Mundo Fesc, 10 (19), pp. 162-179 Enero-Junio, 2020, ISSN 2216-0353, 2216-0388

Vulnerabilidad en la seguridad del internet de las cosas

Vulnerability in the security of the internet of things

[a]Diego Cárdenas-Quintero,[b] Exel Ropero-Silva,[c]Karla Puerto-López,[d]Karla Sanchez-Mojica, [e]Sergio Castro-Casadiego, [f]Jhon Ramírez-Mateus

a Ingeniero Electrónico, diegomauriciocq@ufps.edu.co, Universidad Francisco de Paula Santander, Cúcuta, Colombia
b Ingeniero Electrónico, exelropero@ufps.edu.co, Universidad Francisco de Paula Santander, Cúcuta, Colombia
c Magister en Inegeniería de Telecomunicaciones, karlaceciliapl@ufps.edu.co, Universidad Francisco de Paula Santander, Cúcuta, Colombia
d Maestría en curso en Ingeniería Industrial, investigaciones@fesc.edu.co, Fundación de Estudios Superiores Comfanorte, Cúcuta, Colombia
e Magister en Ineniería Electrónica, sergio.castroc@ufps.edu.co, Universidad Francisco de Paula Santander, Cúcuta, Colombia
f Maestría en curso en Ingeniería Industrial, jhonjairorm@ufps.edu.co, Universidad Francisco de Paula Santander, Cúcuta, Colombia

Recibido: Julio 16 de 2019 **Aceptado:** Noviembre 22 de 2019

Forma de citar: D. Cardenas-Quintero, E. Ropero-Silva, K. Puerto-López, K. Sanchez-Mojica, S. Castro-Casadiego, J. Ramirez-Mateus "Vulnerabilidad en la seguridad del internet de las cosas", *Mundo Fesc,* vol. 10, no. 19, pp. 162-179, 2020

Resumen

En poco tiempo, internet cambió rápidamente la manera en la que trabajamos y la actual fase, llamada el Internet de las Cosas (IoT), permitirá la conexión del mundo físico a la red. Este trabajo busca conocer de IoT sus generalidades, comunicación, amenazas y metodologías que contrarresten los peligros existentes. Finalmente, el aumento de dispositivos IoT conectados es inminente, lo que conllevará a la creación de nuevas tecnologías; por ende, se debe prestar atención a los grandes cambios tecnológicos, principalmente en temas de seguridad y privacidad de la información, ya que la vulnerabilidad en la mayoría de dispositivos de IoT permite a los atacantes tener acceso remoto al dispositivo o tomar el control completo del sistema. Debido a este crecimiento y a los problemas existentes en IoT es necesaria la alianza entre empresas para crear soluciones que permitan tener una mayor seguridad, y así, más usuarios implementen esta tecnología sin el temor a que su información sea manipulada, un tema que involucra a la comunidad en general.

Palabras clave: Internet de las cosas, privacidad, seguridad, vulnerabilidad.

Autor para correspondencia:
*Correo electrónico: karlaceciliapl@ufps.edu.co

Abstract

In a short time, the Internet quickly changed the way we work and the current phase, called the Internet of Things (IoT), will allow the connection of the physical world to the network. This work seeks to know about IoT its generalities, communication, threats and methodologies that counteract the existing dangers. Finally, the increase in connected IoT devices is imminent, which will lead to the creation of new technologies; therefore, attention should be paid to major technological changes, mainly in matters of information security and privacy, since the vulnerability in most IoT devices allows attackers to have remote access to the device or take full control of the system. Due to this growth and the existing problems in IoT, the alliance between companies is necessary to create solutions that allow greater security, and thus, more users implement this technology without fear that their information will be manipulated, an issue that involves the community in general

Keywords: Internet of things, privacity, security, vulnerability.

Introducción

A lo largo del tiempo, Internet ha evolucionado de forma rápida y notoria, atravesando múltiples fases. Desde su etapa inicial de "internet del contenido", en que era básicamente una base de datos estática de documentos de hipertexto interconectados; se ha llegado más recientemente al “internet de las personas” donde las redes sociales y el consumo de video han tomado un protagonismo indiscutible. Según todas las predicciones, y según apunta ya la propia realidad, la próxima fase será el “internet de las cosas” [1]

El internet de las cosas (Internet of Things, IoT) se refiere a la interconexión de objetos cotidianos a la red. Esta tecnología de rápido avance y desarrollo, ha buscado facilitar y mejorar la calidad de vida del hombre, pero con grandes riesgos inminentes como la confidencialidad de los datos, integridad de la información, identidad de los usuarios, entre otros, son amenazas a la que están expuestos los tantos dispositivos conectados a internet [2], [3].

Hoy en día es fácil acceder a toda esta información, por eso, es importante identificar la vulnerabilidad que presentan los dispositivos IoT en temas de seguridad al conectarse a la red, y conocer las medidas de protección recomendadas, concientizando la necesidad que existe de protegerlos para garantizar la privacidad de los datos [4].

Un ejemplo de ello, es el primer hackeo demostrado realizado a dispositivos inteligentes durante el 23 de diciembre de 2013 y el 6 de enero de 2014, en el que se usaron 100.000 dispositivos conectados como routers, centros multimedia, televisores y por lo menos un refrigerador para enviar al menos 750.000 correos electrónicos con contenido malicioso (spam) a empresas e individuos en todo el mundo. Según los analistas de seguridad de la empresa Proofpoint, quienes descubrieron el ataque, aseguraron que la mayoría de estos dispositivos no tienen software anti-malware instalado, no encriptan sus datos y son enviados con las mismas contraseñas administrativas predeterminadas [5].

También, el ataque al monitor de bebés Foscam en 2015, donde la familia que utilizaba este monitor inalámbrico fue víctima de un hacker. El Hacker tomó el control de la cámara y la movió siguiendo a la madre mientras le hablaba y le hacía comentarios sobre el niño. Este caso, y como muchos otros más, pone como relevancia la importancia en la privacidad de los consumidores en lo que respecta al mundo conectado de IoT [6].

Además, el ataque causado el 21 de octubre

de 2016, donde se generó una interrupción generalizada de internet en los Estados Unidos por más de dos horas, ocasionado por la gran cantidad de dispositivos conectados a la red que no contaban con protección y aún mantenían las contraseñas por defecto, permitió tres ataques de denegación de servicio distribuido (DDoS) al sistema de resolución de nombres (DNS) durante ese día [7].

Por eso, "cuantos más dispositivos y puntos de ingreso haya en una red, más oportunidades tendrán los ciber criminales de infiltrarse." "Conscientes de estos peligros, los expertos de Kaspersky Lab revisan periódicamente los datos recopilados por diversas fuentes, incluidos nuestros honeypots, dispositivos que se utilizan como señuelos para atraer la atención de los ciberdelincuentes y analizar sus actividades. Las actualizaciones más recientes son sorprendentes: durante la primera mitad de 2018, el número de modificaciones de malware dirigidas a dispositivos IoT que fueron observadas por los investigadores se elevó a más del triple en comparación al número registrado en todo 2017" [6], [8], [9].

En este artículo de revisión se dará un estudio acerca de la vulnerabilidad del IoT tanto a nivel nacional como internacional, entendiendo cómo se comunican los dispositivos IoT, analizando los tipos de amenazas que pueden presentarse en estos sistemas y revisando los diferentes modelos de seguridad sugeridos por algunos autores, que permiten contrarrestar las debilidades en seguridad producidas en la diversidad de dispositivos en el mercado de IoT [10], [11].

Materiales y métodos

En el planteamiento metodológico de este trabajo, se creó una tabla para la revisión bibliográfica, con los siguientes campos (categorías de análisis): Autor y año, título, objetivo, método de análisis, resultados y conclusiones. Una vez organizada la información, se agruparon los documentos en cuatro núcleos temáticos, a saber: IoT a nivel general, comunicación de dispositivos IoT conectados a la red, amenazas en la privacidad de los datos y modelos o metodologías en seguridad.

En primer lugar, se muestra un panorama general del Internet de las Cosas, donde se incluyen sus características, se describe la evolución que ha tenido internet, sus retos actuales y futuros, de modo que IoT es lo más relevante de los últimos tiempos y es la puerta a un mundo inteligente totalmente interconectado. De igual manera, y debido al aumento de datos, se mencionan las brechas en seguridad e información y los parámetros técnicos para IoT en Colombia.

Por lo cual, a nivel internacional, María Romero de la Universidad Politécnica de Madrid, España, en el 2017 analiza desde el punto de vista de la protección y la privacidad, los riesgos que supone el Internet de las cosas en general mediante un repaso del pasado, presente y predicciones futuras, sus características y campos de aplicación; y el internet de las cosas médicas en particular para los usuarios al mismo tiempo revisa la legislación vigente con la que podemos hacer frente a estos desafíos y las modificaciones que deberán realizarse para adaptar el marco legal a las amenazas del IoT. Para terminar, la autora indica que la información y la protección de los datos de los usuarios y su privacidad es, precisamente, una de las amenazas más importantes del IoT en cualquier área de aplicación. El aumento de datos y su tratamiento, y el aumento de actores que puedan acceder a ellos hace que se deba prestar atención a este desafío por parte de todas las partes implicadas, como pérdida de autonomía, pérdida de control de nuestros datos, derecho a decidir, robo de identidad, sobrecarga de datos, control de

dispositivos, usos "poco éticos" de nuestra información, y rastreo y seguimiento del individuo [12].

Consecuentemente, los autores José Chacón Rangel, Anderson Flórez Fuentes y Johel Rodríguez de la Universidad de Pamplona, sede Villa del Rosario, Colombia, en el 2015 en su trabajo titulado "La Inteligencia Artificial y sus contribuciones a la física médica y la bioingeniería" analizan la inclusión de la Inteligencia Artificial en los avances informáticos orientados bajo la premisa de dotar a los dispositivos tecnológicos de capacidades propias de la inteligencia humana. Además, ilustran la comprensión y el modelado de las capacidades de procesamiento de información de la mente humana como principio para sistemas inteligentes. [13]

También, los autores María Ruiz, Arturo Serrano, Eduardo Álvarez y Edith García en el Congreso Internacional de Investigación en Tijuana, México, en el 2017 analizan el Internet de las cosas en la era de 5G y de Blockchain como retos en ese país, identificando si las condiciones y estrategias nacionales (de usuarios, empresas y gobierno), pueden enfrentarse a los retos actuales y futuros en estas temáticas de telecomunicaciones, mediante una descripción del Internet de las Cosas y 5G, detallando la tecnología de Blockchain, presentando la convergencia entre blockchain e IoT; y revisando los retos en México. Para terminar, es la opinión de los autores, que las tecnologías 5G y el IoT serán relevantes en un futuro cercano, para dar forma a la explotación comercial del Internet en los próximos años, el impacto de ésta tecnología diluirá aún más el concepto de fronteras geográficas, en la medida en que proveedores internacionales de IoT ofrezcan servicios en los distintos países, y esto puede impactar en temáticas de seguridad personal, industrial y nacional, si no se cuenta con una legislación que proteja los intereses regionales, industriales, personales o nacionales [14].

Por su parte, 5G Américas, al ser una organización sin fines de lucro compuesta por proveedores de servicios y fabricantes líderes de la industria de las telecomunicaciones con su sede en Bellevue, Washington, en 2016 presentan los diversos aspectos de la tecnología celular y reseña las nuevas soluciones que abordarán los requisitos futuros de los casos de uso del Internet de las cosas en América Latina, de manera descriptiva y evolutiva, menciona como los dispositivos, la conectividad y los servicios de TI constituirán la mayor parte del mercado de IoT en el 2020. Por último, esta organización indica como IoT se dirige a una gran revolución que habilita al mundo inteligente que nos rodea, siendo evidente la evolución amplia en el uso de medios inalámbricos, donde miles de millones de dispositivos operan en una gran red, e IoT tiene la oportunidad de aumentar la conectividad en el resto del mundo [15].

Asímismo, Karen Rose, Scott Eldridge y Lyman Chapin miembros de Internet Society, organización mundial que apoya y promueve el desarrollo de internet como una infraestructura técnica, para que sea abierto, globalmente conectado, seguro y confiable, en Virgina, USA, en el año 2015 realizan una breve reseña sobre el Internet de las Cosas para entender mejor los problemas y desafíos de un mundo más conectado, analizando cinco áreas claves de IoT como los son la seguridad; la privacidad; la interoperabilidad y los estándares; cuestiones legales, reglamentarias y relacionadas con los derechos; y economías emergentes y cuestiones relacionadas con el desarrollo. En definitiva, para los autores, IoT promete abrir la puerta a un mundo revolucionario, un mundo "inteligente" totalmente interconectado en el cual las

relaciones entre los objetos y su entorno y las personas se entrelazarán aún más [16].

Por otro lado, Carlos Cortés del centro de estudios en libertad de expresión y acceso a la información de la Universidad de Palermo en Buenos Aires, Argentina, en 2014 en su trabajo llamado "El 'internet de las cosas': más internet que otra cosa" que tiene como objetivo ofrecer un panorama sobre el tema conocido públicamente como el 'internet de las cosas' (IoT), plantea el antecedente histórico de la computación ubicua, describe los retos técnicos que implica hablar de un internet de las cosas y habla sobre los riesgos de un entorno de objetos interconectados. Así mismo, indica que en un escenario futuro de millones de dispositivos conectados a la red implicará una explosión exponencial del tráfico. Si esta realidad es desafiante para Estados Unidos o Europa, es abrumadora para los países de la región latinoamericana. Así, cualquier discusión sobre IoT debe tener en cuenta los retos que aún subsisten en infraestructura y acceso a internet. Por último, concluye que los riesgos en materia de privacidad, seguridad y autonomía que surgen en el IoT no son distintos a los que encontramos asociados hoy al entorno digital en general. Si hubiera que plantear alguna diferencia, ésta reside en la escala: en un contexto de IoT, estos riesgos parecen acentuarse [17].

Además, El Centro de Seguridad TIC de la Comunidad Valenciana como primer centro formado en España con personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de esa comunidad, en 2014 realiza un análisis de estado de la seguridad en que se encuentran los dispositivos englobados en la categoría de IoT con recopilación de los incidentes más relevantes hasta la fecha y ejemplos con situaciones domésticas comunes, donde se logran identificar brechas en seguridad e información y en el control de dispositivos IoT. Estos concluyen, que para que exista confianza en el uso de las nuevas tecnologías es necesaria la participación de todas las partes (desde el desarrollo del producto e implementación del mismo, hasta el usuario final que lo configura y hace uso del dispositivo), es decir, la tecnología debe ser una evolución y no un retroceso en seguridad y privacidad de sus usuarios [2].

De la misma forma, a nivel nacional, Rafael Niño, profesional del grupo de Ingeniería de la Agencia Nacional del Espectro (ANE), y esta, como entidad encargada de planear estratégicamente el uso del espectro radioeléctrico (ERE), así como su vigilancia y control en todo el territorio nacional colombiano, en el 2018 define los parámetros técnicos para promover el internet de las cosas en Colombia, proponiendo mecanismos de gestión del ERE para promover mayor conectividad en Colombia a través del estudio de diversas tecnologías y aplicaciones, como por ejemplo el Internet de las cosas. Para finalizar, el autor describe mediante una tabla los tipos de conectividad inalámbrica y posibles bandas de frecuencia a ser usadas para aplicaciones de IoT, teniendo en cuenta los tipos de red por área de cubrimiento, el uso del espectro, los tipos de servicios comerciales, las posibles bandas de frecuencia y tecnologías que son usadas en diferentes países alrededor del mundo; la variedad de relaciones entre estos parámetros generales, permite ampliar las opciones para la implementación de IoT [18].

Igualmente, los autores Manuel García, Héctor Ariza, Martha Pinzón y Anderson Flórez, en el 2016, en su trabajo titulado "Buenas prácticas aplicadas a la implementación colaborativo de aplicativos web", muestran el desarrollo e implementación de un sistema web de

préstamo de recurso para la Universidad de Pamplona sede Villa del Rosario, Colombia, que permitió tanto a docentes sacar prestado un recurso para apoyo de su clase como a administrativos en caso de la realización de un eventos. Este trabajo muestra la importancia de la compilación de métodos para optimizar las actividades que comprenden el desarrollo de un sistema de información. [19]

Dentro de este orden de ideas, David Leonardo Pinzón Niño de la Universidad Santo Tomás, en el 2015 establece el cuerpo del conocimiento existente alrededor de la temática del internet de las cosas (IoT), mediante una revisión bibliográfica que permita identificar las oportunidades de investigación y desarrollo para fortalecer las iniciativas del grupo de investigación INVTEL de la Universidad, consolidando y clasificando el conocimiento especializado que circula en la sociedad relacionado a IoT. En conclusión, para el autor, el término IoT resulta complejo porque se puede se puede desarrollar a través de la convergencia de varios desarrollos que interactúan entre sí para hacer de IoT una realidad. Es por ello que IoT resulta uno de los avances tecnológicos más relevantes de los últimos tiempos, por su desarrollo e investigación [20].

En segundo lugar, se estudian los lineamientos fundamentales en seguridad de IoT y su comunicación, teniendo en cuenta los protocolos y tecnologías más relevantes en IoT, y el tráfico de información en aplicaciones para IOS.

Es por ello, que a nivel internacional, Yassine Chahid, Mohamed Benabdellah, Abdelmalek Azizi de la Mohammed First University en 2017 proporcionan un estado del arte de los principales protocolos que gestionan la comunicación la IoT, en su artículo llamado "Comparación de protocolos de Internet de las cosas, arquitectura, vulnerabilidades y seguridad: estado del arte", En este trabajo muestran un estudio general sobre los protocolos más conocidos utilizados en IoT como wifi, Bluetooth, zigBee y NFC; esto ayuda a comprender mejor el funcionamiento de cada protocolo, su arquitectura y sus vulnerabilidades. Como resultado de su estudio demuestran que cada protocolo tiene sus ventajas y desventajas, a diferencia de otros protocolos. Finalmente concluyen que, en el mundo se desarrollan varios protocolos para gestionar la comunicación en la IoT, pero dado que cada protocolo tiene sus fallas, también aumenta el número de vulnerabilidades [21].

De esta manera, Juan Martínez, Jezreel Mejía, Mirna Muñoz, Yolanda-Meredith García del Centro de Investigación en Matemáticas CIMAT, del Instituto Tecnológico Superior Zacatecas Norte, México, en 2016 hablan de la seguridad del internet de las cosas, analizando el tráfico de información en aplicaciones para IOS, con el objetivo de demostrar qué tan fácil es interceptar tráfico https y que, aunque las conexiones se hagan mediante este protocolo, no se debe transmitir información sensible de los usuarios sin cifrar. En este análisis obtuvieron como resultado que las aplicaciones transmiten una cantidad considerable de información personal sin cifrar que, aunque la mayoría de ésta pudiera parecer no muy comprometedora, el simple hecho de que alguien pueda acceder a los hábitos de una persona y conocer dónde vive, lugares dónde ejercitarse, cuanto tiempo en promedio dura su rutina de ejercicio, etc., es un gran riesgo, porque estos datos podrían ser útiles para delincuentes [22].

En relación a las ideas anteriores, a nivel nacional, González Larín Yeisson Germán de la Universidad Piloto de Colombia en 2016 en su trabajo titulado "El Internet De Las Cosas Y Sus Riesgos Para La

Privacidad", expone la tendencia del internet de las cosas, además, da a conocer las principales tecnologías de comunicación y da una breve explicación de las principales vulnerabilidades y riesgos a los que las personas, sociedades y/o empresas se pueden ver expuestos al incursionar en el IoT. En él explica como en la actualidad se están dando alianzas entre empresas que están inmersas en la tecnología IoT para crear protocolos de comunicación más seguro. Por último, concluye que contar con los objetos de uso cotidiano conectados a Internet, implica serios problemas para la privacidad de la información, a esto se suma la indiferencia hacia la seguridad de muchos fabricantes y, aunque algunos trabajan para asegurar sus dispositivos, no lo hacen al ritmo al que avanza la tecnología [23].

Asimismo, los autores Yuri Medina y Haider Miranda, de la Universidad de Pamplona en 2015 en su trabajo titulado "Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES", presentan la criptografía como una de las principales categorías de la seguridad informática que convierte la información de su forma normal en un formato ilegible. Esto debido a que la seguridad es uno de los retos relevantes de la Internet y los desarrollos informáticos [24].

En tercer lugar, se tienen en cuenta las amenazas en seguridad y privacidad de información, temas más preocupantes en la población, así como la integridad física, debido a que en tecnología IoT se presentan vulnerabilidades en privacidad del contenido, ausencia en el cifrado de transporte de información, entre otras. Por tanto, se debe considerar la seguridad de la información en estos dispositivos desde la concepción y desarrollo de productos, dependiendo el entorno en que serán implementados, ya que no existen estándares en el tema de IoT, ni protocolos que se puedan aplicar.

Por consiguiente, a nivel Internacional, los autores Alberto Domínguez, Miguel Vargas-Lombardo de la Universidad tecnológica de Panamá, en 2018 realizaron un estudio sobre el estado del arte en salud inteligente y el internet de las cosas (IoT), donde proponen implementar en los dispositivos IoT utilizados en salud una capa de seguridad informática extra sin importar que el fabricante la tenga embebido en su producto, dicha capa dificulta que el atacante pueda manipular nuestros equipos a su conveniencia o que pueda explotar una falla conocida en un dispositivo que pueda afectar la vida, salud e integridad del paciente; el estudio muestra la gran necesidad de crear nuevas tecnologías que permitan conservar la seguridad de los pacientes, esto debido a que las empresas en la actualidad no enfocan el trabajo en la seguridad de los datos sino en entregar a los usuarios métodos fáciles de utilizar la tecnología IoT [25].

Por lo tanto, Hanan Mustapha, Ahmed M Alghamdi de la Universidad Metropolitana de Manchester, en 2018 en su trabajo llamado "Ataques DDoS en el Internet de las cosas y sus métodos de prevención" abordan los ataques DDoS en IoT y los problemas de seguridad en IoT que sirven a los atacantes DDoS para cumplir su objetivo. En su trabajo se encontró que las vulnerabilidades más comunes en la tecnología IoT que permiten los ataques DDoS son: Autenticación y autorización, redes inseguras, falta de cifrado, y en software seguro. Igualmente demuestran que los métodos de detección y prevención DDoS más eficientes se realizan mediante el uso de modelos de redes específicos, la mayoría de los cuales son redes definidas por software (SDN) y virtualización de funciones de red (NFV). Finalmente concluyen que al garantizar una mejor seguridad en IoT evitará problemas de privacidad, pérdida de datos y fugas de información, también, que al combinar las tecnologías de red SND y NFV se pueden

detectar ataques DDoS antes de que ocurran por medio del análisis de tráfico automatizado [26].

Por eso, Javier Castellanos Cañadas en el 2017 realiza un proyecto que consiste en el análisis de seguridad y vulnerabilidad de dos dispositivos de IoT tanto a nivel de software como de hardware, con el fin de explotarlos y obtener los máximos privilegios del equipo. En donde usa dos dispositivos usados en la tecnología IoT de diferentes fabricantes con el objetivo de identificar posibles deficiencias de seguridad. En donde se encontró que uno de los fabricantes diseño e implemento el dispositivo teniendo en cuenta diferentes aspectos relativos a la seguridad, y donde el otro dispositivo no parece haber sido diseñado e implementado basándose en la seguridad, sino más bien una integración un tanto pobre de distintos componentes de terceros. Esto demostró que actualmente no hay una legislación, norma o protocolo que exijan a los fabricantes de los dispositivos IoT seguir una metodología desde el diseño a la implementación teniendo en cuenta la seguridad que estos dispositivos deben llevar para tener a salvo la información que ellos almacenan [27].

También, Miguel Castro Sola de la Universidad de Jaén, España, en el 2016, en su trabajo final de grado llamado internet de las cosas Privacidad y seguridad, realiza un estudio sobre las cuestiones de privacidad y seguridad de los datos en el paradigma de internet de las cosas, en donde analiza en profundidad todos los cambios que va a suponer la implantación de esta nueva forma de entender la tecnología en general, y la manera de hacer las cosas tanto cotidianas como laborales, asimismo explica y analiza en mayor detalle los diferentes grupos de amenazas a la seguridad, que serán: seguridad en el software, seguridad en la configuración y funcionalidad, seguridad en el hardware, seguridad en los usuarios. Por último, concluye que la seguridad y privacidad de nuestros datos e información es uno de los aspectos que más preocupan a la población, así como nuestra integridad física [28].

Asímismo, Fabian Cuzme de la Pontificia Universidad Católica del Ecuador, en el 2015, en su tesis "el Internet de las Cosas y las condiciones de seguridad", establece los mecanismos de seguridad a considerar con la innovación tecnológica de IoT, mediante una investigación descriptiva y experimental, realiza un análisis de la información relevante en la adopción del IT y los niveles de seguridad que se están considerando, con el fin de proponer un desarrollo de esquemas para diseñar objetos inteligentes con niveles de seguridad aceptables. En su conclusión, identifica que los desarrolladores de esta tecnología deben considerar la seguridad durante la concepción y desarrollo de productos IoT dependiendo del entorno en el que vayan hacer implementados; también identifica un esquema de seguridad para entornos IoT, donde están involucrados componentes como dispositivos/sensores, puertas de enlaces, canales de transporte, facilitación/plataformas de recolección de información y aplicaciones que permiten ver la información estructurada [29].

Por su parte, Vicente José Pastor Pérez y José Ramon Coz Fernández, en el 2015, en su artículo llamado "La Ciberdefensa militar ante el reto de Internet de las Cosas", definen uno de los riesgos más grandes en Ciberdefensa, y es el incremento de dispositivos conectados a la red, con un efecto multiplicador en las posibilidades de lanzar ataques DDos; estos ataques, lanzados sobre los dispositivos pueden suponer, en algunos casos del ámbito de la defensa, amenazas a la vida humana. Para finalizar, los autores describen, desde su punto de vista, IoT como uno de los principales motores de cambio de la Ciberdefensa en el futuro, y es necesario

realizar desde ya y con premura, cambios importantes en los elementos de soporte a la Ciberdefensa, incluyendo estrategias, políticas, procedimientos, programas, proyectos, tecnologías y gestión, para poder dar respuestas a los nuevos riesgos introducidos [30].

De este modo, a nivel nacional, Ivan Castaño del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), Tito Neira de Scotiabank, Diego Zuluaga de Isagen, Mayor Milena Realpe del Comando Conjunto Cibernetico, Fayçal Daira, de Stormshield, Estados Unidos, Sandra Rueda del Departamento de Ingeniería de Sistemas y Computación (DISC) de la Universidad de los Andes y Luis Javier Parra de Info Projects, en el 2018 participaron en el tercer foro de seguridad de la información realizado en la Universidad de los Andes para comprender, adoptar y ser capaces de potencializar a las organizaciones hacia los cambiantes desafíos que plantean el rápido crecimiento que ofrece internet de las cosas para mejorar la calidad de vida de la sociedad, concientizando el conflicto entre las operaciones y la seguridad, y cómo mejorar las soluciones de protección en la industria mediante situaciones reales. Para terminar, estos definen un reto importante de cómo vamos a gestionar estos dispositivos, si no hay estándares en el tema de IoT, ni protocolos que se puedan aplicar, pese a que cada vez están más conectados a nuestras redes; hay que mantener actualizados los sistemas de defensa, buscar alternativas; y el análisis de vulnerabilidades se hizo más complejo porque tenemos un nuevo punto desde donde se pueden meter diferentes tipos de infección o de ataques [31].

Dentro de este orden de ideas, Coy Sosa William Andrés de la Universidad Piloto de Colombia en 2016 Describe las diferentes falencias que los dispositivos del internet de las cosas (IoT) pueden llegar a tener, en su trabajo titulado “Iot - El Internet De Las Cosas Y Sus Riesgos En Los Pilares De La Seguridad De La Información”. En el nombra 25 vulnerabilidades en la seguridad de los dispositivos IoT de un estudio realizado por la empresa HP. Las vulnerabilidades hacen que los atacantes puedan tener acceso remoto al dispositivo, en algunos casos hacer escalamiento de privilegios y allí tomar control completamente del sistema. Para finalizar concluye que Uno de los grandes retos que tienen los desarrolladores que hacen sus aplicaciones sobre IoT es que necesitan optar por implementar metodologías de seguridad para proteger la información de los usuarios que adquieren estos dispositivos [32].

Finalmente, en cuarto lugar, se describen métodos o metodologías para evaluar riesgos y contrarrestar medidas adecuadas a la seguridad de los sistemas IoT, un ejemplo de ello, son las políticas de control de acceso a la información mediante un protocolo de identidad, así se brinda mayor confianza a los usuarios al tener un control total y no depender de entidades externas. Es por esto, que debe existir un desarrollo continuo con herramientas que estén a la vanguardia en temas de seguridad, y construir sistemas IoT seguros para el futuro.

En relación con este tema, a nivel internacional, Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini de la Universidad de Insubria en 2018 proponen aplicar una metodología de propósito general para evaluar el riesgo a los sistemas de extremo a extremo, en su trabajo titulado “Una metodología de evaluación de riesgos para el Internet de las cosas”, el enfoque propuesto tiene en cuenta las características y componentes tanto estáticos como dinámicos de un sistema de IoT de una manera objetiva, siguiendo el ciclo de vida completo de los datos. En este trabajo se describen los pasos usados en el

método de evaluación de riesgos adoptado en la solución e integrado en el contexto de IoT. Con este método se puede obtener el riesgo de una amenaza siguiendo cinco pasos, estos pasos van desde examinar los tipos de amenazas, dar un valor a las vulnerabilidades en el sistema y hasta como se debe de actualizar el sistema teniendo en cuenta el grado de vulnerabilidad. Como resultado de la implementación del método para la evaluación de riesgos se han señalado posibles ataques y vulnerabilidades en un sistema real considerando, como ejemplo ilustrativo, un middleware IoT existente, poniendo de manifiesto sus potencialidades y debilidades. Por último, concluyen que, Para evaluar las vulnerabilidades, o el grado de robustez, de un sistema frente a posibles ataques internos y externos, es importante llevar a cabo las contramedidas adecuadas, agregar y/o modificar módulos de seguridad específicos [33].

También, Sibin Mohan, Mikael Asplund, Gedare Bloom, Ahmad-Reza Sadeghi, Ahmad Ibrahim, Negin Salajageh, Paul Griffioen y Bruno Sinopoli en la Conferencia Internacional sobre software embebido de Turín, Italia 2018 exploran temas en seguridad con el fin de construir sistemas de IoT seguros para el futuro, fundamentando nuevas teorías sobre el uso de blockchain, entendiendo las amenazas que enfrentan y la importancia de mantener la integridad de los sistemas IoT, así, como la confiabilidad de los datos. Finalmente se concluye que para comprender algunos de los requisitos y tendencias en seguridad de IoT deberían ayudar a los diseñadores y usuarios a desarrollar / utilizar dichos sistemas de una mejor manera [34].

Por otro lado, Anas Abou El Kalam, Aissam Outchakoucht y Hamza Es-Samaali en la Primera Conferencia Internacional sobre herramientas y usos digitales en París, Francia 2018, proponen un proceso 'basado en emergencias' que apunta a beneficiarse de la tremenda cantidad de objetos inteligentes y extrae las características significativas que no podemos recoger en sistemas pequeños. También, proponen un marco de control de acceso dedicado a los entornos de IoT basado en tres conceptos extremadamente poderosos: redes Blockchain, para satisfacer necesidades de la triada de la CID (Confidencialidad, Integridad y Disponibilidad) en IoT. Por último, se les brinda confianza a los propietarios de dispositivos IoT al tener un control total y con la propuesta de redes blockchain para garantizar el control de acceso sin confiar en entidades externas, herramientas de aprendizaje y sistemas de reputación explícita basada en comentarios [35].

Es por ello, que Norma Pérez, Miguel Bustos, Mario Berón y Pedro Rangelde la Universidad Nacional de San Luis en Portugal, en el 2018 realizan un análisis sistemático de la seguridad en Internet de las cosas describiendo la línea de investigación que aborda el estudio y análisis de seguridad en IoT. Dicho estudio comprende los principales lineamientos en los ejes fundamentales de la seguridad en IoT, estudiando cada capa y las problemáticas de seguridad que pueden ocurrir en dichas capas, y los diferentes modelos de seguridad que permiten contrarrestar las vulnerabilidades producidas en la diversidad de dispositivos en el mercado de IoT. Estos finalmente, detectan diversas vulnerabilidades que pueden ser contrarrestadas utilizando métodos técnicos y herramientas centradas en la seguridad de los dispositivos, también en el análisis de la arquitectura de IoT permitió determinar las amenazas (pérdida de datos, manipulación de datos, pérdida de privacidad, etc.) producidas en cada capa. A fin de reducir estas inseguridades deben ser consideradas en los dispositivos IoT, determinando la existencia de diferentes modelos para detectar amenazas que

permiten contrarrestar la seguridad de software [11].

Además, Kevin Padilla de la Universidad Carlos III de Madrid, España, en el 2015 realiza un estudio de un protocolo de identificación para el Internet de las cosas, proporcionando a los entornos de IoT, mecanismos que permiten establecer una política de control de acceso a la información y dispositivos, mediante el desarrollo de una plataforma de simulación de software, con el objetivo de ser capaz de probar el funcionamiento de la identidad digital en entornos simulados. Para finalizar, el autor en este proyecto presenta una solución para resolver algunos de los mayores problemas de seguridad que tiene actualmente Internet de las cosas, utilizando el protocolo de identidad OpenID, ya que los entornos IoT cuentan con un mecanismo de control de acceso a las cosas, lo que asegura la seguridad mediante la identificación, la autenticación y autorización. La utilización de la tecnología de la identidad es una opción viable para ser aplicada en entornos de IoT, que brinda a los proveedores de servicios, un mecanismo de control de acceso simple, ligero, eficiente y abierto [36].

Por consiguiente, José Antonio Sánchez Alcón, Lourdes López Santidrián y José Fernán Martínez del Centro de Investigación en Tecnologías de Software y Sistemas Multimedia para la Sostenibilidad de la Universidad Politécnica de Madrid, España, en 2014 proponen una solución para garantizar la privacidad en internet de las cosas, mediante técnicas que resulten de la colaboración entre las áreas empresarial, legislativa y tecnológica para dar confianza a los actores involucrados. Este trabajo se centra en la seguridad y privacidad ante las vulnerabilidades técnicas propias de las redes inalámbricas de sensores. La propuesta reúne el conocimiento sobre seguridad y privacidad generado para internet de las cosas por las áreas jurídica, tecnológica y empresarial, en un sistema informático capaz de canalizar la colaboración entre dichas áreas. La finalidad es seleccionar de forma automática las políticas de seguridad y privacidad que deben aplicarse a los nuevos productos y servicios. La colaboración entre esas tres áreas, posibilitaría la emisión de certificaciones de confianza para las partes interesadas y eliminar las posibles barreras de desconfianza [37].

Inclusive, S sicari, A rizzardi, A Coen-Porisini del departamento de ciencia teórica y aplicada de la Universidad de Insubria y L.A Grieco del Departamento de Ingeniería eléctrica y de información del Politécnico de Bari en 2014 en su artículo llamado "Seguridad, privacidad y confianza en Internet de las cosas el camino por recorrer" Presentan los principales desafíos de investigación y las soluciones existentes en el campo de la seguridad IoT. En este trabajo analizan las soluciones disponibles más relevantes relacionadas con la seguridad, privacidad y confianza en el campo de IoT. donde indican que las soluciones adecuadas deben diseñarse e implementarse independientes de la plataforma explotada para garantizar: confidencialidad, control de acceso y privacidad para los usuarios y las cosas, confiabilidad entre dispositivos y usuarios, cumplimiento de las políticas de seguridad y privacidad definidas, así mismo, rebelan que se requieren esfuerzos de investigación para enfrentar la integración de IoT y las tecnologías de comunicación en un middleware seguro, capaz de hacer frente a las restricciones de protección definidas [38].

Algo semejante ocurre a nivel nacional, donde Didier Ahimelec Castro Castro y Jorge Andrés González Carmona de la Universidad Nacional Abierta Y A Distancia en el 2018 presentan en su trabajo de grado la construcción de procedimientos

para minimizar las vulnerabilidades a las que se ven expuestas las organizaciones frente al IoT, con el objetivo de Identificar los elementos que componen la seguridad informática en las IoT, teniendo en cuenta lograr soluciones prácticas de trabajo frente a las vulnerabilidades a las cuales se ven expuestos los usuarios de los servicios en la internet y los artefactos que sirven como herramientas de manifestación. En este trabajo identifican los elementos que componen las IoT y establecen sus vulnerabilidades, seguidamente determinan cuáles son los riesgos a los cuales están expuestas las organizaciones frente al auge del IoT y los mecanismos que pueden ser adoptados para minimizar las vulnerabilidades. Como resultado de este trabajo crean el manual de procedimientos para usar de una forma más segura la IoT, en donde se dan las recomendaciones necesarias a los fabricantes, a los desarrolladores, a los implementadores y por último a los usuarios para obtener mayor seguridad de nuestros datos e información privada que almacenan estos dispositivos o la que fluyen a través de ellos [39].

De igual manera, Alejandro Ramírez García de la Escuela Colombiana de Ingeniería Julio Garavito en el 2018, presenta una solución para tener mayor resguardo ante ataques en los dispositivos de la IoT, en su trabajo llamado Sistemas multi agentes para la defensa de redes IoT. En él muestra como la seguridad en la IoT tiene grandes desafíos debido a las restricciones que tienen los dispositivos en cuanto a poder de procesamiento, memoria y la baja velocidad de transmisión de datos, esto lleva a usar algoritmos que no están a la vanguardia ante la seguridad, como son los algoritmos de criptografía de curvas elípticas (CCE) o el de cifrado simétrico por bloques. Estos algoritmos presentan un nivel moderado ante la seguridad en los IoT pero debido a que son ultraligeros son eficientes y superan las restricciones en estos dispositivos. Por último, concluye que para tener una herramienta ideal de seguridad se debe tener desarrollo continuo con herramientas de vanguardia ya que cada día existen personas interesadas en encontrar nuevas brechas de seguridad que se deben solventar para tener un internet más seguro para todos [40].

También, Nicolas Moreno Guataquira, Stefany Morón Castro y Andrés Felipe Vega Torres de la Escuela Colombiana de Ingeniería Julio Garavito en el 2017, en su trabajo titulado "seguridad para IoT, una solución para la gestión de eventos de seguridad en arquitecturas de internet de las cosas", detallan el proceso para la elaboración de un dispositivo que permite tener unos servicios de seguridad para mitigar posibles ataques a los diferentes dispositivos IoT presentes en las arquitecturas de Smart Home. La solución de gestión de eventos se implementó de la siguiente manera, diseño e implementación de un dispositivo Centinela IoT para la generación y envío de eventos de seguridad hacia una plataforma de gestión de eventos en la nube, después se crean directivas y reglas de correlación específicas para los dispositivos IoT, y por último, se dan respuestas a los ataques, estas están catalogadas como respuestas activas en donde se identifica el ataque específico y se plantea una respuesta sobre el dispositivo, generando una acción directa sobre él o la red, para mitigar el ataque sobre los diferentes dispositivos [41].

De igual manera, Jorge Alaberto Virguez Lozado de la Universidad Piloto de Colombia, en el 2016 identifica la vulnerabilidad que presentan los dispositivos IoT en temas de seguridad al conectarse a la red mediante estudio de estadísticas y un modelado de riesgo centrado en características de privacidad y seguridad, que consta de cuatros pasos que son: modelar la

aplicación, enumerar las amenazas, mitigar las amenazas y validar las mitigaciones. Su conclusión radica en que los estándares de seguridad para IoT están emergiendo aceleradamente dado los recientes reportes de brechas de seguridad en dispositivos de IoT, lo cual hace que las compañías corran contra el reloj para proteger sus activos de información de las intrusiones externas e internas, pero también estos estándares, metodologías, recomendaciones y marcos de endurecimiento para nuevas compañías que están en el proceso de implementación, son de gran ayuda para ayudar a mitigar los riesgos de seguridad en IoT [7].

Por último, Luis Carlos Luis García de la Universidad Nacional de Colombia, en el año 2014 estudió el impacto técnico y económico de la transición de internet al internet de las cosas (IoT) para el caso Colombiano, describiendo los diferentes aspectos técnicos necesarios para la implantación del Internet de las cosas en el país, el estado actual de la infraestructura de las empresas líderes en el sector de las telecomunicaciones y el impacto económico que esa transición conlleva a nivel del hogar y la industria. Para finalizar, el autor indica que el despliegue generalizado de Internet de las cosas tanto a nivel nacional como internacional debe ir de la mano de políticas claras sobre el manejo de la información y la seguridad de la misma, para generar un ambiente de confianza en los usuarios, y tener mayor facilidad de adopción y utilización en los países, debido a que esta es la principal preocupación mostrada por las personas para el uso de este tipo de tecnologías [42].

Resultados y discusión

Como consecuencia de lo anteriormente descrito, se presenta la síntesis de los resultados obtenidos y los aspectos más relevantes encontrados en los documentos.

Cabe resaltar que se tiene una proyección de incremento masivo en la cantidad de dispositivos conectados en los próximos años; las tasas de crecimiento previstas son muy superiores a las de la mayoría de las demás industrias que figuran en las proyecciones, con tasas de crecimiento anuales que oscilan entre 14 y 29 por ciento. Por cada habitante, habrá al menos 2, quizá hasta 6, "cosas" conectadas en el año 2020. "Las cosas" claramente constituirán la mayor parte de los dispositivos conectados para ese año. Hoy, la cantidad de dispositivos conectados que no son "cosas" (es decir, smartphones, computadoras, tabletas, etc.) es casi equivalente a la cantidad de cosas conectadas, por ejemplo, Allied Business Intelligence (ABI) afirmó que había 7 mil millones de smartphones, PCs y similares al año 2016. "Las cosas" superarían en crecimiento a los smartphones, computadoras y demás por un amplísimo margen, según las previsiones [15].

Resulta razonable que IoT tenga la oportunidad de aumentar la conectividad alrededor del mundo, las nuevas tecnologías conectadas a la red como autos, universidades, parques y ciudades inteligentes, etc., aumentará la cantidad de dispositivos conectados a internet, de la misma forma, esto conllevará a la creación de nuevas tecnologías de conexión como 5G y próximamente 6G, permitiendo la asignación de nuevas direcciones IP para contrarrestar la demanda de dispositivos conectados y tráfico en la red [43].

Debido a esa proyección de IoT, en la actualidad se están dando alianzas entre empresas que están inmersas en esta tecnología para crear protocolos de comunicación más seguros; estas empresas se están dedicando al estudio de la privacidad de la información y detectando las vulnerabilidades que se encuentran tanto en el software y hardware, así como en la red y

la nube. Además, se están creando normas y leyes que permiten tener mecanismos para mantener segura la información que almacenamos en la nube o que circula por la red, y aunque es importante que existan este tipo de normativas, se quedan cortas frente a la realidad por la que atraviesa el mundo moderno, la llamada "era digital" que gira en torno a la información [23].

No cabe duda, que al no existir una estandarización en los protocolos de comunicación para un mundo IoT más seguro, ha surgido la necesidad de crear alianzas entre grandes empresas para satisfacer estas falencias, pero cada una de ellas se verá influenciada a mejorar sus puntos débiles y resolver inconvenientes que se les presente de manera puntual, sin existir normas o leyes de organismos internacionales que garanticen la seguridad y comunicación de la información entre dispositivos IoT, la red y la nube, y evidentemente mejorar la calidad de estos dispositivos [23].

En relación a la problemática expuesta y, según estudios revelados por Hewlett Packard, fueron más de 25 vulnerabilidades de seguridad que presentaron los dispositivos IoT, entre los que se pueden encontrar falencias en la privacidad del contenido, en la autenticación y autorización, ausencia en el cifrado de transporte de la información, software y firmware inseguros, interfaces web inseguras entre otras. Estas vulnerabilidades hacen que los atacantes puedan tener acceso remoto al dispositivo, en algunos casos hacer escalamiento de privilegios y allí tomar control completamente del sistema. Esta vulnerabilidad se da gracias a que la mayoría de los dispositivos que abarcan el internet de las cosas no reciben parches de seguridad ya que al momento de que salen de fábrica están expuestos a estas falencias. Los peligros y riesgos más comunes desde en el 2016 como ataques informáticos a redes, malware, software malicioso y los hackers, del 28% al 47% de las organizaciones han experimentado brechas en seguridad sobre dispositivos IoT, pero dichas brechas aun no superan la cantidad de ataques sobre las redes comunes de comunicaciones [7], [32].

En consecuencia, las restricciones de almacenamientos que tienen los dispositivos IoT obligan a transmitir la información por la red y llevarlos a la nube, por esta razón aumentan las amenazas en el tráfico de información, y debido a que los protocolos de internet no son seguros en el momento de enviar o transmitir los datos de los dispositivos a la nube, puede facilitar el acceso a los hackers al violar la seguridad en un punto de la comunicación. Al mismo tiempo, se hace necesario concientizar a los usuarios a proteger sus datos, por ejemplo, cambiando las contraseñas que traen por defecto los dispositivos IoT, ya que las cifras demuestran que los ataques a estos dispositivos en temas de seguridad van en aumento y al no hacerlo, se deja una ventana por donde pueden acceder a nuestro sistema y así robar la información [7], [44].

También, a partir del estudio y análisis de los dispositivos digitales basados en la tecnología IoT se detectaron diversas vulnerabilidades que pueden ser contrarrestadas utilizando métodos, técnicas y herramientas centradas en la seguridad de los dispositivos. El estudio de la arquitectura de IoT permitió determinar las amenazas como perdida de datos, manipulación de datos, perdida de privacidad, etc.; y con el fin de reducir estas inseguridades deben ser considerados en los dispositivos IoT diferentes modelos para detectar amenazas que permiten contrarrestar la seguridad de software; por tal motivo se ha demostrado la importancia de que los entornos de IoT incorporen mecanismos de seguridad y, en concreto, mecanismos de identificación para el control de acceso a servicios. Actualmente

Internet de las Cosas carece de este tipo de mecanismos, siendo manifiestamente insuficiente el nivel de seguridad [36], [45].

Por ende, ante el incremento de los riesgos presentes en IoT, se deben crear soluciones que permitan tener una mayor seguridad, para que más empresas y usuarios implementen esta tecnología sin el temor a que su información sea manipulada o que personas externas son fines maliciosos se puedan adueñar de ella. En la actualidad, todos estos riesgos y el avance creciente de la tecnología han incentivado y permitido el aumento de investigaciones científicas para crear metodologías que satisfagan estas necesidades y hagan segura la transmisión de la información en estos dispositivos IoT.

Conclusiones

Para el mundo moderno y la actual era digital en auge, es preocupante el inminente crecimiento de la tecnología y más aún, la cantidad de dispositivos IoT conectados a internet; si bien es cierto que IoT está cambiando de manera radical la manera de comunicarnos a nivel mundial y mejorando la calidad de vida del ser humano, debido a la mayor interacción permitida entre las cosas y el entorno, es necesario entender que algunas de las infraestructuras existentes no están a la vanguardia de la evolución tecnológica que se está generando alrededor del mundo, aumentando la desigualdad tecnológica existente entre los países desarrollados y subdesarrollados.

En definitiva, lo más importante a tener en cuenta según el área de utilidad de los dispositivos, es estandarizar los protocolos de comunicación para IoT, principalmente en temas de seguridad; por esto es necesario que organizaciones a nivel mundial sean pioneras en generar normas y leyes concernientes al mundo de IoT tanto en los dispositivos como en el transporte de sus datos, incluyendo políticas de seguridad desde su diseño, fabricación y configuración e implementación por parte de todas las personas que interactúan en IoT.

Evidentemente, una de las amenazas más significativas de IoT cualquiera que sea su campo de aplicación, es la información y privacidad de los datos; algo semejante ocurre con otras vulnerabilidades presentes que no solo son de pérdida de la información, cómo lo son, aquellas donde corre peligro directamente la vida humana, ya que algunos de estos dispositivos IoT son implantados en nuestros cuerpos para controlar y monitorear algunos de los órganos internos, por ello, debido a estos riesgos y la inminente manipulación de dicha información en IoT, la seguridad no debe recaer sólo en los fabricantes al diseñar dispositivos fáciles de usar, sino también, que contengan sistemas que resguarden los datos que almacenen o transmitan estos dispositivos; de la misma forma, los usuarios deben tomar conciencia de la importancia de darles un buen uso para mantener segura su información.

En todo caso, actualmente los usuarios deben confiar en los sistemas de seguridad de IoT y el trato de la información que circula por ellos, pero eso no los hace exentos del inminente peligro descrito anteriormente, por consiguiente, la necesidad de crear métodos o metodologías que no solo se enfoquen en los dispositivos IoT, sino que también tengan en cuenta la interacción por parte de los usuarios, y además, normas y leyes internacionales que permitan conservar la seguridad y privacidad en estos, con la finalidad de contrarrestar las vulnerabilidades más presentes en IoT, como por ejemplo, la autenticación y autorización, y el cifrado en el transporte de la información; y así prevenir ataques masivos a internet y a estos dispositivos. Sin embargo, para que estas nuevas metodologías tengan mayor impacto, deben permitir actualizaciones en

masa como lo hacen hoy día los computadores y celulares, ya que la protección será simultánea a todos los dispositivos IoT, cerrando brechas y toda puerta por donde se puedan filtrar los datos, previniendo así, el robo de información.

Finalmente, la falta de innovación tecnológica no ha permitido el posicionamiento de Colombia en América Latina y mucho menos a nivel mundial, por eso es importante considerar la cooperación de las empresas públicas y privadas que permitan tener una base para la implementación de tecnología IoT, e incentiven a los fabricantes a invertir en una infraestructura de comunicaciones sólida y segura, que se ajuste a la demanda, y esté a la vanguardia y auge de la actual era digital. De la misma forma ocurre con nuestra región, el poco interés por parte del gobierno ha causado pocos avances tecnológicos en materia de IoT, es por ello, que se debe incentivar a las universidades y empresas locales en la investigación de esta tecnología para mejorar la productividad y volver a la región más competitiva, así como al país.

Referencia

[1] D. Little y Telbroad. Resumen recomendaciones normativas y regulatorias para promocionar los contenidos y aplicaciones y el Internet de las cosas, 2016

[2] Centro de Seguridad TIC de la Comunidad Valenciana. "Seguridad en Internet de las Cosas. Estado del arte", 2014

[3] Centro de Estudios de Movilidad de la Asociación española. "Estado del arte e implicaciones de seguridad y privacidad en el Internet de las Cosas", 2017

[4] Centro Cibernético Policial, "Informe Amenazas del Cibercrimen en Colombia 2016 – 2017", 2017

[5] I. Pérez, "Nevera inteligente involucrada en ciberataque con spam", 2018

[6] Gemalto, "Un Internet de las Cosas más seguro", 2016.

[7] J. A. Virguez Lozano, "IoT: La Evolución de la Seguridad en el Internet de las Cosas", 2016

[8] Gadgerss. Ataques a dispositivos IoT se triplicaron en primer trimestre del 2018. [Online]. Available: https://gadgerss.com/2018/09/21/ataques-a-dispositivos-iot-se-triplicaron-en-primer-trimestre-del-2018/

[9] M.Á. Arroyo Moreno, J. Bardallo Gay, J.J. Domenech Sánchez, F.J. Gómez López, y R. Salado Lucena, "Seguridad IoT en Sanidad ¿estamos preparados?", 2018

[10] Ó. Perera Bartual, "Análisis y parametrización de la seguridad en sistemas IoT", 2018

[11] N.B. Pérez, M.A. Bustos, M. Berón y P. Rangel Henriques, "Análisis sistemático de la seguridad en internet of things", 2018

[12] M.T. Romero García, "La protección de datos ante el Internet de las cosas", 2017

[13] J.G. Chacón Rangel, A.S. Flórez Fuentes y J.E. Rodríguez Fernández, "La inteligencia artificial y sus contribuciones a la física médica y la bioingeniería", *Mundo FESC*, vol. 5 no. 9, pp. 60-63, 2015

[14] M. Ruiz Soto, A. Serrano Santoyo, E. Alvarez y E. Garcia, E. "Análisis del Internet de la Cosas en la Era de 5G y de Blockchain: Retos en Mexico", 2017

[15] 5G Américas, "Internet de las Cosas en America Latina", 2016

[16] K. Rose, S. Eldridg y L. Chapin, "La Internet de las Cosas - Una Breve Reseña", 2015

[17] C. Cortés, "El "Internet de las Cosas": Más internet que otra cosa", 2014

[18] R. A. Niño Vargas, J. Barrera y P. Herrera Hernández, "Definición de los Parámetros Técnicos para promover el Internet de las Cosas en Colombia", 2018

[19] M.G. García Sandoval, H.D. Ariza Torrado, M. Lucia Pinzón y A. S. Flórez Fuentes. "Buenas prácticas aplicadas a la implementacion colaborativo de aplicativos web", *Mundo Fesc*", vol 5, no 10, pp. 27-30, 2016

[20] D.L. Pinzón Niño, "Panorama de aplicación de internet de las cosas (IoT)", 2016

[21] Y. Chahid, M. Benabdellah y A. Azizi, A, "Internet of Things Protocols Comparison, Architecture, Vulnerabilities and Security", 2017

[22] J. Martínez, J. Mejía, "La Seguridad en Internet de las Cosas: Analizando el Tráfico de Información en Aplicaciones para iOS", 2016

[23] Y.G. González Larín, "El Internet de las Cosas y sus riesgos para la privacidad", 2016

[24] Y.T. Medina Vargas y H. A. Miranda Méndez, "Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES". Mundo FESC, vol. 5, no. 9, pp. 14-21, 2015

[25] A. Domínguez y M. Vargas Lombardo, "El estado del arte: Salud inteligente y el internet de las cosas", 2018

[26] H. Mustapha y A. M. Alghamdi, "DDoS Attacks on the Internet of Things and Their Prevention Methods", 2018

[27]J. Castellanos Cañadas, "Seguridad & Reversing en dispositivos IoT", 2017

[28]M. Castro Sola, "Internet de las Cosas, Privacidad y Seguridad", 2016

[29]F.G. Cuzme Rodríguez, "El Internet de las cosas y las consideraciones de seguridad", 2015

[30]V.J. Pastor Pérez y J.R. Coz Fernández, "La Ciberdefensa militar ante el reto de Internet de las Cosas", 2015

[31] I. Castaño, T. Neira, D. Zuluaga, M. Realpe, D. Faycal, y S. Rueda, "Ciberseguridad en la era del internet de las cosas", 2018

[32]W. A. Coy Sosa, "IoT - El Internet de las Cosas y sus riesgos en los pilares de la Seguridad de la Información", 2016

[33]S. Sicari, A. Rizzardi, D. Miorandi y A. Coen Porisini, "A risk assessment methodology for the Internet of Things", 2018

[34]S. Mohan, M. Asplund, G. Bloom, A.R. Sadeghi, A. Ibrahim, N. Salajageh, B. Sinopoli, "The future of IoT security: special session", 2018

[35]A.A. El Kalam, A. Outchakoucht y H. Es-Samaali, "Emergence-Based Access Control: New Approach to Secure the Internet of Things", 2018

[36]K. Padilla Cañadas, "Estudio de un protocolo de identificación para el internet de las cosas", 2015

[37] J.A. Sánchez Alcón, L. López Santidrián y J. F. Martínez, "Solución para garantizar la privacidad en internet de las cosas", 2015

[38]S. Sicari, A. Rizzardi, L. A. Grieco y A.Coen-Porisini, "Security, privacy and trust in Internet of Things", 2015

[39]D.A. Castro Castro y J. A. GonzálezCarmona, "Construcción de procedimientos para minimizar las vulnerabilidades a las que se ven expuestas las organizaciones (frente al IoT.)", 2018

[40]A. Ramirez Garcia, A. “Sistemas multi agentes para la defensa de redes IoT”, 2018

[41]N.M., Guataquira, A. F. Vega Torres y S. Morón Castro, “Seguridad para IoT, una solución para la gestión de eventos de Seguridad en arquitecturas de Internet de las Cosas”, 2017

[42]L. Luis García, “Estudio del impacto técnico y económico de la transición de internet al Internet de las Cosas (IoT) para el caso Colombiano”, 2015

[43] D. Rico Bautista, J. A. Parra-Valencia y C. D. Guerrero, “IoT: Una aproximación desde ciudad inteligente a Universidad inteligente”, 2017

[44]S. Rueda, “Seguridad, gran reto para internet de las cosas”, 2014

[45]J. M. Martínez Caro y M. D. Cano Baños, “Un caso práctico de aporte de seguridad en IoT”, 2016