de estos datos está dando paso a nuevos modelos de negocio y aplicaciones que nunca habían existido antes y que abren la puerta a la transformación digital. (Alvarado, 2006)

El internet está teniendo una gran evolución, dando a conocer las cinco etapas:

- Pre-internet: conocida como humano a humano
- Internet de los contenidos: donde surge el www, email y los medios de entretenimiento
- Internet de los servicios: con web 2.0 con ejemplos como *e-productivity* y el *e-commerce*
- Internet de la gente: impulsando este el social media como Skype, Facebook, Twitter, YouTube, etc.
- Internet de las cosas: donde hay una conexión máquina con máquina.

Cuando nace el www y el email, las empresas empiezan a adquirirlos; creando sus sitios web para darse a conocer y/o dar a conocer información, a su vez usan los emails los cuales los inician usando exclusivamente de trabajo, lo cual ahora ya cualquiera tiene correo tanto empresarial como personal. (López J. J., 2016)

El IoT presenta factores muy favorables para las industrias como mejorar el desempeño de los procesos, la reducción de costos, la creación de productos y servicios innovadores y por ende nuevas oportunidades de ingresos. (López J. J., 2016)

Las aplicaciones del IoT realmente pueden ser en cualquier ámbito y hoy en día ya se ven ejemplos en verticales como la manufactura, alimentos, industria, agricultura, logística, energía, ambientes, ciudades, automatización de casas, salud, etc. (López J. J., 2016)

En el IoT debemos entender que existen fuerzas que son fundamentales para lograr su correcta operación y correlación, estas pueden ser políticas, estándares, mecanismos de gestión de gobierno, temas legales, privacidad, socios de negocio, elementos de influencias económicas, misión y negocio, seguridad, proveedores y la búsqueda de experiencia, todo esto deberá regir los componentes tecnológicos que generan el ecosistema siendo estos productos, social , movilidad, analítica la nube y los sistemas que a su vez se ven conectados mediante la gente y los *Gateway* tecnológicos a los enlaces y las cosas. (López J. J., 2016)

Cabe destacar que los principales elementos de influencia que favorecen al IoT son:

- Bajo costo de procesamiento
- *Smartphones*
- Cobertura *wireless*
- *Big data*
- IPv6

En cambio, los principales retos hoy en día son:

- Generar una plataforma para generar desarrollo apropiado UX UI.
- Conectividad y desarrollo de los sistemas y la eficiencia en el IPV6.
- Un modelo de negocios que no gestione una cadena de valor lineal, sino que ésta se incorpore a un ecosistema donde todos los participantes aumenten sus ganancias a través de estas tecnologías.
- Muchos de los sistemas IoT están pobremente diseñados e implementados, utilizan diversos protocolos y tecnologías creando una compleja configuración.
- Poca o carente madurez de las tecnologías IoT y procesos para aplicarles.
- Mantenimiento y Gestión de los dispositivos inmaduros.
- Altos riesgos en seguridad.

Poca interacción entre participantes provoca la no alineación de mejores prácticas al momento.

Todo esto nos da un mundo conectado y genera las principales inquietudes alrededor de la tecnología donde primeramente figura la seguridad, la integración de sistemas, las inversiones en redes, la creación de áreas que analicen y aporten valor derivado de los datos y la correcta inversión en sensores. (López J. J., 2016)

Le recomiendo comenzar una estrategia de negocio que le permita entender cómo funcionar en un mundo que se inclina a tener ecosistemas digitales, un lugar donde de manera integral las tecnologías trabajan de forma convergente y en tiempo real para unir las cosas, la analítica, los sistemas y la gente, todo esto mediante una inteligencia generada de su estrategia. (López J. J., 2016)

Todos debemos comprender que la seguridad será un factor fundamental ya que cada vez más elementos estarán conectados a la red y por ende pueden ser el objetivo de un ataque o violación y la integridad de este dependerá mucho del como usted monte su estrategia. (López J. J., 2016)

Desarrollo de la agilidad de los procesos de la empresa

Si bien IoT ofrece enormes oportunidades para la mejora de los procesos, muchas organizaciones no cuentan con la agilidad necesaria para aprovechar estas mejoras. Nuestros encuestados están de acuerdo con esta afirmación. Según ellos, el principal reto para lograr un uso eficaz de IoT es la “dificultad de actualizar los procesos de la empresa para las nuevas soluciones de IoT”, por delante de la “financiación inadecuada” y la “falta de un argumento comercial claro para implementar soluciones de IoT”. Un reto es la dificultad cada vez mayor de “ver” el aspecto de los procesos de una organización, especialmente debido a que estos procesos se han integrado en software del tipo ERP (planificación de recursos empresariales). La investigación y la experiencia han demostrado que es importante solucionar la eficiencia de los procesos antes de aplicar tecnología para automatizarlos. La agilidad de los procesos de la empresa también depende de factores como la cultura empresarial, la capacidad de gestión de procesos empresariales y las características de los procesos únicas de cada organización.25 Además, salvo en el caso de las empresas emergentes, las organizaciones ya han establecido procesos empresariales para definir sus operaciones. Estos procesos suelen ser muy complejos e integrar tareas y recursos de una forma única. El equipo y los recursos antiguos complica aún más el asunto.

Planificación del personal del futuro

Las organizaciones deben prepararse para el personal del futuro: uno que pueda impulsar las oportunidades de transformación prometidas por IoT y datos, con las competencias adecuadas a las preocupaciones y resultados específicos del sector.

Además de trabajadores con conocimientos informáticos y de análisis, las organizaciones necesitarán desarrolladores expertos en IoT para implementar las soluciones de IoT. La empresa de investigación VisionMobile calcula que el

número de desarrolladores de IoT aumentará de 300 000 en 2014 a 4,5 millones en 2020.

¿Qué tipo de alcances implica el IoT para las empresas?

IoT se refiere a un sistema ciber-físico-social que utiliza sensores conectados a un núcleo. Los sensores pueden ser humanos, biológicos, mecánicos o electrónicos; sienten y responden a un estímulo y emiten su estado. Los sensores pueden ser tan diversos como aquéllos utilizados en el monitoreo de estados, de bacterias, de tiras bimetálicas, y de aquéllos electromecánicos y electrónicos. (Manzano, 2015)

Los sistemas del Internet de las Cosas también varían: pueden ser tan simples como las alertas programadas de nuestros dispositivos personales y accesorios, o pueden ser lo suficientemente poderosos como para controlar una misión en Marte vía remota. (Manzano, 2015)

Estamos hablando acerca de varios trillones de objetos físicos conectados a varios millones de computadoras y varios cientos de millones de dispositivos como teléfonos móviles, '*wearables*', equipo industrial (turbinas de gas, aros de aceite, redes de servicios públicos), vehículos conectados y flotillas, ciudades inteligentes (estacionamientos, iluminación, cámaras de vigilancia). Y todo esto interactúa con un mundo de miles de millones de personas y un flujo de información nutrida para los sistemas empresariales de fondo. (Manzano, 2015)

¿Cuáles son las oportunidades para las empresas?

- Permitirá inimaginables formas en las cuales los productos serán utilizados por los consumidores.
- Iluminará las complejas relaciones entre sus clientes, proveedores, usuarios finales y otros interesados.
- Ofrecerá en tiempo real información que permitirá a la empresa irrumpir en el mercado con nuevos productos y/o servicios.

Para varias industrias que proveen productos industriales o de consumo, entregar 'un producto como servicio' será un nuevo modelo de negocio, que las empresas serán capaces de controlar de forma remota, automatizar y gestionar los activos a lo largo del ciclo de vida del activo. (Manzano, 2015)

Las empresas podrán alcanzar un nivel más profundo de entendimientos del consumidor si encuentran la manera de persuadir al consumidor a compartir información personal acerca de '*wearables*', autos conectados y *gadgets* para hogares inteligentes. Esto tendría que llevar a una mejor experiencia al consumidor, servicios basados en el uso de ellos e incentivos relacionados en el comportamiento de los conductores basado en las aseguradoras. (Manzano, 2015)

¿Cuáles son los retos para las empresas?

Los sistemas del Internet de las Cosas son complejos: se distribuyen, se trabajan en redes laborales, son dinámicos, evolucionan, y son subjetivos (sujetos a potencialidades humanas). (Manzano, 2015)

- La complejidad y desarrollo escalable de los sistemas ciber-socio-físicos interconectados.
- La diversidad de miles de tipos de sensores y funciones, vendedores y sus ecosistemas.
- La interoperabilidad de diferentes protocolos de comunicación, hardware, software, middleware y sistemas empresariales.
- Evolución de la tecnología: como la rápida evolución en el terreno del Internet de las Cosas.
- Big Data a menor escala: manejo de procesos en tiempo real del flujo de información y configuración inteligente en los límites del big data de menor escala.

- Privacidad, seguridad y cumplimiento normativo.

Capítulo VII: Seguridad del IoT

La seguridad en IoT parece estar en tela de juicio. Las últimas noticias sobre los dispositivos IoT apuntan a que los hackers tienen un nuevo objetivo. De hecho, hay ya estudios, como este de Gartner, en el que afirma que para el año 2020 más de un cuarto de los ciberataques que se produzcan tendrán en el punto de mira a un dispositivo IoT. Esto es así, por la expansión de este concepto que cada vez forma parte ya de los objetos cotidianos en cualquier hogar. (Cárdenas, 2016)

Seguridad en IoT y el valor de los datos

No puede existir el uno sin el otro. Los datos y IoT están íntimamente relacionados, En la actualidad, las grandes empresas valoran estos datos sobremanera pero no ponen ningún remedio a dotar de una mayor seguridad a la protección de este valor. Un dato alarmante sobre esta situación es que menos del 10% del presupuesto de seguridad en IoT está destinado a la seguridad pese a que cada día hay más peligro de sufrir un ataque. (Cárdenas, 2016)

Los usuarios al descubierto

Los usuarios ante esta situación se encuentran que sus datos personales son facilitados tanto al dispositivo en concreto como a las empresas que gestionan estos sistemas. No tienen otra si quieren disfrutar de estos servicios, pero los usuarios no quieren ser el blanco de estas brechas de seguridad ni los proveedores de estos servicios y/o productos quieren quedar expuestas al no haber tomado antes las medidas adecuadas. (Cárdenas, 2016)

Lo que sí que parece seguro es que los hackers en estas situaciones suelen sacar provecho. En esta noticia del Washington Post, podemos ver cómo los hackers a través de los dispositivos IoT se dedicaron a enviar información masivamente a

grandes empresas hasta que los servidores de estas empresas no podían más y caían. (Cárdenas, 2016)

Seguridad antes de que sea tarde

En este paradigma la realidad salta a la luz y vemos cómo saltan noticias relacionadas con estos tipos de problemas. Empresas punteras cómo Spotify o el mismísimo Twitter ofrecen fallos que desde la vista del consumidor se traduce en una falta de miramientos hacia la seguridad de los usuarios a través de sus cuentas y datos personales. Como fin último de esto, los usuarios pierden la confianza en ofrecer sus datos o adquirir dispositivos IoT hasta que la industria no muestre una solución a este problema. (Cárdenas, 2016)

Sin embargo, no todo está perdido y hay tiempo para crear estándares y dotar de seguridad antes de que sea demasiado tarde. (Cárdenas, 2016)

Gestionar la seguridad en un entorno IoT será uno de los desafíos más grandes de ciberseguridad en 2016, pues conforme continúe el crecimiento en el uso de dispositivos inalámbricos y aplicaciones móviles, junto con el incremento en el uso de IoT en los negocios, las organizaciones se quedarán atrás en su capacidad de proteger sus datos críticos. (Beninatto, 2016)

La seguridad, en cualquier entorno, especialmente en IoT, cuya característica principal es la conexión entre objetos, debe pensarse y concebirse bajo un enfoque integral y convergente. Por lo que es importante gestionar unificadamente la seguridad lógica o digital y física; esto porque en varias organizaciones de TI se han enfrentado a entornos tecnológicos donde la administración de la seguridad digital se administra, por un lado, y la lógica por otro. (Beninatto, 2016)

Con esto en cuenta sabemos que un modelo que tome en cuenta la convergencia de activos lógicos y físicos, ya que las amenazas y vulnerabilidad recientes se basan precisamente en una correlación que involucra ambos puntos de entrada.

De ahí que la gestión de la seguridad deba ser hecha de forma igualmente convergente. (Beninatto, 2016)

Cifras de seguridad IoT

La seguridad, en su aspecto más técnico, se puede definir como aquellas actividades enfocadas a proteger un determinado dispositivo o servicio, así como todo aquello con lo que interactúa e intercambia con otros dispositivos o servicios, ya sea información, datos, señales, etc. Utilizando como base la anterior definición, la seguridad de IoT se podría definir como aquellas actividades encaminadas a la protección de los objetos y sus comunicaciones o interacciones con otros objetos. (López A. T., 2014)

Así, aunque la seguridad siempre es un tema muy relevante a tener en cuenta, su importancia resulta aún mayor cuando nos encontramos ante ámbitos de aplicación tales como el de la salud, donde ya se está trabajando con “objetos” en el cuerpo de pacientes, como el caso de marcapasos, que pueden ser controlados y accedidos por el personal médico. Se puede intuir las graves consecuencias que podría tener accesos no autorizados a este tipo de objetos en pacientes: no sólo filtración de datos, sino algo realmente peligroso para sus vidas. (López A. T., 2014)

En base a la importancia que a priori parece constituir la seguridad en IoT, se analiza el número de artículos científicos dedicados a estos temas.

Como se puede apreciar, para tratar de obtener el mayor número posible de artículos relacionados con la seguridad aplicada a IoT, se utilizan diversos patrones de búsqueda. En concreto: “Internet of Things Security”, “RFID Security” y “Sensor Security”. Aún con la ampliación del espectro de búsqueda, la publicación de artículos científicos encontrados sobre seguridad en IoT es muy baja y prácticamente no ha cambiado en los últimos años. (López A. T., 2014)

Para contrastar los datos anteriores se lleva a cabo una búsqueda de las patentes relacionadas con la seguridad de IoT entre los años 2009 y 2014.

De nuevo, tal como puede observarse en la figura 5, el número de patentes relacionadas con la seguridad en IoT no representa un incremento sustancial en los últimos años, sólo se aprecia un leve repunte en la seguridad relacionada con RFID entre 2011 y 2012, algo que demuestra que hubo un mayor interés en estos temas. Estos datos obtenidos claramente contrastan con el crecimiento exponencial que en general sí ha experimentado el IoT, como ya se observó en los números presentados de este sector. (López A. T., 2014)

Por tanto, de las cifras obtenidas podría entenderse que la seguridad de IoT no parece un tema que haya llamado especialmente la atención de los investigadores. Sin embargo, como ya se pudo intuir al comienzo del presente artículo, la seguridad, y sobre todo en ciertos ámbitos de aplicación, debiera merecer mayor interés. Otra conclusión que podría extraerse de estas cifras tan ínfimas es que las tecnologías sobre las que se basa IoT son tan seguras por definición o es tan sencillo aplicar soluciones de seguridad conocidas, que no se requieren nuevos esfuerzos para mejorar lo ya existente. En el siguiente apartado se aporta información que permite demostrar la realidad sobre este tema y que apunta hacia la necesidad de prestar mayor atención a la seguridad en el IoT. (López A. T., 2014)

La seguridad de IoT: un tema preocupante para los expertos

El increíble desarrollo del IoT está cambiando por completo la tradicional percepción que se tenía de Internet, hacia una visión integrada de objetos “inteligentes” que interactúan entre sí. Tanto es así, que el número y diversidad de sensores y dispositivos desplegados está creciendo de forma realmente alarmante. Tal como se había apuntado, dentro de este nuevo paradigma, y especialmente en ámbitos en los que se manejan datos sensibles, la pérdida de información o acceso incontrolado puede afectar seriamente a la privacidad de sus

usuarios, por lo que la seguridad se constituye como un factor clave en el desarrollo y despliegue de estos nuevos escenarios. Este es un tema preocupante, ya que en a día de hoy no se dispone de una guía clara de acción para la seguridad IoT.

Los expertos apuntan que una de las principales barreras para la implantación de IoT es precisamente la seguridad y la privacidad. El porqué es bien sencillo: por un lado, las restricciones que imponen los dispositivos y redes de la IoT impiden la aplicación directa de soluciones tradicionales de seguridad. En concreto, protocolos tradicionales de seguridad y criptografía requieren una gran cantidad de recursos de memoria y proceso, algo de lo que habitualmente carecen los dispositivos IoT. Por tanto, la adaptación de soluciones de seguridad a este nuevo paradigma se presenta como un gran desafío. Además, cabe destacar que, a diferencia de otros entornos más tradicionales, los dispositivos de IoT suelen trabajar en condiciones de mayor dificultad, en cuanto a los entornos que les rodean, entornos que muchas veces no están controlados e incluso son hostiles o propensos a ataques malintencionados.

Presente y futuro seguridad IoT

Grandes fabricantes como Intel han apostado fuertemente por mejorar la seguridad de IoT, convencidos de la potencia y crecimiento de este sector en auge. Así, Intel ha presentado muy recientemente tecnologías que ayudan a mejorar la protección de IoT, como por ejemplo su tecnología de protección de datos para transacciones, que tiene por objetivo asegurar las transacciones de objetos IoT (Intel Data Protection Technology for Transactions) o la pasarela de soluciones para el Internet de las Cosas (Intel Gateway Solutions for the IoT), que conecta de forma más segura los objetos IoT con Internet e incluso con soluciones en la nube.

Por su parte, la compañía Cisco dentro de sus iniciativas para fomentar el desarrollo del IoT, ha llevado a cabo este año el concurso “El Gran Desafío de Seguridad del Internet de las Cosas”, donde recibió postulaciones provenientes de más de 33 países, entre start-ups, empresas y universidades, premiando las cuatro mejores soluciones con un premio total 300.000 dólares, repartidos en premios de 75.000 dólares, además de otorgarles un espacio de exposición en el próximo Foro Mundial del Internet de las Cosas.

La consultora Gartner, según uno de sus últimos estudios, asegura que al final del año 2017 más del 20 por ciento de las empresas dispondrá de servicios digitales dedicados a la protección de sus iniciativas empresariales mediante dispositivos y servicios en IoT. Gartner señala que ya existen muchas iniciativas empresariales que están utilizando el IoT, por lo que el papel que jugará en los negocios y en la industria obligará a las empresas a tener que invertir en su seguridad.

Aparte de las iniciativas y opiniones acerca de la seguridad en IoT, la gran cantidad de noticias aparecidas en los últimos años en los distintos medios, donde se apunta a accesos no autorizados a información privada altamente sensible en servicios como el iCloud de Apple o escándalos como el acceso de la NSA de EEUU a millones de cuentas en Verizon, no hacen más que elevar el nivel de preocupación por la seguridad y la privacidad en el uso de los servicios informáticos.

Pero no todo son malas noticias, ya que según InfoWorld [10] gracias al IoT el crecimiento de empleos en el sector de la seguridad informática está viviendo un momento vertiginoso, ya que se están creando miles de puestos de trabajo.

Aspectos de seguridad que se deben cubrir y vincular entre ellos

Seguridad lógica: Incluye la administración de la seguridad en dispositivos móviles (ya sea en entornos BYOD o híbridos), en el centro de datos, en las

arquitecturas *cloud* y las redes IP. Se requiere poner atención a la seguridad en el uso de software, sistemas, procesos y programas, así como al control de los usuarios autorizados para usarlos, y su acceso a la información y datos. Al utilizar soluciones de seguridad basadas en software se pueden proteger los datos y la información que almacena o circula en las plataformas arriba mencionadas. (Beninatto, 2016)

Seguridad física: Considera la gestión de identidad, la detección de fraude, soluciones de procesamiento de imágenes (fotografía y video), y vigilancia del lugar y perimetral. Integrar la seguridad del ambiente de TI con la seguridad física refuerza y permite el control de acceso total que requiere una organización, sobre todo en un ambiente como el de IoT, donde pueden existir muchos puntos de entrada. Al sincronizar la identidad –física y lógica– de los usuarios, es posible controlar el acceso hacia determinados recursos físicos empresariales. Algunas soluciones de este tipo son las biométricas, que se basan en la identificación por huella dactilar, iris, rostro, geometría de la mano, etcétera. (Beninatto, 2016)

Servicios administrados de seguridad: Se enfocan en una administración del riesgo y el cumplimiento para dejar que usted se ocupe de su negocio y deje en manos de terceros la preocupación por la gestión de la seguridad cibernética. El surgimiento de tecnologías como IoT y su implementación hacen necesario atender las nuevas vulnerabilidades que se podrían generar; sin embargo, ¿cómo hacerlo cuando usted tiene que poner su atención en temas como la generación de nuevos clientes y mantener el nivel de ventas? Una buena alternativa está en delegar a un tercero esta gran misión, un experto que brinde soluciones de seguridad empresariales integrales. (Beninatto, 2016)

Servicios profesionales: Donde usted pueda encontrar el apoyo de consultores estratégicos que brinden servicios de asesoría profesional para afrontar los retos de seguridad que demandan las nuevas tecnologías como el Internet de las Cosas, y le ayuden a llevar su negocio hacia delante con decisión y confianza. La

clave en este rubro es tener una visión estratégica donde se alineen el negocio y la tecnología con los procesos, las herramientas y las técnicas. (Beninatto, 2016)

Los tres pilares de la seguridad del IoT

El IoT va a impactar en la manera en que interactuamos con el mundo que nos rodea. Miles de millones de cosas van a "hablar" unas con otras, desde televisores, refrigeradores y automóviles hasta medidores inteligentes, monitores de la salud y *wearables*. El IoT promete una conveniencia sin igual. Sin embargo, la obtención y la retención de la confianza del consumidor en la privacidad y la seguridad es fundamental para que el IoT alcance su máximo potencial. Los datos que se mueven alrededor del IoT van a brindar información de cada uno de nosotros. El gran desafío es proteger esa información.

Existen varias formas en que un atacante puede acceder a distintas características o a distintos datos de un dispositivo conectado. Los tres puntos principales que suelen ser objeto de los hackers son: el dispositivo, la infraestructura de la nube y la red.

Hay tres pilares fundamentales para proteger un dispositivo del IoT y así garantizar que tanto la información en reposo como la información en movimiento se mantengan a salvo. El arsenal de Gemalto protege el dispositivo desde su diseño y fabricación, y durante todo el ciclo de vida, y resguarda los datos de los ataques maliciosos.

Primer pilar - La seguridad del dispositivo:

Miles de millones de dispositivos conectados van a aumentar el uso de las aplicaciones de software y de los datos que se encuentran en los recursos de las empresas y en los dispositivos de consumo, lo que implica nuevos puntos de ataque para los hackers maliciosos. Las soluciones de software integrado de

Gemalto para la electrónica de consumo y la tecnología M2M ayudan a los fabricantes de dispositivos originales (OEM) de consumo e industriales y a los operadores de redes móviles a hacer frente a estos desafíos de seguridad, entre ellos al robo de propiedad intelectual debido al entorno no regulado en el que operan estos dispositivos.

Segundo pilar - La seguridad de la nube:

Las amenazas más urgentes vienen del entorno de la empresa o del entorno de la nube al que estos dispositivos inteligentes están conectados. Las soluciones de Gemalto para el cifrado de datos y la seguridad de la nube brindan un portfolio completo para que los proveedores de servicios en la nube y las empresas protejan sus recursos. Nuestra solución de licencias y derechos basados en la nube ayuda a las empresas de tecnología a aprovechar todo el potencial del entorno de la nube y así garantizar la seguridad de la propiedad intelectual.

Tercer pilar – La gestión del ciclo de vida de la seguridad

Si bien a menudo se pasa por alto, la gestión del ciclo de vida de los componentes de seguridad del dispositivo y del espectro de la nube es un elemento fundamental para una estrategia de seguridad digital robusta y de largo plazo. La seguridad no es una actividad de una sola vez, sino una parte en evolución del ecosistema del IoT. El agregado de nuevos dispositivos, el desmantelamiento del dispositivo al final de su vida útil, la integración del dispositivo en un nuevo ecosistema de la nube o viceversa, la gestión de la descarga de *firmware/software* seguro son actividades que necesitan una gestión completa de las identidades, las claves y los *tokens*. Gemalto brinda soluciones para la creación de una infraestructura de gestión del ciclo de vida de la seguridad sostenible con capacidades que incluyen la gestión de la identidad y el acceso, la gestión criptográfica, la monetización de software y la gestión de tokenización y del elemento seguro.

Recomendaciones de seguridad de IoT

Para los usuarios y consumidores:

- Cambiar las contraseñas por defecto por unas robustas y utilizar el cifrado más robusto posible.
- Conectar dispositivos a una red separada, cuando sea factible.
- Deshabilitar o proteger el acceso remoto a dispositivos mientras no sea necesario.
- Investigar y aprovechar las medidas de seguridad implantadas en el dispositivo.
- Deshabilitar características no utilizadas.
- Instalar actualizaciones tan pronto estén disponibles. (Falcón, 2016)

Para fabricantes:

- Utilizar conexiones cifradas.
- Anonimizar los datos y recopilarlos sólo cuando sea estrictamente necesario.
- Requerir un cambio obligatorio de las contraseñas por defecto por otras robustas y no permitir contraseñas “quemadas” en el código.
- Permitir la configuración de reglas detalladas de control de acceso.
- Implantar medidas que dificulten ataques de fuerza bruta para adivinar credenciales de acceso.
- Verificación mutua de certificados SSL y de listas de revocación de certificados.

- Implementar medidas inteligentes de *fail-safe*[10] cuando la conexión o la energía del dispositivo falla.
- Realizar análisis de seguridad del código fuente y ofuscarlo si es accesible para los usuarios. (Falcón, 2016)

Capitulo VIII: Ventajas y desventajas del IoT

En este capítulo se muestra una tabla comparativa de las ventajas y desventajas del uso de IoT, así como se muestra una tabla con las diferentes empresas que usan IoT y una descripción de sus productos.

[10] A prueba de fallos

Ventajas	Desventajas
• Hace la comunicación mucho más sencilla. • Es posible conocer e interactuar con muchas personas de todas partes del mundo. • La búsqueda de información se vuelve mucho más sencilla, sin tener que ir forzadamente a las bibliotecas tradicionales. • Es posible encontrar muchos puntos de vista diferentes sobre alguna noticia. • Es posible la creación y descarga de software libre, por sus herramientas colaborativas. • La computadora se actualiza periódicamente más fácil que si no tuviéramos internet. • Es posible encontrar soporte técnico de toda clase sobre alguna herramienta o proceso. • El seguimiento de la información a tiempo real es posible a través del Internet. • Es posible comprar fácilmente a otras tiendas de otros p • Es posible compartir muchas	• Así como es de fácil encontrar información buena, es posible encontrar de la misma forma información mala, desagradable (pornografía, violencia explícita, terrorismo) que puede afectar especialmente a los menores. • Te genera una gran dependencia o vicio del internet, descuidándote de muchas cosas personales o laborales. • Hace que los estudiantes se esfuercen menos en hacer sus tareas, debido a la mala práctica del copy/paste. • El principal puente de la piratería es el internet • Dependencia de procesos. Si hay un corte de internet, hay muchos procesos que se quedan varados por esa dependencia. • Dependencia de energía eléctrica. Si hay un corte de energía en la casa, adiós internet (no es el caso de la telefonía convencional). • Hace que nazcan otros males tales como el spam, el malware, la

cosas personales o conocimientos que a otro le puede servir, y de esa manera, se vuelve bien provechoso. (Carrascal, 2015)	proliferación de los virus, el phising, etc. (Carrascal, 2015)

Empresas que utilizan IoT

Cisco

Espera desempeñar un papel importante, facilitando todo aquello a través de su línea de routers conectados a la red, switches integrados y software de red centrado en aplicaciones. Cisco ha tenido recientemente algunas dificultades con su iniciativa IoT, cuando su ejecutivo que lideraba dichos esfuerzos renunció.

IBM

Cuenta con una variedad de productos de este tipo, incluyendo una plataforma de mensajería para datos de máquina a máquina (M2M) llamada MessageSight, junto con MobileFirst, que da a los objetos capacidades móviles, y BlueMix, una plataforma de desarrollo para aplicaciones que pueden gestionar la recopilación y el análisis de datos IoT.

Intel

La empresa ofrece una gama de opciones, desde la alta eficiencia de energía del procesador X1000 QuarkSoC con capacidad para cargas de trabajo bajas, hasta chips Xeon para el procesamiento de alta resistencia. Intel tampoco es la única compañía de procesadores manifestándose en el mercado IoT. Su competidor ARM también está preparando sus chips para un mundo de sensores.

Microsoft

La compañía está haciendo esto a través de una variedad de productos, incluyendo sistemas operativos Windows Embedded personalizados destinados a recopilar y analizar datos, así como a través de productos en su nube Azure como: Intelligent Systems, una oferta actual de modo-vista previa que descarga el análisis de data pesada a la nube. (Butler, 2014)

Oracle

El movimiento del IoT se refiere fundamentalmente a la creación de más datos, y Oracle dice que todos esos datos necesitan un lugar donde ser almacenados. La empresa cuenta con un conjunto de servicios, que incluyen una plataforma para habilitar Java en dispositivos integrados con sensores, una plataforma de middleware para la creación de aplicaciones para capturar datos, y bases de datos para almacenar todo. (Butler, 2014)

Qualcomm

Qualcomm ayudó a crear AllJoyn, un framework IoT de código abierto para conectar dispositivos que ahora es administrado por la Fundación Linux. Si bien hay muchos esfuerzos para que los dispositivos se conecten a Internet, Qualcomm considera que es importante tener un protocolo común de código abierto estándar, como AllJoyn, para unirlos. (Butler, 2014)

Amazon

La nube va a jugar un papel importante en el Internet de las Cosas, y el más grande jugador de infraestructura de la nube que hay es Amazon Web Services. AWS está listo para tomar todos los datos y permitir a los clientes hacer un análisis de la misma. AWS tiene una variedad de plataformas de datos, incluyendo sus bases de datos relacionales RDS, su base de datos DynamoDB NoSQL así como su herramienta de almacenamiento de datos Red Shift; así como nuevas herramientas de análisis, como Kinesis, un servicio de procesamiento en tiempo

real para datos de streaming. Si los datos de IoT viven en la nube, AWS podría desempeñar un rol importante en este mercado. (Butler, 2014)

Conclusión

Debido al gran avance que está teniendo la tecnología, en cuanto a la conexión entre los dispositivos y el usuario. Facilita a las personas realizar sus actividades rutinarias tanto en el hogar como en el trabajo, y aunque tiene grandes beneficios, también tiene sus desventajas, sobre todo en la seguridad ya que los hackers podrían acceder a información, las corporaciones no quieren compartir sus datos, y las personas individuales pueden no gustarle la ausencia total de privacidad. Por estas razones, el Internet de las cosas puede muy bien ser rechazado más tiempo de lo que realmente necesita ser.

En 2020, habrá un incremento de dispositivos conectados, el cual cada persona dispondrá de una media de 26 dispositivos conectados. La pregunta que nos planteamos es cómo asegurar que nuestra red está preparada para este nuevo entorno.

En todo tipo de foros y congresos oímos hablar sobre el Internet de las Cosas (IoT) y los retos que plantea a la seguridad TI.

A nadie sorprende que la conectividad basada en IP gane terreno día a día. Lo que sí es nuevo es que el público al que se dirige está cambiando y la conectividad es cada vez más personal. Ya no está limitada a los usuarios de alta tecnología (relojes y drones), sino que está presente en prácticamente cualquier dispositivo – desde los juguetes infantiles al menaje de la cocina y, por supuesto, los medios. Los compradores de estos productos tecnológicos no son precisamente expertos en seguridad, muchos de ellos ni se plantean esta problemática. De hecho, su principal prioridad a la hora de adquirir el dispositivo es su facilidad de uso. (Laguna, 2016)

Referencias

Cárdenas, A. (7 de diciembre de 2016). *Secmotic*. Retrieved 3 de febrero de 2017 from https://secmotic.com/blog/seguridad-en-iot/

Cabezudo, V. (1 de marzo de 2014). *Muy canal*. Retrieved 24 de enero de 2017 from http://www.muycanal.com/2014/03/01/historia-internet-of-things

Laguna, J. L. (16 de noviembre de 2016). *isms*. Retrieved 6 de febrero de 2017 from isms: https://www.ismsforum.es/noticias/836/preparandose-para-la-revolucion-de-iot.-por-jose-luis-laguna./

Carrascal, D. (Octubre de 2015). *cosas y el internet*. From http://cosasyelinernet.blogspot.mx/2015/10/internet-de-las-cosas-ventajas-y_12.html

Cordoba, S. (1 de Julio de 2016). *Cultura Informática*. Retrieved 24 de enero de 2017 from Cultura Informática: http://culturainformatica.co/inforgrafia-internet-de-las-cosas-kevin-ashton/

López, A. T. (noviembre de 2014). Retrieved 5 de febrero de 2017 from http://www.cait.upm.es/vigilancia_tecnologica/pluginfile.php/228/mod_resource/content/2/Seguridad%20Internet%20de%20las%20Cosas%20(versi%C3%B3n%20Final).pdf

López, J. J. (16 de noviembre de 2016). *The it profile*. Retrieved 28 de enero de 2017 from The it profile: http://www.theitprofile.com/opinionti/2016/11/16/iot-empresarial-columna/

López, N. (3 de octubre de 2014). *insite*. Retrieved 5 de enero de 2017 from https://insite.com.co/historia-del-internet-de-las-cosas/

Alvarado, J. (2006). *SG Buzz*. Retrieved 1 de febrero de 2017 from SG Buzz: https://sg.com.mx/revista/51/el-impacto-real-del-iot-las-empresas#.WJIU-_l97Dc

Beninatto, H. (28 de enero de 2016). *Forbes* . Retrieved 3 de febrero de 2017 from http://www.forbes.com.mx/iot-desafio-a-la-seguridad/#gs.ZC1vuAo

Butler, B. (21 de mayo de 2014). *CIO*. Retrieved 6 de febrero de 2017 from CIO: http://cioperu.pe/fotoreportaje/16123/las-10-empresas-de-internet-de-las-cosas-mas-poderosas/?foto=2

Datagora. (3 de JUNIO de 2016). From http://www.datagora.es/2016/06/03/el-crecimiento-de-iot-sobrepasa-todas-las-expectativas/

Evans, D. (Ed.). (Abril de 2011). Retrieved 24 de enero de 2017 from cisco: http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

Falcón, L. A. (Ed.). (14 de marzo de 2016). *A un clic de las TIC*. Retrieved 3 de febrero de 2017 from http://aunclicdelastic.blogthinkbig.com/el-reto-de-la-seguridad-en-iot/

Genexus. (18 de Febrero de 2016). Retrieved 25 de enero de 2017 from http://www.genexus.com/noticias/leer-noticia/la-evolucion-del-internet-de-las-cosas?es

Grail, C. (23 de octubre de 2017). *What´s the bid data idea*. Retrieved 5 de Enero de 2017 from http://whatsthebigdataidea.com/2017/10/23/cisco-predicts-50-billion-iot-connected-by-2020/

Hartwell, P. (3 de Febrero de 2014). *Reporte digital*. Retrieved 28 de enero de 2017 from http://reportedigital.com/transformacion-digital/internet-de-las-cosas-tendencia-futuro-empresas/

Hernández, L. d. (marzo de 2018). *Programar facil.com*. From Arquitectura IoT, prototipando los dispositivos del futuro: https://programarfacil.com/podcast/arduino-wifi-proyectos-iot/#IoT_requerimientos_de_la_arquitectura

infoPLC. (23 de septiembre de 2014). Retrieved 5 de enero de 2017 from http://www.infoplc.net/blogs-automatizacion/item/102107-iot-internet-cosas-automatizacion-industrial

IT Sitio empresas. (26 de enero de 2015). Retrieved 3 de febrero de 2017 from http://empresas.itsitio.com/ar/iot-impulsara-la-economia/

IW122grupo3. (n.d.). Retrieved 5 de Enero de 2017 from http://iw122grupo3.wikispaces.com/4.+AMBITOS+DE+APLICACION

Jones, F. (23 de enero de 2015). *business review america latina*. Retrieved 28 de enero de 2017 from http://www.businessreviewamericalatina.com/tecnologia/1245/IoT-la-interconectividad-del-futuro-INFOGRAFA

Manzano, H. (19 de enero de 2015). *Mundo Contact*. Retrieved 1 de febrero de 2017 from Mundo Contact: http://mundocontact.com/el-internet-de-las-cosas-y-las-oportunidades-para-el-sector-empresarial/

Marruecos, E. (26 de noviembre de 2016). Retrieved 26 de enero de 2017 from http://elena72mm.blogspot.mx/2015_11_01_archive.html

Microsoft. (2016). Retrieved 8 de abril de 2016 from Microsoft: https://www.microsoft.com/en-us/server-cloud/internet-of-things/default.aspx

Morales, J. A. (2016). *egomexico*. Retrieved 12 de marzo de 2017 from egomexico: http://www.egomexico.com/tecnologia_rfid.htm

Noriega, J. P., & Jiménez, L. E. (n.d.). *El tiempo*. Retrieved 30 de enero de 2017 from http://www.eltiempo.com/multimedia/infografias/que-es-el-internet-de-las-cosas/15119081

quees.info. (n.d.). Retrieved 8 de diciembre de 2016 from quees.info: http://www.quees.info/que-es-internet-de-las-cosas.html

Sanz, E. (n.d.). *Muy Interesante*. Retrieved 8 de abril de 2016 from Muy Interesante: http://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-el-qinternet-de-las-cosasq

Singh, P. (19 de diciembre de 2015). *letechworld*. Retrieved 8 de mayo de 2016 from letechworld: http://www.letechworld.com/blog-iot-smart-living-but-safety-first/

SorayaPaniagua. (15 de abril de 2012). Retrieved 7 de diciembre de 2016 from SorayaPaniagua: http://www.sorayapaniagua.com/2012/04/15/un-poco-de-historia-sobre-internet-de-las-cosas/

The Digital Business News. (16 de marzo de 2016). Retrieved 26 de Enero de 2017 from http://www.theplace4change.com/blog/el-iot-en-los-negocios

Valle, D. B. (6 de noviembre de 2014). Retrieved 5 de enero de 2016 from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/40044/6/dbliznakoffTFM0115memoria.pdf