Vinculación entre la vulnerabilidad de las redes y la seguridad de la información: el internet de las cosas, el caso Colombia

Yeral Leonardo Diaz Infante

Luis Carlos Ballesteros

Profesor TC auxiliar magister

Informe de revisión de literatura

Universidad Cooperativa de Colombia
Ingeniería de Telecomunicación
2019

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN DEL TEMA

La comunicación, es sin lugar a duda, un proceso complejo que forma parte integral del ser humano, pues le permite establecer relaciones dentro y fuera del contexto social donde habitualmente interactúa, ampliar su horizonte comunicacional e impulsar el crecimiento propio y colectivo con miras a satisfacer sus requerimientos.

En esta dirección, el desarrollo tecnológico pasa a jugar un papel fundamental dentro de todo el proceso de comunicación que se gesta entre los individuos, ampliando no solo las relaciones personales, sino que además fortalece el intercambio comercial, social y económico de un país. Ahora bien, a lo largo de los años la innovación tecnológica ha ido en ascenso, muestra de ello, es la proyección alcanzada por el internet en todo el globo terráqueo, trascendiendo barreras, creando vías alternas de comunicación y ajustando los canales para acoplar las relaciones a distancia de persona a persona, persona a objeto, objeto a objeto.

Es el caso del internet de las cosas, en adelante IoT, la cual desde una perspectiva muy particular es concebida como un desafío tecnológico del siglo XXI, ya que abre una brecha entre la innovación tecnológica y la integración interactiva entre objetos o cosas sin la intervención directa del ser humano en pro de optimizar su calidad de vida. No obstante, es un tema que comenzó a sonar en los años 90, pero sin mayor repercusión en la sociedad, debido a que se tenía la concepción que internet era una fuente almacenadora de datos accesible para cualquier persona sin importar la ubicación, ya a partir del año 2000 pasa a ser una estructura plurivalente, integrando el principio comunicacional de todo con todos.

Al respecto, Cisco (2011), señala que el IoT ha ido adquiriendo importancia en tiempo y espacio, debido a que representa la transformación real del internet y se traduce en un salto agigantado al progreso innovador de las telecomunicaciones y a la forma en que el individuo se comporta, asimila, trabaja y se distrae, convirtiendo el internet en una infraestructura sensorial al servicio de seres humanos proactivos. Por su parte, la Revista ElectroIndustria (2015), explica que el IoT ha generado un impacto sorprendente y que solo es equiparable con los momentos de mayor ascenso experimentados por la “revolución tecnológica”.

Por lo tanto, se infiere que el IoT representa un evidente progreso en el mundo de las telecomunicaciones, esto, por la amplitud y mejoras que provee a los procedimientos utilizados en los sistemas de comunicación de proporciones mayores y que obligatoriamente se asocia a las comunicaciones inalámbricas, sensores; inclusive a micro tecnología, pasando a formar parte de la cotidianidad del individuo; así como, a la unificación de mecanismos físicos a la electrónica, programas, sensores,

“actuadores” y “conectividad”, que admite establecer conexión entre objetos, obtener información y conmutar datos, según lo expuesto por el reporte presentado por la Unión Internacional de Telecomunicaciones UIT, (2005: 32) y el informe técnico de Cisco (2011).

En efecto, el comportamiento o modo operativo del internet de las cosas viene dado por la conexión de un APP o controlador a un protocolo de red, como ipv6, pero este protocolo depende de un código fuente que contiene las instrucciones de operatividad que activa el dispositivo interconectado a la red, para finalmente emitir una respuesta al usuario que lo solicita.

Es necesario realizar un análisis sobre los elementos internos y externos utilizados que conforman el internet de las cosas, estos elementos se pueden clasificar en 8:

- Comunicación: para permitir el intercambio de información entre dispositivos.
- Sensores: para permitir el intercambio de información entre dispositivos.
- Almacenamiento: para los datos recogidos de los sensores y de los sistemas de seguimiento e identificación.
- Actuadores: para llevar a cabo las acciones dirigidas desde el mundo digital al físico.
- Dispositivos de interacción con humanos en el mundo físico
- Procesamiento, para proporcionar datos a los sistemas de minería de datos y a los servicios.
- Localización y seguimiento, para la determinación de la ubicación física y el seguimiento
- Identificación, para proporcionar la identificación única de un objeto físico en el mundo digital. (Aguliar L, Delgado J, Garcia P. 2015)

De esta manera, la presente investigación centra su atención en analizar la vinculación entre la vulnerabilidad de las redes móviles y la seguridad de la información con el internet de las cosas en Colombia a través de una revisión bibliográfica de artículos científicos e investigaciones empíricas relacionadas con el tema. En el contexto tecnológico actual, la vulnerabilidad y la seguridad conforman una dupla y una es directamente proporcional a la otra, significa que la susceptibilidad que revele el acceso a los datos es el resultado directo del grado de seguridad con el cual es manejada y resguarda la información del dispositivo conectado a la red. Basado en lo anterior es necesario definir que es la seguridad de los datos “es la ciencia que estudia métodos de protección de datos en los sistemas de red, e incluye controles criptográficos, controles de acceso, controles de flujo de información, controles de inferencia y procedimientos para respaldo y seguridad” Pérez N, Bustos M, Mario M, Henríquez P. (2018)

No obstante, existe mecanismos de seguridad que pueden ser empleados para garantizar una conectividad con mayor seguridad y reducir las posibilidades a sufrir una violación de los niveles de privacidad en los datos e información manejados por el usuario, destacando entre ellos elementos como: la autenticación, control de acceso, confiabilidad e integridad de los datos, no repudio y por último la disponibilidad, el cual es garante de que el acceso al uso del dispositivo sea desde

una entidad legal, ahora, la ausencia de alguno de estos componentes es razón suficiente para dar cabida a la violación de la privacidad y confiabilidad de los datos.

Sobre este particular, Ayala, I., Pinilla, M. y Fuentes, L. (2013), sostienen que la seguridad se ha convertido en un verdadero problema y que a pesar de los mecanismos ideados continúa causando estragos en usuarios y desarrolladores, pues al estar integrado por tantos dispositivos y objetos conectadas a la red puede presentar susceptibilidad en los niveles de seguridad y quedar expuesta a cualquier amenaza masiva produciendo serias consecuencias; agregan, además, que no hay un sistema totalmente seguro, debido a que puede ser embestido de múltiples formas, y acceder a los datos de los usuarios en cualquier momento.

En definitiva, la debilidad del internet de las cosas son los datos y no los dispositivos conectados, significa entonces que la protección comienza por el sensor cuya función es captar la dimensión física de los datos, verificar su almacenamiento, proteger los datos circulantes y los que se mantienen inactivos, de modo que no existe un método exclusivamente seguro para el resguardo de los datos transmitido entre los puntos enlazados en una red, poniendo en duda la invulnerabilidad de las redes y la seguridad que se brinda al usuario, Fruehe, J. (2015).

En consecuencia, los niveles de probabilidades para el usuarios de encontrarse frente a situaciones de riesgos (secuestro, robo, estafas, entre otros) es muy alto, visto que resulta complicado ser prudente con la información manipulada a través de un ordenador conectado, aunado a ello se encuentra el hecho de que los estándares de estos dispositivos no son completamente confiables, posibilitando el ataque a la privacidad de los datos, y por ende aumenta el alcance y la inseguridad para los consumidores, Dans, E. (2016).

Es importante, destacar, que en América Latina el internet de las cosas ha ganado espacios importantes, tal como sucede con Colombia quien actualmente se posiciona entre los primeros lugares por la integración tecnológica que ha implementado, fusionando telemetría, telemática para conectar controladores y emitir respuestas en tiempo real. En efecto, mediante el internet de las cosas Colombia brinda soluciones a varios requerimientos con implementaciones que abarca sectores vulnerables al tratamiento de los datos, como el transporte, salud, empresarial y muchos otros, que evidentemente requieren una supervisión especial para prevenir ataques que pongan en peligro la privacidad de los usuarios, siendo claro que el IoT puede cumplir con los estándares de uso, pero, no debe dejar a un lado la seguridad que requiere su manipulación, en pro de garantizar un servicio que mitigue los riesgos y proteja la integridad del consumidor.

1.1.1. Justificación

El surgimiento del internet refleja un cambio significativo en el modelo de comunicación que se venía manejando, modificando radicalmente la manera de vivir, ejercer las actividades laborales y de comunicación de la sociedad, dando apertura al crecimiento personal y colectivo. De modo, que el internet revolucionó las tecnologías, sembrando precedentes importantes en el mundo de la informática y las telecomunicaciones; como punto referencial entre tantos avances experimentados por el mismo, se encuentra el internet de las cosas cuya aparición se remonta a 1990, no obstante, Virgüez (s.f.), afirma que fue en el 2008-2009 cuando realmente adquiere sentido el término y despierta el interés público, por las adecuaciones para facilitar el modo de vida.

Ahora bien, el internet de las cosas se caracteriza por utilizar computadores, sensores y redes para dar seguimiento a los dispositivos conectados, cada uno de los cuales cumple un fin específico como, por ejemplo, en la salud, el hogar, empresas, grandes industrias, entornos de producción a medida, vehículos, ciudades, entre otros, su universo de aplicación es extenso y dada la amplitud e importancia de los entornos donde es puesta en práctica puede aumentar el nivel de vulnerabilidad de la privacidad y por ende la seguridad de los datos.

Desde esta perspectiva, el estudio sienta sus bases en el análisis de la vulnerabilidad y seguridad de los datos del internet de las cosas. Con esto se prevé mediante la revisión bibliográfica describir los fenómenos que repercuten en la protección adecuada de la información de cada usuario y contraponerse con la realidad actual de Colombia en esta materia. Considerando, la relevancia del tema y trascendencia del mismo se justifica desde lo teórico, evidenciando una realidad que sirve de base para desarrollar teorías útiles a futuros estudios; metodológicamente se fundamenta en el uso de métodos, técnicas de análisis y procedimientos de recolección de información propios de la investigación documental; desde el ámbito académico se inserta dentro de la línea de investigación, seguridad, privacidad y protección en el IoT.

1.1.3. Objetivo de la revisión

Contrastar a través de una revisión bibliográfica la vinculación entre la vulnerabilidad de las redes móviles y la seguridad de la información con el internet de las cosas en Colombia.

2. METODOLÓGIA

Metodológicamente el estudio se caracteriza por tener un enfoque cualitativo, ya que su fundamento primordial es la revisión sistemática de fuentes bibliográficas relacionadas con el tema que se investiga. al respecto, Blasco, J. y Pérez, J. (2007), explican que la investigación cualitativa explora los hechos que se dan en un contexto social, se basa en la observación real de los fenómenos que el momento que ocurre el evento e interpretando las causas y efectos de este. Por otro lado, Taylor, S. y Bogdan, R. (1987), señalan que la investigación cualitativa, es un método de trabajo que le permite al investigador llevar adelante estudios experimentales, es decir, indagar la realidad, entenderla, interpretarla y describirla con base a las experiencias de sus propios protagonistas y se caracteriza por ser inductiva y holística.

De acuerdo con los objetivos propuestos a partir del ejercicio de revisión bibliográfica, se establece un alcance descriptivo-explicativo, en la medida en la que se busca contrastar la vinculación entre la vulnerabilidad de las redes móviles y la seguridad de la información con el internet de las cosas en Colombia. En palabras de Arias, F. (2006), el investigador está frente a un estudio descriptivo cuando identifica un fenómeno, un hecho o conjunto de elementos que es susceptible para caracterizarlo para poder organizarlo y observar el comportamiento de este. En particular, se piensa en la vulnerabilidad de las redes móviles y la seguridad de la información con el internet de las cosas en Colombia y con base a los resultados alcanzados emitir un criterio propio.

Más allá del ejercicio descriptivo, Arias, F. ob. Cit., menciona además que el alcance explicativo permite ocuparse tanto de la determinación de las causas (investigación post facto), como de los efectos (investigación experimental), mediante la prueba de hipótesis. Sus resultados y conclusiones constituyen el nivel más profundo de conocimientos y en este caso, dar cuenta de los mecanismos que pueden ayudar a superar las falencias respecto a la seguridad de la información y las redes móviles.

Ahora, sobre la base de las técnicas empleadas y dada que la investigación se encamina al análisis de la vinculación entre la vulnerabilidad de las redes móviles y la seguridad de la información con el internet de las cosas en Colombia por medio de la revisión bibliográfica, como ya se hizo referencia anteriormente, se asume que el estudio se desarrolla bajo un diseño documental. Para Arias, F. (2006), los diseños documentales se fundamentan en la exploración, análisis, evaluación e interpretación de datos provenientes de fuentes secundarias, es decir, estudios ya investigados y cuyo contenido se encuentra en documentos impresos, electrónicos o audiovisuales. Tomando en cuenta estos elementos metodológicos, se establece una búsqueda de documentos relacionados con el tópico central, asegurando que se trata de fuentes confiables y de revistas conocidas.

3. RESULTADOS

En el presente apartado se efectúa la revisión sistemática de artículos científicos, libros, revistas arbitradas o cualquier otro documento que refleje estudios sobre el tema que se desarrolla y sirva de soporte para dilucidar el escenario actual del internet de las cosas y la vinculación que se desprende entre la vulnerabilidad de las redes móviles y la seguridad de la información en Colombia.

Con el internet de las cosas el mundo se está desarrollando a una velocidad inaudita, “un ecosistema digital en el que los impulsos y la información circulen de forma Big Dates, esto se denomina así gracias a las bases gigantes datos a las que tenemos ahora” Arantza M. (2016)

Sobre este particular, Domínguez, A. y Vargas, M. (2018), refiere que en el mundo de hoy resulta imposible hablar de privacidad a nivel de redes móviles, pues no existen mecanismos completamente blindados a la violación de la seguridad, lo cual causa alarma y llama al diseño e incorporación de normas de seguridad apropiadas y esto, solo será posible si se parte de la aplicación de métodos, técnicas y estrategias de desarrollo idóneas. Para Castro, M. (2016), la vulnerabilidad del internet de las cosas se relaciona con el nivel de seguridad que tengan el dispositivo IoT, pues el responsable del mantenimiento del software del mismo es de quien crea el hardware, lo que conlleva a concluir que la falta de protección puede producirse por poca experiencia en el área o por la falta de un presupuesto que le permita al fabricante poner al servicio del usuario un sistema de seguridad con condiciones óptimas para bloquear las constantes amenazas a la que siempre estará expuesto.

Argumenta, además el autor, que las personas tienen que estar conscientes y asumir que este tipo de sistema no fueron creados para estar “conectados a la red”, situación que tiende a incrementar los índices de vulnerabilidad y por ende el riesgo. De otra parte, se encuentra el contexto donde se ubican los dispositivos IoT, ya que generalmente se coloca en lugares de libre acceso, por ejemplo, en los “sensores de los semáforos”, dificultando su protección y aumentando la amenaza. Claro, existen otros puntos de seguridad que pueden ser vulnerables, como son la seguridad en la transmisión de los datos, seguridad del software, seguridad del hardware, seguridad en la configuración y funcionalidad e incluso la misma seguridad de los usuarios.

En contraste, Rueda, J. y Talavera, J. (2017), explican que la seguridad en las aplicaciones IoT se han incrementados, en respuesta a la vulnerabilidad que se han evidenciado en este tipo de tecnologías y que se ha manifestado, bien sea a través de la red, mediante el control para acceder o en el colapso que pudiesen experimentar en un momento determinado la red producto de la cantidad de personas conectadas de manera simultánea. Bien, ¿Es posible determinar los problemas de seguridad del internet de las cosas? Hernández, D., Mazon, B., y Escudero, C. (2018), aseguran que si es posible y puede lograrse tomando como referencia las “redes inalámbricas y la seguridad en las redes EPC”. En este sentido, el enfoque se centra en tres puntos clave: la confiablidad, la integridad de los datos y por último la autenticidad y la disponibilidad de los datos.

Según el autor, el proceso de comunicación móvil entre los equipos conectados en el internet de las cosas presenta una singular vulnerabilidad a los ataques maliciosos, ya que los mensajes son trasferidos o se trasfieren por el aire permitiendo que puedan ser interceptados y modificados. En cuanto a la integridad y autenticación, es imperante, que cada dispositivo que integra la red sea autenticado por niveles y de este modo certificar que los datos que se transmiten son íntegros. Es decir, que el canal de comunicación emisor-receptor envía y recibe respectivamente el mensaje sin alteraciones de ningún tipo. Por último, no debe dejarse a un lado la disponibilidad, pues es un punto susceptible del cual tiende hacer uso quienes boicotean la señal de comunicación en la comunicación inalámbrica para inutilizar la funcionalidad del proceso comunicativo y ajustarlo a su propia conveniencia.

La Corporación GSMA (2017) hace referencia a estudios previos (los cuales no detalla), ponen en clara evidencia las constante amenazas a las cuales se han visto expuestas las redes inalámbricas o redes móviles desde su surgimiento. Este es un problema que ha venido abriendo espacios en todo el mundo de forma permanente, por ejemplo, en los países europeos, América del Norte y África presentan cifras de vulnerabilidad en el manejo de datos a través de IoT muy similares (GSMA, 2017), lo cual demuestra, sin lugar a dudas, que las redes móviles tienen una tendencia elevada de susceptibilidad y por ende en riesgo de sufrir cualquier tipo de ataque, sin importar la tecnología y cobertura los niveles de seguridad siguen por debajo de los estándares normales que establecen las directrices internacionales.

Cuzme, M. (2015), plantea que no se trata de establecer qué nivel de seguridad tiene o no un dispositivo conectado al internet de las cosas, por el contrario, el problema es determinar mecanismos de seguridad realmente óptimos (programas de criptografía, regulación de permisos, accesos, creación de claves) que puedan aplicarse al hardware o software para asegurar el tránsito de los datos por la red y protegerlo de alteración o interpretación. Es importante acotar, que Cuzme, M. al igual que Hernández, D., Mazon, B., y Escudero, C. (2018), considera que la seguridad empieza por el hardware y el software, adicionando la seguridad de la red y la seguridad que proporciona la nube.

Hirshberg, P. (2010), menciona que el internet de las cosas es quizás la estructura con mayor complejidad creada por el hombre. A pesar, de ser considerada el “boom” tecnológico del siglo XXI, no está excepto de encontrar fuertes obstáculos que influyen en seguridad y privacidad de los datos y por ende en la información que se transmite de polo a polo. Bien, el objetivo que se plantean hoy los desarrolladores es buscar nuevas alternativas y estándares para garantizar un manejo eficaz del internet de las cosas. Para el autor, las principales amenazas de la IoT es la infraestructura que actualmente se emplea, la ausencia de “interoperabilidad entre los sistemas”, una mejor inversión en dispositivos IoT y las limitantes impuestas por los mismos usuarios.

A criterio de Liñan, A., Vives, A., Bagula, A., Zennara, M. y Pietrosemoli, E. (2015), el internet de las cosas no solo llego para posesionarse del mercado tecnológico, sino

para cambiar la concepción que el usuario podía tener sobre la seguridad y privacidad de los datos e información. De manera que, todo dispositivo conectado a la red IoT que almacena datos, comunica, guarda o "procesa datos sensibles", representa un riesgo abierto o latente. Afirman los autores, que según los hallazgos de un estudio llevado a cabo por la HP el 70% de los dispositivos que se conectan al internet de las cosas "contienen vulnerabilidad a la seguridad".

Los hallazgos del estudio llevado a cabo por la HP pusieron en evidencia que los problemas que generan los dispositivos conectados al internet de las cosas se asocian a: "interfaz web" inestable, certificación exigua, "servicios de red inseguros", inexactitud de encriptado en la trasferencia de datos, dudas sobre los niveles de privacidad, interfaz en la nube sin los niveles de seguridad idóneos, interfaz móvil con los niveles de seguridad por debajo de los estándares permitidos, falta de seguridad en la configuración de los dispositivo IoT, software "inseguro", seguridad física defectuosa.

Para López, M. (2019), la seguridad y la privacidad del internet de las cosas en un tema polémico y que genera preocupación. A saber, este tipo de aplicaciones recopila cantidades elevadas de datos que guardan relación con el comportamiento de los individuos, situación que ha venido a desencadenar incertidumbre en usuarios, sobre el manejo de los datos y las medidas de seguridad que pudiesen tomar para prevenir la sustracción de información y violación de su privacidad. En este sentido, el internet de las cosas según el autor está llamado a incrementar los niveles de seguridad y esto es posible lograrlo través del uso de redes móviles sobre plataformas tecnológicas inalámbricas de "corto alcance".

Fayçal, D. y Mayor, M. (2018), puntualizan que el internet de las cosas ganó espacios de una manera vertiginosa a nivel global, consolidándose como uno de los mayores avances tecnológicos del siglo XXI. Ciertamente, trajo consigo una infinidad de beneficios al usuario, pues al lograr conectar los dispositivos a la red se logra mejorar en gran escala la calidad de vida de los individuos, pero, decreció los niveles de seguridad de los datos que eran manejados por ellos y aumenta la vulnerabilidad y se pone en peligro la privacidad de la información. Acotan, que en el internet de las cosas a nivel de redes móviles hay diseños en los cuales se dejaron a un lado la seguridad, puesto que al crear el dispositivo no fue tomada en cuenta y el punto concreto es como gestionarlos si el problema emerge simultáneamente con el dispositivo y el esquema bajo el cual se establece el internet de las cosas no cuenta con estándares ni protocolos para utilizar, aun cuando diariamente el número de usuarios conectados a la red se incrementa. Otro reto que enfrenta la IoT es el manejo de la infraestructura, pues la capacidad de recepción tiende a colapsar por la cantidad de dispositivos acoplados a la red, produciendo mayores riesgos y vulnerabilidad.

Ramírez, D. y Rodríguez, E. (2016), consideran que la seguridad del internet de las cosas tiene que estar pensada en la "seguridad cibernética" y evidentemente la seguridad física para mostrar los activos "físicos y digitales", elevar la protección y las

ventajas estratégicas de funcionalidad. Así mismo, se debe tener especial cuidado en los puntos tentativos para ser atacados por hackers, pues generalmente se enfocan en el dispositivo conectado al IoT, “infraestructura de la nube” y la red.

En el caso de Colombia, Sanmartín, P., Ávila, K., Viloria, C. y Jabba, D. (2016), señalan que dado el incremento que ha experimentado el uso de redes móviles asociada al internet de las cosas se han iniciado planes para modernizar y asegurar el uso de las redes móviles, a través de regularizaciones que impulse, en primer lugar un aprovechamiento seguro de las redes inalámbricas y segundo fomentar la inversión en redes inalámbricas con tecnología de vanguardia y de este modo, tratar de subsanar la vulnerabilidad de las mismas a mediano plazo.

4. DISCUSIÓN

El internet de las cosas hace alusión al uso de la tecnología que es empleada para interconectar aparatos. Es así que, la esencia del IoT es el control que ejerce el usuario sobre el artefacto a control remoto o en su defecto recibir notificaciones ante la presencia de alguna falla. Su aplicación es infinita y abarca múltiples escenarios que va desde el hogar hasta el control de ciudades enteras, las cuales pueden ser vigiladas por sensores en tiempo real.

Otra de las grandes ventajas del internet de las cosas viene dada por el impulso al crecimiento económico y social, puesto que, permite la ampliación de los servicios basados en el uso y aprovechamiento de la tecnología por parte de la sociedad. Desde esta perspectiva, el IoT se fundamenta en la utilización de la “tecnología inteligente”, con la finalidad de establecer una interconexión de cosas sin limitar ni el tiempo ni el espacio. Tal como se ha venido refiriendo en otros apartados, el internet de las cosas se ha transformado en un proceso emergente para dar apertura a nuevas investigaciones y hacer nuevos aportes a estudios ya existentes, debido a que es una aplicación heterogénea que se adecúa a las demandas del usuario y a las nuevas tecnologías.

Ahora bien, todo el escenario descrito ha conllevado a que aumente el número de usuarios en la red, y es evidente que, a mayor cantidad de personas conectadas, mayor será la amenaza de colapso y son esos puntos bajos los que son empleados por agentes maliciosos para atacar la red e interceptar la comunicación y ajustarla a sus intereses. En el caso del internet de las cosas el objetivo se enfoca en aprovechar la vulnerabilidad de los dispositivos conectados a la red IoT, a la inseguridad que puede generar la nube, el hardware, el software e incluso la propia red.

De acuerdo con Domínguez, A. y Vargas, M. (2018), las redes móviles no garantizan la privacidad, pues no hay instrumentos legales, ni técnicos que garanticen la seguridad absoluta de los datos, por lo tanto, cualquier usuario es susceptible para ser víctima de personas inescrupulosas. En este orden de ideas, Colombia ha buscado establecer barreras para modernizar las redes móviles y mejorar los niveles

de seguridad, pues se prevé que para el 2022 el alcance de dispositivos conectados será del 70%, esto según, cifras del portal web:https://caracol.com.co/radio/2017/09/25/tecnologia/1506347724_142242.html.

Mientras que, para Castro, M. (2016), la vulnerabilidad del internet de las cosas es directamente proporcional al nivel de seguridad que tenga el dispositivo IoT, en consecuencia, se asume que la vulnerabilidad se relaciona con la seguridad, puesto, que un dispositivo que nazca o sea creado sin contar con los estándares de calidad pertinentes en hardware y software, siempre será un objetivo fácil para que se vulnere los protocolos de seguridad.

En este contexto, el internet de las cosas juntamente con las redes móviles tiende a ser las que presentan mayor vulnerabilidad, gracias a las características bajo las cuales opera. Rueda, J. y Talavera, J. (2017), al igual que Hernández, D., Mazon, B., y Escudero, C. (2018), argumentan que la vulnerabilidad de las redes móviles y la seguridad de la información que se transfiere a través de dispositivo conectados a la red inalámbrica IoT presenta debilidades, puesto que las redes inalámbricas carecen de confiabilidad, integridad, autenticidad disponibilidad. En cuanto a la disponibilidad puede afirmarse que es quizás el elemento de mayor consideración, ya que hace referencia a la ubicación de los dispositivos IoT, los cuales son accesible para cualquier persona, por ejemplo, Colombia cuenta con “lámparas inteligentes”, “sensores de movimiento” que pudiesen estar expuestas y al alcance de cualquier persona.

En esta dirección, GSMA (2017) señala que los ataques que sufren los dispositivos IoT son el resultado del contexto al cual se exponen, agrega que es un problema mundial que presenta atributos muy similares y que aumenta ante la mirada atónita de los mismos fabricantes y/o desarrolladores.

El planteamiento anterior pone en evidencia, que no hay excepciones ante la susceptibilidad de las redes inalámbricas y pues para alcanzar la optimización funcional y operativa se debe empezar por ajustar los estándares de calidad a las directrices internacionales, para estar a la altura de otros países.

Como lo explicaba anteriormente Cuzme, M. (2015), la seguridad de los dispositivos conectados al internet de las cosas y el cuidado de la privacidad de la información se debe dar a través de programas de criptografía, regulación de permisos, accesos y creación de claves que se puedan aplicar al hardware o al software para asegurar el tránsito de los datos por la red y protegerlo de alteración o interpretación.

En consecuencia, es responsabilidad de las empresas proveedoras de servicios establecer políticas para mejorar la calidad del hardware, el software, crear instrumentos de seguridad para salvaguardar la información de ataques maliciosos, optimizar las aplicaciones y los canales de conectividad, tal como se ha venido haciendo paulatinamente en Colombia. Por su parte, Hernández, D., Mazon, B., y Escudero, C. (2018), consideran que los mecanismos de seguridad que apliquen las empresas tienen que tomar en cuenta obligatoriamente el hardware y el software, la seguridad de la red y la seguridad que proporciona la nube. En fin, estas debilidades pueden ser consecuencia de pruebas técnicas improcedentes, pero también puede ser producto de prácticas erradas de seguridad por parte del usuario.

Hirshberg, P. (2010), menciona que el internet de las cosas es quizás la estructura con mayor complejidad creada por el hombre. A pesar, de ser considerada el “boom”

tecnológico del siglo XXI, no está excepto de encontrar fuertes obstáculos que influyen en seguridad y privacidad de los datos y por ende en la información que se transmite de polo a polo. A criterio del autor, es necesario buscar mecanismos que se fundamenten en incorporar estándares y protocolos al internet de las cosas, aumentar las inversiones para el diseño de dispositivos de mejor calidad.

Es evidente, que uno de los mecanismos de mayor relevancia que pueden aplicar las empresas es mejorar la calidad de los dispositivos IoT y para ello es imperante considerar las debilidades que han venido presentando cada uno de ellos, producto quizás de la misma afluencia de usuarios o de fallas que nacen a la par del equipo.

Liñan, A., Vives, A., Bagula, A., Zennara, M. y Pietrosemoli, E. (2015), considera que el mercado tecnológico ha influido a grandes escalas en la seguridad y privacidad de los datos, pues un alto porcentaje de los dispositivos que se instalan en la IoT son vulnerables a los niveles de seguridad. Por lo tanto, se reafirma que la seguridad de los datos juega un papel preponderante en la vulnerabilidad de las redes. ¿En qué sentido? conviene subrayar, debido a que, si se tienen unos niveles de seguridad deficientes o por debajo de los parámetros reglamentarios, entonces aumenta automáticamente el riesgo a sufrir ataques.

Para López, M. (2019), la seguridad y la privacidad se vincula con la cantidad de datos que se manipule a través de las redes, pues el incremento de datos ocasiona colapsos y esto a su vez aumenta la vulnerabilidad y pone el peligro la seguridad de la información, en otras palabras, es un proceso cíclico de causas y efectos. No cabe duda, que la seguridad de los datos es proporcional a la vulnerabilidad de las redes, ya que, si los códigos de seguridad no cumplen con los requerimientos o ajustes pertinentes, la red se ve expuesta a cualquier amenaza que puede causar serias consecuencias al usuario.

Por último, Fayçal, D. y Mayor, M. (2018), Ramírez, D. y Rodríguez, E. (2016), Sanmartin, P., Ávila, K., Viloria, C. y Jabba, D. (2016), coinciden al afirmar que la seguridad de los datos es parte elemental de la vulnerabilidad de las redes, es decir, son variables que dependen una de otra y funcionan de manera conjunta, situación que conlleva a que la ausencia o falla de alguna de ellas desmiembre todo un proceso tecnológico.

De acuerdo con lo anterior y teniendo en cuenta la vulnerabilidad y lo expuestos que están los datos de las personas y las empresas se han venido desarrollando delitos por la exposición que tienen los datos, los Gobiernos han tenido que intervenir tomando medidas y dictando algunas normas, como lo son: “ley orgánica de protección de datos personales en España, o la ley 1581 de 2012 sobre protección de datos personales en Colombia esto con el fin de propender por la salvaguarda de dichos datos, en especial en cuanto a la información almacenada de forma digital ” Chaparro M (2015).

En Colombia los gobiernos se han basado en uno de los principios consagrados en la constitución política, ya que esta es la ley suprema de un país, en su articulo 15 expresa lo siguiente: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución” (constitución política de

Colombia), este es primer antecedente importante y del cual se desprenden las leyes, decretos algunos nombrados en el presente documento.

Colombia	Ecuador	Argentina
"Por medio de la sentencia C-748/2011, la Corte Constitucional de Colombia encontró ajustada a la Constitución la mayoría del texto del proyecto de ley estatutaria por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1581/2011 y decreto 1377/2013" Caballero V (2016). Por resion de la corte constitucional	➢ Ley de comercio, firmas electrónicas y mensajes de datos ➢ Ley sistema nacional del registro de datos públicos ➢ Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales: (Alvares E, 2017)	➢ Constitución Nacional articulo 19 ➢ Constitución Nacional articulo 43 ➢ Ley 25.326 (Hoferek S, 2019)

De acuerdo a los datos plasmados en la tabla inmediatamente anterior, se identifica algunas falencias en las normas hasta el momento dictadas por los gobiernos, es necesario tomar la seguridad de los datos ya sean personales o comerciales como un derecho fundamental, para poder darle la importancia necesaria, pues inevitable no perjudicar otros derechos al tener exposición de los datos en la red. Sin dejar atrás que las personas que pueden manipular o acceder a la información debe tener responsabilidad moral "implica que los principios de prevención y precaución son ineludibles. Los requerimientos de privacidad y protección de datos personales de personas físicas y jurídicas, y la seguridad de la información se deben considerar desde la concepción y durante todo el ciclo de vida de la tecnología" (Feldgen M, P.10.2018)

5. CONCLUSIONES

El internet de las cosas sin duda alguna es uno de los avances tecnológicos que más revuelo ha causado en el siglo XXI, gracias a la capacidad con la cual cuenta para contrastar protocolos por medio de los cuales se abren canales de comunicación, donde interactúan elementos físicos y virtuales que han adoptados identidades y cualidades que lo identifican en las redes de información y comunicación. Al principio, tal vez fue controversia y hasta absurda la forma como se pretendía conectar objetos o cosas inteligentes a los procesos de los modelos del negocio, para establecer una comunicación e intercambio de datos e información con el medio ambiente mediante sensores.

No obstante, en la actualidad el internet de las cosas es un aliado de las comunicaciones. Ciertamente, presenta debilidades que con los años se han tratado de ir mejorando, pero, es evidente que aún falta mucho por hacer, pues es un proceso que requiere adecuarse a las demandas tecnológicas y a las necesidades de los usuarios. Ahora bien, tomando como referencia los objetivos de investigación propuestos se concluye:

Que las principales debilidades a nivel de privacidad que presentan las redes vienen dadas por la falta de políticas que permitan resguardar la integridad de la información transmitida por medio de las redes.

La protección de las redes en el internet de las cosas es un problema que se vincula directamente con el fabricante del dispositivo que se conecta a la red IoT, es decir, las principales debilidades están en hardware y software.

Por otro lado, se determinó que la seguridad de la red es importante para poder asegurar el tránsito de datos, pues actualmente el internet de las cosas no cuenta con estándares ni protocolos de seguridad que garanticen la confiabilidad de los datos, la integridad y la disponibilidad.

Los mecanismos que ponen al alcance del consumidor las empresas proveedoras de servicio no son confiables, pues aun cuando se han establecido instrumentos para proteger los datos, la amenaza continúa latente y en la medida que avanza la tecnología se incrementan los riesgos.

Por último, queda totalmente claro que la seguridad de los datos es directamente proporcional a la vulnerabilidad de las redes, debido a que la calidad de los datos garantiza el nivel de seguridad y fortalece la infraestructura de las redes contra ataque y violaciones de la privacidad.

BIBLIOGRAFÍA

Alvares E. paradigmas de la protección de datos personales en ecuador. análisis del proyecto de ley orgánica de protección a los derechos a la intimidad y privacidad sobre los datos personales. En: revista de derecho. (2017). Recuperado de: http://167.172.193.213/index.php/foro/article/view/500/487

Aguilar L, Delgado J, García P. Seguridad en internet de las cosas. En Universidad pontificia de Salamanca de España (2015). Recuperado de: https://pdfs.semanticscholar.org/2bb7/3003c65cec328d6f5d1bd75b8f9320c4b4f2.pdf

ARIAS, Fidias. El proyecto de investigación. 4ª ed. Caracas, Venezuela: episteme, 2006, p. 23-46. ISBN: 980-07-8529-9. Recuperado de: https://ebevidencia.com/wp-content/uploads/2014/12/EL-PROYECTO-DE-INVESTIGACI%C3%93N-6ta-Ed.-FIDIAS-G.-ARIAS.pdf

AYALA, Inmaculada, PINILLA, Mercedes Amor y FUENTES, Lidia. Abordando la heterogeneidad del internet de las cosas: una solución de agentes auto–configurables. En: Revista researchgate. No. 10 (octubre 2013); p. 3. ISSN 29-2643-249. Recuperado de: https://www.researchgate.net/publication/292643249_Abordando_la_heterogeneidad_en_la_Internet_de_las_cosas_una_solucion_de_agentes_auto-configurables

Arantza M. (2016) Big data y el internet de las cosas. Recuperado de : https://books.google.es/books?hl=es&lr=&id=cAbeDwAAQBAJ&oi=fnd&pg=PT18&dq=que+problema+hay+con+el+internet+de+las+cosas+&ots=hEhhZAkV_B&sig=JfBGEktv0dywiZbCmB-Sn5aTtrg#v=onepage&q=que%20problema%20hay%20con%20el%20internet%20de%20las%20cosas&f=false

BLASCO, Josefa y PÉREZ, José. Metodologías de investigación en las ciencias de la actividad física y el deporte: ampliando horizontes. Venezuela: funda-Upel, 2007, p. 12-14. ISBN: 182.00-3028-11. Recuperado de: https://rua.ua.es/dspace/bitstream/10045/12270/1/blasco.pdf

Caballero V. La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. Revista Prolegómenos - Derechos y Valores. (2016). Recuperado de: http://www.scielo.org.co/pdf/prole/v20n39/v20n39a11.pdf

CASTRO SOLA, Miguel. Internet de las cosas. privacidad y seguridad. Jaén, 2016. Trabajo de pregrado (Informática), universidad de Jaen. Departamento de informática. Recuperado de: https://sinbad2.ujaen.es/sites/default/files/publications/Memoria_0.pdf

CARACOL NOTICIAS. El Internet de las Cosas comienza a aterrizar en Colombia [en línea] https://caracol.com.co/radio/2017/09/25/tecnologia/1506347724_142242.html [citado en10 de agosto de 2019].

CISCO**.** Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo. EEUU. Informe técnico, 2011. Recuperado de: https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

CORPORACIÓN GSMA. El internet de las cosas y los accesorios tecnológicos. España: Asociación GSMA, 2017, p. 13-26. ISBN: 028-127-852-90. Recuperado de: https://www.gsma.com/latinamerica/resources/5g-internet-de-las-cosas/?lang=es

Constitución política de Colombia. Recuperado de : https://colombia.justia.com/nacionales/constitucion-politica-de-colombia/titulo-ii/capitulo-1/#articulo-15

CUZME, Fabian. El internet de las cosas y las consideraciones de seguridad. Quito, 2015. Trabajo de postgrado (maestría en redes de comunicaciones), Pontificia Universidad Católica del Ecuador. Facultad de Ingeniería. Recuperado de: http://repositorio.puce.edu.ec/bitstream/handle/22000/8492/INTERNET%20DE%20LAS%20COSAS%20TESIS%20Y%20CONSIDERACIONES%20DE%20SEGURIDAD%20-%20FINAL.pdf?sequence=1&isAllowed=y

Chaparro M. Legislación informática y protección de datos en Colombia, comparada con otros países (2015). Ed: revistas INVENTUM Universidad uniminuto. Recuperado de: https://revistas.uniminuto.edu/index.php/Inventum/article/view/1014/953

DAVE E. Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Business Solutions Group (IBSG). [en línea] https://s3.amazonaws.com/academia.edu.documents/34766160/internet-of-things-iot-ibsg.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1541000456&Signature=Qlo2gbMfIVwzGIqAxXbzOg1NSUA%3D&response-content-disposition=inline%3B%20filename%3DInternet-of-things-iot-ibsg.pdf. [citado en abril 02 de 2016].

DOMÍNGUEZ, Alberto y VARGAS, Miguel. El estado del arte: Salud inteligente y el internet de las cosas. En: Revista ID+tecnológico. No. 1 (02 de marzo de 2018); p. 1-4. ISSN 201-395042-X09. Recuperado de: https://revistas.utp.ac.pa/index.php/id-tecnologico/article/view/1809

FAYÇAL Daira y MAYOR Milena. Internet de las cosas en un mundo digitalizado. En: Revista tecnológica de información y comunicación. No. 8 (03 de

febrero de 2018); p. 3-5. ISSN 003-294072-2001. Recuperado de: http://servicio.bc.uc.edu.ve/educacion/eduweb/v11n1/v11n12017.pdf

Feldgen M. Internet de las cosas y los ciudadanos. En: revista tecnología y sociedad de Buenos Aires (2018). Recuperado de: http://200.16.86.39/index.php/TYS/article/viewFile/1510/1431

FRUEHE, J. Internet de las cosas (inseguras). [en línea] https://www.forbes.com/sites/moorinsights/2015/09/15/the-internet-of-insecure-things/#73be542d1732 [citado en 19 de marzo de 2015].

HERNÁNDEZ, Dixys, MAZON, Bertha y ESCUDERO, Carlos. Internet de las cosas (IoT). En: Revista Researchgate. No. 15 (21 de agosto de 2018); p. 53-60. ISSN 78-9942-24-120-7. Recuperado de: https://www.researchgate.net/publication/327702411_Capitulo_3_Internet_de_las_cosas_IoT

HIRSHBERG, Peter. (2010). Internet de las cosas. En un mundo conectado a objetos inteligentes. California: fundación de la innovación Bankinter. 2011, pp.58. ISBN: 998-289005-90. Recuperado de: http://boletines.prisadigital.com/El_internet_de_las_cosas.pdf

Hoferek S. (2019) El derecho a la intimidad, la protección de datos personales y el big data a la luz del ordenamiento jurídico argentino. En:Universidad siglo xxl. Recuperado de: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/17186/HOFEREK%20SILVIA.pdf?sequence=1&isAllowed=y

LA VOZ DE LA G5 Y ELT PARA LAS AMÉRICAS. Internet de las cosas en América Latina. 3ª ed. Madrid: OCDE, 2016, pp. 12-15. Recuperado de: https://revistadigital.sre.gob.mx/images/stories/numeros/n94/kirton.pdf

LIÑAN, Antonio., VIVES, Álvaro., BAGULA, Antonio., ZENNARA, Marco. y PIETROSEMOLI, Ermanno. Internet de las cosas. Comunidad de programadores, No. 16 (mayo 23 de 2015); 90-116. ISSN 189-009-23-B-9. Recuperado de: https://www.lawebdelprogramador.com/pdf/2439-INTERNET-DE-LAS-COSAS.html

LÓPEZ, Manel. Internet de las cosas. Transformación digital de la sociedad. 4ª ed. España: RA-MA, 2019, pp. 22-36. Recuperado de:

https://www.ra-ma.es/libro/internet-de-las-cosas_93304/

Pérez N, Bustos M, Mario M, Henríquez P. Análisis sistemático de la seguridad en internet of things. Ed universidad nacional d san Luis Portugal (2018). Recuperado de: http://sedici.unlp.edu.ar/bitstream/handle/10915/68387/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

RAMÍREZ, David y RODRÍGUEZ, Erika. Diseño de un método para identificar necesidades y oportunidades para la implementación de Internet de las cosas (IoT) aplicable a oficinas de trabajo donde permanezcan entre 30 y 70 personas y planteamiento de un caso práctico de solución en las oficinas de la Agencia Nacional del Espectro. Bogotá D.C., 2016. Trabajo de pregrado (Ingeniería en Telecomunicaciones). Universidad Distrital Francisco José de Caldas. Facultad tecnológica. Recuperado de:

repository.udistrital.edu.co › bitstream › RamirezMadridDavidAndres2017

RUEDA, Johan y TALAVERA, Jesús. Similitudes y diferencias entre Redes de Sensores Inalámbricas e Internet de las Cosas: Hacia una postura clarificadora. En: Revista colombiana de computación. No. 2 (20 de abril de 2017); p. 62-74. Recuperado de: https://revistas.unab.edu.co/index.php/rcc/article/view/3218

SANMARTIN Paúl, ÁVILA Karen., VILORIA César y JABBA Daladier (2016). Internet de las cosas y la salud centrada en el hogar. Salud Uninorte, No. 2, (mayo-agosto, 2016), pp. 337-351. ISSN 2019-009-L18. Recuperado de: http://rcientificas.uninorte.edu.co/index.php/salud/article/viewArticle/7580

TAYLOR, S. y BOGDAN, R. Metodología de la investigación. 1ª ed. Caracas: Venezuela: Ra-Mar, 1987, p. 45-56. ISBN: 180-02-5559-9. Recuperado de: https://asodea.files.wordpress.com/2009/09/taylor-s-j-bogdan-r-metodologia-cualitativa.pdf

VIRGÜEZ, J. (s.f.). IoT: La Evolución de la Seguridad en el Internet de las Cosas. [en línea] http://polux.unipiloto.edu.co:8080/00003509.pdf