RETOS EN LA SEGURIDAD DE DISPOSITIVOS PARA EL INTERNET DE LAS COSAS (IoT)

DONAEL STIVEN BARÓN ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERIAS – ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

RETOS EN LA SEGURIDAD DE DISPOSITIVOS PARA EL INTERNET DE LAS COSAS (IoT)

DONAEL STIVEN BARÓN ROMERO

Proyecto de Grado – Monografía presentado para optar por el titulo de ESPECIALISTA EN SEGURIDAD INFORMATICA

DANNY FERNADO LEON JARAMILLO
Director de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERIAS – ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 2020

DEDICATORIA

Me permito agradecer a Dios por permitir llegar al paso final de la Especialización en Seguridad Informática y haber aprendido muchas cosas valiosas para así poder continuar por el camino de aprendizaje de las nuevas innovaciones tecnológicas.

A mis padres y hermanos por el apoyo dado durante el transcurso de la Especialización y por el ánimo dado en los momentos difíciles.

A cada uno de los tutores que me acompañaron en el transcurrir de esta Especialización ya que sin su valioso aporte podemos construir nuevos conocimientos.

A mis amigos y compañeros de trabajo por el acompañamiento y su valiosa ayuda en los momentos difíciles.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

TABLA DE CONTENIDO

pág.

INTRODUCCIÓN *17*

1. DEFINICIÓN DEL PROBLEMA *19*

1.1 ANTECEDENTES DEL PROBLEMA 19

1.2 FORMULACIÓN DEL PROBLEMA 19

2 JUSTIFICACIÓN *20*

3 OBJETIVOS *21*

3.1 OBJETIVOS GENERAL 21

3.2 OBJETIVOS ESPECÍFICOS 21

4 MARCO TEÓRICO *22*

4.1 DEFINICIÓN 22

4.2 COMPONENTES Y CARACTERÍSTICAS 30

4.3 PLATAFORMAS 33

4.4 SEGURIDAD 37

4.5 LOS CIBERATAQUES 49

4.6 SOLUCIONES 56

4.7 IMPACTO EN LA SOCIEDAD COLOMBIANA 66

4.8 EL ECOSISTEMA 72

4.9 ACTUALIDAD EN COLOMBIA 74

4.10 CLOUD COMPUTING 76

4.11 BIG DATA 80

4.12 INTELIGENCIA ARTIFICIAL Y EL IOT 84

5 RESULTADOS DE LOS OBJETIVOS *93*

5.1 DESARROLLO DE OBJETIVO GENERAL 93

5.2 DESARROLLO DE OBJETIVO ESPECÍFICO 1 94

5.3 DESARROLLO DE OBJETIVO ESPECÍFICO 2 95

5.4 DESARROLLO DE OBJETIVO ESPECÍFICO 3 98

5.5 DESARROLLO DE OBJETIVO ESPECÍFICO 4 99

6 CONCLUSIONES.....100
7 BIBLIOGRAFÍA.....102

LISTADO DE ILUSTRACIONES

Pág.

Ilustración 1. Revolución industrial. Telectrónika (2018). 22
Ilustración 2. Seguridad IoT. Evaluandosoftware.com (2017). 37
Ilustración 3. Comparativa Dispositivo – Datos. Evaluandosoftware.com (2017)...47
Ilustración 4. Distribución mundial dispositivos IoT. CERT-PY, (2016). 49
Ilustración 5. Principales lugares afectados por ataques al IoT. Tripadvisor, (2019). 53
Ilustración 6. Ejemplo ataque ransomware. Bisso, (2017). 54
Ilustración 7. Proceso de robo de números de tarjetas de crédito. Paganini, (2017). 55
Ilustración 8. Ciclo de vida seguridad Internet de las Cosas. Gemalto, (2017). 61
Ilustración 9. Uso del Internet de las Cosas por Linz AG. Cisco, (s.f.). 65
Ilustración 10. Internet de las Cosas en la salud. Sanmartín, Avila, Vilora Núñez, & Jabba Molinares, (2016). 66
Ilustración 11. Plaza Claro en Bogotá. PYD, (2017). 75
Ilustración 12. Modelos de servicios Cloud Computing. Fu, (2017).....77
Ilustración 13. Cloud Computing. Wikipedia, (2019). 79
Ilustración 14. Big Data. Phillip, (2019). 80

GLOSARIO

DATAMINING: La explotación de grandes cantidades de datos a través de tecnologías que permiten que se produzca de forma automática o semiautomática. Gracias al Datamining, es posible visualizar patrones de comportamiento que explican cómo se comportan los datos y se detectan los errores.

LATENCIA: Se entiende al tiempo de respuesta en el que un dispositivo puede establecer conexión, independientemente del ancho de banda. Mientras mayor latencia, más lenta será la conexión del dispositivo a la red.

BIG DATA: Es el procesamiento masivo de datos y la transferencia de los mismos entre los dispositivos. Es uno de los términos más utilizados, puesto que es una de las esencias de esta tecnología.

E-SALUD: Conjunto de TICs (Tecnologías de la Información y Comunicación) utilizadas en herramientas para el diagnóstico, prevención, seguimiento y tratamiento de patologías. En la actualidad, estos instrumentos se conectan a la red para un mejor análisis y compartir información entre doctores, pacientes y familiares.

HARDWARE: Es el conjunto de elementos físicos que conforman los dispositivos tecnológicos, es decir, la parte tangible de la tecnología como, por ejemplo: pantallas, baterías, teclados.

IoT: La abreviatura de “Internet of Things” (Internet de las Cosas en inglés) representa todos los objetos de uso diario que utilizan el Internet para ofrecer una experiencia más completa y la conexión entre dispositivos. Por ejemplo, las pulseras de seguimiento cardiaco se conectan a la red y también pueden vincularse con los Smartphones, etc.

M2M: "Machine to machine" hace referencia al intercambio de información o comunicación entre dos dispositivos o más.

SMART CITIES: Se entienden a las ciudades que aumentan su eficiencia gracias a la conexión de red. Son muchos de los elementos que la conforman (vehículos, aparcamientos, carreteras, establecimientos, etc.). Estos elementos se conectan a la red y entre ellos para que los usuarios puedan disfrutar de mejores servicios.

SMART HOUSE: Una casa inteligente es aquella que tiene varios dispositivos conectados a Internet y entre ellos. En definitiva, juna Smart House permite al usuario controlar varios dispositivos del hogar mediante su móvil u otro dispositivo remoto.

SMART FARMING: La agricultura se suma al IoT. El desarrollo de aplicaciones y dispositivos tecnológicos para la agricultura han permitido la automatización de procesos como la optimización de resultados.

SOFTWARE: Son los elementos no físicos de los dispositivos tecnológicos. Este término hace referencia a aquello que no puede ser tocado, pero es vital para el funcionamiento. En el caso de los teléfonos inteligentes, las aplicaciones, el sistema operativo y otras funciones conforman el software.

4.5 G: Se encuentra entre la red 4G y la 5G. Está enfocada principalmente al Internet de las Cosas (IoT). En este caso, la red no solo se centra únicamente en ofrecer mayor velocidad, sino menos latencia. Esto quiere decir, que con ella será más difícil y menos probable que los dispositivos conectados se desvinculen de ella para que trabajen continuamente sin interrupciones.

RFID: Radio Frequency Identification (Identificación por radiofrecuencia en inglés). Es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID (son pequeños dispositivos, similares a las pegatinas, que pueden ser incorporadas o adheridas a un producto, un animal o una persona. Estas pegatinas contienen antenas para permitir recibir y responder peticiones por radiofrecuencia desde un emisor-receptor RFID). Su propósito fundamental es transmitir la identidad de un objeto (similar a un número único de serie) mediante ondas de radio.

RESUMEN

Desde la entrada de la red de redes en nuestras vidas se ha producido un gran cambio en la sociedad en general, un ejemplo de ellos es la comunicación de las personas, los pasatiempos y hasta la forma de estudiar tuvieron avances gracias al auge causado por el Internet y las Tecnologías de la Información (TIC) y en algunos casos han sido positivos. Este boom tuvo repercusión directa en las empresas y en la economía, ya que, con el desarrollo de modernos dispositivos, se empezaron a prestar nuevos servicios, generando más empleo y otras formas de comunicarnos con el mundo exterior sin siquiera moverse de sus casas como son los Smartphone.

Actualmente el Internet está llegando cada vez más a los hogares y se ha mejorado los índices de conectividad y velocidad que se puede apreciar en la medida de que las grandes empresas públicas y privadas han venido aprovechando estas tecnologías para migrar tramites que se hacen presenciales a realizar virtualmente, buscando la satisfacción del cliente y aportando a la reducción de gastos a las mismas.

Además, es significativo comprender que una buena conectividad conlleva una gran responsabilidad. El reto del Internet de las Cosas (IoT) es la confidencialidad de la información porque como sabemos los sistemas informáticos avanzan en la medida que los dispositivos inteligentes lo hacen los objetos que lo rodean y en este momento nos encontramos expuestos a los ciberataques y aquí es donde está el desafío de nosotros los usuarios, los gobiernos y los administradores de red es la de diseñar la seguridad necesaria para que nuestras vidas y la recopilación de datos de la misma no sea un elemento vulnerable, sino que sea beneficiosa y poder estar conectados de manera constante, sacando el máximo provecho al IoT y si podemos observar que los problemas de privacidad y confianza están presentes en los perfiles de configuración de estos y la cantidad de elementos que almacenará de

cada uno de los individuos que los emplean.

Palabras claves: Internet de las cosas, conectividad, cambios, implicaciones, beneficios, sociedad.

ABSTRACT

Since the entrance of the network of networks in our lives there has been a great change in society in general, an example of them is the communication of people, hobbies and even the way of studying made progress thanks to the boom caused by the Internet and Information Technologies (ICT) and in some cases have been positive. This boom had a direct impact on businesses and the economy, since, with the development of modern devices, they began to provide new services, generating more employment and other ways of communicating with the outside world without even moving from their homes as they are. the Smartphone.

Currently, the Internet is increasingly reaching households and has improved connectivity and speed rates that can be seen to the extent that large public and private companies have been taking advantage of these technologies to migrate paperwork that are made face to face virtually, seeking customer satisfaction and contributing to the reduction of expenses to them.

In addition, it is significant to understand that good connectivity carries great responsibility. The challenge of the Internet of Things (IoT) is the confidentiality of information because as we know computer systems advance to the extent that smart devices do the objects that surround it and at this time we are exposed to cyber-attacks and here is where the challenge of us users, governments and network administrators is to design the necessary security so that our lives and the data collection of it is not a vulnerable element, but it is beneficial and able to be connected constantly, making the most of the IoT and if we can see that the privacy and trust problems are present in the configuration profiles of these and the amount of elements that will store of each of the individuals who use them

Keywords: Internet of things, connectivity, changes, implications, benefits, society

INTRODUCCIÓN

El IoT es una evolución tecnológica que representa el futuro de las comunicaciones y la informática y su desarrollo depende las innovaciones en los diferentes campos de las redes (los sensores inalámbricos o la misma nanotecnología). Lo primero es conectar cada uno de los dispositivos que uno maneja diariamente y que tienen disponibilidad de conectarse a Internet, su identificación se realiza por radiofrecuencia y al ser identificados se pasa a la siguiente fase donde se encuentra la recolección y procesamiento de los insumos almacenados en el dispositivo conectado. Actualmente existen más de miles de millones de personas que se encuentran de una u otra forma conectadas a la red, tanto en su vida social, laboral, académica y familiar para estar comunicados, contribuyen en la toma de decisiones, en un mundo en el cual antes era todo físico (recopilar de la información de los usuarios de un banco en tarjetas tomado por medio de escritura) con lo digital (bases de datos de los clientes de la entidad bancaria), dentro de la posibilidad de permanecer “ONLINE” y localizable, está surgiendo una nueva generación de consumidores que da por hecho contar con conexión wifi y cualquier avance técnico que permita la movilidad.

El Internet de las Cosas, es uno de los movimientos en redes de comunicaciones que más se ha hablado últimamente porque si uno tiene algún dispositivo que tenga la disponibilidad de conectar a la red, se convierte automáticamente en una nueva fuente de información para todas las personas que vienen diariamente a sus vidas o en sus respectivos empleos. Pero, a la gente del común les resulta un tema extraño, hay quienes se preguntarán que es la sociedad interconectada, nos servirá en algo, que utilidad o beneficios nos traerá, será posible que esté a nuestro alcance o que cambios tendrá en la vida cotidiana, son solo algunas inquietudes que se tratará de resolver por medio de esta monografía, que en otras palabras vendría a

decir que el IoT es la evolución del mundo de las telecomunicaciones.

Actualmente se habla del Internet de las Cosas, como el último de los saltos de las redes de comunicaciones. Se busca determinar ¿por qué es valiosa su confidencialidad?, sus beneficios y posibles aplicaciones. La IoT al ser una tecnología nueva se requiere tener conocimientos para adaptarse a los cambios de la era digital (la inteligencia artificial, el pensamiento analítico, entre otros). Algunas estadísticas de este tema se pueden consultar en el informe de la Consultoría Forrester de junio de 2016. El problema del IoT es que se ha implementado y ha estado creciendo de manera rápida, ya que esto conlleva a agujeros de seguridad, por ende, últimamente han aumentado la cantidad de ciberataques debido a estas fallas, una demostración de ello fue el llevado a cabo por el botnet Mirai que era capaz de lanzar ataques de DDoS (Denegación de Servicio) a una velocidad de 650Gbps. Algunos ejemplos de estos problemas son los encontrados en cámaras IP con contraseñas por defecto, lavadoras, neveras, máquinas expendedoras de bebidas liquidas gaseosas o refrescos, porque se conectan a la red, pero no tiene ninguna clase de garantía y de aquí se desprenden la razón de realizar conexiones que permitan facilitar la vida diaria de cada uno de nosotros, mediante la automatización de procesos y de disponer información a la mayor brevedad posible, un ejemplo, es el control de semáforos y señales de tránsito al optimizar el flujo vehicular, reducir la contaminación ambiental y los tiempos en los recorridos dentro de las ciudades inteligentes.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Esta monografía se basa en dar un pequeño análisis a un tema de vital importancia para todo el mundo como es el internet de las cosas. Como es sabido el internet de las cosas está siendo potenciado en los objetos más comunes en cada una de nuestras viviendas, como son los portátiles, las PDAs, los celulares inteligentes, entre otras, que se conectaban por medio de circuitos cerrados, como lo son las cámaras, los sensores de movimiento, los escáneres, los cuales están conectados a una estación de video o una computadora y que además se puede conectar a una red local de una empresa. Es por eso que cualquier dispositivo que puede conectarse a Internet se puede volver fuente de información, realizando así la transformación en la forma de hacer negocios de una pequeña organización (ya sea pública o privada) y a su vez el día a día de millones de personas. Para tomar un ejemplo fiel del internet de las cosas tendríamos al ejemplo de un parking, en donde por medio de sensores de movimiento u otros, nos indicaría si los puntos de parqueo libres o no, además podemos hacer que el sistema de parking le indicará al conductor el lugar de parqueo designado, sin la necesidad de ir de piso en piso buscando uno.

.

1.2 FORMULACIÓN DEL PROBLEMA

La pregunta que se haría para la presente monografía es:

El Internet de las cosas conectará productos, compañías y ciudades, con esto en mente, ¿Cuáles serían los beneficios de los dispositivos que se usarán, se han considerado las posibles amenazas o vulnerabilidades por su uso y qué tipo de información será guardada, procesada y recolectada por los dispositivos IoT?

2 JUSTIFICACIÓN

El internet de las cosas (IoT) es una evolución tecnológica que representa el futuro de las comunicaciones y la informática y su desarrollo depende las innovaciones en los diferentes campos de las redes, como son los sensores inalámbricos o la misma nanotecnología. Lo primero que se debe hacer es la de conectar cada uno de los dispositivos que cada uno maneja diariamente y que tienen disponibilidad de conectar a internet, con la identificación de estos dispositivos por medio de radiofrecuencia y cuando sea identificados se pasa a la siguiente fase que es la de la recolección y procesamiento de la información del dispositivo conectado.

Actualmente existen más de miles de millones de personas que se encuentran de una u otra forma conectadas a internet tanto en su vida social, laboral, académica y familiar para estar comunicados, contribuyen a que la tecnología sirva como una herramienta de colaboración y de toma de decisiones, en un mundo donde antes era todo físico (como guardar la información de los clientes de un banco en tarjetas con la información de cada uno de ellos tomado por medio de escritura) con lo digital (bases de datos de los clientes de un banco), dentro de esta posibilidad de estar permanentemente conectado y localizable, está surgiendo una nueva generación de consumidores que da por hecho contar con conexión Wifi y cualquier avance técnico que permita la movilidad.

La razón de realizar conexión con la red es la de facilitar la vida diaria de cada uno de nosotros, mediante la automatización de procesos y de disponer información a la mayor brevedad posible, como, por ejemplo, el control de semáforos y señales de tránsito para optimizar el flujo, reducir la contaminación ambiental y los tiempos en los recorridos dentro de las ciudades inteligentes.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Realizar un estudio monográfico que permita determinar los problemas, beneficios y cambios a partir del uso de tecnologías disruptivas como el Internet de las Cosas (IoT, Internet of Things, por sus siglas en inglés) en la sociedad colombiana.

3.2 OBJETIVOS ESPECÍFICOS

1. Conocer el Internet de las Cosas (IoT), sus beneficios, sus complicaciones y cambios en la vida de las personas, empresas y en la sociedad en general.
2. Recopilar información necesaria para realizar la investigación para la monografía.
3. Dar a conocer el futuro informático de muchos de los objetos que marcarán esta nueva revolución digital.
4. Describir conceptos básicos sobre el Internet de las Cosas (IoT).

4 MARCO TEÓRICO

4.1 DEFINICIÓN

Ilustración 1. Revolución industrial. Telectrónika (2018).

El vocablo IoT significa la interconexión digital de objetos cotidianos con Internet, pero para otros autores es:

CSIRT – CV[1] nos presenta la siguiente definición:

> "IoT hace referencia a los dispositivos que se pueden interconectar a través de la red. El vocablo va mucho más allá, por la razón de englobar todos los instrumentos que hasta ahora el momento no tenían conectividad como las neveras, los televisores, lo que permite controlar de forma remota por medio de aplicaciones de Internet el uso de los mismos. La tendencia es que siga evolucionando exponencialmente. Un ejemplo de ello, en la vida real se encuentra en la domótica, ya que a los usuarios se les permita disponer de un dispositivo instalado en sus casas para verificar el encendido de la calefacción o de las luces, abrir y cerrar persianas o el control sobre los accesos a la casa. La expansión del IoT trajo consigo la llegada de los wearables (usables), que son pequeños aparatos electrónicos que lleva un individuo capturar información de ciertas actividades que realiza. Algunos ejemplos son los relojes con

GPS, que además disponen de acelerómetro, pulsímetro, entre otros. Estos también encajan en esta categoría las Google Glass, los sensores incorporados a la ropa, las zapatillas Nike+ o los localizadores en los llaveros".

COLCOM 2014[2], en Foros ISIS nos presenta la siguiente definición:

"IoT, es una red de dispositivos inteligentes interconectados, contando con cierta autonomía y que puede responder a comandos remotos de sus propietarios. Un ejemplo es el Smart Grid que tiene la función de controlar la distribución de la electricidad. Uno de los retos del IoT es garantizar una confianza cuando se envíen estas señales a los aparatos electrónicos y cómo afectará la privacidad de las personas. Desafortunadamente a nadie se le ocurrió pensar en los riesgos que traían consigo, se idearon parches y / o actualizaciones de seguridad para mitigarlos, pero se encontraron con algunas vulnerabilidades y fallas en los códigos de las aplicaciones puestas desde la fábrica".

---

[1] Centre Seguretat TIC de la Comunitat Valenciana CSIRT – CV. Generalitat Valenciana. Unión Europea. Seguridad en Internet de las cosas: Estado de arte. Documento público. 42 p. Disponible en: http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

[2] COLCOM 2014. Foros ISIS No. 5. Seguridad, gran reto para internet de las cosas. Págs. 41 – 42. Disponible en: https://sistemas.uniandes.edu.co/es/images/foroisis/revista/5/pdf/V5_01:Foros_ISIS_5_Seguridad_gran_reto_para_internet_de_las_cosas_pdf

La Fundación de la Innovación Bankinter[3] nos presenta la siguiente definición:

> “IoT es la integración de instrumentos cotidianos conectados a Internet por redes fijas o inalámbricas. Con el IoT todo objeto es fuente de estudios o análisis y esto empieza a transformar la forma en cómo se hacen las operaciones comerciales, la organización de las empresas y el quehacer diario de millones de personas. Las aplicaciones IoT han sido enmarcadas en llegar al consumidor, ya que son los directos descubridores de los pros y contras que traen estos en la vida diaria. El IoT ha incursionado en sectores de logística, la salud, el medio ambiente y en los consumidores y el primer aparato de difusión de esta tecnología fue el Smartphone. En este informe, el IoT está compuesto en varias capas: la primera capa compuesta por el hardware, que es la parte física, en donde encontramos que los sensores son las piezas fundamentales del IoT, ya que ellos permiten que los objetos interactúen con los ordenadores a través de la red y recopilan información valiosa sobre el entorno y se puede observar tres tendencias: la miniaturización que consiste en la reducción de los mecanismos electrónicos y que va de la mano con la nanotecnología, un ejemplo son los microprocesadores, el desarrollo de nuevas tecnologías que es la infraestructura capaz de conectarse con la mejor calidad y velocidad que se pueda ofrecer la generación de transmisión de datos 3G o LTE, 4G, Wifi hostposts (son puntos calientes de conexión inalámbrica en los aeropuertos, cafeterías, bibliotecas, entre otros) y la creación de elementos simples e inteligentes y por ende, cobra vital importancia los algoritmos (que son un conjunto ordenado y finito de pasos que permite la ejecución de una tarea o resolución de un problema y se busca satisfacer los requerimientos del negocio), uso de nuevos servicios en tiempo real como la gestión de incidentes, supervisión de labores humanas y se encuentra con la utilización de software óptimo para la realización de las actividades y

explotación de otras fuentes y así poder tener un cambio radical en los modelos transaccionales".

A propósito de la definición de este concepto, Elena Sanz[4] dice:

"El IoT es un concepto que nació en el Instituto de Tecnología de Massachusetts – MIT, donde trata la revolución de las relaciones entre los objetos y las personas, que de manera directa se conectaran con ellos y a la red. Todo esto es gracias al sistema RFID (Radio Frequency Identification- Identificación por radiofrecuencia) que es un microchip que podrá integrar cualquier objeto del hogar, trabajo o de la ciudad. De acuerdo con la declaración del CEO de Ericsson, Hans Vestberg: "*Si un individuo se conecta a la red, le cambia la vida, pero si todas las cosas y elementos se conectan el que se renueva es el mundo*"".

[3] Fundación de la innovación Bankinter. El internet de las cosas en un mundo conectado por objetos inteligentes. 2011. 78 págs. Disponible en: http://www.belt.es/expertos/imagenes/XV_FTF_El_internet_de_las_cosas.pdf

[4] SANZ, Elena. ¿Qué es el internet de las cosas? En: Revista Muy interesante. Disponible en: https://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-el-qinternet-de-las-cosasq

A propósito de la definición de este concepto, María Alejandra Medina[5] dice:

> “Kevin Ashton fue quien acuño el termino IoT y que hoy se utiliza al referirse a un mundo en el que todo – la casa, electrodomésticos, carros, mobiliario urbano, máquinas industriales – estará conectado a Internet, y su objetivo principal es arrojar reportes en tiempo real que permita tomar decisiones. Un modelo de ello sería cuando se llene el bote de basura de una determinada calle, la idea es que alguien del servicio de aseo lo sepa inmediatamente y lo solucione a la mayor brevedad posible. Estuvo en Colombia en el lanzamiento de la firma Claro de la nueva generación de transmisión de datos 4.5G que hará parte de la revolución tecnológica. este pionero dijo que el cambio significativo se verá en la calidad de vida, que por medio del celular podamos especificar enfermedades y una de estas y por ende una de las más letales es la Enfermedad pulmonar Obstructiva Crónica, usando mecanismos instalados, el paciente solo necesita soplar en un micrófono y con la grabación del sonido se pueda diagnosticar si padece o no de EPOC. Por consiguiente, en el año de 1999, él trabajaba en P&G (Procter & Gamble) y tenía que resolver un problema y era que sus productos tradicionales no están disponibles en las tiendas y que la solución estaba en colocar sensores conectados a la red, con el fin de saber cuándo se estaban agotando y así poder reabastecer rápidamente el producto agotado. Era una teoría loca de los años 90s. La expresión, se manejaba en pequeños grupos de técnicos hasta la llegada de Twitter, pues gozaba de un acrónimo único y corto. El término ha cambiado mucho ya que se imaginaban tener todos los objetos interconectados era fundamental y que estos viajaban a la computadora con el sistema instalado, se esperaba que los aparatos cayeran en sus precios a pocos centavos, y lo que no imaginaron fue la proliferación de las conexiones Wifi, los celulares y la tecnología GPS. Según él, la seguridad digital es muy buena pero su puesta en marcha es muy mala

con frecuencia. Los mayores retos de la implementación de IoT no es el hardware, no es el software, no es la conexión, no son las velocidades de las redes sino el verdadero reto es el procesamiento de los valores capturados y almacenados porque son un vasto volumen de elementos valiosos y continuos".

Domodesk[6], nos presenta la siguiente definición:

"El IoT es la consolidación a través de la red de redes de una red, que puede alojar una gran multitud de objetos o aparatos, es decir, conectar todas las herramientas del mundo en sí, como los vehículos, electrodomésticos, dispositivos mecánicos (calzado, muebles, maletas, etc.), para pretender, que esta tecnología pueda hacernos mejorar nuestras vidas y proporcionar una mayor confianza. Por consiguiente, se busca la calidad de vida de las personas, pero nos encontramos con una preocupación y es lo referente a los temas de seguridad y privacidad de los datos ya que se vuelve en un control de manos ajenas que nos hace ser más vulnerables. La IoT trae algunas ventajas, un ejemplo de ello es la de saber en cada momento en donde se encuentra un elemento así haya sido hurtado de su vivienda usando los sensores instalados y conectados. El IoT estaría dotado de varias capacidades:

- La comunicación y cooperación, es decir, la capacidad de conectarse a los servicios de Internet y establecer comunicaciones con los servidores, intercambiar y actualizar los datos entre ellos.

- Capacidad de direccionamiento, es decir, configurar y localizar los objetos desde cualquier parte de la red.

- Identificación con tecnologías como RFID (identificación por radiofrecuencia), NFC (Cerca de un campo de comunicación), códigos de barras de lectura óptica, entre otros.

- Localización, es decir, saber en todo momento en donde se encuentra el objeto.

- Actuación, de acuerdo con el tipo de dispositivo puede manipular su entorno.

El nivel de inteligencia de estos dispositivos se divide en cuatro (4) niveles:

- Identidad: sistema de identificación será único.

- Ubicación: Podrá saber en dónde está o ha estado el objeto.

- Estado: Comunicará su estado y sus características.

- Contexto: Será capaz de percibir su entorno.

Los protocolos de comunicación que usara son: ZigBee (IEEE 802.15.4), BlueTooth LTE, 6LowPan, Wifi, GSM y TCP/IP, por medio de la tecnología M2M (intercambio de información entre dos máquinas) y son dispositivos capaces de establecer transmisiones con un servidor y con otros mecanismos M2M. Se divide en dos componentes:

- Los dispositivos de gestión que son los encargados de la administración de los datos, algunos ejemplos son las alarmas de

los hogares, contadores, paneles de información, puntos de venta, entre otros.

- Los dispositivos de M2M que son los instrumentos conectados de manera remota para capturar, recoger y mantener la información con el servidor.

- Servidor que recibe y envía la información de las máquinas y a la vez haga una gestión eficiente de la misma.

Red de comunicación, es el conjunto de medio físico por donde viaje la información y que puede ser de dos clases: cableado o inalámbrico, siendo este último el más adecuado puesto que carece de lógica implementar Internet de las Cosas (IoT) por cables, a no ser que sea un dispositivo que por su diseño necesite ser usado de esa manera".

---

[5] MEDINA C, María Alejandra. La historia detrás del internet de las cosas, 2017. Disponible en: https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678

[6] DOMODESK. A fondo: ¿Qué es el IoT (¿Internet de las cosas?). Disponible en: http://www.domodesk.com/221PEREZ, Vicente. -que-es-iot-el-internet-de-las-cosas.html

4.2 COMPONENTES Y CARACTERÍSTICAS

A propósito de los componentes del IoT, Berni Hidalgo Castro, Jack González Jiménez y Royers Murillo Castro[7], nos dice lo siguiente:

> "Antes de entrar en saber cuáles son las características, es fundamental conocer los componentes fundamentales que hacen del IoT una realidad y son:
>
> - Hardware que tiene como fin realizar que los objetos físicos respondan y que se permita proceder a la recuperación de los datos y responder a las instrucciones impartidas por el usuario.
>
> - Software: que debe tener la habilitación para la recolección, almacenamiento, procesamiento y manipulación de datos.
>
> - Infraestructura de comunicación que son los protocolos y tecnologías que permiten las transmisiones entre dos objetos físicos que pueden intercambiar información.

Con estos componentes en mente, nos preguntamos cuales son los pro y contras que trae a nuestras vidas el IoT. En las ventajas encontramos la facilidad de comunicación e intercambio de datos, la simpleza de las tareas diarias o cotidianas, la salud, la confiabilidad en su monitoreo en tiempo real y en las desventajas están la seguridad de los dispositivos ante ataques cibernéticos, la dependencia al no poder disponer de la tecnología por alguna razón, la estabilidad de la conexión a Internet, la simplicidad del acceso a información no adecuada y la dificultad de no controlarla, por su gran cantidad y volumen al momento de la recolección de la misma, por los sistemas electrónicos del IoT".

A propósito de las características del IoT, Berni Hidalgo Castro, Jack González Jiménez, Royers Murillo Castro[8] y Ricardo Vega[9], nos dice lo siguiente:

> “El Internet de las cosas (IoT), es una combinación de software y de hardware, convirtiendo al producto o a la aplicación en un dispositivo de tipo inteligente. Por ello se encuentra que estos productos o estas aplicaciones tengan seis características en común y son:
>
> - La conectividad, este rasgo dota al IoT de toda su potencia porque permite la coexistencia y acceso a la red sin importar el medio circundante y por ello se puede capturar y transmitir datos indistintamente dentro de una ciudad.
>
> - Sensibilidad, así como nosotros somos capaces de entender el mundo que nos rodea y a las personas gracias a nuestros sentidos. En el IoT esto se logra por medio de dispositivos que son los encargados de transportar señales o indicaciones a las máquinas, usando tecnologías de detección y reconocimiento de movimientos y expresiones faciales. En otras palabras, las hemos dotados con el fin de que puedan comprender nuestra compleja sociedad y den respuestas eficaces a los problemas que se presentan cotidianamente.
>
> - Intercambio, gracias al establecimiento de una comunicación entre el mundo físico, las personas y las máquinas, de igual modo sucede en el IoT, ya que la característica de expresividad porque es la clave a la hora de crear los productos que interactuarán con la sociedad. Por ello, es adecuado saber que los datos obtenidos y capturados del usuario, serán las interfaces visuales y parte del éxito cuando se decidan tomar una vida simple y cómoda, donde

se establecerán los requisitos óptimos para que la información recolectada sea almacenada en buenas condiciones ambientales y sea llevada por medio de dispositivos a buen término.

- Energía, es la fuente que hace mover nuestros dispositivos, pero desafortunadamente no se cuenta en la actualidad con un sistema inteligente que pueda aprovechar tanto la generación, la eficiencia y la infraestructura de transporte de dicha resistencia, que hasta este momento solo es empleada por medio de acumuladores (pilas) que tienen la desventaja que con el tiempo se van deteriorando y que la energía de las baterías pueden ser utilizada por el dispositivo que tenga la capacidad de transmitirla y a la vez ponerla a funcionar normalmente.

- Seguridad, sobre este tema todas las partes que están involucradas (creadores, intermediarios y usuarios finales) tienen que buscar criterios sólidos que deben cumplir con los pilares de la seguridad de la información (la confidencialidad, la integridad y la disponibilidad de esta) y con el estudio realizado nos permite garantizarla y protegerla con el uso de las respectivas medidas adoptadas en los servicios de custodia de los datos y el manejo de los incidentes de estos, ante ataques cibernéticos".

[7] HIDALGO CASTRO, Berni, GONZÁLEZ JIMÉNEZ, Jack y MURILLO CASTRO, Royers. El internet de las cosas, 2017. Disponible en: http://alfarosolis.com/content/PDFs/IF7100/Semana14/Iot.pdf

[8] Ibíd.

[9] VEGA, Ricardo. Seis características clave del Internet de las cosas, 22 de octubre de 2015. Disponible en: https://ricveal.com/blog/6-caracteristicas-clave-del-internet-de-las-cosas/

4.3 PLATAFORMAS

A propósito de las plataformas IoT, Berni Hidalgo Castro, Jack González Jiménez, Royers Murillo Castro[10] y Álvaro Cárdenas[11], nos dice lo siguiente:

> "Las plataformas IoT son espacios entre los sensores de los dispositivos y las redes. Esta plataforma se pone a la disposición de los instrumentos sensibles que proporcionará la información usando aplicaciones dándole sentido a la gran cantidad y volumen de datos que son generados por los cientos de aparatos que se usan cotidianamente en cada una de nuestras vidas. Para que una de estas se considere 'plataforma IoT' tiene que cumplir con cuatro condiciones:
>
> - Plataformas de conectividad / M2M que se especializan en los dispositivos conectados a las redes de comunicaciones, un ejemplo de ello son las tarjetas SIM.
>
> - Backend IaaS (Infraestructura como un servicio backend) que proporciona alojamiento y potencia para las aplicaciones y los servicios.
>
> - Plataformas de software específicos para hardware, es decir, que las empresas venden sus propios dispositivos conectados a su backend y que nadie más puede usarlos.
>
> - Extensiones / Software para empresas de consumo, es decir, que pueden convertirse en algún momento como plataformas IoT, cuando estas sean muchas más avanzadas. Actualmente existe paquetes empresariales y sistemas operativos que permiten la integración de los dispositivos IoT, un ejemplo de ello es Microsoft

Windows 10.

Las propiedades de una plataforma IoT, se clasifican en ocho bloques:

- La conectividad y la normalización, que garantiza la transmisión de datos y la interacción con todos los dispositivos por medio de protocolos y formatos diferentes gracias a una interfaz que puede ser gráfica.

- La gestión de los dispositivos, que garantiza que los aparatos interconectados están funcionando correctamente.

- Las bases de datos, que deben ser de almacenamiento escalable por el gran volumen de información y velocidades que se manejen.

- El procesamiento y gestión de la acción, es decir, la programación de las actividades programadas en los sensores y para realizar la ejecución de las instrucciones dadas a los mismos.

- Analítica, es decir, el análisis de la información obtenida y almacenada en los dispositivos.

- La visualización, es decir, observar las tendencias de los cuadros de mando cuando los datos son visualizados en los dispositivos.

- Las herramientas adicionales, porque permite a los desarrolladores de los prototipos, probar y comercializar los dispositivos creados.

- Interfaces externas, es decir, la integración de las API (Interfaces de Programación de Aplicaciones), SDK (Kits de Desarrollo de Software) y las puertas de enlace.

Entre las plataformas IoT más conocidas tenemos:

- Amazon Web Services (AWS) IoT, ofrece características como el registro para reconocer los aparatos conectados, SDK (Kit de desarrollo de software), sombras del dispositivo, puerta de seguridad y motor de reglas de evaluación de mensajes entrantes.

- Microsoft Azure IoT, ofrece características como las sombras del dispositivo, un motor de reglas, registro de identidad y monitoreo de la información.

- ThingWorx IoT Platform, ofrece características como conectividad fácil de los dispositivos con la plataforma. Elimina la complejidad en la mejora de las aplicaciones IoT, programa de intercambio entre desarrolladores para un rápido desarrollo, aprendizaje integrado automatizado en el análisis de grandes cantidades de datos y la implementación de soluciones IoT basados en la nube.

- IBM Watson, ofrece características como la gestión de dispositivos, comunicaciones seguras, intercambio y almacenamiento de datos en tiempo real.

- CISCO IoT Cloud Connect, ofrece características como conectividad de voz y datos, gestión del ciclo de vida del SIM, control de sesiones IP y facturación e informes personalizados”[10] [11].

[10] HIDALGO CASTRO, GONZÁLEZ JIMÉNEZ y MURILLO CASTRO, Op. Cit.

[11] CÁRDENAS, Álvaro. Plataforma IoT - Secmotic, 28 de noviembre de 2016. Disponible en: https://secmotic.com/blog/plataforma-iot/

4.4 SEGURIDAD

Ilustración 2. Seguridad IoT. Evaluandosoftware.com (2017).

Con ello, se refiere a la protección que es necesaria para salvaguardar nuestra información ante ataques por parte de ciberdelincuentes y Margaret Rouse[12], nos dice lo siguiente:

> "La solidez del IoT, es un área preocupada por salvaguardar los dispositivos y redes conectadas, por su creciente demanda de manera exponencial. Por lo general están provistos de sensores incluidos, que son usados en las transmisiones industriales de M2M, las estructuras eléctricas inteligentes, la automatización de viviendas y edificios, las comunicaciones entre vehículos y las computadoras adaptadas en ellos. La verdadera preocupación son los aparatos empleados para IoT, se venden con viejas versiones de sistemas operativos integrados y sin actualizaciones de seguridad, que consigo trae muchas veces no se puede cambiar las contraseñas predeterminadas. Uno de los puntos importantes es mejorar la protección, directamente a través de Internet, segmentando la red, teniendo acceso restringido, además cuando se

segmente, se debe monitorear e identificar tráfico anómalo potencialmente peligroso".

A propósito de la seguridad del IoT, Logicalis[13] nos dice lo siguiente:

> "El IoT posee un impacto en la forma de interactuar con el mundo que nos rodea (los televisores, frigoríficos, automóviles, medidores inteligentes, monitores de salud, entre otros) y son elementos que forman parte de la nueva tecnología innovadora. Así como cuando llegas las cosas son buenas, el IoT guarda desventajas al ser un objetivo de los ciberdelincuentes. El principal objeto de la seguridad del IoT es la obtención y retención de la confianza de los usuarios, ya que de estas averiguaciones obtendremos una imagen realista de los gustos y convicciones de cada uno de los clientes y el gran reto es protegerla, asegurarla y conservarla adecuadamente. Desafortunadamente, los medios de comunicaciones hacen alusiones a los usos maliciosos de los instrumentos IoT, pasando por alterar un marcapasos hasta tomar el control total de un vehículo. No debemos creer que las implicaciones de garantía pueden ser económicas o productivas para una empresa, sino que se supone que el compromiso de las empresas es dar tranquilidad y manejo de la confidencialidad de la información que nos comparten y la cual tiene la obligación de defenderla ante cualquier ataque. Se debe poner de manifiestos los principales peligros a los que se enfrenta los aparatos IoT y son la cantidad y volumen de datos a manejar por los dispositivos, los perfiles públicos no deseados, la escucha secreta y la encriptación de los mensajes".

Monserrath Vargas[14], nos dice lo siguiente:

> "El IoT es una tendencia donde los dispositivos se conectan no solo a la red, sino que se interconectan entre sí y nos conecta. Cuando se enciende un

bombillo desde una localización remota, los refrigeradores podrán avisar si hay o no alimentos, y los sistemas de vigilancia le dirán si está bien o mal vestido. Según Denise Giusto, investigadora de ESET Latinoamérica, afirmo que uno de las principales preocupaciones del IoT es el tema de seguridad porque termina siendo un añadido del proceso. De acuerdo con una investigación realizada en el año 2015 por Hewlett-Packard, demostró que el 90% de los aparatos recolectaban datos de las personas, el 70% se conectaba a la red, pero enviaba mensajes no encriptados y el 80% tenían problemas de privacidad. Los instrumentos IoT evaluados fueron diez (televisores, cámaras web, termostatos, tomas de corriente, controladores de riego, cerraduras de puertas, alarmas, etc.). Por ende, se dan unas recomendaciones, tanto a los usuarios como a los desarrolladores de aplicaciones y estas sugerencias son para el consumidor, en el instante que adquiera un artículo IoT, se debe asegurar que codifique o disfrace la información y que se pueda acceder a ellos con el uso de una contraseña, leer las condiciones de los servicios (en algunos países puede ser un delito y en otros no); por parte de los programadores deberían usar la autenticación en dos pasos, es decir, que al momento de autenticarse a un servicio de Internet en cualquier dispositivo IoT, se le pida acceso al sistema y a manera de paso adicional asegurarse si el que accedió a la cuenta fue el cliente o un tercero por medio de una pregunta secreta y su respuesta es conocida por el titular de la misma".

---

[12] ROUSE, Margaret. Seguridad del internet de las cosas. Revista TechTarget – Search DataCenter en español, febrero de 2017. Disponible en: http://searchdatacenter.techtarget.com/es/definicion/Seguridad-de-Internet-de-las-Cosas

[13] LOGICALIS: BUSSINESS AND TECHNOLOGY WORKING AS ONE. La seguridad del internet de las cosas, en el punto de mira. 10 de mayo de 2017. Disponible en: https://blog.es.logicalis.com/seguridad/la-seguridad-del-internet-de-las-cosas-en-el-punto-de-mira

[14] VARGAS L, Monserrat. Seguridad: el principal reto del internet de las cosas, 07 de julio de 2016. Disponible en: http://www.nacion.com/tecnologia/informatica/seguridad-el-principal-reto-para-internet-de-las-cosas/S4KUHLUCOFHXDJPOWEW4OLSAA4/story/

Karen Stark[15], nos dice lo siguiente:

> “Las penetraciones en la red y las infracciones de datos en IOT, se ha vuelto una práctica diaria en los sectores: nuclear, minorista, sanidad, consumo, social, etc., y el motivo principal es simple, la totalidad de los instrumentos IoT son pocos íntegros debido a su escasa o nula protección. La mayoría de los ingenieros que desarrollan los aparatos tienen una formación sobre la probabilidad del sistema para que cumpla una función determinada en ciertas condiciones por un tiempo en los procesos y arquitecturas especificas en cada una de las aplicaciones desarrolladas, mientras tanto los especialistas TI tiene capacitaciones en ciberseguridad, por ello una solución real a los problemas presentados es la unión de ambos, desde el comienzo de los proyectos que se crean, con el fin primordial de dar confianza, integridad y fiabilidad a la información que es almacenada o enviada por estos. Algunos mecanismos de estabilidad de los dispositivos IoT son: Autenticación de los puntos de origen y destino, supervisión de los patrones de tráfico, cifrado de los paquetes y envío de los mensajes por medio de un túnel seguro, identificación de los mismos determinando cuáles son o no fiables y los desconocidos, aplicación de las políticas que controlan el acceso y servicios en la red, uso de firewalls y sistemas de detección y prevención de intrusos, etc”.

[15] STARK, Karen. La seguridad del internet de las cosas, 28 de agosto de 2017. Disponible en: http://www.evaluandosoftware.com/la-seguridad-del-internet-las-cosas/

Rómulo Vargas[16], nos dice lo siguiente:

> "El IoT surge por la motivación y necesidad de las organizaciones por las demandas de control remoto de las operaciones, en donde se debían controlar sensores de movimiento, de humedad, de accesos, etc., debido a su éxito se empezaron a construir para uso individual y de utilidad en la vida cotidiana, ya que se puede supervisar el cuarto de los niños, vigilar la temperatura, la iluminación y todos conectados vía WIFI y que pueden ser accedidos por cualquier dispositivo móvil. Si aplicamos en el quehacer diario nos encontramos con los recordatorios de la agenda personal (visualizado en un televisor Smart o por un software descargado), poder tomar las mediciones de nuestro ritmo cardíaco y calor corporal y así enviarla a un sistema de climatización del lugar de nuestra vivienda en el cual se encuentra instalado, por medio de reconocimiento de voz e indicarle si deseamos prender y apagar los electrodomésticos. En su conjunto parece muy bueno, pero uno se pregunta, ¿es segura la tecnología IoT? Desde un punto de vista práctico la respuesta es **SI**, sin embargo, no existe seguridad 100% infalible. Si alguna vez quiere realizar la conexión de cada uno de los dispositivos al IoT, se debe consultar con un profesional que conozca el IoT y preguntar sobre los beneficios y riesgos, la confidencialidad de los datos almacenados y los tipos de aparatos disponibles. Algunos de los errores más comunes en la configuración de estos son: Contraseñas en blanco o predeterminadas, las marcas de las empresas fabricantes que son poco reconocidas y que además muchos de ellos son diseñados con Backdoors (puertas traseras) ocultas de fábrica, envío de información a nubes pocos confiables, comunicación en canales inseguros sin tener técnicas de encriptación".

[16] VARGAS, Rómulo. La seguridad en tiempos del internet de las cosas (IoT), 2016. Disponible en: http://www.maint.com.ec/la-seguridad-en-tiempos-del-internet-de-las-cosas/

Carmen Jane[17], nos dice lo siguiente:

> “La definición de los expertos informáticos sobre la situación de la confiabilidad de los dispositivos interconectados al IoT, es de “ESTADO DE PÁNICO”, esto debido a los ataques sufridos por Twitter, Amazon y Spotify, el pasado 21 de octubre de 2016, se encontraron que tenían fallas de provenientes de fábrica, un ejemplo fue la contraseña que trae por defecto el aparato y que nadie podía cambiarlos. El gurú Phil Zummermann, quien es el inventor del protocolo PGP (que es un programa de criptografía usado en Internet, con el objetivo de proteger nuestra privacidad), había calificado la seguridad del IoT, como un desastre, porque se encontraban muchas vulnerabilidades detectadas pero que no fueron escuchadas. Tras este ataque ISACA, reclama que todos los instrumentos que desean conectarse a IoT tengan los mismos requisitos de confianza a la hora de comercializarlos. Los fallos de los aparatos que se encuentran conectados a IoT pueden traer consigo riesgos a la vida de las personas, algunos problemas se reflejarían en los controles de vigilancia, los servicios médicos, los semáforos, los cambios de vías férreas, entre otros. Según especialistas en ciberseguridad, dicen que los fabricantes crean soluciones con poca memoria, ya que, para ellos, es más beneficioso la reducción de los costes de producción que la calidad del elemento o software fabricado”.

[17] JANE, Carmen. Alerta por la inseguridad del internet de las cosas, 29 de octubre de 2016. Disponible en: http://www.elperiodico.com/es/sociedad/20161029/alerta-por-la-seguridad-del-internet-de-las-cosas-5595145

Iván Martín Barbero[18], nos dice lo siguiente:

> “Respecto a la estabilidad del IoT, es evidente las vulnerabilidades que poseen los dispositivos y consigo permiten que los ciberdelincuentes tengan una puerta atractiva para realizar sus hazañas o desafíos porque estos ofrecen poca resistencia, un caso de esto son los ataques DDoS (Denegación de Servicios). Otro punto de falla sobre la seguridad, es parte de los usuarios ya que muchos no cambian la contraseña que viene por defecto, y es significativo recordar lo que dice en su informe ForeScout, que un hacker solo puede necesitar de tres minutos en ingresar en su dispositivo y su reparación fácilmente dure días o semanas. Uno de los factores que se deben tener en cuenta a la hora de conectar aparatos IoT es el establecimiento de protocolos claros y generales consiguiendo que la protección sea real, un ejemplo es la estandarización del protocolo WEP o WPA en los Routers WIFI. En otras palabras, el IoT tiene cosas importantes como son la facilidad de controlar una casa inteligente, pero a la vez es peligrosa si no se utilizan de la forma correcta ya que sus consecuencias pueden a ser desastrosas”.

Irfan Saif, Sean Peasley y Arun Perinkolam[19], nos dice lo siguiente:

> “Desde su punto de vista, la seguridad del IoT tiene un lado oscuro y la creación de datos y su alta velocidad al momento de compartirlos y esto ya es un peligro, por ejemplo, al realizar la localización de un vehículo se supone que es una vulneración de la privacidad del conductor, pero si se efectúa el hackeo del mismo automóvil finalizando en la toma su control ya es considerado una amenaza. Lo que separa IoT de Internet es la eliminación de las personas, es decir, cuando está en la red, el usuario requiere ingresar algunas referencias para poder efectuar compras, visitar páginas web o abrir las redes sociales habituales como Facebook,

mientras que el IoT no solicita la participación de los usuarios porque por medio de esta tecnología, la información es recogida por sensores y los analiza a una gran rapidez. Por ello se necesita tener en cuenta tres recomendaciones:

- La prevención, en donde establecemos distintas capas y filtros para complicar el acceso a la información:

    - La seguridad, en donde los sensores que capturan y analizan la información pueden contener malware o código malicioso, filtraciones y/o identificación de spoofing, entre otros.

    - El permiso de la interoperabilidad que consiste en el intercambio de información entre dos o más dispositivos conectados permitiendo dar servicios en línea a los clientes, sin embargo, el problema se presenta cuando se trabajan sobre los mismos datos, pero con diferentes formatos.

    - Realizar retrofitting (reequipamiento), es decir, cambiar las versiones antiguas de los dispositivos que se usan por unos más modernos porque puede significar invertir menos recursos económicos que en desarrollar nuevas tecnologías, como es el caso de los sensores de los sistemas de control industrial (ICS, por sus siglas en ingles).

    - La funcionalidad extendida, es algo a lo que pasa con el retrofitting, pero con la opción de incorporar dentro

de los dispositivos de protocolos con los cuales no estaba previsto que funcionará, por lo tanto, se logra endurecer las medidas de seguridad ante las vulnerabilidades presentadas en anteriores versiones.

- Mantenerse alerta cuando se presenten fallos de seguridad y en el menor tiempo posible solucionarlos.

- Resistencia al neutralizar las amenazas y así impedir que se propaguen. Se debe tener en cuenta las fuentes de riesgo porque estas se encuentran en continuo cambio impidiendo poder identificar el peligro y su pronta solución. Un ejemplo son los datos, en donde se establece un ciclo de vida de los mismos y que estos no puedan ser retenidos más allá del tiempo estipulado, con lo cual las empresas recopilan muchísima información que es valiosa y que tiene un mejor contenido".

[18] MARTIN BARRERO, Iván. La seguridad del internet de las cosas (IoT), un grave problema a resolver, 26 de octubre de 2016. Disponible en: https://cincodias.elpais.com/cincodias/2016/10/26/lifestyle/1477469985_167878.html

[19] SAIF, Irfan, PEASLEY, Sean and PERINKOLAM, Arun. Safeguarding the Internet of the Things: Being secure, vigilant, and resilient in the connected age, Issue 17, 2015. Disponible en: https://www2.deloitte.com/es/es/pages/about-deloitte/articles/La-proteccion-del-Internet-de-las-Cosas-seguridad-vigilancia-y-resistencia-en-la-era-digital.html

Ahmed Banafa[20], nos dice lo siguiente:

> “La seguridad del Internet de las Cosas, engloba advertencias que se encuentran en tres (3) categorías: privacidad y custodia de los datos de carácter personal y las amenazas a la confiabilidad de los dispositivos que usan IoT son devastadoras. Cabe recordar que estos son un objetivo primordial y principal en la realización de espionaje industrial tanto a nivel nacional e internacional. Se necesita evaluar cuáles son las necesidades reales a defender porque el IoT hace es una asignación virtual de un objeto físico, por ejemplo, los automóviles y los hogares, ya que al ocurrir un incidente las infraestructuras físicas se ven amenazadas, el medio ambiente en donde se encuentra, el suministro de servicios esenciales, entre otros aspectos. Se evidencia que la mayor duda del IoT es que a los clientes no les importan la estabilidad de los aparatos que conecta como su preocupación suprema y según Paul Henry, director de VNet Security LLC y profesor en el SANS Institute: “*el problema se presenta cuando un dispositivo se usa para atacar a un tercero*”. Algunos casos los podemos observar al tener un software de procedimientos automáticas y por cualquier orden queda atrapado en un bucle infinito, ocasionando caídas del sistema o en el momento que una estructura eléctrica es pirateada y se apagan las luces en una zona de la ciudad, esto lo vemos en algunas ocasiones a los individuos no les importa demasiado, sin embargo sucede completamente lo contrario en el resto de la sociedad y puede derivar en retrasos de operaciones, accidentes de todo tipo, inseguridad e inconvenientes médicos a las personas que son claustrofóbicas y muchas otras consecuencias. Se requiere reforzar la protección del IoT, usando herramientas de cifrado de mensajes, mejor calidad en el logueo de los usuarios, codificación sólida, API normalizadas y probadas de manera eficiente y predecible y por parte de los creadores de aplicaciones, es la mejora de la escritura de código con el fin de garantizar y fiabilidad a lo que se programa, normas en la creación de los códigos, desarrollar capacitaciones en

análisis de incidentes presentados y procurar rigurosidad en las pruebas que se lleven a cabo sean eficientes y prácticas. Es por eso que el IoT tiene el compromiso de ser blindada y segura, con atención especial en la conservación de la información, lo cual es difícil de conseguir, no obstante, es posible de alcanzar".

Ilustración 3. Comparativa Dispositivo – Datos. Evaluandosoftware.com (2017)

[20] BANAFA, Ahmed. Internet de las cosas: seguridad, privacidad y protección, 13 de mayo de 2015. Disponible en: https://www.bbvaopenmind.com/internet-de-las-cosas-seguridad-privacidad-y-proteccion/

Rob Waugh[21], nos dice lo siguiente:

> “La estabilidad de los aparatos IoT es bastante vulnerable, debido a los ataques por parte de ciberdelincuentes por una sencilla razón, los usuarios no cambian la contraseña que viene de fábrica en los instrumentos. En este ataque se constató por medio de imágenes tomadas por las cámaras alrededor de las casas, las empresas, los bebes durmiendo, entre otros casos, y recordando que es significativo cambiar las claves que trae los objetos electrónicos es reafirmar la seguridad de estos. Ante esto. nos dan algunos consejos para tener en cuenta a la hora de asegurar nuestro dispositivo apropiadamente:
>
> - Cambiar las contraseñas por defecto de todo y cambiar las contraseñas del router.
> - Separar las cosas realmente importantes.
> - Deshabilitar la vista remota y asegurarse de las defensas del router estén al día.
> - Bloquear las cámaras ya que son atractivas para los cibercriminales y no asumir que un dispositivo es seguro.
> - Los sistemas de calefacción deben contar con contraseñas decentes.
> - Asegurarse que el firewall está al día y usar filtros MAC”.

[21] WAUGH, Rob. Seguridad en internet de las cosas: cómo proteger tus dispositivos Smart, 25 de noviembre de 2014. Disponible en: https://www.welivesecurity.com/la-es/2014/11/25/seguridad-internet-de-las-cosas/

4.5 LOS CIBERATAQUES

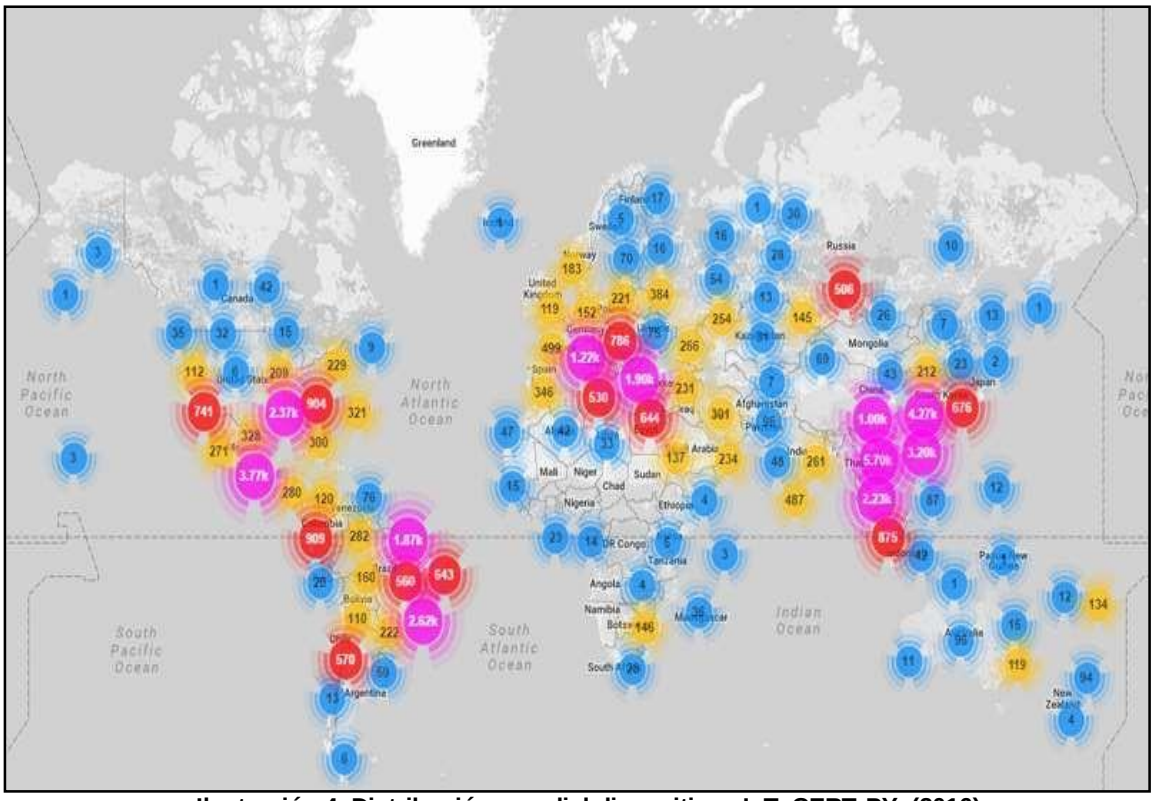

Ilustración 4. Distribución mundial dispositivos IoT. CERT-PY, (2016).

A propósito de la seguridad del IoT, PowerPlanet[22], Esther Mucientes[23], Vicente Pérez[24] y Diario ABC[25] nos dicen lo siguiente:

> "El IOT es el mundo interconectado digitalmente buscando que nuestras vidas sean fáciles. En la gráfica se deduce que en el año 2020 habrá alrededor de 26 billones de aparatos con el sistema de adaptación y conectados al IoT, según la consultoría Gartner. Los problemas del IoT, se han empezado a manifestar cuando se empezó a implementar ya que ha crecido de un modo muy acelerado y conlleva a tropezar con enormes vacíos de seguridad, lo que lleva a los ciberdelincuentes a ocasionar ataques, obligado por la inseguridad que transportan consigo. Un ejemplo de mala garantía se encuentra en las cámaras IP con las claves de fábrica sin modificar. Los atacantes los realizan,

aprovechando las vulnerabilidades que cada uno de ellos trae. Cabe recordar el ciberataque realizado al IoT, ocurrido en el 2016, con Mirai (botnet) que era capaz de lanzar grandes flujos de información a un mismo punto de destino a una velocidad de 650Gbps, también llamado Ataque de Denegación de Servicios Distribuido o DDoS. El malware en cuestión escanea los elementos y los infecta mediante sesiones Telnet con las credenciales de acceso por defecto y cargando la secuencia maliciosa en la memoria principal, su funcionamiento se conoció debido a la publicación de su código fuente en los foros de hacking. Se debe de ser consciente de que los dispositivos no son inteligentes tal cual se cree ya que, al lograr ser accedidos, se podrá dirigir ciberataques a gran escala, evitando males mayores se recomienda a los fabricantes eliminar o capacitar a los usuarios para cambiar las contraseñas que tienen los equipos electrónicos y que estos se podrán actualizar de forma remota y automática ante las amenazas, además de prevenir los recurrentes incidentes en las fallas encontradas. Después del caos provocado al IoT, la compañía china Hangzhou Xiongmai Technology, informo que en dicho acto ciberdelincuencial se usó deliberadamente solicitudes a sus servidores alojados en la nube, por ende, se bloqueó los accesos a los sitios de Netflix, Twitter, Amazon, Spotify, entre otros. La empresa decidió por tal motivo retirar los productos que fueron comprados antes de abril de 2015. Los posteriores a esta fecha, ya vienen parchados o actualizados y no suponen un peligro potencial".

ITUser[26], nos dice lo siguiente:

"Los problemas de solidez del IoT, también pueden afectar a los sistemas hospitalarios, ya que aumentan sus riesgos y los daños que puede producir a los datos de los pacientes por medio de Ransomware y DDoS. Ante este panorama la ENISA (Agencia de la Unión Europea para la Seguridad de Redes y la Información, que funciona desde el 2005 en

Grecia, teniendo como objetivo garantizar una cultura de protección en beneficio de los ciudadanos, los consumidores, las empresas y organizaciones del sector público de la UE, con el fin de cumplir los requisitos que están incluidos en la legislación actual y futura de la misma), se realizó un informe con una serie de propuestas materializadas en tres recomendaciones:

- Las organizaciones de asistencia sanitaria deben cumplir requisitos de seguridad TI para sus dispositivos IoT e implementar medidas de última generación.
- Los hospitales inteligentes deben identificar los activos y que se encuentran interconectados o conectados al IoT, realizando la identificación por medio de usuario y contraseña y adoptar prácticas específicas para su uso.
- Incluir desde el inicio a las entidades hospitalarias a la hora de diseñar sistemas y servicios e incorporar la calidad a la seguridad existente".

[22] POWERPLANETONLINE. Problemas del IoT (Internet of Things), 13 de junio de 2017. Disponible en: http://blog.powerplanetonline.com/problemas-del-iot-internet-of-things/

[23] MUCIENTES, Esther. Así se gestó el ciberataque más grave de los últimos 10 años, 22 de octubre de 2016. Disponible en: http://www.elmundo.es/tecnologia/2016/10/22/580b10e5268e3e06158b45e0.html

[24] PÉREZ, Vicente. El "Internet de las cosas", una nueva ventana para la ciberdelincuencia, 07 de noviembre de 2016. Disponible en: http://www.abc.es/tecnologia/redes/abci-internet-cosas-nueva-ventana-para-ciberdelincuencia-201611041537_noticia.html

[25] Diario ABC de España. Un fabricante chino retira sus productos de EE. UU. tras ciberataque masivo, 25 de octubre de 2016. Disponible en: http://www.abc.es/tecnologia/electronica/imagen/abci-fabricante-chino-retira-productos-eeuu-tras-ciberataque-masivo-201610251427_noticia.html

[26] ITUSER. IoT hace a los hospitales más vulnerables a los ciberataques, 28 de noviembre de 2016. Disponible en: http://www.ituser.es/seguridad/2016/11/iot-hace-a-los-hospitales-mas-vulnerables-a-los-ciberataques

Alberto Iglesias Fraga[27], nos dice lo siguiente:

> “El número de ataques informáticos crece de manera exponencial anualmente y las cadenas hoteleras no iban a ser la excepción, ya que estos han sido exitosos por la caída de servicios esenciales hasta el robo de información personal y bancaria de los huéspedes. Por consiguiente, se dan algunos ejemplos de los ciberataques más notorios realizados a estas y son:
>
> - Hard Rock Hotel & Casino Las Vegas, en este el ataque fue realizado por un hacker que accedió a los sistemas de pago y recopiló toda la información sobre las transacciones realizadas del periodo de octubre de 2015 a marzo de 2016, en el cual obtuvieron los números de tarjetas de crédito, su titular, la fecha de caducidad de la tarjeta y el código de verificación de esta.
>
> - Contra esta cadena hubo otro ciberataque con malware entre septiembre de 2014 y abril de 2015, en donde los clientes que realizaban sus pagos en el bar o que compraron la icónica camiseta sufrieron de la misma vulnerabilidad con el acceso al sistema de pago, desafortunadamente el hotel reconoció que había pasado más de ocho meses en detectar la intromisión y comenzaron a tomas medidas.
>
> - La cadena de hoteles Hyatt, Marriott e intercontinental, el ataque se realizó por medio de un malware en donde causo el robo de más de ocho mil (8000) transacciones realizadas entre 2015 y 2016, porque el atacante descubrió una vulnerabilidad en la seguridad de los datos bancarios de los huéspedes.

- Las Vegas Sands que pertenece a Sheldon Adelson, es un blanco predilecto de los atacantes. Durante el año 2014, un grupo de ciberatacantes iraníes, quienes reaccionaron ante estas declaraciones en el programa nuclear de su país, poco después realizaron unas pruebas a un resort del magnate en Pennsylvania y detectaron las vulnerabilidades, paso siguiente, hicieron caer todos los sistemas informáticos que controlan las mesas de juego, las máquinas tragamonedas y otros ordenadores esenciales en sus tiendas y restaurantes y hurtaron cuarenta millones de dólares (U$ 40’000.000).

- Hilton Hotels, en donde los ciberataques lograron hurtar la información de las tarjetas de crédito utilizadas en sus hoteles durante noviembre de 2014 y abril de 2015. No se conoció la cantidad de clientes afectados ni el número de las transacciones agregadas por el hacker, pero la empresa le pidió a sus usuarios que revisaran sus extractos bancarios y buscarán movimientos anómalos provocados por el ataque”.

Ilustración 5. Principales lugares afectados por ataques al IoT. Tripadvisor, (2019).

[27] IGLESIAS FRAGA, Alberto. Ciberataques contra los hoteles: los cuatro más notorios, 19 de noviembre de 2016. Disponible en: http://www.ticbeat.com/seguridad/ciberataques-contra-los-hoteles-los-cuatro-casos-mas-notorios/

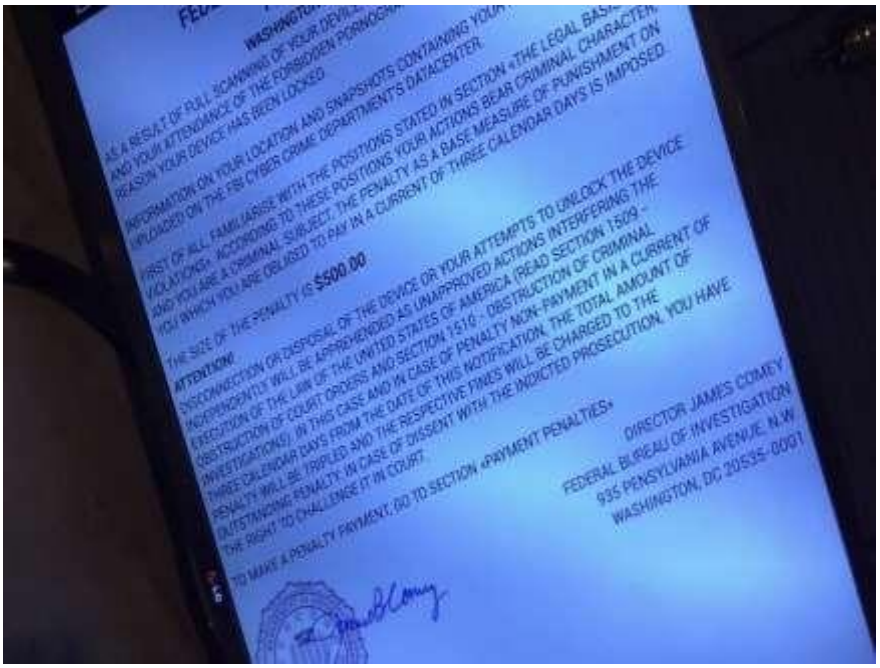

Ilustración 6. Ejemplo ataque ransomware. Bisso, (2017).

Pierluigi Paganini[28] [29], nos dice lo siguiente de otros ataques a dispositivos IoT fueron:

> “Durante el día de navidad del año 2016, el ingeniero de software Darren Cauthon, reportó en su televisor Smart TV de marca LG, fue infectado con un ransomware (programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo) y que pedía quinientos dólares (U$500) para desbloquear el dispositivo. La infección se produjo cuando su esposa descargó una APP al TV que prometía poder observar películas gratis. El nombre de este era Cyber.Police o también conocido como FLocker y Frantic Locker que apareció en mayo de 2015, los expertos los han estudiado y han descubierto alrededor de mil doscientas (1200) variaciones de ellos”.

> “Durante el año 2016, regresó el MMD (Malware Must Die). Los ciberdelincuentes han transformado el modelo del ataque alrededor y que

tiene como objetivo conseguir los números de las tarjetas de crédito y sus respectivas credenciales de las páginas web que se especializan en transacciones. Los atacantes usan varias formas de atacar, por medio del protocolo HTTP (envían solicitudes malformadas, métodos inválidos de búsquedas, uso de servidores de correo electrónico) con o sin iniciar una sesión SSL. Los sitios predilectos son: PayPal, Linkedln, Facebook, Gmail, PlayStation Store y Network, Ubisoft, entre otros".

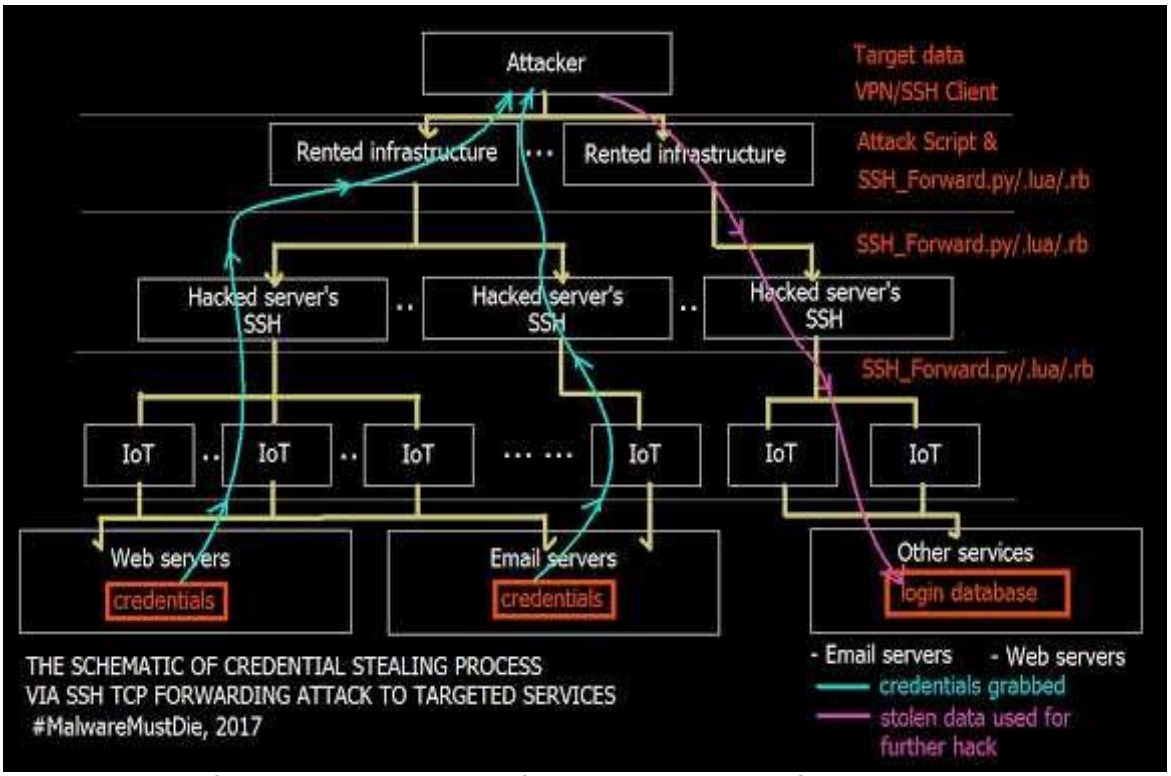

Ilustración 7. Proceso de robo de números de tarjetas de crédito. Paganini, (2017).

[28] PAGANINI, Pierluigi. It has happened again, ransomware infected an LG Smart TV. Disponible en: http://securityaffairs.co/wordpress/54991/malware/lg-smart-tv-ransomware.html

[29] Ibíd. Disponible en: http://securityaffairs.co/wordpress/56864/cyber-crime/ssh-tcp-direct-forward.html

4.6 SOLUCIONES

Ante los problemas y a ataques a los dispositivos de IoT, las compañías de software y hardware han empezado a incursionar en este campo, entregando arquitecturas y parches de seguridad. A propósito de las soluciones al IoT, Symantec[30] [31] nos dice lo siguiente:

> "En su documento sobre arquitectura de referencia, los dispositivos IoT tiene problemas de seguridad que son únicos para cada uno que son distintos de los sistemas tradicionales de las Tecnologías de la Información (TI) y que la estabilidad de IoT se puede cubrir en cuatro piedras angulares:
>
> - Protección de las comunicaciones, la seguridad está basada en sus fundamentos principales que son el cifrado, la autenticación y la administración de las contraseñas. Actualmente existen librerías de código abierto que realiza las tareas de traducción, sin embargo, las empresas siguen tomando riesgos al intentar realizar la gestión de las claves por sí mismos. Diariamente se realizan operaciones de comercio electrónico y se emplea un modelo de confianza simple y muy sólido que permite autorizar a los sistemas de otras compañías y empezar a disfrutar de los intercambios cifrados con ellos. Este tipo de familiaridad usa una lista de Autoridades de certificación (CA), que busca autenticar teléfonos móviles, medidores inteligentes de energía eléctrica y de decodificadores de la televisión de cable o satélite, entre otros. Con el manejo de CA se puede manejar certificaciones y credenciales para que la validación en el momento de autenticarse sea real y hacerlo fácilmente con protocolos estándares TLS y Datagrama TLS (privacidad en capa de

transporte).

- Protección de equipos electrónicos, en el momento que los aparatos traen poca resistencia y no son parchadas, los ciberatacantes aprovechan estos fallos y provocan ataques de gran magnitud dejando inoperantes a un grupo completo de usuarios, por lo cual se pide proceder con la apertura de las capacidades de actualización por el aire (OTA) en los dispositivos y que sean integrados antes de salir de la fábrica, con ello se busca que esta modernización, se incluyan con las reajustes tanto a nivel software y firmware, sin embargo, deben ofrecer una verdadera seguridad ante la larga cantidad de ciberataques que van apareciendo diariamente. Igualmente hay muchas amenazas, como son los datos maliciosos, la autenticación, las conexiones y vulnerabilidades y/o configuraciones incorrectas. Los atacantes usan las debilidades e instalar backdoors, sniffers, recopiladores de información, extracción confidencial de documentos del sistema, entre otras. Los programas malignos (malware) son instalados totalmente en la memoria de los mecanismos IoT y pueden desaparecer después de reiniciarlos, no obstante, esto acarrea ocasionar daños complejos en los mismos. Los asaltos informáticos son realizados desde internet o directamente en el medio físico, es decir, teniendo al alcance al objeto que será atacado. En el tiempo que se produce la irrupción, se dispone de pocos instantes para encontrar el elemento infectado y sacarlo de la red y si no es descubierto rápidamente se logra que este camino sea la puerta de entrada en una futura arremetida. Los ciberdelincuentes saben cuál es el componente comprometido y siendo así convertirla en la vía de infección al resto de la distribución sistemática de la empresa. Por tal razón, la

tranquilidad tiene que ser integral con la combinación del soporte lógico inalterable y verificación de código, garantizando la más alta protección, además de incluir el 'hardening' (asegurar procedimientos mediante eliminación de servicios innecesarios), listas blancas, aislamiento de aplicaciones (applications sandboxing), tecnologías basadas en reputación, antimalware y encriptadores de archivos, imágenes y discos duros.

- Administración de equipos, todos los dispositivos IoT se harán con la técnica de Ingeniería inversa, es decir, se construyen y empiezan a usar y se buscan los problemas y vulnerabilidades que pueda tener para realizar los correspondientes mantenimientos y se actualizarán por medio de las actualizaciones por el aire (OTA), incluyendo firmware, además de otras funcionalidades:

    - Actualizaciones de configuraciones.

    - Gestión de contenidos y telemetría en análisis a la seguridad.

    - Gestión de telemetría y control para el correcto funcionamiento del sistema.

    - Diagnóstico y remediación.

    - Gestión de credenciales de control de acceso a la red (NAC).

    - Gestión de permisos.

- Comprensión del sistema, mediante la supervisión y el análisis a manera de solución en cada uno de los entornos de los dispositivos IoT, llevará muchos años en estar listos, como, un ejemplo son los sistemas de controles industriales, que son usados en la fabricación de petróleo y gas, no se pueden modificar hasta este listo un plan operativo de reemplazo que sea completo o en los equipos hospitalarios donde está prohibido realizar modificaciones para agregar mayor seguridad. Es por eso que lo más significativo es usar herramientas que no sean tan invasivas y que tenemos que consideran es que en la actualidad los aparatos IoT son muy demandados y por ello se busca que estos tengan una opción de modo de detección que ayude a asegurarlos de cualquier falso positivo y que no de problemas ante caídas de la red.

Por lo anterior, se presentan algunas soluciones prácticas, como son:

- Soluciones para el sector automotor, como, por ejemplo, entretenimiento informativo integrado en vehículos (IVI), módems, bus de área de controlador (CAN), controladores integrados, puerto de diagnóstico incorporado (OBD-II).

- Seguridad para los sistemas de controles industriales (ICS), como, por ejemplo, la automatización industrial, controladores lógicos programables (PLC), estructuras conectadas que constituyen la red troncal del sector industrializado 4.0.

- Soluciones para el sector de atención sanitaria, como es la mejor seguridad en los equipos de última generación.

- Soluciones para los dispensadores automáticos de dinero, como son los programas maliciosos en los cajeros y las infracciones que recaen en las tarjetas de crédito por su indebido uso".

Gemalto[32], nos dice lo siguiente sobre sus soluciones:

"El IoT impacta en el mundo que nos rodea y comienza a hablar entre ellos, desde los televisores, los refrigeradores, los automóviles hasta los medidores inteligentes, pero lo que más preocupa es la aprobación de confianza por parte del consumidor con la privacidad y seguridad de sus datos en los dispositivos. Todo ello lo que se busca es la innovación y poder disfrutar de los beneficios de una sociedad conectada. Según este proveedor, los equipos IoT se deben de asegurar en sus tres pilares fundamentales y que se garantice la información tanto en movimiento como en reposo. Estos cimientos son para protección de un dispositivo y empieza en su diseño y fabricación y los cuales son:

- Primer pilar - La seguridad del dispositivo: A medida que van aumentando los equipos conectados, aumentan el uso de las aplicaciones y datos, lo cual también trae nuevas formas de puntos de ataques a los hackers. Algunas soluciones por parte de esta empresa se encuentran en la adquisición de la tecnología M2M que ayudan a los fabricantes de dispositivos originales (OEM) en su desarrollo, a los industriales y a los operadores de redes móviles.

- Segundo pilar - Tranquilidad en la nube: sus soluciones están en la codificación y seguridad de los datos, por medio de licencias y derechos, con lo que se garantiza la estabilidad de la propiedad

intelectual.

- Tercer pilar - La gestión del ciclo de vida, saber cuál es el tiempo de uso de un dispositivo es primordial en la creación de estrategias de garantía robusta y de largo plazo. Las soluciones que se brindan en las infraestructuras, son la administración del acceso al sistema, las claves privadas y/o públicas, el incremento de la rentabilidad con el cumplimiento de las exigencias del mercado y el trámite del token como elemento seguro".

Ilustración 8. Ciclo de vida seguridad Internet de las Cosas. Gemalto, (2017).

[30] Symantec. Seguridad del internet de las cosas (IoT), 2016. Disponible en: https://www.symantec.com/es/mx/solutions/internet-of-things

[31] Symantec. An Internet of Things Reference Architecture, 2016. Disponible en: https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

[32] GEMALTO: SECURITY TO BE FREE. Seguridad integrada y en la nube para e internet de las cosas, 2018. Disponible en: http://www.gemalto.com/latam/iot/seguridad-en-iot

Cisco[33], nos dice lo siguiente sobre sus soluciones:

> “La consultoría Gartner dice que el IoT es la red física de objetos que están interconectados con la tecnología que permite comunicarnos, sentirnos, interactuar con los estados internos y externos o con el medio ambiente que nos rodea. Según Cisco, en el año 2030 habrá más de quinientos mil millones (500’000.000.000) de equipos conectados al IoT. Estos dispositivos generaran metadatos que se usaran para estudiarlos, agregarlos, analizarlos y ofrecerlos a manera de información en la toma de decisiones y acciones informadas con anticipación. El IoT ayuda transformar los procesos y modelos de negocio de la empresa, potenciando la eficiencia de la fuerza de trabajo y su respectiva innovación. Los datos proporcionados son la materia prima de los negocios, ya que son la fuente de nuevas ideas. Las soluciones por parte de ellos, se basan en tres pilares:
>
> - Productividad, permite realizar innovaciones y obtener cosas para aumentar la productividad, estas mejoras permiten:
>
> - Acelerar el tiempo de comercialización.
>
> - Mejorar la eficiencia y la disponibilidad de suministros.
>
> - Impulsar la flexibilidad organizacional.
>
> - Optimizar la utilización de activos.
>
> - Implementar el mantenimiento predictivo.
>
> - Mejoramiento de los dispositivos, reemplazando equipos

obsoletos por otros que cuenten con control y elementos de regulación.

- Crear nuevos modelos y servicios comerciales (Monetización), los dispositivos conectados a la IoT tienen sensores que pueden detectar la ubicación, el entorno y proporciona datos brutos y análisis de las aplicaciones que se descargan o se tengan instalados, pero además de estos crear oportunidades de negocios, buscando que los usuarios no paguen por el producto físico sino por el resultado final, creando modernos flujos de ingresos y abriendo nuevas expectativas en el mercado como:

    - Creación de modelos de negocios.

    - Ofrecimiento de nuevos servicios.

    - Creación o mejoramiento de la ventaja competitiva.

- El compromiso por medio de experiencia del usuario, se busca aprovechar los datos e involucrarlos en el mejoramiento y así buscar habilitar las mejores prácticas a los clientes y empleados, un ejemplo de ello es que los dispositivos, con ayuda de los sensores pueda alertar a los consumidores sobre problemas y congestiones recurrentes en los desplazamientos desde su casa, al trabajo, a los hospitales, entre otras. Al mejorar las experiencias, se satisface las expectativas de todos los que participan en el ciclo. La responsabilidad se refleja:

    - Entregando servicios personalizados para deleitar a los clientes.

- Personalización de los entornos de los empleados de acuerdo con sus preferencias.

- Optimización de la experiencia del ciudadano.

Cisco da un ejemplo de la utilización de su infraestructura, con la empresa Linz AG porque fue capaz de participar y personalizar la experiencia de sus corredores ayudando en lo siguiente:

- Tiquetes de autodiagnósticos de equipos, mediante la realización de transacciones con las tarjetas de crédito o efectivo mientras son monitoreadas desde una locación central, estas máquinas están conectadas con Cisco Industrial Ethernet Switches, con esto el personal estaba preparado para cualquier alteración o mal funcionamiento del sistema y sus reparaciones fueran más rápidas.

- Pantallas dinámicas con transparencia que usan video en tiempo real, con esto se puede mostrar en pantalla, los horarios del tren y anuncia los eventos o incidentes que pueden causar retrasos en el transporte y su beneficio es nota en la rapidez de los desplazamientos y la satisfacción del cliente o usuario.

- Análisis para impulsar la mejora, por medio de Cisco se analiza el flujo del tráfico y este es analizado en tiempo real buscando optimizar y mejorar la precisión de los cronogramas establecidos.

- Tranvías inteligentes, la empresa Linz AG tiene cincuenta y seis (56) rutas de servicio gratuito, los servicios de Internet pueden soportar hasta quinientos (500) usuarios conectados

simultáneamente al Wifi, además de enviar los cambios a los conductores en sus horarios, entre otros aspectos".

Ilustración 9. Uso del Internet de las Cosas por Linz AG. Cisco, (s.f.).

[33] CISCO. At a glance- Internet of Things, 2016. Disponible en: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

4.7 IMPACTO EN LA SOCIEDAD COLOMBIANA

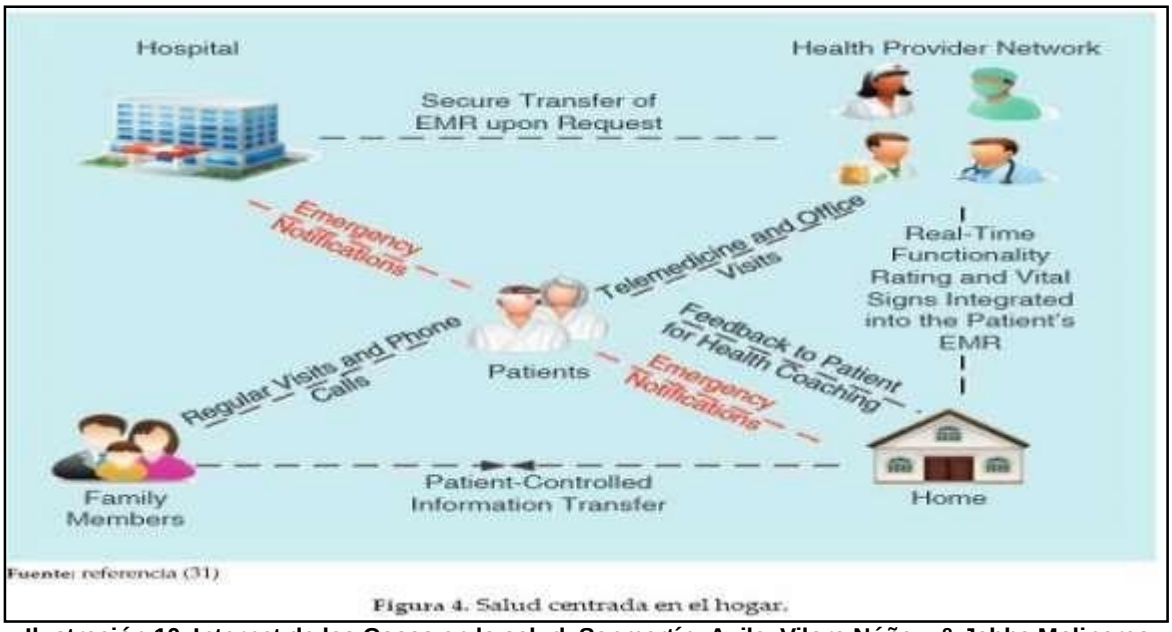

Ilustración 10. Internet de las Cosas en la salud. Sanmartín, Avila, Vilora Núñez, & Jabba Molinares, (2016).

A propósito del impacto del IoT, Ana María Velásquez Durán[34], nos dice lo siguiente:

> "El impacto del IoT, en el quehacer diario en Colombia se reflejará con la llegada de avances tecnológicos, por ejemplo las casas inteligentes que tiene conectado los sensores de las luces y el aire acondicionado y su respectiva monitorización, vigilancia hídrica que es desarrollada por una empresa de soluciones tecnológicas llamada Lagash que vigila ríos como el Nare, el Magdalena en sus cercanías al departamento Antioquia con el objetivo de medir el crecimiento de sus caudales, uso de drones CNX midiendo la temperatura en los cultivos de grandes extensiones, esta solución captura imágenes con distintas longitudes de onda, después se procesan estos pixeles y se traslada a un sistema de Inteligencia Artificial (IA) con el fin de detectar patrones, analizada la información, los agricultores pueden ejecutar los planes de resiembra y proceder con los controles de maleza, reduciendo el consumo

de agroquímicos en un treinta por ciento (30%). Otros modelos son los carros autónomos y los electrodomésticos interconectados a la nube. De acuerdo con el CEO de Identidad Technologies, Andrés Sánchez, si las organizaciones no se meten en el IoT, seguramente se acabarán porque es lo que sucede con las revoluciones y ya han pasado tres de ellas. Dentro de las empresas colombianas podemos decir que han aumentado el uso de las aplicaciones de IoT, utilizando las plataformas Azure de Microsoft para uso de sus servicios, alojamiento y desarrollo de nuevas funcionalidades y Cloud Platform de Google que ofrece asistencia en el procesamiento de altos volúmenes de datos de los equipos conectados en tiempo real. Otro caso en el uso de los dispositivos IoT, se evidencia en los vehículos de transporte de la compañía Alpina, poseen un detector de acciones o estímulos, en donde cada medio minuto recibe reportes de los recorridos hechos, cuando recogen la leche de las fincas, la aplicación es ofrecida por la sociedad Wiznez".

Diego Ojeda[35], nos dice lo siguiente sobre el impacto en la sociedad:

"La llegada de la red móvil 4.5G al país, la infraestructura del IoT es una realidad. Esta tecnología ha evolucionado en su incorporación en muchos países, porque cualquier objeto se puede conectar directamente a la red bien sea en la vida cotidiana (el uso de las llaves de la casa y de los vehículos) o en la industria (empleo de los instrumentos de monitoreo instalado en las líneas de producción). Por consiguiente, la compañía Claro traerá a Colombia la nueva generación de transmisión de telecomunicaciones móviles, ya que significa una mejora en la red, posibilitando tener mayores velocidades y servirán como habilitantes para el Internet de las Cosas y esto explicó Iader Maldonado, director de Operaciones de Redes, dando algunos ejemplos:

- Tener un carro que le informe a su propietario por medio de un

mensaje cuyo motor necesita mantenimiento o una nevera que le indica al usuario sobre los productos que están próximos a caducar.

- Sensores que detectan fugas de agua, gas o que avise a los bomberos si hay un incendio o cuando se está violentando las guardas de seguridad de una casa

- Relojes que transmiten señales de posicionamiento para permitir conocer la ubicación de sus hijos a los padres.

- Se trabaja en una aplicación llamada MoveTrack para realizar seguimiento de carros y bicicletas".

---

[34] VELASQUEZ DURAN, Ana María. Drones y sensores: así usan el internet de las cosas en el país, 25 de octubre de 2017. Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-se-usa-el-internet-de-las-cosas-en-colombia-144004

[35] OJEDA, Diego. ¿Qué es el Internet de las cosas y por qué se acerca más a Colombia?, 05 de octubre de 2017. Disponible en: https://www.elespectador.com/tecnologia/que-es-el-internet-de-las-cosas-y-por-que-se-acerca-cada-vez-mas-colombia-articulo-716699

Mientras tanto, El Diario El Heraldo[36] y Caracol Radio[37], nos dice lo siguiente sobre el impacto en la sociedad:

> “El IoT conecta todo lo cual genera cercanía con la sociedad. El IoT es una realidad en Colombia y antes que el término se popularice, ahora vemos las cosas que traerá el nuevo mundo de hiperconectividad. El IoT es un sistema de máquinas o equipos equipados para la recopilación de datos y estar comunicados entre sí. El IoT hace parte de nuestro diario vivir, un ejemplo, son los datafonos que se usan en la realización los pagos. Actualmente, se encuentra disponibles aplicaciones como MoveTime que es un reloj que indica en dónde se encuentran los niños por medio de GPS y MoveTrack que se usa en la localización de las mascotas. Otras herramientas son, Smart Home que son soluciones de seguridad en las cámaras de video vigilancia en tiempo real y que se pone en contacto con el Smartphone, además de los aparatos que pueden controlar la temperatura, humedad, luces y cerraduras del hogar, y es más conveniente en las empresas porque representan mejoras en la productividad en términos de control de costos, manejo de presupuestos, información de clientes. También se ofrecen ofertas integrales en servicios de mini vehículos eléctricos eco amigables. Esta conectividad en nuestras casas permite mayor protección, con sensores en puertas y ventanas, creando alertas que nos permita conocer cuándo se abre o cierra una puerta o ventana.
>
> Vemos esto en cortos periodos de duración, entonces nos podemos imaginar lo que se viene en el largo plazo como medidas ingeniosas para las ciudades, las industrias, las casas, la monitorización de automóviles, los controles de seguridad, los ahorros de energía en alumbrado público, soluciones eficaces a los problemas de transporte y movilidad, además de la logística en la recolección de basuras, expedientes clínicos

electrónicos, fitbands, relojes y basculas inteligentes y todo gracias a los sensores que estarán integrados los dispositivos que recopilarán la información necesaria de cada uno de ellos y enviada con posterioridad a su respectivo análisis. Con la llegada de la red móvil 4.5G, los usuarios gozarán mayor conectividad, interacción con redes inalámbricas, conectando capitales, hogares, vehículos y debido a la habilidad con la cual fue creado el Internet de las Cosas (IoT) y que ha permitido su constante monitoreo y control en tiempo real.

De acuerdo con lo dicho por el presidente de Claro Colombia, Carlos Zenteno: "*fuimos los primeros en ofrecer servicios prepagos, se trajeron la generación de transmisión de voz y datos GSM, 3G, 3.5G y 4G, pioneros en la Sim Card, Triple Play y convergencias con el servicio multiplay y por ello estamos listos en dar el siguiente paso hacia las redes móviles 4.5G y 5G, con el uso de las tecnologías NB-IoT en equipos sencillos y la tecnología LTE-M para dispositivos con mayor demanda de velocidad (objeto y máquina)".*

El IoT resume la posibilidad de que los computadores, celulares y algunos equipos de electrónica no sean los únicos que se puedan conectar a Internet sino que se unió una gran variedad de dispositivos provistos de sensores y todo esto con el objetivo de facilitar la existencia de las personas y a las empresas consiguiendo ser productivas y seguras y que podrán verse muy pronto reflejado en Colombia, por ejemplo se lanzó la oferta de IoT en las casas hogares y las industrias permitiendo que el país crezca hacia la conectividad omnipresente de los países del primer mundo que usan esta tecnología en sectores del agro, la salud y la creación de capitales inteligentes. Para Carlos Zenteno, presidente de Claro dice: "*la nueva era de los individuos y las compañías pueden tener infinitas oportunidades de conectarse con las cosas que más le interesa. A nivel individuo puede unir la vida diaria con el*

control de la casa, electrodomésticos, vehículos, además de saber cómo están las mascotas, la familia. En la empresa con el dominio de procesos productivos, los transportes, las redes de distribución y enormes posibilidades de solución a problemas estructurales de las ciudades como son la seguridad, la recolección de basuras y la movilidad"".

---

[36] DIARIO EL HERALDO. El 'Internet de las cosas' es una realidad en Colombia, 12 de octubre de 2017. Disponible en: https://www.elheraldo.co/ciencia-y-tecnologia/el-internet-de-las-cosas-es-una-realidad-en-colombia-411505

[37] CARACOL RADIO. El internet de las cosas comienza a aterrizar en Colombia, 25 de septiembre de 2017. Disponible en: http://caracol.com.co/radio/2017/09/25/tecnologia/1506347724_142242.html

4.8 EL ECOSISTEMA

Como se ha plasmado anteriormente, el IoT es la interconexión de todas las cosas con Internet, pero cuál será la infraestructura necesaria para que funcione y de acuerdo con Adriana Molano[40] nos dice:

> "Para que sea posible se requiere de conexiones a la red, dispositivos conectables, lectores que puedan leer los datos que recogen, con el fin de dar respuestas a los problemas de la vida cotidiana y es por ello que el mundo necesita prepararse con la infraestructura requerida que pueda soportar las infinitas cantidades de interconexiones que abra cuando entre en auge el IoT. Algunos casos los podemos encontrar por medio de los Gobiernos, instituciones y empresas que se han unido en reducir la brecha informática y al mismo tiempo, coordinar todos los lugares de unión de cualquier tipo de dispositivo. Otros ejemplos interesantes, se encuentra en el país con las zonas de acceso a Internet nombrándolo "Plan Vive Digital 2014 – 2018", que se ha implementado en la totalidad de nuestro territorio y los sitios gratuitos de conexión a la red inalámbrica llamados puntos calientes (Hostposts Wifi) en ciudades como Bogotá. Dentro de esta estructura tecnológica se debe tener en cuenta:
>
> - Dispositivos conectables. En este campo saltan términos conocidos como nanotecnología, movilidad, hardware y software libre, y que todos ellos forman parte del ecosistema funcional del IoT y de acuerdo con la URJC y Carriots[38], señalan que actualmente es posible el IoT por múltiples factores, por ejemplo, la popularización de las placas madre libres, el abaratamiento de los sensores, el mejoramiento de las comunicaciones y las plataformas IoT.
>
> - Software y aplicativos. Se encuentra actualmente en auge las

tendencias digitales como las Apps, ya que sus algoritmos buscan dar soluciones inmediatas a las necesidades requeridas, aquí se integran las plataformas con los sensores ubicados en las ciudades, en los programas de análisis y respuesta de información en los sistemas M2M que transmiten datos y los convierte en acciones, ya que estos son la base del IoT. Es por ello por lo que el concepto de Smart City (ciudad inteligente que por medio de las Tecnologías y la Innovación examinan la forma de proveer una infraestructura que garantice un desarrollo sostenible, incrementando la calidad de vida y la eficacia en la utilización de los recursos disponibles y participación de los ciudadanos)[39] y el IoT están muy unidos porque ambos conceptos, tienen en las comunicaciones entre máquinas su principal fundamento.

- Análisis de información. En la actualidad los datos son más valiosos que nunca y nuestro mayor activo y el reto actual es poder analizarlos e interpretarlos ayudando a tomar las decisiones acertadas. La velocidad con la cual se debe adoptar al IoT dependerá desde la vista social, es decir, las preocupaciones que se tiene con los dispositivos frente a la seguridad y privacidad que se obtengan de ellos, además de la gran cantidad que se puede acumular y que no se disponga de los medios de almacenamiento necesarios y requeridos para salvaguardarlos".

[38] EVERLET, Álvaro y PASTOR, Javier. Introducción al Internet de las Cosas: Construyendo un Proyecto de IOT, noviembre de 2013. Disponible en: https://www.carriots.com/newFrontend/imgcarriots/press_room/Construyendo_un_proyecto_de_IOT.pdf

[39] YouTube. ¿Qué es una Smart City?, 28 de octubre de 2014. Disponible en: https://www.youtube.com/watch?v=lKpoi8lf_tI

[40] MOLANO, Adriana. Internet de las cosas: Concepto y ecosistema, 01 de octubre de 2014. Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/7821-internet-de-las-cosas-concepto-y-ecosistema.html

4.9 ACTUALIDAD EN COLOMBIA

Sobre este aspecto tenemos que comentar la reciente apertura del Edificio Plaza Claro, y esto nos dice la sección Tecnosfera del Periódico El Tiempo[41]:

> "Con la inauguración de Plaza Claro, que se encuentra ubicado en la zona del Salitre en la ciudad de Bogotá, contando con tres torres de diez (10) pisos cada una, que ofrecerá espacios comerciales que tendrá noventa (90) locales, incluyendo restaurantes, un supermercado Carulla, un teatro de cine de Cinépolis, puestos de entretenimiento a los niños y una gran variedad de tiendas de moda y marcas retail de empresas nacionales e internacionales, zonas empresariales en donde albergará sedes corporativas de Nokia, Huawei, Ericsson y HITTS (es una compañía desarrolladora de software y proveedora de servicios informativos corporativos) y conjuntos residenciales que contará con una franja de 2300 parqueaderos y se invirtieron cerca de 200 millones de dólares (U$ 200'000.000) en su construcción. El proyecto fue inaugurado por el presidente Juan Manuel Santos y con la presencia de Carlos Slim Junior. Además, este edificio gozará del primer centro de experiencias para el IoT en Colombia y que estará abierto al público. El mandatario agradece a la organización por contribuir de manera enorme en la modernización tecnológica del país y que la moderna edificación no tiene nada que envidiarle a los del resto del mundo. Por su parte, el director del Consejo de Administración de América Móvil dijo que ha invertido doce mil millones de euros (€$12.000.000.000) en el sector y que guarda un fuerte agradecimiento a su equipo de profesionales, que les ha permitido ser competitivos. Daniel Hajj dice que somos los precursores de la recién creada infraestructura llamada GIGA RED 4.5G y que brindará la capacidad de disfrutar video y voz en alta definición y buscando simultáneamente el objetivo de masificar el IoT".

Ilustración 11. Plaza Claro en Bogotá. PYD, (2017).

[41] TECNOSFERA. Claro abre centro de internet de las cosas y realidad virtual, 06 de junio de 2018. Disponible en: http://www.eltiempo.com/economia/empresas/inauguran-plaza-claro-que-tiene-internet-de-las-cosas-y-realidad-virtual-227406

4.10 CLOUD COMPUTING

Sobre este aspecto, Juan Hernández[42] y Amazon[43], nos dicen lo siguiente:

> "Cloud Computing (computación en la nube), es una tecnología donde el hardware y el software son proporcionado en un servicio de otra empresa por medio del Internet y por lo general de una manera transparente. Estos servicios alojados permiten que las empresas consuman recursos informáticos a modo de utilidad, es decir, como si estuviéramos consumiendo electricidad en lugar de construir o mantener infraestructuras computacionales en las casas o en las oficinas y existen tres tipos de ellas:
>
> - Infraestructura como Servicio (IaaS), es alojamiento web ordinario, en el cual su paga una suscripción mensual o una tarifa por los Gigabytes o Megabytes consumidos.
>
> - Software como Servicio (SaaS), cuando una aplicación completa se usa en el sistema de otra persona, un ejemplo de ello es el correo electrónico basado en la web y los documentos de Google.
>
> - Plataforma de Servicio (Paas), desarrollo de aplicaciones con el uso de las herramientas basadas en la Web para que se ejecuten en sistemas de software y hardware proporcionado por otra compañía. Un ejemplo de ello, son los sitios web de comercio electrónico como Force.com de salesforce.com y Google App Engine".

[42] HERNÁNDEZ, Juan. ¿Qué es y para qué sirve el Cloud Computing?, 11 de febrero de 2016. Disponible en: http://blog.editafacil.es/que-es-y-para-que-sirve-el-cloud-computing/

[43] Tipos de Cloud Computing, 2018. Disponible en: https://aws.amazon.com/es/types-of-cloud-computing/

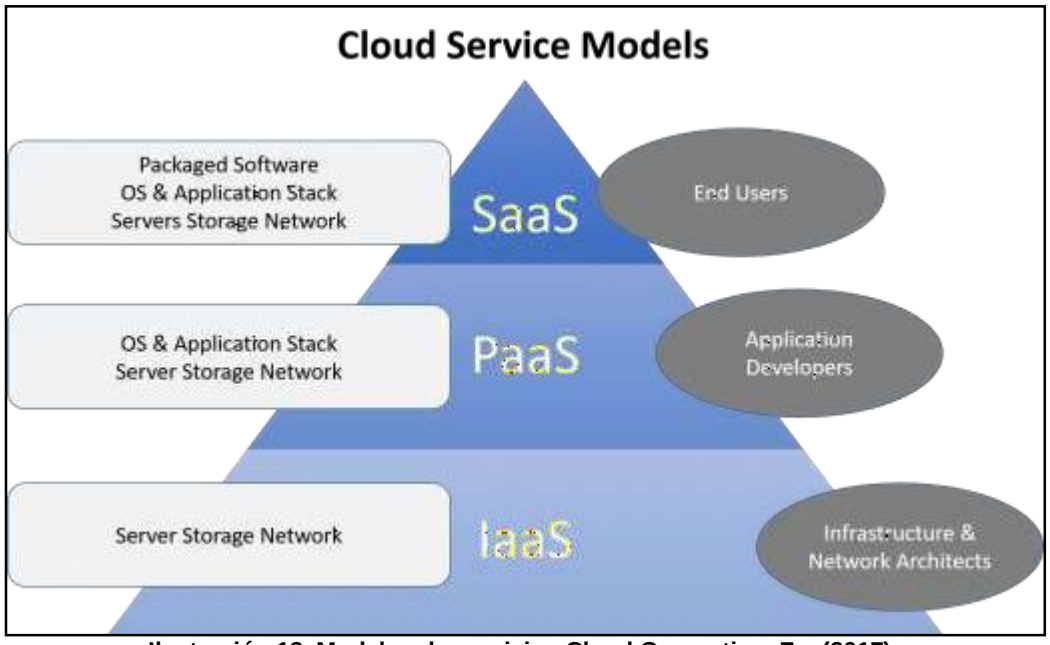

Ilustración 12. Modelos de servicios Cloud Computing. Fu, (2017).

El Cloud Computing tiene sus ventajas y desventajas como nos lo dice, ENAE Bussiness School[44]:

"Dentro de las ventajas tendremos:

- Escalabilidad, mientras una empresa pequeña comprará una licencia entretanto una compañía grande o multinacional adquirirá quinientas (500) licencias y por lo tanto ambas compartirán los mismos servicios.

- Independencia de los puertos físicos, ya que cualquier tipo de dispositivo (Smartphone, tablets) o un café internet será nuestra oficina.

- Equipamiento, ya que no nos preocuparemos por las constantes actualizaciones o cambios de los equipos para estar al día ya que de esto se encargará la empresa que nos provea el servicio.

- Eficiencia en caídas y backups, ya que las empresas que nos provean los servicios estarán en equipadas para elaborar frentes a estas contingencias que se presenten.

- La implementación del software que ya estará probada por los miles o millones de usuarios en el planeta.

- La personalización de las aplicaciones por parte de cada uno de los usuarios.

- Las actualizaciones automáticas que se harán para mejorar el rendimiento y que son surgidas por la experiencia y los requerimientos de los miles o millones de usuarios que lo utilizan a diario.

Dentro de las desventajas están:

- Dependencia del proveedor por el suministro de buenas políticas para la preservación de los datos, aunque se pueden realizar backups periódicos a nuestros respectivos ordenadores o dispositivos de trabajo.

- La mayor desventaja es cuando por alguna razón se cierra el enlace de internet, pero hay solución a esto, por ejemplo, el uso del servicio de WIFI o realizar nuestras labores diarias por medio de la conexión OFFLINE.

- La vulnerabilidad a la privacidad de los datos como, por ejemplo, los accesos a nuestros correos electrónicos, las contraseñas que

usamos, los protocolos, entre otros, pero que hoy en día hay muchas soluciones contra estas vulnerabilidades y no estaría mal tomar precauciones".

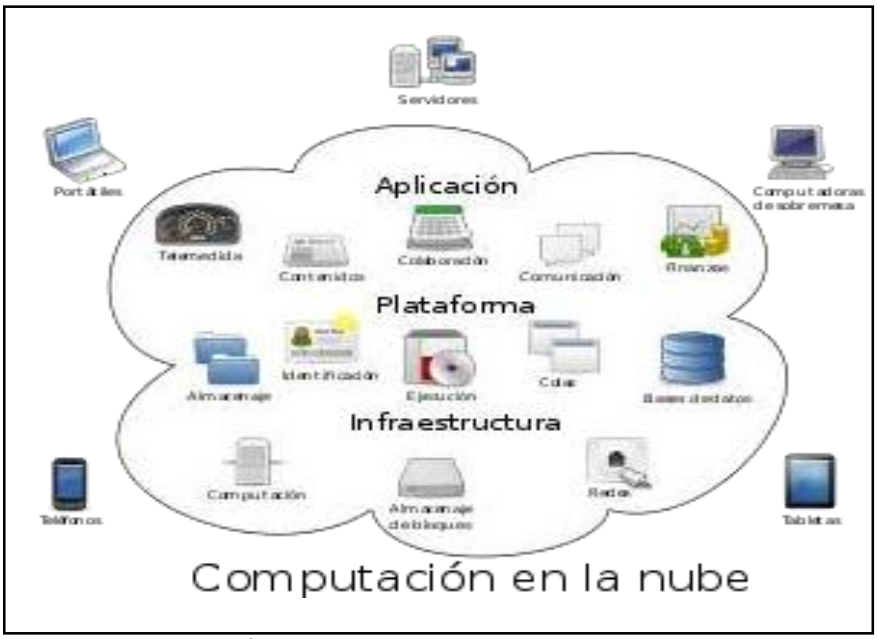

Ilustración 13. Cloud Computing. Wikipedia, (2019).

[44] Ventajas y desventajas del Cloud Computing, 25 de junio de 2010. Disponible en: https://www.enae.es/blog/ventajas-y-desventajas-del-cloud-computing#gref

4.11 BIG DATA

Ilustración 14. Big Data. Phillip, (2019).

Sobre este aspecto, Jean Tricket[45] nos dice lo siguiente:

> "Big Data es la posibilidad de aprovechar comercialmente una gran cantidad de información y creación de nuevos servicios. Actualmente se están acumulando cada vez más y por lo general en formato digital pero que a su vez son poco estructurados y por lo tanto son difíciles de explotar y por ello esta gestión nos ayuda a extraerlos de forma inteligente y darles valor. Sus principales fuentes salen de finanzas y economía (balances, cotizaciones, precios, hipotecas), intercambios M2M (por medio de los sensores instalados en carros, contadores), reportes socioambientales (clima, astronomía, médicos, natalidad), social media (estudios, estrategias, tácticas y casos de éxito de marcas sociales como Facebook, Twitter) y movilidad (fotos, elementos de geolocalización). Las tecnologías que permiten su explotación son un grupo de técnicas habituales en las bases transaccionales, los modelos predictivos, estadísticas, inteligencia artificial, procesamiento de lenguaje natural, redes neuronales, pattern matching (búsqueda de patrones), entre otras. Se diferencia de Bussiness Intelligence porque la primera deduce conclusiones a posteriori analizando el conjunto de datos de manera global y la segunda busca los detalles de la repetición de las secuencias, un ejemplo es la secuencia de genes del ADN".

Para Ronny Suarez[46], nos dice la importancia de Big Data en el sector de la salud:

> “Un dato no es relevante, sin embargo, al procesarlo en conjunto son entendidos y transformados en sabiduría y en este ejemplo se explica el concepto de pirámide de la información en el mundo de la informática y así buscar los alcances en materia de sanidad por medio del Big Data.
>
> El termino es complicado, no obstante, su significado es simple porque los datos complejos que se generan en grandes cantidades y se procesan con ayuda de herramientas tecnológicas para la toma de decisiones.
>
> Su uso es aplicado en todos los campos y no necesariamente en el campo de la salud. El presidente de Colombia, Iván Duque, en uno de sus discursos de campaña dijo cuyo uso permitirá entre otros logros, conocer el estado de vitalidad de cada individuo en tiempo real garantizando su atención en cualquier parte del país.
>
> Juan Mesa, director del sector público para Colombia y Ecuador de Oracle, dice que el Big Data forma parte de la transformación digital que viven las empresas de salud y que buscan el rediseño del modelo de atención del paciente y tomando patrones de identificación de grupos de riesgos que pueden tener la posibilidad de contraer una enfermedad respiratoria aguda (IRA) y buscando el empoderamiento de los pacientes y actuar de manera proactiva en la toma de acciones preventivas, reduciendo los índices de este padecimiento. Con la construcción de la historia clínica unificada electrónica permitirá la interoperabilidad de los sistemas hospitalarios, un ejemplo de ello se desarrolla en el departamento de Cundinamarca pero que es muy difícil de extender a todo el país.

El ingeniero Oscar Poveda, experto en Macrodatos y vicepresidente de una EPS dice que la entidad de salud que se interese por este campo deberá realizar una minería de datos con lo que se tiene en el momento en sus bases, las historias clínicas de sus afiliados, prescripciones de medicamentos y encontrar necesidades puntuales y crear una estrategia o modelo de atención, con el fin de valorar y gestionar las referencias individuales de cada paciente. Big Data no es magia y su éxito se basa en la calidad de las fuentes que entra al proceso. Son claves la captura y procedimiento mediante la trazabilidad, integridad y veracidad de estos.

Se trabaja con grandes volúmenes de información que se encuentra alojada en Terabytes (TB), y debe ser variada y además de contar con la capacidad de las herramientas tecnológicas que ayudarán en su procesamiento a una alta velocidad y teniendo esto, buscar las máquinas que aprendan predicciones (machine learning), un ejemplo sería:

- ¿cuántas mujeres pueden contraer cáncer de mama? Cabe recordar que existen empresas que tienen toda la infraestructura ya montada incluyendo el software que realiza los análisis usando la figura del alquiler.

Un ejemplo de Big Data de este sector se encuentra en la EPS Salud Vida y les ha ayudado en la toma de decisiones. Con su uso han podido caracterizar a sus afiliados y agruparlos en grupos de riesgos, en donde cada afiliado es intervenido de manera personalizada y pasaron de gestionar cinco mil (5.000) a más de ochenta mil (80.000) pacientes. Según Claudia Morales, vicepresidenta de la EPS, dice que están trabajando arduamente en poder incluir a toda la población afiliada a la EPS (1.3 millones que pertenecen al régimen subsidiado) en una base unificada de modo que el asociado a la entidad tenga una historia clínica

completa en el cual se registre la información de contacto, historial de atenciones y factores de riesgo".

[45] TRIQUET, Jean. ¿Para qué sirve el Big Data en mi empresa?, 2017. Disponible en: http://director-it.com/index.php/es/ssoluciones/data-center-cloud-virtualizacion/almacenamiento/127-%C2%BFpara-que-sirve-el-big-data-en-mi-empresa.html

[46] SUAREZ, Ronny. El 'Big Data' en salud: presente y futuro de la atención, 21 de agosto de 2018. Disponible en: https://www.eltiempo.com/vida/salud/como-se-puede-aplicar-el-big-data-en-salud-258536

4.12 INTELIGENCIA ARTIFICIAL Y EL IOT

Para el licenciado en informática de la facultad de Contabilidad y Administración de Tecomán Luis Alberto García Fernández[47], nos dice lo siguiente sobre la Inteligencia Artificial:

> "La Inteligencia Artificial es una ciencia que trata de explicar el funcionamiento mental, basándose en una serie de pasos organizados de un proceso que se debe seguir con el fin de controlar las cosas, tiene varias combinaciones de varios campos como la robótica, los sistemas expertos, entre otros y que persiguen el mismo objetivo tratar de crear máquinas que pueden razonar de manera idéntica a un ser humano y dentro de los estudios encontramos las redes neuronales, el control de los procesos y los algoritmos genéticos. Cuando estos aparatos puedan pensar igual que las personas, se requiere en primera instancia comprobar si son capaces de mantener un diálogo o conversación sobre cualquier tema específico.
>
> Se cree que los comienzo de la Inteligencia Artificial son del año 1943 al tratar de definir que la neurona es un dispositivo binario con varias entradas y salidas. En 1956 se volvió a tocar el tema, en otro campo independiente. En los 60s y 70s, la mayoría de las tecnologías eran propias de los grandes centros de investigación y uno de estos avances fue los sistemas expertos. La IA es terreno autónomo de la informática que busca asemejar la conducta inteligente que se observa en la naturaleza para la toma de decisiones de igual manera que los seres humanos, sin embargo, el verdadero objetivo de estas investigaciones es la de aumentar la utilidad de las máquinas y sus procesos. Un ejemplo de ello es la construcción de una réplica real de la compleja **red neuronal del cerebro humano** e imitar sus actuaciones. Las redes

neuronales son modelos computacionales inspirado en las neuronas, capaz de simular algunas funciones de aprendizaje de las personas, su experiencia se obtiene analizando automática y sistemáticamente los datos y determinar las reglas del comportamiento. Se aplica a problemas de clasificación y series de tiempo porque usan variaciones, tendencias, métodos, pronósticos y precisiones. En este modelo se representa con una unidad binaria cada instante de su estado (activo o inactivo) y su interacción se realiza por medio de la sinapsis, es decir, la transmisión de impulsos nerviosos eléctricos entre dos o más células nerviosas.

La característica de la Inteligencia Artificial es que incluye el desarrollo de variados campos como la robótica, la comprensión y la traducción de lenguajes, el reconocimiento y aprendizaje de palabras de máquinas o los varios sistemas computacionales expertos que se encargan de reproducir el comportamiento humano. Estas tareas reducen costos y riesgos de la manipulación humana en áreas peligrosas, mejoran el desempeño del personal inexperto y el control de calidad en el área comercial.

La Inteligencia Artificial está presente en la robótica con la construcción de autómatas realizados a partir de dispositivos compuestos de sensores que reciben datos de entrada enviados a una computadora y esta envía de vuelta las acciones que el robot tiene que realizar. Actualmente, los robots se construyen con rapidez, calidad y precisión para los procesos de fabricación de las grandes empresas.

Las investigaciones de la Inteligencia Artificial se hallan en muchos sectores como los métodos de aprendizaje automático, los campos de neurobiología y lingüística, la síntesis y comprensión de imágenes, la construcción de algoritmos, principios estadísticos, entre otros. Las

áreas de aplicación de la IA están el procesamiento de información, finanzas, cartografía, ingeniería, equipamientos y sistemas de armamento. Dentro de las aplicaciones comerciales se encuentra la monitorización de equipos, procesos de fabricación, datos financieros, interfaces inteligentes, desarrollo de software, programación neurolingüística y problemas matemáticos complejos".

Dentro de las ventajas y desventajas de la Inteligencia Artificial, el Diario de Yucatán de México[48] y Selectiva[49] con la ayuda de la oficina Gestión de Recursos Humanos, nos dicen lo siguiente:

"En las empresas, el uso de estas tecnologías es cada vez más frecuente. Desde la atención telefónica de los clientes por medio de chatbots y llegando a sistemas de producción complejos o hasta la búsqueda de personal idóneo en las oficinas de recursos humanos. La Inteligencia Artificial actualmente se dedica a realizar tareas sencillas o poco criticas ya que permiten agilizar procesos, automatizar labores complejas y aumentar la seguridad en algunos sectores como los químicos y farmacéuticos. Dentro de las ventajas que trae la IA son:

- Reducción de costos y salarios adicionales.
- Generación de ingresos.
- Desarrollo de aplicaciones con tareas complejas que el hombre nunca hubiera hecho.
- Predicción de situación a largo plazo.
- Reducción de los tiempos en realizar tareas específicas.

- Se han logrado grandes hallazgos y avances.
- Probabilidad de error casi nula.
- Posibilidad de crear bots para interactuar con los consumidores.
- Realización de tareas repetitivas.
- Realización de tareas peligrosas.
- La Inteligencia Artificial nunca se cansa.

Dentro de las desventajas de la Inteligencia Artificial tenemos:

- Constantes actualizaciones y mantenimiento.
- Son sistemas expertos que requiere de mucho tiempo y dinero.
- Son máquinas autosuficientes, que pueden desplazar a los humanos.
- El uso irracional y exagerado de esta tecnología y dependencia de estas.
- Sentido de desplazamiento del ser humano por la máquina.
- No tiene emociones como los seres humanos.
- Necesitan creatividad.

- En manos equivocadas puede ser peligrosas.

- Solo actúan para lo que están programadas.

- Desempleo”.

Sobre la Inteligencia Artificial y el Internet de las Cosas, el profesor Ahmed Banafa[50], nos dice lo siguiente:

> “La IA y el IoT, son términos reales que proyectan una imagen futurista y de ciencia ficción que han causado una disrupción (abertura) en los negocios del 2017 y que las empresas tienen que tener total entendimiento del potencial del IoT y combinarla con la IA porque su avance es muy rápido permitiendo que las máquinas inteligentes tomen decisiones con pleno conocimiento de causa y con la intervención humana en su mínima expresión. El profesor Banafa nos ofrece una definición sencilla de estos dos conceptos:
>
> El IoT es un sistema de objetos físicos, sensores, actuadores, elementos virtuales, individuos, servicios, plataformas y redes interrelacionadas que tiene identificadores separados y la capacidad de transferir información de manera independientes, varios casos prácticos los vemos en la agricultura de precisión, en la supervisión de pacientes remotos y en los coches sin conductor. En pocas palabras, el IoT recopila e intercambia comunicaciones con el entorno y con los continuos adelantos ofreciendo posibilidades buscando facilitar la vida de las personas, así como las mejoras en la eficiencia, la productividad y la seguridad de los negocios. Algunos ejemplos que son recopilados por la IoT son: la predicción de accidentes y delitos en las ciudades, los reportes proporcionados por los

marcapasos a los médicos en tiempo real, la optimización de los rendimientos a través del mantenimiento de equipos y maquinarias, los datos de los electrodomésticos conectados en los hogares inteligentes, entre otros. Estos avances en los beneficios del IoT se traduce en la siguiente operación:

$$Velocidad\ del\ análisis\ de\ Big\ Data + Precisión\ del\ análisis\ de\ Big\ Data = Beneficio\ total\ del\ IoT$$

Fuente: Ahmed Banafa

La Inteligencia Artificial es el cerebro o motor que permite analizar y tomar decisiones a partir de los datos recopilados por el IoT. Este funcionamiento mutuo se puede observar en equipos de seguimiento deportivo, en Google Home, Alexa de Amazon y Siri de Apple. Por lo tanto, el IoT recopila enormes volúmenes de información de cada uno de los dispositivos que son conectados al Internet, se necesita de sistema de interpretación para entenderlos, razón por la cual la IA entra en acción por ser una herramienta perfecta en el manejo de estas grandes cantidades y darles un sentido en la toma de resoluciones por parte de las personas o de las empresas ya que esta recopilación es algo fácil de realizarlo pero lo que es la comparación y la organización son otras entidades que tiene un único significativo y es la de mejorar la velocidad y la precisión del estudio en la IA. Los tipos de análisis del IoT que serán útiles en la IA son:

- La preparación de los datos.
- El descubrimiento de los datos.

- La visualización de los datos en streaming.
- Precisión de las series temporales de los datos.
- Análisis predictivo y avanzado.
- Los datos geoespaciales y de ubicación en tiempo real.

Algunos de los campos que beneficiaría la IA al IoT serían: macrodatos visuales, sistemas cognitivos, sensores, operaciones conectadas y remotas y mantenimiento preventivo y predictivo.

Los retos a superar la IA con el IoT son: la compatibilidad, la complejidad, la confidencialidad y la seguridad, las cuestiones éticas y jurídicas, la estupidez artificial o la de entender las reacciones / emociones humanas, en otras palabras, el concepto GIGO (Garbage In - Garbage Out, que significa en términos de programadores, indicar al usuario que si ingresa datos erróneos en la aplicación, la entrega de los resultados será también errónea)".

Sobre la inteligencia artificial (IA) y el Internet de las Cosas (IoT), el ingeniero Sergio Scaglia[51] nos dice lo siguiente:

"El Internet ha impactado en nuestras vidas, ya que podemos relacionarnos, comunicarnos, realizar compras en línea, información hasta capacitarnos y se ha transformado en una necesidad del quehacer diario y de esta forma es como nace el IoT. Cuando se habla de cosas,

hacemos referencia cualquier tipo de objeto o dispositivo que es capaz de conectarse a la red y aquí se dividen en dos grupos:

- Los sensores que realizan mediciones como la temperatura, la presión, la detección de movimientos de objetos e individuos hasta los infrarrojos de las cámaras de vigilancia. Todos estos reportes son enviadas por Internet y ejecutar el procesamiento de la información recopilada obteniendo beneficios para los usuarios.

- Los dispositivos como son los electrodomésticos, ropas, herramientas de trabajo, aparatos industriales. La información recopilada es enviada para permitir el monitoreo y controlar dichos equipos en su buen uso y eficiencia.

El objetivo principal del IoT es la de buscar beneficios tanto a las personas como a los equipos que se conectan a Internet. Con esta conexión permite monitorear y controlar por medio de acceso remoto de los dispositivos, sin la necesidad de estar presentes y todo ello se encamina a incrementar el valor del usuario en la recopilación de información y tomar las decisiones necesarias y corregir cualquier situación o incidente que ocurra.

Un ejemplo de ello, un sensor de Monóxido de Carbono (CO_2) que pueda detectar los riesgos de muerte para los seres humanos y los animales. Este dispositivo cuando ocurre un peligro emite un sonido o en algunas ocasiones que no son escuchadas siempre ocurren tragedias. La inhalación de CO_2 causa mareos, debilidad, pérdida de conocimiento y en algunos casos provoca decesos. Por consiguiente, la intervención del IoT permitiría detectarlo sino también la opción de notificar de la situación de emergencia a las personas que se encuentran fuera de la vivienda

como son los paramédicos, vecinos, entre otras y así poder resolver la circunstancia ocurrida.

La información recopilada por los sensores y los dispositivos conectados a Internet posibilita organizarla, almacenarla y analizarla para extraer conocimiento y lograr mejorías en los desempeños (eficiencia y eficacia). Con esto en mente, la Inteligencia Artificial (IA) desempeña un rol preponderante ya que nos ayuda en la desarrollar predicciones, por medio de patrones de comportamiento o eventos que son difíciles de visualizar de manera manual y actuar de modo planificado, sin incurrir en gastos mayores. Los campos de aplicación del IoT son la agricultura, la cría de ganado, las plantas de tratamiento y en los medidores de energía, agua y gas, entre otros. Los beneficios son la optimización de procesos, reducción de costos, mejoras de los servicios al cliente, trayendo consigo mayor valor al usuario y ganancias".

---

[47] GARCIA FERNÁNDEZ, Luis Alberto. Uso y aplicaciones de la Inteligencia Artificial, 2004. Disponible en: https://www.uv.mx/cienciahombre/revistae/vol17num3/articulos/inteligencia/

[48] Ventajas y desventajas de la Inteligencia Artificial, 19 de mayo de 2018. Disponible en: http://www.yucatan.com.mx/tecnologia/ventajas-desventajas-la-inteligencia-artificial

[49] Inteligencia Artificial: Ventajas y desventajas de su adopción en las empresas, 2018. Disponible en: https://selectiva.es/ventajas-y-desventajas-de-inteligencia-artificial/

[50] ¿Porque Internet de las cosas necesita Inteligencia Artificial?, 18 de julio de 2017. Disponible en: https://www.bbvaopenmind.com/por-que-internet-de-las-cosas-necesita-inteligencia-artificial/

[51] SCAGLIA, Sergio. Inteligencia Artificial: el "Internet de las cosas" y la expansión de lo digital, 14 de julio de 2018. Disponible en: https://losandes.com.ar/article/view?slug=inteligencia-artificial-el-internet-de-las-cosas-y-la-expansion-de-lo-digital

5 RESULTADOS DE LOS OBJETIVOS

5.1 DESARROLLO DE OBJETIVO GENERAL

Objetivo General: Realizar un estudio monográfico del estado del arte de la seguridad de los dispositivos para el Internet de las Cosas (IoT), dando a conocer los retos, beneficios y dificultades para el control de un objeto a través del uso de internet.

Para el desarrollo y cumplimiento de este objetivo, se empezó con una mirada genérica para entender el origen del Internet de las Cosas (IoT), y poco a poco se va introduciendo en el tema, obteniendo una visión más amplia y específica, conociendo las diferentes tecnologías y aplicaciones que tiene en la actualidad.

Para este fin se realizó una búsqueda bibliográfica de información por medio de las siguientes fuentes y cuya información esté relacionada con el Internet de las Cosas, como son artículos de páginas de internet, informes, periódicos, revistas, páginas web especializadas y otras publicaciones periódicas. Luego se optó con la selección de los artículos relevantes de acuerdo a los siguientes criterios:

- Claridad en su contenido.
- Los artículos fueran lo más actuales posibles (desde el 2011).
- Los artículos tuvieran información sobre los temas a tratar, en este punto fueron definidos los siguientes 12 tópicos:
    - Definición
    - Plataformas
    - Soluciones
    - Inteligencia Artificial
    - Cloud Computing
    - Big Data

- Ciberataques
- Actualidad en Colombia
- Componentes y características
- Seguridad
- Impacto en la sociedad colombiana
- El ecosistema

5.2 DESARROLLO DE OBJETIVO ESPECÍFICO 1

Objetivo Específico: Conocer el internet de las cosas (IoT), sus beneficios, sus dificultades y cambios en la vida de las personas, empresas y en la sociedad en general.

En el desarrollo de este objetivo, se evidencio que el Internet de las Cosas (IoT) aun se encuentra en la fase inicial y que a medida que pasa el tiempo irá evolucionando no solo en el aspecto técnico sino también en el aspecto legal para que su funcionamiento no tenga problemas y que no provoque cualquier tipo de rechazo por parte de los empresarios, que es donde se encuentran los mayores beneficios que traerá dicha tecnología. Por ello, se deben establecen las mejoras que se requieran y predeterminar los pasos para su implementación e implantación sean satisfactorias en cualquier área del sector productivo que lo necesite.

Esta tecnología trae numerosas aplicaciones para el entorno productivo de las empresas como por ejemplo en el campo del transporte de mercancías en donde se presentaba una carencia y era la incertidumbre en el traslado de las mercancías en un tiempo predeterminado pero con la llegada de los servicios de GPS (Sistema de Posicionamiento Global por sus siglas en ingles), se puede dar las coordenadas geográficas para que las empresas puedan controlar en vivo, el recorrido de sus mercancías hasta llegar con sus respectivos compradores, buscando de esta manera gestionar de una manera más eficaz todas las operaciones relacionadas con el transporte, mejorando algunos aspectos generales como la coordinación, la

gestión de los stocks (inventarios) o la misma seguridad de las mercancías transportadas hasta su entrega y beneficiando a todas las partes involucradas, desde los proveedores hasta el cliente o usuario final.

5.3 DESARROLLO DE OBJETIVO ESPECÍFICO 2

Objetivo específico: Recopilar información necesaria para realizar la investigación para la monografía.

En el desarrollo del objetivo de recopilación de información fue para obtener respuestas a las preguntas generadas en cada uno de los tópicos seleccionados permitiendo encontrar diferentes maneras de abordarlo. El Internet de las Cosas es un tema bastante extenso y tiene una alta complejidad para su comprensión y con ello se ha pretendido seguir una secuencia argumental que va desde los aspectos generales y poco a poco exponiendo un mayor nivel de detalle en cada uno de los temas.

El trabajo inicia con una breve introducción sobre el Internet de las cosas (IoT) en la actualidad, cuales son los dispositivos que más son usados para la interconexión de los aparatos por medio de la red y su rápido auge en la gran mayoría de países y finalizando con las conclusiones obtenidas durante el desarrollo del tema escogido. El documento se divide en doce capítulos y son:

- En el primer capítulo, se observa la definición del término Internet de las cosas desde el punto de vista de varios autores llega a un sola interpretación que es la interconexión de objetos cotidianos con Internet y los cuales se conectan por medio de identificadores de radiofrecuencia de los sensores que tienen incorporados cada uno de estos aparatos, permitiendo el intercambio de información y debido a ello su crecimiento ha sido de manera exponencial, captando las miradas de las empresas de software para el desarrollo de aplicaciones en este nuevo ámbito informático.

- En el segundo capítulo, observamos cuales son los componentes que tiene el Internet de las cosas como son el software, el hardware, los protocolos usados y las ventajas y desventajas de ello. Dentro de las características que debe tener como la conectividad, la sensibilidad, la interacción, la energía y la seguridad.

- En el tercer capítulo, se observa cuáles son las plataformas en las cuales se puede utilizar el Internet de las Cosas, las propiedades que deben poseer estas plataformas y las empresas que prestan estos servicios en la actualidad.

- En el cuarto capítulo, observamos cuales son las medidas de seguridad que se deben tener en cuenta a la hora de conectar nuestros dispositivos a la red, la importancia de tener buenos sistemas de protección para proteger la información que vamos enviando a la red y la confidencialidad e integridad de la misma. Con ello en mente, buscamos que todo lo que envía por el Internet de las cosas sea de manejado de manera correcta y no exponer nuestras vidas a personas no deseados y siempre estar pendiente de las respectivas actualizaciones o parches de seguridad en cada dispositivo conectado.

- En el quinto capítulo, se abarca los diversos tipos de ciberataques que ha sufrido el Internet de las cosas en los lugares en donde se ha implementado. Estos ataques están dirigidos a tres puntos importantes y son: la seguridad física, donde se limita el acceso al servidor físico y los componentes de hardware, como, por ejemplo, las salas cerradas de acceso restringido para el hardware del servidor y los dispositivos de red. Una de las maneras fáciles de manejar esta implementación es mantener a los usuarios no autorizados fuera de la red, la seguridad del sistema operativo, es decir, mantener

actualizados el software usado por la empresa, como son los Service Packs y mejoras de seguridad cuando se realizan actualizaciones del sistema operativo y la seguridad de los archivos, con ello se busca que los archivos solo sean accedidos por personal autorizado y con los privilegios adecuados para la modificación, actualización o borrado de información.

- En el sexto capítulo, observamos las soluciones de algunas compañías para la prevención de estos ataques como son la protección de las comunicaciones, de los equipos electrónicos y su administración y la comprensión del sistema en sí. Además del uso de estas soluciones en empresas que han implementado el Internet de las cosas.

- En el séptimo capítulo, observamos cómo ha sido el impacto en la sociedad colombiana con la llegada del Internet de las Cosas en las actividades diarias de las empresas como son la monitorización y vigilancia de los ríos por medio de sensores.

- En el octavo capítulo, se refiere a las estructuras que serán necesarias para su funcionamiento como son la clase de dispositivos a conectar, los softwares y aplicativos, la recolección y posterior análisis de la información.

- En el noveno capítulo, observamos cómo nos estamos preparando para su llegada masiva por medio de las empresas de telecomunicaciones que están en el país como es el ejemplo de Claro y su recién inaugurado edificio inteligente llamado Plaza Claro y la aparición de las redes de transmisiones 4.0G y 4.5G.

- En el décimo capítulo, observamos el ingreso de la computación en la nube no como infraestructura real sino como un servicio proporcionado por una

empresa por medio de internet de una manera transparente, además de las ventajas y desventajas del mismo que consigo traería.

- En el onceavo capítulo, observamos uno de los nuevos campos para el análisis de los grandes volúmenes de información que el Internet de las cosas traerá y en donde el Big Data cobra una gran importancia para lograr el objetivo propuesto de administración de datos. Un ejemplo de ello lo encontramos en la EPS Salud Vida con el manejo de las historias clínicas de todos sus afiliados, reuniéndolos en grupos de riesgos para su atención personalizada.

- En el doceavo capítulo, observamos como la Inteligencia Artificial es un nuevo componente en el Internet de las cosas porque de alguna manera podemos adicionar a una máquina un pequeño cerebro para que pueda analizar y comprender como un ser humano y además de poder tomar decisiones por cual propia sin recurrir a otros.

.

5.4 DESARROLLO DE OBJETIVO ESPECÍFICO 3

Objetivo específico: Dar a conocer el futuro informático de muchos de los objetos que marcarán esta nueva revolución digital.

Como es sabido, el Internet de las Cosas (IoT) creará una nueva infraestructura tecnológica para toda la sociedad y con ello vendrán cambios profundos en la economía global durante mucho tiempo. Desde hacen algunos años, día a día millones de dispositivos son conectados por parte de almacenes, sistemas de transporte, cadenas de producción, redes de distribución eléctrica y de agua, oficinas, hogares, tiendas y hasta incluso vehículos que se pueden supervisar continuamente y revisar su funcionamiento con el envío de todos estos datos a través de Internet para tomar los correctivos correspondientes ante fallas que se puedan presentar.

Por consiguiente, la información recopilada se usó para conocer cuál es su definición, cuales son los componentes y características esenciales que tiene el Internet de las Cosas (IoT). Se muestra los diferentes ciberataques a los cuales se ha enfrentado, las soluciones a las que las empresas especializadas han realizado para sus clientes y protección de estos dispositivos. Podemos encontrar una pequeña mirada al avance que ha tenido esta tecnología en el país o como se ha venido trabajando para poderla implementar y además se puede evidenciar cual ha sido los resultados que se han obtenido en el campo de la salud para la organización de las hojas de vida de los pacientes y que cualquier doctor que lo atienda pueda saber cuál es el estado de salud del paciente atendido en la EPS.

5.5 DESARROLLO DE OBJETIVO ESPECÍFICO 4

Objetivo específico: Describir conceptos básicos sobre el internet de las cosas (IoT).

En este apartado se realizó la respectiva recopilación de información y se seleccionaron los artículos que se encuentran relacionados a los temas como Cloud Computing que es la infraestructura virtual proporcionada para los servicios de computación y almacenamiento a través de una red y que normalmente es Internet; las plataformas que permiten integrar los recursos y permitir el intercambio eficaz de información entre las empresas; el Big Data, son los grandes volúmenes de información (estructurados o no estructurados) generados por los dispositivos y que luego deben ser analizados para poder descubrir relaciones o patrones que hay entre ellos; la Inteligencia Artificial que son programas creados para la ejecución de operaciones o conductas comparables a la mente humana, como son el aprendizaje o el razonamiento lógico y el ecosistema que nos define la conexión a Internet por medio de computadores y dispositivos conectados, usando los protocolos de telecomunicaciones definidos (IPv6).

6 CONCLUSIONES

Dentro del análisis expuesto, es posible concluir que este es un tema de vital importancia en el mundo y está siendo potenciado actualmente por los objetos más comunes usados en nuestras viviendas que se encuentran conectados a la red de redes (Internet) y dentro de sus configuraciones estará los límites de las funciones o permisos que el usuario final dispondrá a cada uno de los dispositivos que serán conectados.

En la actualidad existen muchas formas de encontrar información y se evidencio que no se contaba con elementos nuevos u originales para poder tener un mejor análisis de la temática escogida porque en el país aún en un campo inexplorado, aunque no fue un impedimento y se decidió recurrir a fuentes secundarias en donde hay muchos estudios sobre el IoT en diferentes partes del mundo, obteniendo documentación de gran importancia y se aprendió a distinguir y escoger cual es confiable y la que no lo sea.

En relación con lo expuesto, el IoT está encaminado a las empresas industriales para la automatización de los procesos, buscando una mayor productividad. Antiguamente los grandes empresarios no les dedicaban algún tiempo a los datos recopilados, pero en la actualidad estos son un elemento nuevo con valor comercial. Dando lugar a la resolución de problemas en soluciones específicas, aprovechando las nuevas tecnologías que cuentan con la posibilidad de conectar a millones de personas y dispositivos de manera conjunta.

Por lo tanto, estos dispositivos están más propensos a ser atacados por la gran variedad de ciberataques dirigidos a las vulnerabilidades de la seguridad y la privacidad de la información de los usuarios, por ello es necesario desde un comienzo, permitir tener soluciones ante estas amenazas como son las buenas

prácticas en las instalaciones tanto de sistema operativo (actualizaciones y parches de seguridad) como de aplicaciones que tenga buena confianza en el lugar de descarga de la misma, configuraciones y mantenimientos preventivos en todo momento para no tener inconvenientes en un futuro cercano.

Finalmente, el IoT cuenta con una terminología propia que fue expuesta en este análisis; la cual en muchos casos era conocida por haberla escuchado en los medios de comunicación. Pero, no se tenía el conocimiento suficiente para poder asociarla a un mundo inteligente totalmente interconectado mediante las relaciones entre los objetos, las personas y su entorno, marcando el inicio de una nueva revolución digital.

7 BIBLIOGRAFÍA

BANAFA, Ahmed. Internet de las cosas: seguridad, privacidad y protección. En: OpenMind. [En línea]. <https://www.bbvaopenmind.com/internet-de-las-cosas-seguridad-privacidad-y-proteccion/> [citado el 13 de mayo de 2015].

CARACOL RADIO. El internet de las cosas comienza a aterrizar en Colombia. [En línea]. <http://caracol.com.co/radio/2017/09/25/tecnologia/1506347724_142242.html> [citado el 25 de septiembre de 2017].

CÁRDENAS, Álvaro. Plataforma IoT – Secmotic. [En línea]. <https://secmotic.com/blog/plataforma-iot/> [citado el 28 de noviembre de 2016].

CENTRE SEGURETAT TIC DE LA COMUNITAT VALENCIANA CSIRT – CV. GENERALITAT VALENCIANA, UNIÓN EUROPEA. Seguridad en Internet de las cosas: Estado de arte. Documento público. [En línea]. <http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf> [s.f.]. 42 págs.

CISCO. At a glance - Internet of Things. [En línea]. <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf> [citado en 2016].

COLCOM 2014. Foros ISIS No. 5. Seguridad, gran reto para internet de las cosas. [En línea]. <https://sistemas.uniandes.edu.co/images/forosisis/revista/5/pdf/V5_01_Foros_ISIS_5_Seguridad_gran_reto_para_internet_de_las_cosas.pdf> [citado en 2014]. Págs. 41 – 42.

Diario ABC de España. Un fabricante chino retira sus productos de EE.UU. tras ciberataque masivo. En: Diario ABC de España. [En línea].<http://www.abc.es/tecnologia/electronica/imagen/abci-fabricante-chino-retira-productos-eeuu-tras-ciberataque-masivo-201610251427_noticia.html> [citado el 25 de octubre de 2016].

DIARIO EL HERALDO. El 'Internet de las cosas' es una realidad en Colombia. [En línea]. <https://www.elheraldo.co/ciencia-y-tecnologia/el-internet-de-las-cosas-es-una-realidad-en-colombia-411505> [citado el 12 de octubre de 2017].

DOMODESK. A fondo: ¿Qué es el IoT (¿Internet de las cosas?). [En línea]. <http://www.domodesk.com/221PEREZ, Vicente. -que-es-iot-el-internet-de-las-cosas.html> [s.f.].

EVERLET, Álvaro y PASTOR, Javier. Introducción al Internet de las Cosas: Construyendo un Proyecto de IOT. En: Carriots y Universidad Rey Juan Carlos (URJC). [En línea]. <https://www.carriots.com/newFrontend/imgcarriots/press_room/Construyendo_un_proyecto_de_IOT.pdf> [citado en noviembre de 2013].

FUNDACIÓN DE LA INNOVACIÓN BANKINTER. El internet de las cosas en un mundo conectado de objetos inteligentes. [En línea]. <http://www.belt.es/expertos/imagenes/XV_FTF_El_internet_de_las_cosas.pdf> [citado en 2011]. 78 págs.

GARCIA FERNÁNDEZ, Luis Alberto. Uso y aplicaciones de la Inteligencia Artificial. En: Revista de Divulgación científica y tecnológica de la Universidad Veracruzana, Volumen XVII, Numero 3. [En línea]. <https://www.uv.mx/cienciahombre/revistae/vol17num3/articulos/inteligencia/> [citado en 2004].

GEMALTO: SECURITY TO BE FREE. Seguridad integrada y en la nube para e internet de las cosas. [En línea]. <http://www.gemalto.com/latam/iot/seguridad-en-iot> [citado en 2018].

HERNANDEZ, Juan. ¿Qué es y para qué sirve el Cloud Computing? En: EditaBlog, el blog de Editafácil. [En línea]. <http://blog.editafacil.es/que-es-y-para-que-sirve-el-cloud-computing/> [citado el 11 de febrero de 2016].

HIDALGO CASTRO, Berni, GONZÁLEZ JIMÉNEZ, Jack y MURILLO CASTRO, Royers. El internet de las cosas. [En línea]. <http://alfarosolis.com/content/PDFs/IF7100/Semana14/Iot.pdf> [citado en 2017].

IGLESIAS FRAGA, Alberto. Ciberataques contra los hoteles: los cuatro más notorios. En: Tic Beat. [En línea] <http://www.ticbeat.com/seguridad/ciberataques-contra-los-hoteles-los-cuatro-casos-mas-notorios/> [citado el 19 de noviembre de 2016].

Inteligencia Artificial: Ventajas y desventajas de su adopción en las empresas. En: Grupo Selectiva. [En línea]. <https://selectiva.es/ventajas-y-desventajas-de-inteligencia-artificial/> [citado el 2018].

ITUSER. IoT hace a los hospitales más vulnerables a los ciberataques. En: ITUser, [En línea]. <http://www.ituser.es/seguridad/2016/11/iot-hace-a-los-hospitales-mas-vulnerables-a-los-ciberataques> [citado el 28 de noviembre de 016].

JANE, Carmen. Alerta por la inseguridad del internet de las cosas. En: Diario El

Periódico. [En línea]. <http://www.elperiodico.com/es/sociedad/20161029/alerta-por-la-seguridad-del-internet-de-las-cosas-5595145> [citado el 29 de octubre de 2016].

LOGICALIS: BUSSINESS AND TECHNOLOGY WORKING AS ONE. La seguridad del internet de las cosas, en el punto de mira. [En línea]. <https://blog.es.logicalis.com/seguridad/la-seguridad-del-internet-de-las-cosas-en-el-punto-de-mira> [citado el 10 de mayo de 2017].

MARTIN BARRERO, Iván. La seguridad del internet de las cosas (IoT), un grave problema a resolver. En: Diario El País. [En línea]. <https://cincodias.elpais.com/cincodias/2016/10/26/lifestyle/1477469985_167878.html> [citado el 26 de octubre de 2016].

MEDINA C, María Alejandra. La historia detrás del internet de las cosas. En: Diario El Espectador. [En línea]. <https://www.elespectador.com/tecnologia/la-historia-detras-de-la-internet-de-las-cosas-articulo-716678> [citado el 05 de octubre de 2017].

MOLANO, Adriana. Internet de las cosas: Concepto y ecosistema. En: Colombia Digital. [En línea]. <https://colombiadigital.net/actualidad/articulos-informativos/item/7821-internet-de- las-cosas-concepto-y-ecosistema.html> [citado el 01 de octubre de 2014].

MUCIENTES, Esther. Así se gestó el ciberataque más grave de los últimos 10 años. En: Diario El Mundo, España. [En línea] <http://www.elmundo.es/tecnologia/2016/10/22/580b10e5268e3e06158b45e0.html > [citado el 22 de octubre de 2016].

OJEDA, Diego. ¿Qué es el Internet de las cosas y por qué se acerca más a Colombia? En: Diario El Espectador. [En línea].<https://www.elespectador.com/tecnologia/que-es-el-internet-de-las-cosas-y-por-que-se-acerca-cada-vez-mas-colombia-articulo-716699> [citado el 05 de octubre de 2017].

PAGANINI, Pierluigi. Exclusive: A criminal group using SSH TCP direct forward attack is also targeting Italian infrastructure. En: Security Affairs. [En línea]. <http://securityaffairs.co/wordpress/56864/cyber-crime/ssh-tcp-direct-forward.html> [citado el 04 de marzo de 2017].

PAGANINI, Pierluigi. It has happened again, ransomware infected an LG Smart TV. En: Security Affairs. [En línea]. <http://securityaffairs.co/wordpress/54991/malware/lg-smart-tv-ransomware.html> [citado el 03 de enero de 2017].

PÉREZ, Vicente. El “Internet de las cosas”, una nueva ventana para la ciberdelincuencia. En: Diario ABC de España. [En línea]. <http://www.abc.es/tecnologia/redes/abci-internet-cosas-nueva-ventana-para-ciberdelincuencia-201611041537_noticia.html> [citado el 07 de noviembre de 2016].

Porque Internet de las cosas necesita Inteligencia Artificial. En: OpenMind. [En línea]. <https://www.bbvaopenmind.com/por-que-internet-de-las-cosas-necesita-inteligencia-artificial/> [citado el 18 de julio de 2017].

POWERPLANETONLINE. Problemas del IoT (Internet of Things). En: Powerplanet.com. [En línea]. <http://blog.powerplanetonline.com/problemas-del-iot-internet-of-things/> [citado el 13 de junio de 2017].

ROUSE, Margaret. Seguridad del internet de las cosas. TechTarget – Search DataCenter en español. [En línea]. <http://searchdatacenter.techtarget.com/es/definicion/Seguridad-de-Internet-de-las-Cosas> [citado en febrero de 2017].

SAIF, Irfan, PEASLEY, Sean and PERINKOLAM, Arun. Safeguarding the Internet of the Things: Being secure, vigilant, and resilient in the connected age. En: Deloitte. [En línea]. <https://www2.deloitte.com/es/es/pages/about-deloitte/articles/La-proteccion-del-Internet-de-las-Cosas-seguridad-vigilancia-y-resistencia-en-la-era-digital.html> [citado en Issue 17, 2015]. 18 págs.

SANZ, Elena. ¿Qué es el internet de las cosas? En: Revista Muy interesante. [En línea]. <https://www.muyinteresante.es/curiosidades/preguntas-respuestas/ique-es-el-qinternet-de-las-cosasq> [s.f.].

SCAGLIA, Sergio. Inteligencia Artificial: el “Internet de las cosas” y la expansión de lo digital. En: Sociedad Los Andes. [En línea]. <https://losandes.com.ar/article/view?slug=inteligencia-artificial-el-internet-de-las-cosas-y-la-expansion-de-lo-digital> [citado el 14 de julio de 2018].

STARK, Karen. La seguridad del internet de las cosas. En: Evaluandosoftware.com. [En línea]. <http://www.evaluandosoftware.com/la-seguridad-del-internet-las-cosas/> [citado el 28 de agosto de 2017].

SUAREZ, Ronny. El ‘Big Data’ en salud: presente y futuro de la atención. En: Diario El Tiempo. [En línea]. <https://www.eltiempo.com/vida/salud/como-se-puede-aplicar-el-big-data-en-salud-258536> [citado el 21 de agosto de 2018].

SYMANTEC. An Internet of Things Reference Architecture. <https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf> [citado en 2016].

SYMANTEC. Seguridad del internet de las cosas (IoT). [En línea]. https://www.symantec.com/es/mx/solutions/internet-of-things> [citado en 2016].

TECNOSFERA. Claro abre centro de internet de las cosas y realidad virtual. En: periódico El Tiempo. [En línea]. <http://www.eltiempo.com/economia/empresas/inauguran-plaza-claro-que-tiene-internet-de-las-cosas-y-realidad-virtual-227406> [citado el 06 de junio de 2018].

Tipos de Cloud Computing. En: AWS. [En línea]. <https://aws.amazon.com/es/types-of-cloud-computing/> [citado en 2018].

TRIQUET, Jean. ¿Para qué sirve el Big Data en mi empresa? En: La tecnología me gusta, Blog de contenidos en español. [En línea]. <http://director-it.com/index.php/es/ssoluciones/data-center-cloud-virtualizacion/almacenamiento/127-%C2%BFpara-que-sirve-el-big-data-en-mi-empresa.html> [citado en 2017].

VARGAS, Monserrat. Seguridad: el principal reto del internet de las cosas. En: Informática Diario La Nación. [En línea]. <http://www.nacion.com/tecnologia/informatica/seguridad-el-principal-reto-para-internet-de-las-cosas/S4KUHLUCOFHXDJPOWEW4OLSAA4/story/> [citado el 07 de julio de 2016].

VARGAS, Rómulo. La seguridad en tiempos del internet de las cosas (IoT). En: Maint. [En línea]. <http://www.maint.com.ec/la-seguridad-en-tiempos-del-internet-de-las-cosas/> [citado en 2016].

VEGA, Ricardo. Seis características clave del Internet de las cosas. [En línea]. <https://ricveal.com/blog/6-caracteristicas-clave-del-internet-de-las-cosas/> [citado el 22 de octubre de 2015].

VELASQUEZ DURAN, Ana María. Drones y sensores: así usan el internet de las cosas en el país. En: Diario El Tiempo. [En línea]. <http://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-se-usa-el-internet-de-las-cosas-en-colombia-144004> [citado el 25 de octubre de 2017].

Ventajas y desventajas de la Inteligencia Artificial. En: Diario de Yucatán. [En línea]. <http://www.yucatan.com.mx/tecnologia/ventajas-desventajas-la-inteligencia-artificial> [citado el 19 de mayo de 2018].

Ventajas y desventajas del Cloud Computing. En: ENAE Bussiness School. [En línea]. <https://www.enae.es/blog/ventajas-y-desventajas-del-cloud-computing#gref> [citado el 25 de junio de 2010].

WAUGH, Rob. Seguridad en internet de las cosas: cómo proteger tus dispositivos Smart. En: Welivesecurity en español. [En línea]. Disponible en: <https://www.welivesecurity.com/la-es/2014/11/25/seguridad-internet-de-las-cosas/> [citado el 25 de noviembre de 2014].

YOUTUBE. ¿Qué es una Smart City? En: Endesa Educa. [En línea]. <https://www.youtube.com/watch?v=lKpoi8lf_tI> [citado el 28 de octubre de 2014].