LA SEGURIDAD DE LA INFORMACIÓN EN EL INTERNET DE LAS COSAS (IoT)

ESLY LORENA MENDOZA DOMINGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2021

LA SEGURIDAD DE LA INFORMACIÓN EN EL INTERNET DE LAS COSAS (IOT)

ESLY LORENA MENDOZA DOMINGUEZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. Joel Carroll vagas M.Sc
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Cali., Agosto 01 de 2021

DEDICATORIA

Este proyecto va dedicado primeramente a Dios que es quien nos da la vida y la salud para continuar con nuestros sueños también a mi familia el principal motor para esforzarme cada vez más y a todas las personas que de una u otra forma han contribuido para llevar a cabo esta especialización, en especial a mi tutor y al director de grado.

AGRADECIMIENTOS

A Dios, primeramente, y a la institución que me permitió llevar a cabo la especialización en esta modalidad, al departamento de sistemas y a los tutores y director que dedicaron tiempo a realizar correcciones para que el trabajo se lleve a cabo de la mejor manera.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Ataques: es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo.[2]

Firmware: es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo, es el software que tiene directa interacción con el hardware, siendo así el encargado de controlarlo para ejecutar correctamente las instrucciones externas.[2]

IoT: Se conoce como la agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes), dónde todos ellos podrían ser visibles e interaccionar. Respecto al tipo de objetos o dispositivos podrían ser cualquiera, desde sensores y dispositivos mecánicos hasta objetos cotidianos como pueden ser el frigorífico, el calzado o la ropa.[1]

Malware: es un término general para referirse a cualquier tipo de "malicious software" (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento.[2]

Routers: es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.[2]

[1] Internet Of Things IoT. [en línea]. DELOITTE. [Fecha de consulta 10 de octubre de 2020] Disponible en: https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

Seguridad: es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.[2]

Vulnerabilidad: se refiere a los puntos débiles de un sistema computacional donde su seguridad informática no tiene defensas necesarias en caso de un ataque.[2]

[2] Significado : Qué es . [en línea]. Significados. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://www.significados.com/

RESUMEN

La presente monografía se enfoca en dilucidar los diferentes riegos a los que los usuarios están expuestos cuando hacen uso de los elementos que actualmente se encuentran conectados al internet, en especial a esa nueva tecnología conocida como IoT por sus siglas en ingles Internet of things, así como, las vulnerabilidades y los diferentes ataques que pueden afectar la seguridad, la integridad y la privacidad de los usuarios usando IoT. El internet de las cosas como se conoce en Colombia está tecnología, se ha catalogado un tema importante en el tema técnico, social y económico. Este se está combinando en productos de consumo, bienes duraderos, vehículos, sector industrial y servicios públicos, sensores y otros objetos de uso cotidiano con conectividad a internet que prometen transformar el modo en que se trabaja, se vive o se juega.

Sin embargo, el IoT presenta desafíos que pueden detener su avance. Muchas son las noticas que se presentan sobre los ataques a los dispositivos que se encuentran conectados a la red IoT, el temor y la preocupación por la seguridad se están apoderando de los usuarios. Para la tecnología asegurar información no es un tema nuevo, las propiedades de implementación de esta tecnología tienen un desafío que los cataloga como únicos y nuevos en su contexto. Enfrentarlos debe ser una prioridad fundamental que garantice la protección de los usuarios los servicios prestados y los productos ofrecidos por el IoT.

Los dispositivos poco seguros se consideran potencialmente vulnerables ya que pueden ser usados como puertas de ataques que permitan a ciber delincuentes explotar vulnerabilidades que ponen en riesgo la protección de datos y seguridad de sus usuarios, es por esto que, recuperar la confianza de los usuarios en cuanto a que el uso de los dispositivos conectados a la red y los servicios se muestren libres o en su defecto protegidos y estarán seguros en la medida en que esta tecnología se propague y haga parte de la vida diaria.

Palabras Claves: IoT, vulnerabilidad, seguridad, ataques, malware, routers, firmware.

ABSTRACT

This monograph aims to present the different risks to which users are exposed when they make use of the elements that are currently connected to the internet of things, the vulnerabilities and the different attacks that can affect security, integrity and privacy of the users. The internet of things has been cataloged as an important issue in technical, social and economic terms. This is being combined in consumer products, durable goods, vehicles, the industrial sector and public services, sensors and other everyday objects with internet connectivity that promise to transform the way you work, live or play.

However, the IoT presents challenges that can halt its advance. Many are the news that are presented about attacks on devices that are connected to the IoT network, fear and concern about security are taking over users. For technology, securing information is not a new issue, the implementation properties of this technology have a challenge that classifies them as unique and new in their context. Addressing them must be a fundamental priority that guarantees the protection of the users, the services provided, and the products offered by the IoT.

Unsafe devices are considered potentially vulnerable since they can be used as attack doors that allow cyber criminals to exploit vulnerabilities that put the protection of data and security of their users at risk, that is why, to recover the trust of users in Regarding the use of the devices connected to the network and the services shown free or, failing that, protected and will be safe to the extent that this technology spreads and becomes part of daily life.

Keywords: IoT, vulnerability, security, attacks, malware, routers, firmware.

INTRODUCCIÓN

El desarrollo y la importancia que la IoT ha alcanzado que la hacen una tecnología de mayor impacto a futuros años según los diferentes informes (National Intelligence Council (U.S.), 2008) (Patrick Guillemin, Peter Friess, 2009) (MEXICO DOCUMENT, s.f.) y se prevé que muchos elementos y dispositivos serán equipados con actuadores y sensores que se conectan a internet en tiempo real a través de redes de acceso, lo cual permite que se generen flujos de datos que deban ser procesados, almacenados, asegurados y presentados eficientemente.

Las conexiones a internet actualmente en su mayoría corresponden a dispositivos utilizados por las personas como son los computadores o los teléfonos móviles. La forma principal de comunicación ante esto son los seres humanos. La experiencia que brinda el IoT es que en un futuro los dispositivos las “cosas” puedan intercambiar información. Si bien el internet de las cosas es una revolución tecnológica que representa el futuro de la informática y las comunicaciones, pero esta a su vez necesita de algunas otras tecnologías de innovación.

Es precisamente todo este concepto de interconexión entre dispositivos y de conexión a la red IoT lo que puede suponer un enorme riesgo para los usuarios, aunque se tengan antivirus y software de protección en los dispositivos como los celulares y computadores, existen dispositivos como los Smart tv o la nevera no cuentan con un nivel de protección (JORDI SALAZAR Y SANTIAGO SILVESTRE), lo que hace que sean blancos de ataque por ciber delincuentes. Son muchas las vulnerabilidades y los ataques a los que los dispositivos que se encuentren conectados a una red IoT pueden estar expuestos entre ellos podemos resaltar las credenciales de acceso a los dispositivos, cifrado inseguro, no realizar actualizaciones de seguridad, dentro d ellos taques se pueden presentar el secuestro de la información o Ransomware, ataques de denegación de servicio DDOS, bots de spam, manipulación entre otros. Por medio de este documento se pretende dar

a conocer las vulnerabilidades y ataques a los que se está expuesto con el fin de mitigar su propagación y alertar a los usuarios sobre el buen uso de las “cosas” conectadas.

1. DEFINICIÓN DEL PROBLEMA

Como se ha venido analizando en la parte introductoria de este documento, el IoT se está propagando como una tendencia tecnológica dominante tanto a nivel empresarial, industrial como de consumo. Se espera que el número de dispositivos conectados sea multiplicado en los próximos años, esto se verá impulsado por el nuevo estándar de red como el 5G o el WiFi 6 que prometen el mejoramiento en las comunicaciones entre máquinas y usuarios augurando una velocidad más alta y una latencia más baja lo cual pretende potencializar el uso del streaming, la realidad virtual o aumentada.

A medida que se va disparando el uso de las “cosas” conectadas se disparan también las posibilidades de sufrir un incidente que exponga la información que comparten los dispositivos o la que se comparte en la red la cual cada vez es más sensible y es aprovechada por los ciber delincuentes como posible puerta de entrada a ataques.

Es por lo que surge el interrogante *¿Cuenta el internet de las cosas (IoT) con las medidas de seguridad para proteger nuestra información?*

La seguridad en los dispositivos que actualmente se conectan a esta red cada vez son más y la seguridad aún no ha llegado a un mínimo confiable, es por lo que hoy se puede decir que no son 100% seguros. No obstante, pese a la pandemia que afronto el mundo iniciando el 2020 referente al Covid-19 hizo que la mayoría de las actividades se trasladaran a nivel virtual lo que implica el aceleramiento de la migración del protocolo de internet versión 4 (IPV4), a la versión 6 (IPV6), dado que las cantidades de direcciones IP dentro de la versión 4 ya se agotaron, por lo tanto para los dispositivos IoT sería un paso importante el funcionamiento dentro del protocolo en versión 6, no solo por la mayor cantidad de direcciones que puede ofrecer sino que además vienen con mejores medidas de seguridad lo cual hace parte del motivo de esta investigación.

2. JUSTIFICACIÓN

Los motivos que llevan a ahondar en esta investigación hace referencia a la seguridad y tratamiento de datos y la forma en que los dispositivos conectados al IoT pueden salvaguardarlos, el avance actual de la tecnología implica que cada día se está más dependientes de una conexión a internet, los aparatos electrónicos que se utilizan para su correcto funcionamiento deben configurarse con una cuenta de usuario que pide parte de la información sensible como lo es número de teléfono, nombre y hasta la ubicación, la mayoría de ellas no funcionan correctamente si no se activa la geolocalización, lo que hace que los usuarios estén más expuestos y con sus datos alojados en un servidor. Dicho servidor es un blanco perfecto para los atacantes ya que pueden presentarse secuestro de datos o ingresar directamente a los dispositivos de los usuarios, es por ello por lo que en esta monografía se quiere dar a entender la importancia que requiere sacar elementos con un alto nivel de seguridad que permitan a los usuarios tener la confianza que sus datos se encuentran a salvo.

La seguridad solo se puede brindar desde la creación del dispositivo o el elemento que va a salir al mercado, evidenciando las posibles vulnerabilidades que pueda tener y atacándolas antes de su puesta en producción, informando sobre actualizaciones de seguridad a través de la cuenta del usuario o en el mismo dispositivo, además de la información referente hasta cuando se entregaran soporte para los mismos. Este es un importante nicho de mercado en la industria tecnológica que ligado a la seguridad puede lograr los objetivos propuestos de manera exitosa, pero para el usuario final puede ser difícil detectar un incidente de seguridad en muchos casos de un producto o un servicio IoT, como también pude ser difícil cuando sus datos personales están siendo expuestos, muchos dispositivos conectados al IoT no cuentan con una interfaz de usuario o en su defecto tienen una muy básica, situación que se complica ya que un usuario no puede interactuar directamente con el dispositivo para modificar actualizaciones o configuraciones.

Puede llegar a ser difícil de precisar la responsabilidad en los daños causados por la falta de una seguridad adecuada en la IoT, generando incertidumbre entre las víctimas a la hora de tener compensación por los daños causados, en ausencia de normas o régimen de responsabilidad sólidos, los usuarios terminan siendo la última instancia pagando los altos precios de la falta de seguridad.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Desarrollar una revisión de literatura de los riesgos y vulnerabilidades a las que están expuestos los dispositivos que se encuentran conectados a una red IoT.

3.2 OBJETIVOS ESPECÍFICOS

- Construir una revisión documental referente a la tecnología de la IoT.
- Caracterizar cuáles son las principales vulnerabilidades a las se encuentran expuestos los dispositivos en una red IoT.
- Describir los diferentes tipos de ataques que se presentan en dispositivos conectados a una red IoT.
- Realizar un resumen analítico con las medidas y mejores prácticas para proteger la información cuando esta se encuentra transando a través de estos dispositivos.

4. MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Kevin Ashton, Profesor del MIT en el año 2009 fue la persona en usar la expresión Internet of Things (IoT) de forma pública por primera vez, desde entonces se masifico de forma exponencial. Asthon acuñó el término públicamente en el RFDI journal. Aunque por sus propias palabras se escuchó que la expresión se venía usando en grupos de investigación desde 1999.[3]

Figura 1 - Kevin Ashton hablando en el LG CNS

Fuente: http://www.lgcnsblog.com/features/entrue-world-2015-kevin-ashtons-keynote-speech/

"Si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiese saberse de cualquier cosa –usando datos recolectados sin intervención humana– seríamos capaces de hacer seguimiento detallado de todo, y poder reducir de forma importante los costes y malos usos. Sabríamos cuando las cosas necesitan ser reparadas, cambiadas o recuperadas, incluso si están frescas o pasadas de fecha. El Internet de las Cosas tiene el potencial de cambiar el mundo como ya lo hizo Internet. O incluso más.". Fueron parte de las palabras expresadas por Ashton en su discurso.

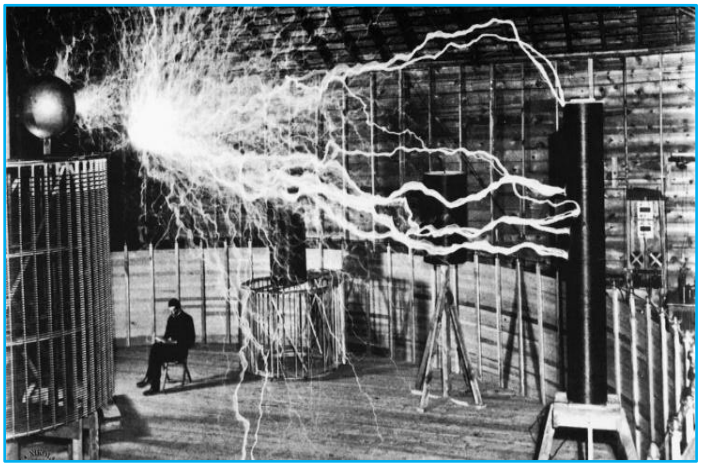
[3] Pensamientos y tecnología, El Origen Del IoT. [en línea]. Bruno Cendón. [Fecha de consulta 10 de junio de 2020]. Disponible en: http://www.bcendon.com/el-origen-del-iot/

A pesar de que el uso público de la expresión se usó hace pocos años, la primera conexión de este tipo data de finales del siglo XIX, más exactamente en 1874 cuando se logró conectar una estación meteorológica en la cima del Mont Blanc con un laboratorio ubicado en París, dicha conexión se logró hacer basada en enlaces de radio de onda corta.

Años más tarde inventores y pensadores como Nikola Tesla y Alan Turing anticiparon el crecimiento de la conectividad global, hablando sobre el gran cerebro lleno de información en que se convertiría un planeta totalmente interconectado y este guardado en un bolsillo.[4]

“Cuando lo inalámbrico esté perfectamente desarrollado, el planeta entero se convertirá en un gran cerebro, que de hecho ya lo es, con todas las cosas siendo partículas de un todo real y rítmico… y los instrumentos que se usarán para ellos serán increíblemente sencillos comparados con nuestros teléfonos actuales. Un hombre podrá llevar uno en su bolsillo” Nikola Tesla Entrevista a la revista Colliers 1926.

Figura 2 – Nikola Tesla



Fuente: http://www.bcendon.com/el-origen-del-iot/

[4] Pensamientos y tecnología, El Origen Del IoT. [en línea]. Bruno Cendón. [Fecha de consulta 10 de junio de 2020]. Disponible en: http://www.bcendon.com/el-origen-del-iot/

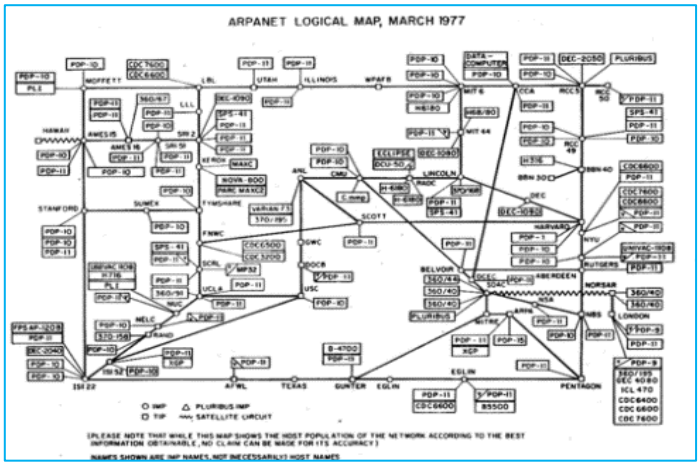
A pesar de la visión temprana de estos científicos, la inmadurez tecnológica de la época no permitió avanzar y llevar a cabo las ideas, solo hasta pasados los años en las décadas de los 60 y 70 el departamento de defensa de EEUU comenzó a publicar los primeros protocolos de comunicación, hasta convertirse en lo que hoy se conoce como Internet. También cabe anotar que estos protocolos fueron de uso militar y académico exclusivamente.

Para la década de los 60 y los 70 fue el tiempo cuando se crearon los primeros protocolos de comunicaciones que definieron la base de lo que actualmente se conoce como internet En 1973 Vinton Cerf y Robert E. Kahn, desarrollaron el modelo TCP/IP que describe cómo deben ser tratados los datos (formateados, direccionados, transmitidos, enrutados y recibidos) para proveer conectividad extrema a extremo entre dos equipos conectados a una red.

En 1983 TCP/IP se convirtió en el corazón de la red ARPANET, reemplazando por completo al protocolo NCP y la red se separó en dos partes, MILNET, para usos militares, y ARPANET para el resto.[5]

[5] Pensamientos y tecnología, El Origen Del IoT. [en línea]. Bruno Cendón. [Fecha de consulta 10 de junio de 2020]. Disponible en: http://www.bcendon.com/el-origen-del-iot/

Figura 3 Mapa lógico de Arpanet (Dominio Público)



Fuente: https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

En 1990 Jhon Romkey en el evento Interop en EE. UU., creó el primer objeto conectado a internet y se trataba de una tostadora que se podía encender o apagar a través de un sistema remoto[6]. La conectividad se realizó a través del protocolo TCP/IP y el control mediante SNMP (Simple Network Management Protocol) o protocolo de gestión de red que fue usado para encender o apagar el electrodoméstico. La comunicación cableada que ofrecía el internet en ese entonces y el costo del hardware era aún elevado los que hizo que las ideas de implementar objetos conectados pasaran inadvertidas durante años.[6]

[6] Pensamientos y tecnología, El Origen Del IoT. [en línea]. Bruno Cendón. [Fecha de consulta 10 de junio de 2020]. Disponible en: http://www.bcendon.com/el-origen-del-iot/

Figura 4 - Tostadora conectada a un control remoto por John Romkey

Fuente: http://www.livinginternet.com/i/ia_myths_toast.htm

En 1993 surgió el proyecto Xcoffee donde estudiantes de la Universidad de Cambridge desarrollaron la primera cámara conectada online para monitorizar si había café en las máquinas de café del departamento. La webcam original actualizaba la imagen de una cafetera unas tres veces por minuto, para que todos los interesados estuvieran al tanto de cuando podían disfrutar de un café recién hecho.[7]

Un año después, Steve Mann, (Universidad de Stanford), conocido como "El padre de la computación vestible" (*The Father of Wearable Computing*), conectó la primera cámara portátil a la web, la imagen a continuación muestra la evolución de esta.

[7] Pensamientos y tecnología, El Origen Del IoT. [en línea]. Bruno Cendón. [Fecha de consulta 10 de junio de 2020]. Disponible en: http://www.bcendon.com/el-origen-del-iot/

Figura 5 - Evolución de dispositivos de computación vestible (Glogger, wikipedia)

Fuente: https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

A comienzos del siglo XXI, con la popularización de la conectividad inalámbrica (celular o WiFi), se produjo la primera explosión en el crecimiento de los objetos conectados. El crecimiento se consolidó especialmente en los últimos años, según han ido surgiendo nuevos conceptos como el WSN (*Wireless Sensor Networks*) o las nuevas tecnologías de acceso radio como LPWA (NB-IoT, LTE-M), para finalmente dar paso al IoT que todos conocen.

Para los años 2000 LG lanza el primer refrigerador conectado a Internet debido a su precio no fue muy bien acogido por los usuarios.

Figura 6 - LG Digital DIOS

Fuente: https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

La empresa francesa Violet también lanzó al mercado Nabaztag (liebre en armenio). Un dispositivo con forma de conejito que se conecta a Internet por ondas wifi el cual se comunicaba con el usuario mediante mensajes de voz, y cambios de color o movimiento en sus orejas, Nabaztag reproduce, habla, escucha y responde a la voz de los usuarios. También les puede despertar mañana con las noticias de actualidad de diarios digitales, la música de su emisora favorita o la información del tiempo; o avisarles cuando llega un correo o un mensaje a sus redes sociales.

Figura 7 - Mascota virtual Nabaztag

Fuente: https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

2008 fue un hito importante en la historia del IoT, ya que fue el primer año en el que los dispositivos conectados a Internet superaron al número de personas conectadas. Y fue cuando hasta el 2009 se usó el término Internet de las cosas IoT tal y como lo explicamos al inicio de este marco teórico.

En ese mismo año Google arranca su proyecto de coches autónomos, Google self-driving car project, que posteriormente pasaría a ser conocido como Wayne, el cual permite a un automóvil conducirse de forma autónoma por ciudad y por carretera, detectando otros vehículos, señales de tráfico, peatones, etc.

Figura 8 - Coche autónomo

Fuente: https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

La empresa Saint Jude Medical fabrica los primeros *implantes cardiacos conectados* también en el 2009. Un adaptador USB inalámbrico recibía los datos del implante y los transmitía posteriormente a los móviles del personal médico.

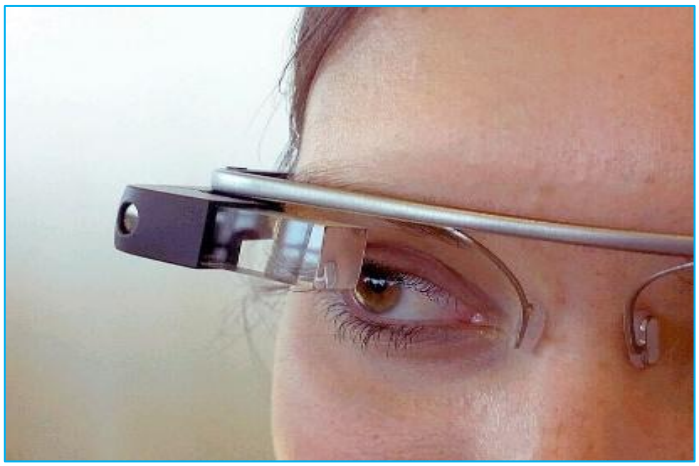
En el 2010 la compañía NEST empieza a fabricar electrodomésticos inteligentes. El primero fue un termostato que optimiza el horario de la calefacción a partir de los patrones de uso de los usuarios.

Para el 2011 los primeros pasos en IoT se dieron con la versión v4 (IPv4). Esto suponía una importante limitación, ya que el número de direcciones que se podían generar era muy reducido. A partir del año 2011 se diseña el protocolo de direccionamiento

de Internet IPv6 posibilitando la identificación de una infinidad de direcciones. Supuso un gran impulso para el desarrollo del IoT ya que, según estima Juniper Research, para 2021 el número de dispositivos, sensores y actuadores conectados superará los 46000 millones. Poco después Samsung, Google, Nokia y otros fabricantes anuncian sus proyectos NFC.

En 2013 Google puso a la venta (para desarrolladores calificados) Glass Explorer Edition, un dispositivo de visualización de tipo gafas de realidad aumentada presentado en el congreso I/O de junio de 2012.

Figura 9 - Google Glass



Fuente: https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

Para el 2014 Intel, Cisco, IBM, GE y AT&T se unen para mejorar la integración de IoT con la industria. Se crea la iniciativa IoT-GSI Global Standards para promover la adopción de estándares para IoT a escala global. Los participantes comparten informes de investigación, documentos técnicos y buenas prácticas de gran valor para el desarrollo del IoT industrial a escala empresarial y global.

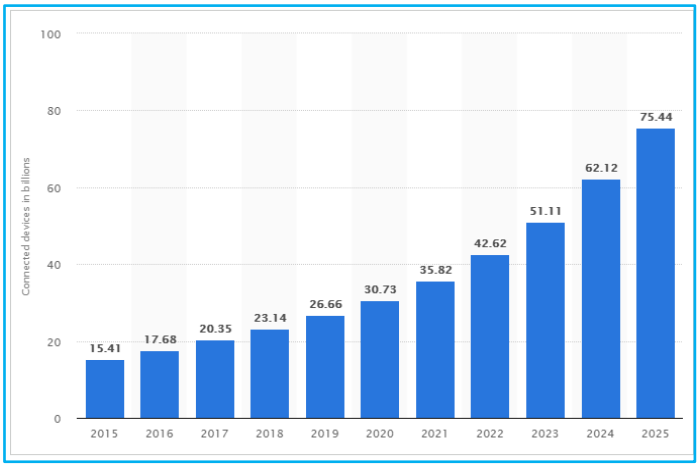
En el 2017 los grandes fabricantes de servicios en la nube ofrecen soluciones IoT: *Azure IoT Edge*, *AWS IoT* y *Google Cloud IoT core*.

Para el futuro se evidencia que la historia del IoT se sigue escribiendo día a día a pasos agigantados, con la aparición de *nuevos dispositivos*, *nuevos protocolos*, *nuevas tecnologías* de acceso, etc. que confluyen con los avances en otras tecnologías como

la *computación en la nube*, *big data*, e *inteligencia artificial,* enriqueciendo y dando cada día más oportunidades de crecimiento al universo IoT.

Estudios actuales que han realizado grandes empresas de IT a nivel mundial auguran que ese cerebro que menciono Tesla en su momento estaría formado en este 2020 por al menos 30 billones de "cosas" inteligentes interconectadas a nivel mundial, además indican que posiblemente esa cifra se duplicaría 4 años más tarde. El exponencial crecimiento al que avanza la tecnología y la cantidad de dispositivos conectados ofrece un amplio menú a la sociedad actual en cuanto a nuevos servicios de innovación.[8]

Tabla 1 - Proyección Crecimiento del número de dispositivos conectados



Fuente: https://www.hiberus.com/crecemos-contigo/introduccion-al-iot-internet-of-things/

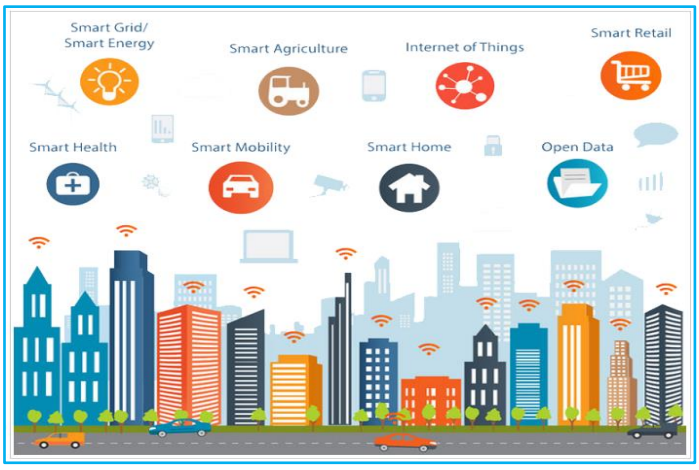
El uso de las plataformas para la sonorización de los objetos que nos rodean supondrá, en el futuro inmediato, una revolución en la forma de obtener información. Con ese gran volumen de datos se podrá, entre otras muchas cosas, optimizar la gestión de la industria (Smart Industry y Smart Energy), del mundo médico (Smart Health), de los hogares

[8] Blog de Hiberus Tecnología: Introducción al IoT, Internet of Things. [en línea]. Jorge Learte. [Fecha de consulta 12 de mayo de 2020]. Disponible en: https://www.hiberus.com/crecemos-contigo/introduccion-al-iot-internet-of-things/

(Smart Home), del mundo agrícola (Smart Farming) o, incluso, de las ciudades (Smart City).[7]

A continuación, se presentan algunos ejemplos de esta nueva era Smart:

Figura 10 - Nueva era Smart



Fuente: https://www.hiberus.com/crecemos-contigo/introduccion-al-iot-internet-of-things/

Pese a lo global y la popularidad que se ha tenido el internet de las cosas o IoT, no existe una palabra que defina el término. Existen muchas definiciones y son usadas por diferentes investigadores de esta nueva tecnología para describir o promover lo que puede significar el internet de las cosas IoT y sus características más importantes. Por ejemplo, para The Internet Architecture Board (IAB) el término “Internet of Things” (IoT) denota una tendencia de cuando un número largo de dispositivos embebidos utiliza los servicios ofrecidos por el internet, estos objetivos llamados “smart objects”, muchas veces no son controlados por un humano, pero son usados en edificaciones, autos o sensores y sistemas que ayudan al medio ambiente.[9]

[9] H. Tschofenig, J. A. Architectural Considereations in Smart Object Networking. Tschofenig, et al., 23, . March de 2015.

Para Internet Engineering Task Force (IEFT), el término “smart objects”, no obstante, tienden a ser dispositivos limitados por los componentes con que son fabricados su memoria, el procesador o el ancho de banda le restan atractivo para poder tener un nivel alto de seguridad.[10]

La IEEE en un magazín llamado Communication Magazine, define el IoT como una relación entre el dispositivo y los servicios de la nube, reconociendo el IoT como un marco en el que representa las cosas y una presencia en internet. Más específicamente indica que el objetivo del internet de las cosas es ofrecer nuevos servicios y aplicaciones que generen conexión entre los mundos físicos y virtuales.[11]

Por otra parte, el diccionario de Oxford indica y define al internet como un elemento de IoT que permite enviar datos a través de una interconexión por medio de dispositivos informáticos.[12]

Las definiciones descritas anteriormente muestran espacios en los cuales la capacidad computacional y la conectividad se pasan a dispositivos, sensores, objetos o puntos diferentes a un computador. la capacidad que estos tienen para generar Se describe al igual que la forma de consumir e intercambiar información muchos de ellos sin necesidad de la ayuda de una persona.

[10] Dave Thaler, H. T. Architectural Considerations in Smart Object Networking, 2020.

[11] IEEE COMSOC. IEEE Internet of Things Initiative, a Multi-Society Technical Group. IEEE Internet of Things Magazine, 2019.

[12] Definition of internet of things in English. Oxford English and Spanish Dictionary, 2021.

4.1.1 MODELOS DE COMUNICACIÓN DEL INTERNET DE LAS COSAS IOT

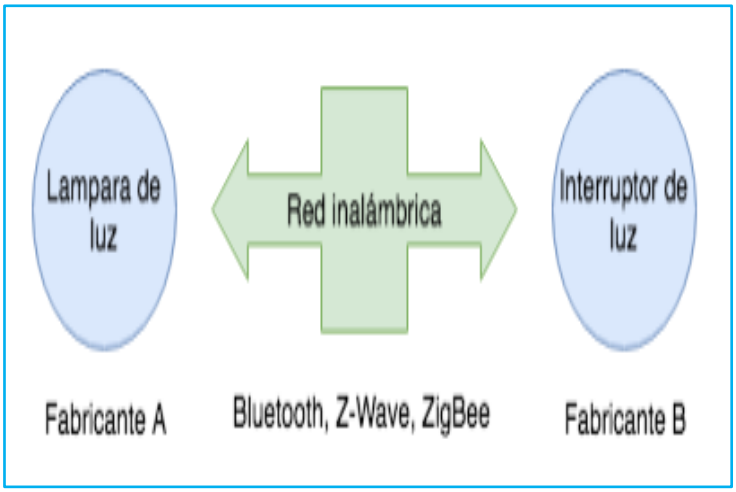
Dentro de los modelos de comunicación del IoT se encuentran:

4.1.1.1 COMUNICACIONES DISPOSITIVO A DISPOSITIVO:

Es la comunicación directa entre dispositivos puede ser dos o más de ellos sin un intermediario. Se comunican por diferentes tipos de redes como la IP o Internet.

Esta comunicación permite conectarse a un protocolo para intercambiar información que permita cumplir la función, esto es comúnmente usado en la automatización del hogar como las lámparas, interruptores, termostatos o cerraduras.[13]
La siguiente imagen muestra una comunicación directa la cual se puede realizar por medio de los protocolos Bluetooth, Z-Wave o ZigBee.

Figura 11 – Comunicación Dispositivo a Dispositivo



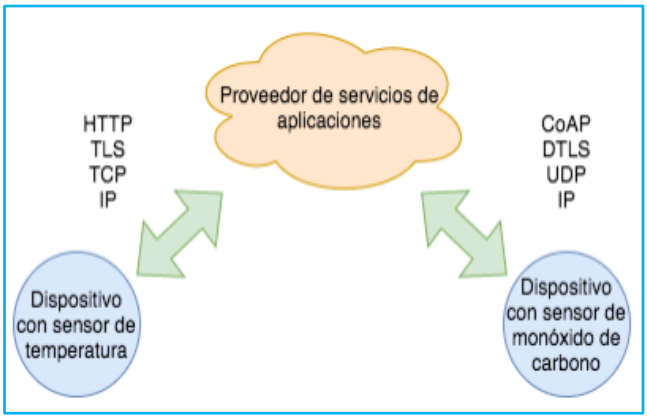
Fuente: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

[13] WHAT IP MEANS AND HOW IT WORKS. [en línea]. IGNACIO MADRID. [Fecha de consulta 26 de marzo de 2020] Disponible en: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

4.1.1.2 COMUNICACIONES DISPOSITIVO A NUBE:

En este modelo el dispositivo tiene conexión directa con un servicio en la nube como un proveedor de servicio que permita el intercambio de datos y controlar el tráfico de los mensajes, como las conexiones por cable Ethernet o WiFi que establece una conexión entre dispositivos y la red IP que finalmente se conecta a un servicio en la nube como lo muestra la siguiente gráfica [14]

Figura 12 – Comunicación Dispositivo a Nube



Fuente: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

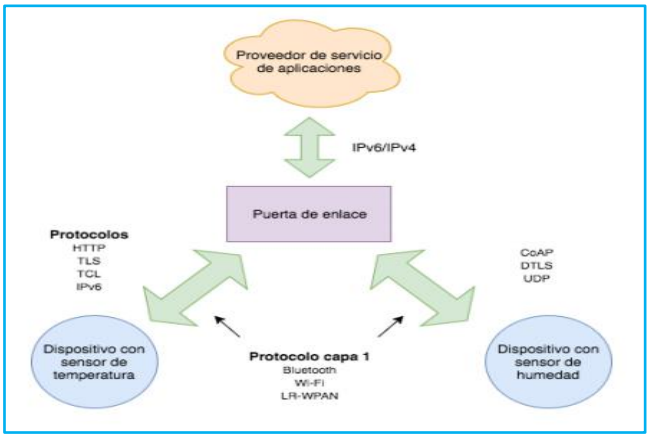
4.1.1.3 COMUNICACIONES DISPOSITIVO A PUERTA DE ENLACE:

En este modelo los dispositivos IoT se conectan a través de in servicio ALG ubicado en otro dispositivo, este cumple con la función de túnel para que el dispositivo IoT pueda llegar a un servicio en la nube, es decir, que existe un software de aplicación que funciona en otro dispositivo IoT que actúa como intermediario entre el dispositivo y el servicio en la nube brindando seguridad y otras funciones.[13]

---

[14] WHAT IP MEANS AND HOW IT WORKS. [en línea]. IGNACIO MADRID. [Fecha de consulta 26 de marzo de 2020] Disponible en: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

Figura 13 – Comunicación Dispositivo a Nube



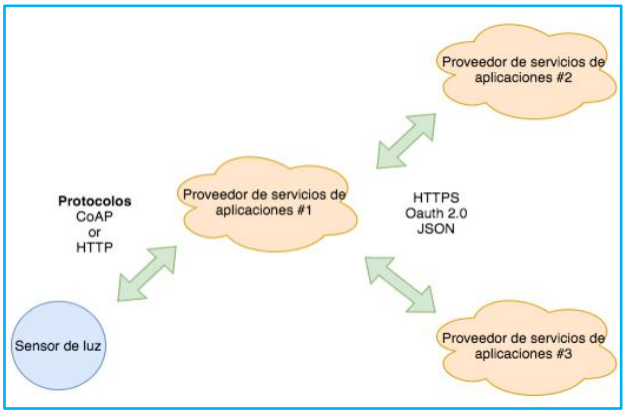
Fuente: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

4.1.1.4 INTERCAMBIO DE DATOS BACK-END:

Este hace referencia a una maquina comunicacional que le permite al usuario exportar y analizar la información de dispositivos inteligentes desde un servicio en la nube combinado con otras fuentes de datos, el servicio en la nube se encarga de recolectar la información de un dispositivo IoT.[15]

[15] WHAT IP MEANS AND HOW IT WORKS. [en línea]. IGNACIO MADRID. [Fecha de consulta 26 de marzo de 2020] Disponible en: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

Figura 14 – Comunicación Dispositivo a Nube



Fuente: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

4.2 MARCO LEGAL

Existen pocas reformas federales de seguridad, lo que indica que el Congreso Americano no se centrará en las regulaciones de IoT en 2020. Lo cual significa que la ley de Mejora de Ciberseguridad de IoT de 2019, presentada en marzo, es lo más probable que no se convierta en ley. Los esfuerzos de la ley es salvaguardar la seguridad gubernamental al establecer estándares de fabricación de IoT para todos los proveedores gubernamentales. Aun así, eso no significa que la acción sobre la seguridad de IoT no se lleve a cabo en el 2020.[16]

La SB 327 del estado de tecnología pesada aprobada a fines del 2018 se convirtió en la primera ley de seguridad específica, como exigir a los consumidores que modifiquen las contraseñas de seguridad que vienen de fábrica en los dispositivos. La última investigación realizada en el mercado estima que habrá 8 mil millones de asistentes de voz digital en uso para el 2023 y el 2020 ha demostrado un aumento en la demanda.

El gobierno está tomando medidas que ayuden a garantizar la privacidad y la seguridad. El reglamento general de protección de datos (GDPR) de la unión europea y la ley de privacidad del consumidor de california (CCPA) son ejemplos que requieren que los proveedores soliciten los permisos para recopilar datos y brinden la seguridad adecuada para protegerlos.

Actualmente también está apareciendo una regulación que requiere estándares mínimos de seguridad para los dispositivos conectados a una red IoT, por ejemplo, en California se requiere que cada dispositivo tenga una contraseña única lisa para usar y que solo recopile los datos necesarios para completar su función aunque los gobiernos tratan de generar leyes y normas que regulen el tratamiento de la información es de cada

[16] Pensamientos y tecnología, El Origen Del IoT. [en línea]. Bruno Cendón. [Fecha de consulta 10 de junio de 2020]. Disponible en: http://www.bcendon.com/el-origen-del-iot/

consumidor directo o indirecto de estos servicios garantizar que la seguridad y la privacidad se mantenga y sea respetada en todo momento. La tecnología del reconocimiento facial fue detenida cuando se implementó en lugares públicos debido a los sesgos raciales y resultados inexactos.

En Colombia, el Gobierno redactó la nueva Ley de modernización del sector de las Tecnologías de la Información y las Comunicaciones (TIC), sancionada el pasado mes de julio del 2019. La Ley TIC, tiene dentro de sus principales objetivos generar un ambiente propicio para que se logre una mayor inversión de empresas de telecomunicaciones que se traduzca en el despliegue de redes; ofrecer mayor certidumbre jurídica para los nuevos inversionistas, y flexibilizar las condiciones de concesión de espectro, además de introducir reformas importantes a nivel institucional.[17]

[17] La nueva Ley TIC y el avance en conectividad en Colombia. [en línea] . MINTIC. [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los-Medios/106166:La-nueva-Ley-TIC-y-el-avance-en-conectividad-en-Colombia.

5. DISEÑO METODOLÓGICO

El enfoque metodológico que se le está dando a esta monografía es desarrollar los objetivos a través de consultas sobre documentos académicos e informes que permitan recopilar la mayor información posible sobre la seguridad del internet de las cosas y la evolución que ha presentado desde que comenzó a utilizarse el término, el avance al tiempo real y las propuestas para salvaguardar la información en el futuro.

6. DESARROLLO DE LOS OBJETIVOS

Tomando como referencia el objetivo principal el cual tiene como fin analizar los riesgos y vulnerabilidades a los cuales están expuestos los dispositivos que se encuentran conectados a una red IoT se procede con el desarrollo de los objetivos que permitirán identificar y llevar a cabo esta investigación.

6.1 REVISIÓN DOCUMENTAL REFERENTE A LA TECNOLOGÍA DE LA IOT

6.1.1 Generalidades

El IoT se representa como abstracto en su concepto, aunque ha llegado a ser popular en los últimos tiempos. Lo que quiere representar le da honor a su título, cosas de uso diario conectados a internet pero que su definición es más profunda en realidad. En otras palabras, es una red de objetos físicos, máquinas, electrodomésticos y más que utiliza sensores APIs para conectarse e intercambiar información por internet.

El internet de las cosas les apuesta a objetos que hasta entonces se conectaban por medio de circuitos cerrados y les permite conectarse ahora por medio del uso de la red de redes. No existe una palabra que defina como tal este concepto, pero se puede decir que es una red que permite la interconexión de objetos físicos por medio del internet. Estos objetos gracias a su conexión en sistemas embebidos permiten que tengan una forma amigable de programación para eventos específicos o tareas que pueden ser asignadas remotamente.

La columna vertebral de este sistema si se puede llamar de esta forma o el cerebro de la operación son los sistemas embebidos, dichos sistemas son basados en chips y circuitos que comparados con un teléfono inteligente puede parecernos elemental, pero cuentan con las herramientas y las capacidades para cumplir con las funciones específicas para las cuales fueron creadas. Cada uno de estos objetos para su funcionamiento cuenta con

una IP específica mediante la cual recibe instrucciones y de esta forma puede enviar y recibir información a un servidor remoto.[18]

En la siguiente imagen se puede observar un esquema de conexión en una vivienda inteligente la cual es controlada por medio de un dispositivo móvil bien sea en este caso un celular o una tablet.

Figura 15 - El Internet de las cosas IoT

Fuente: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

Se conocen como dispositivos IoT a todo lo conectado en una casa inteligente, como son los termostatos, interruptores de luz, cerraduras, cámaras de seguridad y otros electrodomésticos y aparatos inteligentes son dispositivos IoT, además de vehículos autónomos y algunas otras tecnologías.

Pero no es solo la idea de un dispositivo o un hogar inteligente, la tecnología va más allá de todo esto hasta el punto de nombrar ciudades inteligentes o Smart City, el acceso a las empresa o grandes edificios sistematizados, por medio de huellas, reconocimientos faciales o sensores, en cuanto a las ciudades estas tendrán la posibilidad de intercambiar

[18] ¿Qué es el Internet de las Cosas? Todo lo que necesitas saber sobre IoT. [en línea]. Jorge López, DIGITAL TRENDS. [Fecha de consulta: 16 de febrero de 2021]. Disponible en: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

información entre ellas de manera tecnológica sin necesidad muchas veces de una presencia humana se puede tener la información deseada.

Figura 16 - El Futuro del IoT

Fuente: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

Son muchos los entornos donde pueden ser aplicado el internet de las cosas a continuación en la siguiente tabla se detallarán algunos de ellos:

Tabla 3 – Entornos de aplicación del IoT

Industria	Descripción	Ejemplo de uso
Hogar	Edificios, casas	Electrodomésticos, seguridad en el hogar, domótica.
Salud	Dispositivos de monitoreo, dispositivos adheridos al cuerpo o incrustados en él.	Aparatos para monitoreo de signos vitales, marcapasos, bombas de insulina, aplicaciones para discapacitados.
Agricultura	Soluciones integradas para la agricultura y cuidado del medio ambiente	Sensores para fruta y ganado, drones, invernaderos inteligentes, tractores inteligentes.
Fabricas	Dispositivos para monitoreo para la mercancía o fabricación.	Estanterías inteligentes, puertas inteligentes, carretillas anti-accidentes, impresoras 3D, robots colaborativos,
Marketing	Estrategias de publicidad y fidelización	CRM, personalización, recolección de datos, publicidad avanzada,
Big Data	Recolección de información	Los dispositivos conectados comparten datos de uso y estadísticas de consumo
Transporte	Sistema dentro de vehículos	Parqueo automático, vehículos con conductor automático, conexión entre la computadora del vehículo y una app, geolocalización.

Fuente: Autor del documento

Siguiendo con las estadísticas otras fuentes afirman que para el 2025 serán alrededor de 21 billones de dispositivos en conexión o tal vez mayor en mayor cantidad, en cuanto a su expansión aumenta más son los involucrados en este mundo, hogares inteligentes se

encuentran entre los más soñados y el sueño de tenerlos implica renovar dispositivos o electrodomésticos.

Microsoft en uno de sus informes afirma que el 94% de las empresas usarán IoT para fines de 2021. El informe también comprobó que IoT ya es una parte esencial en importantes industrias de fabricación, comercio y transporte, gobierno y atención médica.

“El crecimiento de IoT no muestra signos de desaceleración: se prevé que la adopción aumente en 9 puntos en los próximos dos años, lo que significa que el 94% de las empresas utilizarán IoT para fines de 2021″, señala el documento.

Microsoft contrató a Hypothesis Group para llevar a cabo la investigación durante la primera mitad del 2019 Según explica Windows Central, y los datos provienen de una encuesta realizada en línea que duró alrededor de 20 minutos con más de 3,000 representantes ejecutivos de empresas a nivel mundial, tomando como eje los Estados Unidos, el Reino Unido, Alemania, Francia, China y Japón.

El Internet de las Cosas es considerado además una espada de doble filo ya que puede llevarse a un problema de enfoque. Las "cosas" pueden adoptar fácilmente gran variedad de formas y es precisamente esta variabilidad la que se convierte a la vez en una bendición y una maldición. Dentro de todo esto existen 6 características que resaltan del internet de las cosas:

- **Hardware y Software:** la combinación que genera la **"chispa"** que produce un dispositivo inteligente.

- **La conectividad:** se refiere a mucho más que una conexión WiFi y cargar o enviar información a la web. La conectividad es lo que hace al internet de las cosas y toda su potencia. La conectividad permite **compatibilidad y acceso a la red**, sea cual sea el medio que le rodea.

- **Sensibilidad:** gracias a los sentidos existe la capacidad de interaccionar día a día para sobrevivir. **Los sensores son los encargados de transportar esta visión a las máquinas**. Las diferentes tecnologías de detección y reconocimiento proporcionan los medios para crear las experiencias.

- **Interacción:** gracias a la interacción se puede establecer la **comunicación** entre el mundo físico, las personas y las máquinas.

- **Energía:** sin energía no se puede hacer funcionar los dispositivos en la vida real. El almacenamiento de energía tiende a ser complicado y si se hace uso de las baterías estas tienen un tiempo limitado de vida útil. Además.[19] (Ricardo Vega, 2015)

Seguridad:

Siendo la seguridad el principal objetivo de esta monografía, garantizar la seguridad, la confiabilidad, la resiliencia y la estabilidad de las aplicaciones y servicios de internet es fundamental para fomentar la confianza y el uso de internet.

A medida que se conectan más dispositivos a internet, surgen nuevas oportunidades para explotar potenciales vulnerabilidades de seguridad, los dispositivos mal asegurados son puntos de entrada a los ciber ataques, permitiendo que se reprogramen dispositivos o se perjudique su funcionamiento.

Los desafíos que impone la competitividad de los costos y las limitaciones técnicas del IoT hace que para los fabricantes de los dispositivos no sea fácil diseñar funciones de

[19] 6 CARACTERÍSTICAS CLAVE DEL INTERNET DE LAS COSAS [en línea] Ricardo Vega. [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://ricveal.com/blog/6-caracteristicas-clave-del-internet-de-las-cosas

seguridad adecuadas lo cual a largo plazo genera vulnerabilidades en la seguridad y dificultad en el mantenimiento.

Para complicar más las cosas en un mundo hiperconectado la capacidad de funcionar diariamente sin dispositivos o sistemas conectados a internet tiende a desaparecer. Actualmente poco se consigue en el mercado un dispositivo sin conexión, cada vez existe más dependencia de los dispositivos conectados a la IoT para servicios básicos o esenciales por lo que es requerido que los dispositivos sean seguros aun reconociendo que ningún dispositivo puede llegar a ser 100% seguro.

Esta es la razón por la cual los dispositivos y servicios de la IoT debe considerarse un punto crítico y no puede ser de tipo binario seguro / inseguro. Por el contrario, resulta útil conceptualizar la seguridad del IoT como un espectro de vulnerabilidad según los dispositivos.

La seguridad general y la resiliencia del IoT depende en gran parte de cómo se evalué y se gestione el riesgo de seguridad, esta se puede medir en función del riesgo en el que se vea comprometido, el daño que provocaría, el tiempo y los recursos necesarios para lograr un nivel de protección. Si un usuario no puede tolerar un alto grado de riesgo, por ejemplo, como un operador de un sistema de control de tráfico o una persona a quien se le ha implantado un dispositivo médico que está conectado a internet. Puede que el usuario deba gastar una cantidad considerada de recursos para proteger el sistema o el dispositivo contra un ataque.

Del mismo modo si el usuario no tiene la precaución si la nevera pueda ser hackeada y utilizada para enviar spam no invertirá en un modelo que seguridad que tenga un diseño sofisticado si esto aumenta el valor monetario del dispositivo.

Es aquí donde entran en juego diferentes factores los cuales incluyen una comprensión clara de los riesgos de seguridad actuales y futuros, la estimación d ellos costos

económicos y otros tipos de daños si estos riesgos se materializan, dando como mitigación de los riesgos el costo estimado.

Los desarrolladores de objetos inteligentes para el internet de las cosas deben garantizar que los usuarios no expongan la información de sus usuarios ni de otras personas a daños potenciales. Los fabricantes reducen costos, su complejidad y su tiempo de comercialización. Hoy en día es común encontrar dispositivos del IoT de volumen alto y bajo margen de ganancias lo cual representa un alto costo adicional para los productos embebidos ya que añadir más procesador y memoria para garantizar la seguridad le restaría competitividad al dispositivo.[20]

A nivel económico el resultado de la falta de seguridad en los dispositivos de la IoT puede generar una externalidad negativa [24] donde se imponen una o más partes sobre otras, como por ejemplo la contaminación del medio ambiente, donde los costos de los daños y la limpieza (externalidades negativas) resultado de las acciones de los contaminantes son asumidos por otras partes.

Bruce Schneier comenta que en el caso de la seguridad de la información surge una externalidad cuando el que crea el producto no cubre los costos que ocasionan las inseguridades, una ley de responsabilidad puede convencer al vendedor de que tome en cuenta la externalidad y desarrolle productos con un alto estándar de seguridad, las consideraciones de seguridad aquí planteadas no son nuevas en el contexto de la

[20] THE GUARDIAN: The internet of things: convenience at a price. [en línea] NIKOLE KOBIE. [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security

tecnología de la información, pero la magnitud de los desafíos que pueden surgir en la implementación de la IoT las hacen significativas.[21]
Los desafíos pueden tener una clasificación tal como:

- Muchos dispositivos IoT están diseñados para ser usados o desplegados en una escala masiva superior a la de un dispositivo tradicional conectado a internet.

- El potencial de enlaces interconectados entre estos dispositivos no tiene precedentes. Muchos de estos dispositivos pueden establecer enlaces y comunicaciones con otros dispositivos por lo tanto puede ser necesario considerar las herramientas, estrategias y métodos asociadas con la seguridad del IoT.

- La mayoría de los desarrollos de la IoT consistirán en las colecciones de dispositivos idénticos, esta homogeneidad amplifica el potencial de impacto de cualquier vulnerabilidad de seguridad por las características que todos los dispositivos manejan.

- Los dispositivos desarrollados tienen una vida útil superior a la que se espera para un equipo tecnológico. Estos dispositivos se pueden desplegar en situaciones que harían imposible una reconfiguración o actualización.

- Esto muestra que los mecanismos de seguridad que son adecuados en el momento en que son desarrollados no podrían ser útiles en el transcurso de su vida útil y a medida que las amenazas a la seguridad evolucionan, logrando que se creen vulnerabilidades que puedan persistir durante mucho tiempo.

[21] Information Security and Externalities. [en línea]. Bruce. Schneier. [Fecha de consulta 2 de octubre de 2020]. ENISA (European Network and Information Security Agency) Quarterly: Disponible en: https://www.schneier.com/essays/archives/2007/01/information_security_1.html

6.1.2 Arquitectura IoT

El internet de las cosas – IoT trabaja por medio de dispositivos conectados a internet como su nombre lo indica, por lo tanto, es importante conocer un poco sobre el modelo OSI antes de plasmar la arquitectura y las capas sobre las que el IoT trabaja.

6.1.2.1 Modelo OSI

Fue desarrollado por ISO la organización internacional de normas con el fin de generar la estandarización de protocolos a nivel internacional por medio de capas, fue revisado en 1995 y llamado Open System Interconnection (OSI) o interconexión de sistemas abiertos en español.[22]

Su objetivo es lograr la conexión entre los sistemas de comunicación, está dividido en total por siete capas y cada una de ellas cumple una función la cual se detalla a continuación en la siguiente tabla:

[22] DISEÑO DE UNA RED DE IoT PARA EL HOGAR: Internet of Things (IoT). [en línea]. YOBANY ENRIQUE CHITIVA BERNAL. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/17670/1/2020_diseno_red_iot.pdf

Tabla 4 – Capa de Red y su descripción

Capa	Descripción
7. Capa de Aplicación	- Es la más cercana al usuario final. - Proporciona la interfaz entre la aplicación usada para la comunicación y la red sobre la cual se transmiten los mensajes. - Incluye las funciones de administración - Pertenecen aplicaciones como: correo electrónico, conexión remota, servidores web, transferencias de ficheros
6. Capa de presentación	- Da formato a los datos del dispositivo origen y de esta forma lograr que el dispositivo destino lo pueda interpretar. - Comprime datos para que el dispositivo destino pueda descomprimirlos. - Encripta los datos en su transmisión y desencripta al encontrarse en el destino.
5. Capa de sesión	- Control sobre la comunicación entre las aplicaciones del origen y destino. - Control de diálogo (Full dúplex o half dúplex) - Agrupamiento en el flujo de datos - Recuperación de datos en el último punto de comprobación
4. Capa de transporte	- Mantiene y rastrea la comunicación entre el host origen y destino de manera individual. - Segmenta, administra y rearma los segmentos de los datos de otras capas - identifica a que segmento pertenece cada aplicación o datos recibidos o enviados.
3. Capa de Red	- Direcciona dispositivos finales - Encapsula con ayuda del protocolo PDU la dirección IP de los hosts de origen y destino. - Enruta el camino para el envío de paquetes a otras redes. - Protocolos de internet usados: IPv4 – IPv6
2. Capa Enlace de datos	- Intercambio de datos entre nodos por un medio de red físico - Activa, mantiene y desactiva el enlace - Detección y control de errores (Control de enlace lógico LLC – Control de acceso al medio MAC)
1. Capa Física	- Define las propiedades y características del medio de transmisión - Contienen la información necesaria para llegar al destino y reorganizarla en el receptor final. - Define las reglas que sincronizan y temporizan la comunicación entre el origen y el destino. También define la velocidad de transmisión

Fuente: Autor del documento

Además del modelo OSI también está el modelo TCP/IP, el modelo OSI es el fácil de entender, pero el realmente utilizado es el modelo TCP/IP el cual reduce las siete capas del modelo OSI en cuatro, las cuales comparadas con el modelo OSI quedarían de la siguiente manera y a su vez se detallan los protocolos que intervienen en estas:[23]

Tabla 4 – Modelo OSI vs Modelo TCP/IP y Protocolos

Capas OSI	Protocolos				Capas Modelo TCP/IP
7. Capa de Aplicación	HTTP	MTP	DHCP	DNS	4. Capa de Aplicación
6. Capa de presentación	ASCII	JPEG	MP3	SSL	
5. Capa de sesión	RCP	NetBIOS		SMB	
4. Capa de transporte	TCP		UDP		3. Capa de transporte
3. Capa de Red	IPv4	IPv6	ARP	ICMP	2. Capa de Internet
2. Capa Enlace de datos	VLAN	Ethernet		PPP	1. Capa Acceso red
1. Capa Física	RJ45	802.11	RG232	USB	

Fuente: Autor del documento

6.1.2.2 Arquitectura IOT a 3 capas

IoT maneja también una arquitectura de capas la cual incluye aspectos físicos (cosas) y aspectos virtuales que hacen referencia a los protocolos de comunicación y los servicios.

Este diseño de arquitectura por niveles permite la mejora en la comprensión y permite visualizar de forma global como funciona cada aspecto antes de ser integrado en una aplicación IoT.[24] (IBM, 2020)

[23] Networking I: El modelo OSI. [en línea] José Ramón Maseda Lozano. [16 de junio de 2021]. Disponible en: https://itadmins.es/networking-i-el-modelo-osi/

[24] Simplify the development of your IoT solutions with IoT architectures. IBM. . [en línea]. Strategies for creating scalable, flexible, and robust IoT solutions [Fecha de consulta 26 de marzo de 2020] Disponible en: https://developer.ibm.com/articles/iot-lp201-iot-architectures/

La arquitectura a 3 capas es la más simple de todas las arquitecturas y la primera en ser utilizada, está enfocada técnicamente y centralizada sobre la organización de los elementos en la red IoT lo que la caracteriza. Los 3 bloques descritos en la tabla anterior se detallan a continuación:

- **Capa de Percepción:** Es conocida como la capa sensorial donde las capas identifican su entorno, obteniendo información del entorno físico para interactuar con este.

- **Capa de Internet:** Capa central, que tiene como función principal transmitir la información que se recibe de la capa de percepción, además es la que se encarga de interconectar los dispositivos con otras redes.

- **Capa de Aplicación:** Capa del usuario final, por medio de esta el usuario tiene visible los servicios y aplicaciones que los dispositivos ofrecen.

La siguiente tabla mostrará la comparación entre las capas del modelo OSI con las capas del modelo IoT y los protocolos que esta utiliza para su servicio y funcionamiento:

Tabla 4 – Modelo OSI vs Modelo IoT arquitectura a 3 capas y Protocolos

<table>
<tr><th>Capas Modelo OSI</th><th colspan="3">Protocolos</th><th>Capas Modelo IoT</th></tr>
<tr><td>7. Capa de Aplicación</td><td colspan="2" rowspan="3">HTTP COAP XMPP AMQP VSCP STOMP DDS OPENWIRE</td><td rowspan="5">ZWAVE ZIGBEE THREAD</td><td rowspan="3">3. Capa de Aplicación</td></tr>
<tr><td>6. Capa de presentación</td></tr>
<tr><td>5. Capa de sesión</td></tr>
<tr><td>4. Capa de transporte</td><td rowspan="2">UDPTCP 6LOWWPAN IPv6 IPv4</td><td rowspan="2">SIXFOX</td><td rowspan="2">2. Capa de Internet</td></tr>
<tr><td>3. Capa de Red</td></tr>
<tr><td>2. Capa Enlace de datos</td><td rowspan="2">WIFI LORA LORAWAN BLUETOOTH RFID NFC ETHERNET IEEE 802.15.4 4G 5G</td><td rowspan="2">SIXFOX</td><td rowspan="2">1. Capa de Percepción</td></tr>
<tr><td>1. Capa Física</td></tr>
</table>

Fuente: Autor del documento

Protocolo IP: Dentro de todos los protocolos utilizados este es el principal, al tener conexión para transmitir, navegar, descargar o enviar un correo, videos e imágenes o la interacción de los dispositivos con la red usa el protocolo IP o Protocolo de internet que permite la comunicación entre los dispositivos y el internet por medio de paquetes y un esquema de direccionamiento.[25]

Sin embargo, son muchos los protocolos que hoy en día pueden ser utilizados por la IoT como lo es la tecnología de conexión y transmisión inalámbrica de datos como el WiFi, el Bluethooth o las redes 3G, 4G y la actual 5G.

Dependiendo de su uso se pueden establecer factores como la velocidad, el alcance, la y la seguridad, bajo estos criterios se puede decidir sobre cuál es la mejor alternativa a la hora de elegir una conexión u otra. A continuación, la tabla 6 muestra las diferentes alternativas de conexión que pueden ser útiles en el IoT y que cada fabricante puede comparar al momento de crear un dispositivo:

[25] Bradley Mitchell. Understanding Transmission Control Protocol/Internet Protocol (TCP/IP). LIFE WIRE. (2020).

Tabla 6 – Comparación de protocolos más usados para IoT

Protocolo	Estándar	Frecuencia	Alcance	Velocidad Transferencia
WiFi	802.11 ac	5 GHz	15 metros en interiores y 30 metros en exteriores Aprox	hasta en 1.300 Mbps.
Bluetooth	Bluetooth 5	2.4 GHz	50-150 Mts Aprox	2000Mbps
Z-Wave	Z-Wave Alliance ZAD12837 / ITU-T G.9959	900 MHz	100 metros	250kbps
ZigBee	ZigBee 3.0 basado en IEEE 802.15.4	2.4GHz	10 - 20 metros	250 kbit/s.
Thread	Thread, basado en IEEE802.15.4 y 6LowPAN	2,4GHz (ISM)	N/A	N/A
LoRa WAN	LoRaWAN	Varias	2-5km (entorno urbano), 15km (entorno rural)	0,3-50 kbps.
NFC	ISO/IEC 18000-3	13.56MHz (ISM)	10cm	100–420kbps
SigFox	Sigfox	900MHz	30-50km (ambientes rurales), 3-10km (ambientes urbanos)	10-1000bps
Red de telefonía movil	1G, 2G, 2.5G, 2.75G, 3G, 3.5G, 3.7G, 3.9, 4G, 5G (Sin confirmar)	900/1800/1900/2100	Hasta 3.5 km para GSM Hasta 200 km para HSPA	35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)
Neul	Neul	900MHz (ISM), 458MHz (UK), 470-790MHz	10km	100kbps
6LoWPAN	RFC6282	Bluetooth Smart (2.4GHz), ZigBee o comunicación RF de bajo consumo (sub-1GHz)	N/A	N/A

Fuente:http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

6.1.2.3 Protocolo MQTT

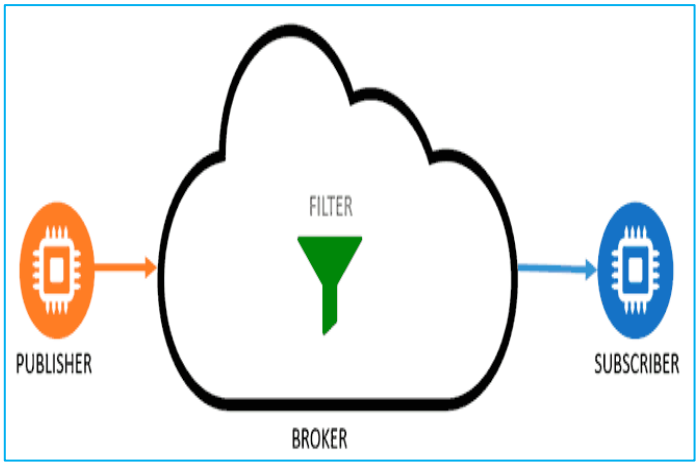
Es un protocolo de mensajería utilizado principalmente para los dispositivos IoT que se utiliza sobre la pila TCP/IP.

MQ: Telemetry Transport, es un protocolo de comunicación M2M (machine to machine) de tipo message Queue. Basado en la pila TCP/IP como se mencionó anteriormente, indicando que la conexión se mantiene abierta y es utilizada en cada comunicación.

Fue creado por el Dr. Andy Stanford-Clark de IBM y Arlen Nipper de Arcom EN 1999 para conectar dispositivos en la industria petrolera y pasó a ser reconocido como estándar en 2014 según OASIS.

Funciona como servicio de mensajería push con patrón pub/sub conectados a un servidor central denominado bróker.

Figura 17 – Protocolo MQTT



Fuente: https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/

El cliente inicia una conexión TCP/IP con el bróker, el cual se encarga de mantener un registro de los clientes que se conectan y la conexión se mantiene abierta hasta que el

cliente finaliza. Los puertos por los que trabaja este protocolo por defecto son: 1883 y 8883 cuando opera por TLS.

La seguridad se maneja por medio de transporte SSL/TLS y autenticación por usuario o contraseña por medio de certificados.[26]

6.1.2.4 FOG COMPUTING O COMPUTACION EN LA NIEBLA

Es conocida como una plataforma virtualizada que provee servicios y almacenamiento a usuarios de una red IoT.

El consorcio OpenFog detalla los siguientes pilares para la computación en la niebla:

1. Seguridad
2. Escalabilidad
3. Apertura
4. Autonomía
5. Fiabilidad, disponibilidad y capacidad de ofrecer servicios
6. Agilidad
7. Jerarquía
8. Capacidad de programación.[27] (ACIS)

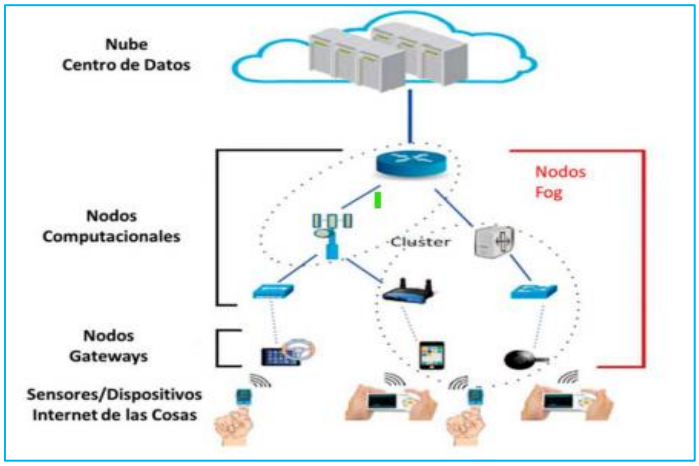
La grafica que se detalla a continuación muestra cómo se desarrolla el ambiente de la configuración en la niebla en sus diferentes capas:

---

[26] ¿Qué es MQTT? Su importancia como protocolo IoT. [en línea]. Zona Geek, Ingeniería, informática y diseño. Luis Llamas . [Fecha de consulta: 26 de junio de 2021]. Disponible en: https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/

[27] Un acercamiento a Fog computing. [en línea]. ACIS. Conceptos claves, ventajas y principales desafíos: (s.f.). Disponible en: https://sistemas.acis.org.co/index.php/sistemas/article/download/121/94/

Figura 18 – Ambiente de la configuración en la niebla



Fuente: 121-Texto del artículo-355-1-10-20200916
https://sistemas.acis.org.co/index.php/sistemas/article/download/121/94/

El Fog Computing tiene como fin la mejora de la eficiencia por medio del procesamiento directo de los datos en una red, logrando la reducción de datos a transferir, pero manteniendo también la información acerca del usuario con el fin de aumentar la seguridad de estos. Dada la cantidad de cosas (dispositivos) conectados a una red procesando información, este modelo lograra que no se genere una sobrecarga de red innecesaria evitando caídas por rendimiento o seguridad.[28]

Este modelo de computación en la niebla o Fog Computing como fue mencionado anteriormente dentro de sus ventajas tienen como fin reducir el tráfico en la red brindando una plataforma de análisis y filtrado de la generación de datos de los sensores, esto es útil para aplicaciones que requieren ser procesadas en tiempo real.

Otras ventajas van ligadas también a la sensibilidad de la ubicación, bajo consumo de energía, seguridad y protección de la privacidad, facilitando la administración del control

[28] UNAB IMPLEMENTACIÓN DE UNA ARQUITECTURA FOG COMPUTING. [en línea]. CASTELLANOS, J. P. [Fecha de consulta 10 de junio de 2021]. Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/11908/2020_Tesis_Javier_Pinzon_Castellanos.pdf?sequence=1&isAllowed=y

de los usuarios y dispositivos en cuanto al acceso y la ubicación. Con este modelo es muy fácil gestionar los datos provenientes de los dispositivos conectados a una res IoT.[29]

6.2 CARACTERIZACIÓN DE PRINCIPALES VULNERABILIDADES A LAS QUE SE ENCUENTRAN EXPUESTOS LOS DISPOSITIVOS EN UNA RED IOT

Vulnerabilidad es el riesgo que un sistema, persona u objeto puede sufrir frente a un peligro, la palabra se origina del latín vulnerabilis vulnus: herida y el sufijo abilis: posibilidad, por lo tanto, indica una posibilidad mayor de ser herido etimológicamente. Los sinónimos asociados a esta son debilidad, flaqueza, riesgo, amenaza y susceptibilidad.

Una **vulnerabilidad informática** hace referencia a los puntos débiles de un sistema de cómputo donde su seguridad no cuenta con las defensas necesarias en caso de un ataque poniendo en riesgo la integridad, disponibilidad o confidencialidad de la información, por lo que es necesario encontrarlas y eliminarlas tan rápido como sea posible. El origen de estas se puede presentar por: fallos en diseños, errores en configuración o carencia de procedimientos.[30]

Ahondando en el tema central origen de esta monografía y luego de conocer la definición de vulnerabilidad, en este punto se clasificaron las diferentes vulnerabilidades a las

[29] Asrar A. Baktyan, A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective. European Union Digital Library. A. T. (2018).

[30] Significados. (2021). [en linea] Significado de. Obtenido de [consultado 15 septiembre 2020] Qué es: https://www.significados.com/

cuales están expuestos los dispositivos IoT tomando como referencia el OWASP TOP 10 INTERNET OF THINGS[31]

6.2.1 Weak, Guessable, or Hardcoded Passwords

Contraseñas débiles, por defecto o embebidas, contraseñas que por medio de un ataque de fuerza bruta pueden ser capturadas, contraseñas por defecto siendo las mismas en diferentes dispositivos, por su sistema de control son contraseñas muy comunes en dispositivos IoT. Esta vulnerabilidad ya ha sido explotada en la red por medio de los dispositivos conectados, los cuales tienen como fin generar ataques de denegación de servicio por medio de bots que tenían una contraseña por defecto en sus accesos.

Esto puede ser solucionado utilizando contraseñas diferentes en todos los dispositivos. Asociándose a una cuenta con el fin de evitar que se encuentre embebida.

6.2.2 Insecure Network Services

Evitar servicios de red innecesarios que se ejecutan en segundo plano en el dispositivo expuestos a una red, la explotación de estas vulnerabilidades pone en juego los pilares de la seguridad de la información como lo es la confidencialidad, la disponibilidad o la integridad de esta e incluso acceso remoto al dispositivo.

Esto puede ser solucionado deshabilitando los servicios innecesarios que se ejecuten en segundo plano en cualquiera de los dispositivos.

[31] OWASP Internet of Things. [en línea] OWASP. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

6.2.3 Insecure Ecosystem Interfaces

Interfases inseguras en el ecosistema, las interfaces API en el backend, web o incluso servicios en la nube que puedan estar mal configurados, comprometiendo los dispositivos y componentes gestionados a través de ellas.

Esto puede ser solucionado implementando controles de acceso a las interfases, filtrando las entradas y salidas con medidas de encriptación

6.2.4 Lack of Secure Update Mechanism

Falta de mecanismos de actualización seguros, validación de versiones de firmware en los diferentes dispositivos, falta de notificación sobre los cambios de seguridad incluidos en las actualizaciones generadas en cada actualización. Esto es muy común en el software que manejan los vehículos inteligentes, sobre los cuales ya se han explotado vulnerabilidades muchos de ellos causando accidentes fuertes o incluso que puedan acceder a toda la información del usuario como recorridos.

Esto puede ser solucionado revisando la integridad del firmware y su procedencia antes de ejecutar la instalación.

6.2.5 Use of Insecure or Outdated Components

Uso de componentes inseguros o desactualizados, estos pueden comprometer el dispositivo, la mayoría usan software de terceros o personalizados o componentes de distintos fabricantes, Tal es el caso de algunas referencias de Intel en sus procesadores los cuales están presentando vulnerabilidades.

Esto puede solucionarse si se verifican las actualizaciones en las librerías y que estas no pertenezcan a versiones que en el pasado hayan estado vulnerables al igual que los componentes de hardware utilizados.

6.2.6 Insufficient Privacy Protection

La insuficiente protección de la privacidad, la forma en que la seguridad de los datos se maneja en estos dispositivos es débil y se puede acceder a ella sin solicitar permisos.
Un estudio de la Universidad de Cornell en 2017 encontró que una casa inteligente no es un castillo mostrando vulnerabilidades de privacidad de tráfico de IoT cifrado, dentro de su reporte mostró: “Examinamos cuatro dispositivos domésticos inteligentes de IoT [...] y encontramos que las tasas de tráfico de su red pueden revelar potencialmente interacciones sensibles del usuario incluso cuando el tráfico es cifrado "

Esto puede solucionarse estableciendo políticas que permitan solo acceder a la información necesaria informando sobre a que accede a cada servicio.

6.2.7 Insecure Data Transfer and Storage

Falta de seguridad en el almacenamiento y transferencia de datos, llevar un control en el acceso dentro del ecosistema, es imprescindible utilizar mecanismos de cifrado al manejar datos sensibles.

6.2.8 Lack of Device Management

Inadecuada gestión de dispositivos, controlar la gestión de activos y actualizaciones, monitoreando sistemas y borrado de dispositivos seguros.

6.2.9 Insecure Default Settings

Configuraciones por defecto inseguras, establecer configuraciones que se enfoquen en la protección del sistema aplicando políticas de conexiones y permisos.
Un ejemplo de este tipo de vulnerabilidades se es referente a permisos de archivos incorrectos y servicios expuestos que son ejecutados como root.

6.2.10 Lack of Physical Hardening

Falta de medidas seguras para el acceso físico a los dispositivos tomando en cuenta que si un atacante puede acceder físicamente a un dispositivo las medidas de seguridad no serían válidas. Por medio de escaneo de puertos se pueden identificar qué dispositivos físicos estarían siendo vulnerables al obtener el acceso se puede tener control total de los dispositivos.

Esto se puede solucionar implementando medidas de seguridad a los dispositivos físicos a personas autorizadas implementando medidas adicionales como circuitos cerrados de vigilancia.[32]

6.3 DESCRIPCIÓN DE LOS DIFERENTES TIPOS DE ATAQUES QUE SE PRESENTAN EN DISPOSITIVOS CONECTADOS A UNA RED IOT

Como se detalló en el apartado anterior las vulnerabilidades son factibles de ser aprovechadas y explotadas por cibercriminales con conocimientos, para realizar distintos ataques digitales no solamente a dispositivos usuales como televisores, neveras, relojes o celulares, sino también a plantas nucleares, centrales de redes eléctricas, sistemas de ventilación de edificios o cerraduras inteligentes de hoteles o edificios con acceso tecnológico.[33]

A continuación, se detallan algunos ataques presentados dadas las diferentes vulnerabilidades en los dispositivos.[34]

---

[32] OWASP Internet of Things. [en línea] OWASP. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

[33] Seguridad de Internet de las Cosas. [en línea]. Colaborador de TechTarget. [Fecha de consulta 10 de septiembre de 2020]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Seguridad-de-Internet-de-las-Cosas

[34] Hamidreza Damghani, L. D. Classification of Attacks on IoT, 20 de NOVEMBER de 2019.

6.3.1 Ataques de fase

En la capa de percepción de datos se pueden generar diferentes tipos de ataques la fuga de datos, la autenticación, la violación y la soberanía son los principales. [35]

Fuga de datos o violación de datos:

Se puede generar de forma interna o externa, involucrando o no hardware o software, exportar datos de forma no autorizada a un destino no autorizado se denomina fuga de datos, suelen ser ejecutados principalmente por personal interno de una organización generando una fuerte amenaza para la confiabilidad.[33]

Pérdida de datos:

Diferente a la fuga, la pérdida de datos se puede generar debido a fallas de software o hardware, incluso desastres naturales.[33]

Autenticación de datos:

Los datos pueden ser falsificados por cualquier intruso, se debe garantizar que estos datos sean percibidos desde usuarios legítimos y verificar que los datos no sean alterados en el tráfico.[33]

Un ejemplo de este tipo de ataque es:

Redes eléctricas.

La empresa Calpine fue víctima de ataque en el año 2013, los ciber delincuentes robaron información los planos de 71 estaciones eléctricas, diagramas de red y ubicaciones.[33]

[35] Hamidreza Damghani, L. D. Classification of Attacks on IoT, 20 de NOVEMBER de 2019.

6.3.2 Ataque a la disponibilidad

La disponibilidad es uno de los pilares de la seguridad de la información un ataque de denegación de servicio o DDoS puede ser el causante de una sobrecarga que impida la disponibilidad.[33]

Inundaciones por atacantes:

Por medio de un ataque de denegación de servicio o DDoS se genera inundación con paquetes maliciosos alterando la disponibilidad de la información.[36]

Inundación por legítimos:

La multitud flash genera una sobrecarga causada por usuarios legítimos que solicitan recursos de manera simultánea. [34]

Inundación por Atacantes suplantadores:

Un número de atacantes suplantando identidad, puede detectarse con el reconocimiento de cada solicitud y manteniendo el número de secuencias de las solicitudes y la IP del solicitante.[34]

Inundación por legitimados agresivos:

Este ataque hace referencia a usuarios inquietos que inician de forma repentina solicitudes similares en corto tiempo, ocasionando una sobrecarga y denegación del servicio.[34]

[36] Hamidreza Damghani, L. D. Classification of Attacks on IoT, 20 de NOVEMBER de 2019.

6.3.3 Ataque según la arquitectura

La confiabilidad en este punto es importante, la descarga de datos deliberada por parte de las organizaciones para obtener servicios, pero estas desconocen la ubicación donde se almacena o procesa la información.[34]

Ataque de agujero de gusano:

Es uno de los ataques más populares en IoT conectando dispositivos como relojes, neveras y hasta vehículos, de este tipo se pueden mostrar los siguientes ataques [34]:

Por medio del tablero digital de un vehículo si se tiene acceso a este es posible realizar modificaciones de velocidad y combustible, además de poder tocar la bocina, activar los limpiabrisas o controlar el aire acondicionado entre muchas otras cosas solo con intervenir las redes inalámbricas.[37]

Las llaves de los vehículos ahora contienen un sistema de chips electrónicos que internamente llevan una codificación que puede ser descifrado por medio de una técnica denominada chip slicing. Esta técnica consiste en analizar los pequeños transistores mediante un microscopio y así interferir con el algoritmo que programa la llave.

La mayoría de los vehículos en su **motor** incorpora la unidad de control electrónico o ECU, desde donde controlan las funcionalidades del vehículo como la aceleración, la dirección o los frenos. El software que contiene envía instrucciones a la computadora del vehículo y de esta manera genera alertas.[35]

[37] Hamidreza Damghani, L. D. Classification of Attacks on IoT, 20 de NOVEMBER de 2019.

Abordar todas las cosas en IoT

Falsificando las direcciones IP de las máquinas virtuales los atacantes tienen la posibilidad de implantar máquinas maliciosas para atacar los usuarios de las VM permitiendo acceder a información confidencial para ser usados como fines malintencionados. [35]

Godput

Es un ataque de rendimiento a nivel de una aplicación, donde un número de bits de información entra a un destino determinado por un determinado tiempo.[35]

Botnet

Este ataque es una cantidad de dispositivos conectados a internet donde sus defensas de seguridad fueron violadas y controladas por un usuario malintencionado estos controles se pueden manejar por medio de canales de comunicación como IRC o el HTTP

Backdoor

En este ataque se tiene acceso a la red evitando los controles de acceso mediante puertas traseras en módem o una conexión externa asíncrona.[38]

6.3.4 Ataques basados en componentes

Como se ha mencionado a lo largo de este documento IoT conecta todo a través de una red comunicando datos de tipo confidencial a la distancia, ocasionando que los datos

[38] Hamidreza Damghani, L. D. Classification of Attacks on IoT, 20 de NOVEMBER de 2019.

puedan ser modificados y fabricados mediante cualquier tipo de dispositivos comprometidos.[36]

6.3.5 Ataques basados en protocolos de conectividad

Los objetos conectados a una red IoT manejan dos tipos de conexión, cableada y la inalámbrica, la conexión cableada hace que esta dependa de otro dispositivo para su funcionamiento, mientras que una inalámbrica obtienen su conexión a través de ondas de radio, estas conexiones manejan propiedades como rangos, velocidad, energía y compatibilidad con la topología y el modelo TCP/IP. Los ataques que se pueden generar a través de los protocolos pueden ser [36].

Spoofing

Este ataque se genera cuando las etiquetas maliciosas pretenden ser las etiquetas válidas y obtienen acceso no autorizado generando suplantación de identidad [36].

MITM

Ataque de hombre en el medio puede ocurrir durante la trasmisión de información, donde el atacante intercepta y modifica el canal de comunicación, este tipo de ataque se genera en tiempo real modificando la información ante el destinatario.[36]

Ejemplos de estos tipos de ataques son:

Ataques a Cajeros automáticos:

Barnaby Jack realizó una demostración en vivo de la vulnerabilidad de Windows CE en los cajeros automáticos ATM en la conferencia de seguridad BlackHat que se realizó en Las Vegas, Nevada. El procedimiento fue realizado de la siguiente manera: uso una llave

universal para abrir el cajero y ejecutó mediante un pendrive USB un rootkit, el cual arrojó como resultado final el “Jackpot” o “JackPotting” el cual comenzó de inmediato a arrojar dinero.[39]

Ataque a implantes físicos:

Siendo empleado de McAfee Jack realizó un experimento donde tomó control de una bomba de insulina desde 100 metros de distancia, al igual que estas bombas los marcapasos vienen con conectividad inalámbrica que les permite a los hackers tomar el control que permite detenerlos o afectar su funcionamiento.[40]

Hacking a marcapasos

Barnaby Jack fue un pirata informático famoso por el ataque realizado a los cajeros ATM y además provocó mejoras de seguridad para los equipos médicos. Dentro de su especialidad se encontraba hallar fallas en ordenadores pequeños de servicio médico y de implementos bancarios como los cajeros, fue felicitado por su creatividad en las conferencias de hackers y fue quien llegó a decir que era posible matar a un hombre a nueve metros accediendo a su marcapasos[41]

Los fabricantes de Medtronic renovaron la forma en la que diseñan sus productos para evitar intromisiones ya que Jack encontraba vulnerabilidades en los equipos sanitarios.

---

[39] Los ciberataques ponen en riesgo la seguridad de los cajeros automáticos. SEGURILATAM, (2020).

[40] Scientific american: Bomba de insulina es vulnerable a piratas informáticos [en línea]. Jim Finkle. [Fecha de consulta 12 de mayo de 2020] Disponible en: https://www.scientificamerican.com/espanol/noticias/reuters/bomba-de-insulina-es-vulnerable-a-piratas-informaticos/

[41] Fallece Barnaby Jack, el «hacker» que podía atacar dispositivos cardiacos. [en línea]. ABC REDES. (s.f.). Disponible en: https://www.abc.es/tecnologia/redes/20130729/abci-barnaby-jack-hacker-muere-201307291016.html?ref=https://www.google.com/

Antes de su muerte se presentaría en la conferencia de Black Hat denominada un gran evento para hackers donde demostraría cómo manipular de forma inalámbrica marcapasos y otros implantes médicos.

6.4 RESUMEN ANALÍTICO CON LAS MEDIDAS Y MEJORES PRÁCTICAS PARA PROTEGER LA INFORMACIÓN CUANDO ESTÁ SE ENCUENTRA TRANSANDO A TRAVÉS DE ESTOS DISPOSITIVOS.

Se estima que para el 2021 la cantidad de hogares inteligentes en los EE. UU. alcance el 28% y en este 2020 más empresas han optado esta tecnología para sus oficinas, a nivel mundial son muchos los hospitales que están utilizando dispositivos IoT para el monitoreo remoto de los pacientes con ayuda de monitoreos portátiles y sensores de salud, permitiendo rastrear pacientes, personal y equipos como lo hacen los GPS.
Un nuevo pronóstico de International Data Corporation estima que para el 2025, habrá más de 41 mil millones de dispositivos conectados que generarán 80 Zettabytes de datos.

La necesidad de considerar la seguridad de manera proactiva todos los días nunca ha sido tan grande, sobre todo contando con que la cantidad de dispositivos conectados crezca a niveles sin precedentes, pasando de los aproximadamente 20 mil millones y en la actualidad a entre 50 mil millones y 75 mil millones para el 2025.

El abrumador uso de la tecnología en todas las industrias y todos los rincones de la vida crea una gran oportunidad para que los ciberdelincuentes aprovechan, tal y como lo demostró la Bonet Mirai que en 2016 utilizó cientos de miles de dispositivos IoT para lanzar ataques DDoS a los servidores DNS, lo cual paralizó gran parte del internet. A medida que crece el número de dispositivos conectados, los abusos también crecen.

Cuando un dispositivo se conecta a una red IoT está recopilando información y datos de sus usuarios, los cuales podrían ser datos sensibles como personales o hábitos de sueño o de salud o de alimentación. Por lo que la cantidad de datos a asegurar debería estar

entre los principales pensamientos de los usuarios cuando compran estos dispositivos y de los proveedores al ser desarrollados.

ESET a principios del 2018 realizó una encuesta donde su resultado arrojó que el 70% de los usuarios aseguran que los dispositivos que más usan y que se encuentran conectados a una red IoT no son seguros, sin embargo, el 52% afirmó que aun así los compraría. Las cifras anteriormente descritas se ven reflejadas en la gran cantidad de dispositivos IoT que actualmente se encuentran en los hogares y en las compras de los consumidores ya que el 2018 superó la venta de dispositivos inteligentes y aun en el 2020 sigue aumentando, mostrando que hay más de 20 mil millones de dispositivos IoT en el mundo lo cual equivale a que cada persona puede llegar a tener hasta 3 dispositivos en su uso.[42]

Uno de los mayores retos para el IoT en este 2021 es mejorar la seguridad y la privacidad de los dispositivos conectados. Shodan afirma ser el primer motor de búsquedas del Internet de las Cosas IoT y lo han calificado como el motor de búsqueda más aterrador del cibermundo. En 2013 su creador John Mtherly, un bioinformático de Austin – Texas, advirtió que existían alrededor de 500 millones de dispositivos conectados con la típica contraseña preestablecida ‘1234’ o ‘admin’. Como se ha venido mostrando a través de esta monografía la cual pretende demostrar que la privacidad y la seguridad siguen siendo la debilidad del internet de las cosas y cuanto más dispositivos se vuelvan presentes dentro de las organizaciones, mayor será el riesgo, ya que el único agujero de seguridad que presenta el internet de las cosas abre la puerta a múltiples ataques y es un tema clave que los profesionales de IT deberán abordar no solo en este 2020 sino en años futuros.

[42] El 70% de los usuarios cree que los dispositivos IoT no son seguros. [en línea]. ESET. [Fecha de consulta 10 de octubre de 2020] Disponible en: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/el-70-de-los-usuarios-cree-que-los-dispositivos-iot-no-son-seguros-2/

La seguridad de los dispositivos IoT es un tema que debe tratarse en serio para cualquier negocio y el IoTSWC19 dio buena cuenta de ellos, sin embargo, estos desafíos se abordan de manera muy fragmentada aun cuando sus fabricantes dicen que se solucionaran lo único que actualmente se observa es la falta de resultados concretos reales.[43]

Se ha generado también una nueva iniciativa denominada IoTopia la cual pretende colaborar con la industria que propone un marco común para estandarizar el diseño, la certificación, la implementación y la administración de dispositivos IoT. La IoTopia busca una forma coherente de saber qué hace realmente un dispositivo conectado y a quien pertenece.

Por otra parte, investigando sobre la seguridad y los riesgos en IoT algunas estimaciones apuntan a que el mercado de IoT en Europa a finales del 2020 alcanzara los 242 mil millones de Euros. La expansión de esta tecnología aporta muchos beneficios, pero como todo avance tecnológico, también aporta riesgos por lo que uno de los dispositivos conectados necesita estar convenientemente asegurados para evitar intrusiones o hackeos.[44]

Es fundamental comprender que las amenazas de seguridad de la res IoT difieren de los entornos de TI tradicionales, ya que en estos escenarios se centran en la seguridad de los datos, mientras que un incidente de seguridad de IoT puede incomodar a las personas a interrumpir las operaciones, causando daños millonarios solo en pocas horas. En estos

[43] Ataques a la IoT: 10 cosas que debes saber . [en línea]. WELIVE SECURITY. (2016). [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2016/12/21/ataques-a-la-iot-debes-saber/

[44] Seguridad y Riesgos en IoT (Internet de las Cosas). [en línea] NTS. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://www.nts-solutions.com/blog/iot-seguridad.html

casos estos ataques pueden dañar los sistemas que controlan procesos físicos o incluso poner en riesgo la vida de las personas. Algunas investigaciones sugieren que el 55% de los profesionales de TI enumeran la seguridad de IoT como su máxima prioridad.

Los ciberdelincuentes pueden encontrar una manera de explotar información en muchos puntos, desde servidores corporativos hasta almacenamientos en la nube en muchos puntos dentro de un ecosistema IoT. No significa que no se deban usar y volver a otras tecnologías, sino que simplemente se debe tomar conciencia de todo aquello que involucre la seguridad de IoT.

7. CONCLUSIONES

Se construye una revisión documental referente a la tecnología de la IoT donde se detalla su historia, los inicios desde donde se hace el nombramiento por primera vez por parte de Kevin Asthon en el año 2009, de allí en adelante se detalla la historia de la primera vez que un dispositivo fue conectado incluyendo las diferentes compañías que fueron evolucionando con la tecnología y se fueron mostrando cada vez más los diferentes dispositivos conectados a una red IoT siendo el teléfono celular hoy en día el más popular, seguido de los dispositivos del hogar como lo son las casas inteligentes, los electrodomésticos y el circuito cerrado de televisión para la seguridad de los hogares incluidos allí las cerraduras y las futuras ciudades inteligentes contando que existen avances en esta parte. Para esto se consultaron diferentes referentes con el fin de obtener un concepto claro de su origen y su evolución hasta el día de hoy y lo que aún está faltando por evolucionar.

Se caracterizaron y detallaron las diferentes vulnerabilidades a las que pueden estar expuestos estos diferentes dispositivos, pasando por una breve definición sobre las vulnerabilidades y luego se clasifican tomando en cuenta el mayor riesgo que pueden causar si estas llegaran a ser explotadas en algún momento mediante algún escaneo realizado por los diferentes atacantes. El riesgo en el que se encuentran expuestos los usuarios de estos dispositivos conectados a la red IoT.

Por otro lado, se clasifican y se describen los diferentes ataques a los cuales han estado expuestos estos dispositivos mostrando ejemplos reales como los clásicos ataques a cajeros automáticos e incluso ataques a dispositivos médicos como marcapasos. De acuerdo con su clasificación se dividieron en ataques por fase, por disponibilidad, según la arquitectura, basado en componentes y por protocolos.

Se realiza un resumen analítico tomando en cuenta las estadísticas desde su evolución hasta lo que ha avanzado el día de hoy, indicando la evolución estimada

hasta aproximadamente el 2025, también de acuerdo a las investigaciones realizadas en la monografía se muestran cifras de usuarios de los dispositivos, tomando en cuenta cuales y cuántos de ellos conocen y tienen claro el nivel de seguridad que deben tener en cuenta al momento de usar estos dispositivos, referente a la seguridad en los dispositivos se muestra también el porcentaje sobre el cual se encuentra la seguridad en este momento y las métricas que se tienen para mejorarla en los siguientes años, se muestra estadísticamente los niveles de contraseñas que se usan, todo esto con el fin de manera estadística generar conciencia entre los usuarios sobre cuáles son las mejores prácticas a tener en cuenta al momento de usar estos dispositivos conectados a la red IoT.

8. RECOMENDACIONES

Luego de todo lo anterior y tomando como base los objetivos que dieron origen a esta monografía, son muchas las medidas que se pueden aplicar para mitigar los riesgos que pueden derivarse por el uso de los dispositivos, el plan de choque para enfrentarlo es dividir lo que puede salvaguardar la información y los puntos de seguridad que deben ser atendidos dentro de la red IoT.

Una de ellas es que los usuarios deban documentarse sobre que es el IoT, conocer sus orígenes y bajo qué fin se crea la tecnología y los principales usos que se le da en la actualidad, conocer cuál es el futuro que se tiene planteado para esta y que tanto compromete nuestra información.

Los dispositivos conectados a una red IoT son propensos a ser vulnerables ya que vienen con configuraciones de fabrica que muchas veces los usuarios no modifican lo que hacen que estos puedan llegar a ser víctimas de ataque ya que quedan expuestos, es importante y se recomienda que al adquirir este tipo de dispositivo se tenga en cuenta lo siguiente con el fin de generar por lo menos la seguridad mínima. Lo que se recomienda en este caso es:

- **Cambiar credenciales por defecto:** (nombre de usuario y contraseña) que vienen por defecto, ya que éstas credenciales son comunes al resto de dispositivos de la marca, Por ejemplo, la botnet Mirai infecta a los dispositivos IoT a través de las credenciales usadas por defecto, instalando código malicioso en los mismos.
- **Red Independiente:** Aislar este tipo de sistemas y los dispositivos que se conecten con ellos en una red independiente, así sé evitara que accedan a la red wifi e interactúen con ellos y deshabilitar la conexión remota.
- **Contraseñas robustas:** Proteger los dispositivos con WPA2 y contraseñas robustas. También es importante proteger la seguridad del router para evitar que alguien conectado a la red pueda acceder a él.

- **Filtrado de tráfico:** Establecer un filtrado de tráfico en la red para evitar que el tráfico no autorizado se dirija hacia algún dispositivo en concreto, o hacia el exterior de la red.
- **Datos cifrados:** La información que contenga o reciba el dispositivo esté cifrada para evitar el robo, la manipulación o la modificación de las acciones a realizar.
- **Antivirus:** realizar análisis periódicos con un antivirus en busca de infecciones, vulnerabilidades o cualquier otra amenaza.
- **Revisar permisos en las apps:** revisar los permisos concedidos son los que necesita y si no, deshabilitar aquellos permisos que no sean necesarios para su funcionamiento.
- **Políticas de privacidad:** leer las políticas de privacidad de los dispositivos para estar consiente sobre qué información recolecta, almacena y el uso que hace de ella la empresa creadora del producto.
- **Actualizaciones:** Mantener actualizado el software de los equipos y el firmware de los dispositivos IoT. Cuando más actualizados estén y tengan los últimos parches de seguridad, más difícil serán de hackear.

Es de conocimiento de los usuarios de dispositivos que se conectan a la red IoT y de los fabricantes que esta tecnología desde su salida ha presentado diferentes fallas en cuanto a la seguridad y las estadísticas lo muestran al igual que las diferentes noticias que se han generado alrededor de ellos, tomando en cuenta los ataques presentados no solo a grandes compañías como es el caso de Garmin sino que incluso a circuitos cerrados de televisión que alguna persona pueda tener en su vivienda con el fin de proteger la seguridad del perímetro. Es importante entonces que los usuarios tengan en cuenta al adquirir los dispositivos o al hacer uso de ellos conocer el nivel de seguridad con el que fueron desarrollados y la actualización de los parches de seguridad que se encuentren a la última versión al igual que el firmware del dispositivo.

9. BIBLIOGRAFÍA

¿Qué es el Internet de las Cosas? Todo lo que necesitas saber sobre IoT. [en línea]. Jorge López, DIGITAL TRENDS. [Fecha de consulta: 16 de febrero de 2021]. Disponible en: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

¿Qué es MQTT? Su importancia como protocolo IoT. [en línea]. Zona Geek, Ingeniería, informática y diseño. Luis Llamas . [Fecha de consulta: 26 de junio de 2021]. Disponible en: https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/

6 CARACTERÍSTICAS CLAVE DEL INTERNET DE LAS COSAS [en línea] Ricardo Vega. [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://ricveal.com/blog/6-caracteristicas-clave-del-internet-de-las-cosas

Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [en línea]. INCIBE. [Fecha de consulta 26 de marzo de 2020]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Asrar A. Baktyan, A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective. European Union Digital Library. A. T. (2018).

Ataques a la IoT: 10 cosas que debes saber . [en línea]. WELIVE SECURITY. (2016). [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2016/12/21/ataques-a-la-iot-debes-saber/

Blog de Hiberus Tecnología: Introducción al IoT, Internet of Things. [en línea]. Jorge Learte. [Fecha de consulta 12 de mayo de 2020]. Disponible en: : https://www.hiberus.com/crecemos-contigo/introduccion-al-iot-internet-of-things/

Bradley Mitchell. Understanding Transmission Control Protocol/Internet Protocol (TCP/IP). LIFE WIRE. (2020).

Cómo Kevin Ashton nombró El Internet de las Cosas [en línea]. Jeff Elder Avast blog. [Fecha de consulta 2 de Septiembre de 2020]. Disponible en: https://blog.avast.com/es/kevin-ashton-named-the-internet-of-things

Cuáles son los vehículos más vulnerables al 'hackeo'. [en línea]. INFOTALLER. [Fecha de consulta 12 de abril de 2020]. Disponible en: https://www.infotaller.tv/reparacion/vehiculos-vulnerables-hackeo_0_1105389472.html

Dave Thaler, H. T. Architectural Considerations in Smart Object Networking, 2020.

Definition of internet of things in English. Oxford English and Spanish Dictionary, 2021.

DISEÑO DE UNA RED DE IoT PARA EL HOGAR: Internet of Things (IoT). [en línea]. YOBANY ENRIQUE CHITIVA BERNAL. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/17670/1/2020_diseno_red_iot.pdf

El 70% de los usuarios cree que los dispositivos IoT no son seguros. [en línea]. ESET. [Fecha de consulta 10 de octubre de 2020] Disponible en: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/el-70-de-los-usuarios-cree-que-los-dispositivos-iot-no-son-seguros-2/

El 'hackeo' de un Tesla Model S arroja más dudas sobre el coche conectado. [en línea]. INFOTALLER. [Fecha de consulta 12 de abril de 2020]. Disponible en: infotaller.tv/concesionarios/hackeo-Tesla-Model-arroja-conectado_0_1058594157.html

Fallece Barnaby Jack, el «hacker» que podía atacar dispositivos cardiacos. [en línea]. ABC REDES. (s.f.). Disponible en: https://www.abc.es/tecnologia/redes/20130729/abci-barnaby-jack-hacker-muere-201307291016.html?ref=https://www.google.com/

H. Tschofenig, J. A. Architectural Considereations in Smart Object Networking. Tschofenig, et al., 23, . March de 2015.

HACKING Y SEGURIDAD EN VEHÍCULOS. [en línea]. INTERPOLADOS. [Fecha de consulta 12 de abril de 2020]. Disponible en: https://interpolados.wordpress.com/2019/02/07/hacking-y-seguridad-en-vehiculos/

Hamidreza Damghani, L. D. Classification of Attacks on IoT, 20 de NOVEMBER de 2019.

IEEE COMSOC. IEEE Internet of Things Initiative, a Multi-Society Technical Group. IEEE Internet of Things Magazine, 2019.

Information Security and Externalities. [en línea]. Bruce. Schneier. [Fecha de consulta 2 de octubre de 2020]. ENISA (European Network and Information Security Agency) Quarterly: Disponible en: https://www.schneier.com/essays/archives/2007/01/information_security_1.html

INTERNET DE LAS COSAS. [en línea]. JORDI SALAZAR Y SANTIAGO SILVESTRE. (s.f.). Disponible en: https://upcommons.upc.edu/bitstream/handle/2117/100921/LM08_R_ES.pdf

Internet Of Things IoT. [en línea]. DELOITTE. [Fecha de consulta 10 de octubre de 2020] Disponible en: https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

La nueva Ley TIC y el avance en conectividad en Colombia. [en línea] . MINTIC. [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los-Medios/106166:La-nueva-Ley-TIC-y-el-avance-en-conectividad-en-Colombia.

Los ciberataques ponen en riesgo la seguridad de los cajeros automáticos. SEGURILATAM, (2020).

Los marcapasos, posibles objetivos de los ciberataques. [en línea]. ANABEL LEAL AGENCIAS. [Fecha de consulta 2 de Septiembre de 2020]. Disponible en: https://www.teinteresa.es/tecno/marcapasos-posibles-objetivos-ciberataques-hackers_0_1861014217.html

MEXICO DOCUMENT. INTERNET OF THINGS IN 2020: ROADMAP FOR THE FUTURE, (s.f.).

Mysterious Hajime botnet has pwned 300,000 IoT devices The Register — Biting the hand that feeds IT [en línea]. John Leyden . [Fecha de consulta 12 de mayo de 2020] Disponible en: https://www.theregister.com/2017/04/27/hajime_iot_botnet/

National Intelligence Council (U.S.). (04 de 2008). Homeland Security Digital Library. Disponible en: Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025: https://www.hsdl.org/?view&did=485606

Networking I: El modelo OSI. [en línea] José Ramón Maseda Lozano. [16 de junio de 2021]. Disponible en: https://itadmins.es/networking-i-el-modelo-osi/

OWASP Internet of Things. [en línea] OWASP. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

Pensamientos y tecnología, El Origen Del IoT. [en línea]. Bruno Cendón. [Fecha de consulta 10 de junio de 2020]. Disponible en: http://www.bcendon.com/el-origen-del-iot/

Peter Friess: Internet of Things Strategic Research Roadmap. [en línea]. Patrick Guillemin, [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf

Scientific american: Bomba de insulina es vulnerable a piratas informáticos [en línea]. Jim Finkle. [Fecha de consulta 12 de mayo de 2020] Disponible en: https://www.scientificamerican.com/espanol/noticias/reuters/bomba-de-insulina-es-vulnerable-a-piratas-informaticos/

Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies. [en línea]. WHITESCOPE. [Fecha de consulta: 18 de Noviembre de 2020]. Disponible en: https://drive.google.com/file/d/0B_GspGER4QQTYkJfaVlBeGVCSW8/view

Seguridad de Internet de las Cosas. [en línea]. Colaborador de TechTarget. [Fecha de consulta 10 de septiembre de 2020]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Seguridad-de-Internet-de-las-Cosas

Seguridad y Riesgos en IoT (Internet de las Cosas). [en línea] NTS. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://www.nts-solutions.com/blog/iot-seguridad.html

Significado : Qué es . [en línea]. Significados. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://www.significados.com/

Simplify the development of your IoT solutions with IoT architectures. IBM. . [en línea]. Strategies for creating scalable, flexible, and robust IoT solutions [Fecha de consulta 26 de marzo de 2020] Disponible en: https://developer.ibm.com/articles/iot-lp201-iot-architectures/

SmartData Collective: Assessing the Severity of SQL Injection Threats to IoT Security [en línea] Ryan Kh. [Fecha de consulta: 18 de mayo de 2020]. Disponible en: https://www.smartdatacollective.com/assessing-severity-sql-injection-threats-iot-security/

THE GUARDIAN: The internet of things: convenience at a price. [en línea] NIKOLE KOBIE. [Fecha de consulta: 05 de septiembre de 2020]. Disponible en: https://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security

Un acercamiento a Fog computing. [en línea]. ACIS. Conceptos claves, ventajas y principales desafíos: (s.f.). Disponible en: https://sistemas.acis.org.co/index.php/sistemas/article/download/121/94/

UNAB IMPLEMENTACIÓN DE UNA ARQUITECTURA FOG COMPUTING. [en línea]. CASTELLANOS, J. P. [Fecha de consulta 10 de junio de 2021]. Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/11908/2020_Tesis_Javier_Pinzon_Castellanos.pdf?sequence=1&isAllowed=y

WHAT IP MEANS AND HOW IT WORKS. [en línea]. IGNACIO MADRID. [Fecha de consulta 26 de marzo de 2020] Disponible en: http://eds.a.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=0&sid=551f1ee0-00d8-4605-ac50-303cadf89df5%40sessionmgr4006

10. ANEXOS

10.1 CLASIFICACIÓN DE VULNERABILIDADES

Tabla 7 – Comparación de protocolos más usados para IoT

CATEGORÍAS DE VULNERABILIDAD	
Mala configuración	Control de acceso abierto o débil
Protocolo o paquete susceptible	Ingeniería social
Diseño de software o falla de codificación	Lógica empresarial defectuosa
Transmisión de comunicación susceptible	Confianza inapropiada oe injustificada
Divulgación de información	Control físico susceptible
Consumo de recursos / capacidad / vida útil	Canales laterales electrónicos susceptibles
Ubicación susceptible	Proximidad susceptible

Fuente: https://www.iotsi.org/#security-context

10.2 CLASIFICACIÓN DE ATAQUES

Tabla 8 – Comparación de protocolos más usados para IoT

	TIPO	
FASE	Fuga o violacion de datos	Soberania de datos
	Perdida de datos	Autenticacion de datos
DISPONIBILIDAD	Inundaciones por atacantes	Inundacion por legitimos (multitud flash)
	Inundaciones por atacantes suplantadores	Inundacion por legitimado agresivo
	Modificadiond e datos sencibles	
ARQUITECTURA	Ataque externo	Ataque de agujero de gusano
	Ataque de reenvio selectivo	Ataque por sumidero
	Ataque de piscina de aguas residuales	Ataque de brujas
	Hello Ataque de inundaciones	Abordar todas las cosas en IoT
	Denegacion de servicio DDoS	Multitud Flash
	Ataque de suplantacion de IP	Ataque de suplantacion de identidad
	Goodput	Centro de datos DC
	Botnet	Confidencialidad
	Seguridad Fisica	Seguridad de software
	Seguridad de la red	Problemas de SLA
	Escucha clandestina	Repeticion de ataque
	Backdoor	Sybil
	Fracaso bizantino	Protecciond e datos y borrado completo de datos
PROTOCOLOS	RFID	SPOOFING
	VIRUS	MITM

Fuente: autor del documento

10.3 ENLACE DEL VIDEO

url: https://youtu.be/fNH6E-692fc