ANÁLISIS DE SEGURIDAD DE VULNERABILIDADES Y ATAQUES PRESENTADOS EN 4 DISPOSITIVOS DE INTERNET DE LAS COSAS

NINO ALEXANDER ARIAS SILVA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA

2019

ANÁLISIS DE SEGURIDAD DE VULNERABILIDADES Y ATAQUES PRESENTADOS EN 4 DISPOSITIVOS DE INTERNET DE LAS COSAS

NINO ALEXANDER ARIAS SILVA

Trabajo de monografía para optar al titulo de especialista en seguridad informática

Director de proyecto

DANNY FERNANDO LEON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA

2019

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El presente proyecto busca realizar un análisis acerca de IoT (Internet de las cosas), basado en aspectos de seguridad en los dispositivos o cosas, identificando las fallas más recurrentes que traen consigo los dispositivos, debido al poco conocimiento que se tiene del mismo, por ser un tema que es naciente y se está empezando a implementar.

A través de un estudio de las vulnerabilidades existentes en la estructura de IoT basadas en configuraciones, controles de acceso, métodos de autenticación, protocolos, aplicaciones, con el apoyo de consultas de fuentes bibliográficas, se establecerán e identificaran diferentes aspectos relacionados con una serie de vulnerabilidades a tener en cuenta en los dispositivos de IoT ya que debido a la masiva conexión de ellos, estos comparten diversos tipos de información a través de los canales de Internet, siendo una fuente para los numerosos ataques a los que cada día se exponen los millones de dispositivos que se conectan o empiezan a conectarse (Juan Anabalon, 2016).

A través de una matriz DOFA, se identificarán una serie de aspectos negativos y positivos relacionados con la seguridad en cada uno de los dispositivos IoT seleccionados, destacando debilidades, oportunidades, fortalezas, amenazas, esto permite establecer una serie de correctivos que ayuden a mejorar esas situaciones negativas y fortalecer los puntos positivos, ayuden a mejorar el fortalecimiento de esta tecnología que se impone a ritmos acelerados con el fin de sacarle el mayor provecho a los dispositivos, protegiendo los procesos del usuario final (Isabella Suarez, 2018).

La finalidad es establecer recomendaciones acerca de mejores prácticas a utilizar en los dispositivos IoT seleccionados, para minimizar las vulnerabilidades que a través de la investigación fueron identificadas, cerrándole las puertas a los diversos ataques que se aprovechan de estas fallas, dándole una gestión adecuada al fortalecimiento y robustez de los dispositivos y así minimizar el riesgo por ataques cibernéticos permitiendo así la confiabilidad en los dispositivos.

PALABRAS CLAVES

IoT, Seguridad, Dispositivos, Arquitectura, Vulnerabilidades, Ataques, Tecnología, Protocolos, Debilidades, Internet, Conexión, Datos, Denegación, Atacantes, Cibernético, Amenazas

ABSTRACT

This project seeks to perform an analysis about IoT (Internet of Things), based on aspects of security in the devices or things, which they bring with them at the time of their implementation, due to the little knowledge they have of it, because they are an issue that is nascent and is beginning to be implemented.

Through a study of the structure of IoT, reviewing bibliographic sources, user experience, and different aspects of vulnerabilities to be taken into account in the IoT devices that can be generated through the connection of millions of them will be established and identified. Who share different types of information through Internet channels, due to the numerous attacks to which the thousands of devices that connect or begin to connect are exposed every day (Juan Anabalon, 2016).

Through a SWOT matrix, different negative and positive aspects of security in IoT devices will be identified, highlighting weaknesses, opportunities, strengths, threats, this allows establishing a series of aspects that allow to correct the negative aspects and strengthen the positive aspects of this technology that imposes itself at accelerated rates in order to get the most out of it (Isabella Suarez, 2018).

All in order to establish what would be the best practices to use in the use of IoT devices, in order to guarantee reliability, giving it an adequate management, strengthening and strengthening the devices for the vulnerabilities found and thus minimize the risk of cyber attacks.

KEYWORDS

IoT, Security, Devices, Architecture, Vulnerabilities, Attacks, Technology, Protocols, Weaknesses, Internet, Connection, Data, Denial, Attackers, Cybernetics, Threats.

INTRODUCCION

El desarrollo y continua evolución de las tecnologías, trae nuevas formas de comunicación, acortando las distancias y teniendo la posibilidad de comunicación en cualquier lugar del mundo, uno de estos avances ha traído consigo la posibilidad de conectar muchos dispositivos a la red de redes, la Internet, transformando la experiencia de vida de los usuarios al conectar desde electrodomésticos de hogar, vehículos, prendas de vestir deportivas, ya que con el uso de sensores estos pueden acoplarse a cualquier elemento y de allí comunicarlos a la red, generando nuevas capacidades en las transferencia de datos, estableciendo una serie de comportamientos que no requieren de la interacción humano-humano, humano-computadora, este avance tecnológico es lo que se conoce como Internet de las cosas.

Por consiguiente el avance tecnológico proporcionado por IoT, puede ser de gran utilidad al momento de controlar una serie de procesos que antes se veían inalcanzables, también la oportunidad de generar una serie de nuevas opciones de negocio basados en la información que cada uno de los dispositivos continuamente está comunicando al conectarse a Internet, ya no es extraño poder contactarnos con dispositivos con los que se interactúa día a día, los cuales hace unos años no se contemplaban que podrían estar conectados a internet y así hacer la vida un poco más cómoda basada en la toma de decisiones inteligentes y autónomas. IoT por tanto ofrece la interconexión de millones de dispositivos utilizando una serie de protocolos que permiten al dispositivo conectarse de manera guiada o no guiada con otros dispositivos y a la red de redes, entre los que destacan conexiones inalámbricas como Wifi que ofrece un rango mayor de alcance con respecto a Zigbee que su cobertura es menor o Bluetooth la cual es más personal, con la comunicación de estos dispositivos inteligentes se generan una serie de soluciones automatizadas que ayudan en los procesos de las industrias en las que destacan las aseguradoras, agrícolas, transporte, deporte, entretenimiento, manufactura, gobierno, salud, educación, automotriz, pero para generar esas soluciones debe existir un interlocutor entre los dispositivos y el usuario final, quien hace estas funciones son las aplicaciones encargadas de recolectar la información que toma de los dispositivos con el objetivo de hacer un análisis de esa información que en un principio no llega a tener un valor o significado, pero con la ayuda de servicios específicos como el Big data, Machine learning, aprendizaje automático busca estructurar la información para a partir de allí encontrar patrones, conductas, comportamientos y así proveer a los dispositivos inteligencia artificial para la toma

de decisiones, de esta manera la información estructurada debe ser enviada al usuario final a través de una interfaz que le permita entender de un manera clara, agradable, interactiva lo que está sucediendo y así mejorar sus procesos y actividades diarias tendiendo una mejor experiencia, entre los beneficios más importantes que aporta IoT son la automatización de procesos, flexibilidad en el trabajo, optimización en el análisis de datos, vigilancia tecnológica, supervisión, datos en tiempo real, conllevando a una nueva concepción de procesos empresariales y nuevas estructuras de trabajo (D. Godoy, E. Sosa, 2014).

Es así que a partir de esta creciente tecnología, nace la necesidad de investigar más sobre la temática relacionada con el Internet de las cosas, pero centrándola en unos puntos específicos que aborden aspectos de seguridad, debido a que todos estos dispositivos están conectados a Internet, compartiendo información personal desde muchos ámbitos como gustos, pasiones, datos comerciales, bancarios, médicos, el control de esta información puede estar en manos de terceros comprometiendo la privacidad de los usuarios algo de mucho cuidado, ya que es una de las características inherentes en el ser humano.

Ya que se hace necesario analizar aspectos de seguridad relacionadas con las vulnerabilidades que presentan algunos dispositivos o cosas del IoT, fuente para que atacantes cibernéticos aprovechen y efectúen una serie de ataques que comprometen la confidencialidad de los usuarios que hacen uso de estos dispositivos, , las cuales servirán de base a la hora de minimizar los riesgos que trae consigo el colocar un dispositivo en la Internet, exponiéndolo ante un ataque, todo esto a través de una investigación exploratoria y cualitativa, partiendo del conocimiento de la estructura de IoT, estableciendo cuales son las capas que la componen, que actividades, tecnologías, protocolos, servicios están presentes en cada una de las capas y como es la interoperabilidad entre cada una de ellas, dando una idea de cómo es el proceso desde que el dispositivo recolecta información y la entrega de manera estructurada a un usuario final a través de una interfaz. El paso a seguir es identificar, detallar a través de fuentes especializadas cuales son las vulnerabilidades más frecuentes que se presentan en los dispositivos IoT en las que se pueden identificar credenciales de acceso, falta o mala implementación de cifrado, cuentas de usuario, falta de actualizaciones, a partir de estas falencias encontradas se argumenta la evolución que han tenido los ataques a través de una serie de generaciones las cuales iniciaron con pequeños virus y han evolucionado a técnicas más complejas con rangos de alcance mayores, a través del uso de malware destaca la capacidad de reclutar otros dispositivos con el objetivo de distribuir los ataques y manipular remotamente los dispositivos, entre los que más

destacan son el código malicioso, exploits, denegación distribuida de servicios, una vez establecida esta visión general, la investigación busca centrarse en 4 dispositivos IoT, con los cuales se pueda hacer un detalle mucho más específico en cuanto a que vulnerabilidades están presentes y cuáles son los ataques más frecuentes que afectan el correcto funcionamiento, los dispositivos que se seleccionaron para esta investigación son de los más utilizados ya que algunos sirven para conectar otros dispositivos a Internet como el router y el punto de acceso, adicional un dispositivo muy utilizado para el monitoreo remoto como las cámaras de seguridad y el ultimo dispositivo que se está masificando como es el smarwatch de uso mucho más personal que los anteriores, tomando esta información específica se plantea un análisis a través de una matriz DOFA estableciendo debilidades, oportunidades, fortalezas y amenazas, para cada una de las vulnerabilidades y ataques específicos de los 4 dispositivos IoT seleccionados, con este análisis efectuado se busca establecer una guía de buenas prácticas, abarcando una serie de ítems que establecen una serie de parámetros de configuración a tener en cuenta para lograr un mayor aseguramiento en los dispositivos y así corregir las vulnerabilidades y minimizar los ataques ya que cada día son más las personas que adoptan esta nueva forma de comunicación, construyendo nuevos modelos de negocio, por tal razón es importante proteger la confidencialidad de la información que continuamente se está generando (David Pelaez, 2018).

1. PLANTEAMIENTO DEL PROBLEMA

Debido al gran número de dispositivos que se conectan día a día a Internet, estos se exponen a una serie de amenazas relacionadas con ciberataques que tienen una complejidad mayor debido a su estructura y alcance, hace unos años las técnicas utilizadas no eran tan estructurados, así que si no se tiene un adecuado nivel de seguridad en los dispositivos, al momento de la puesta en marcha al ser el Internet de las cosas (IoT) una tecnología emergente la cual establece la conexión y comunicación de millones de dispositivos a través de diferentes redes es inherente que surjan una serie de vulnerabilidades tanto a nivel lógico como físico en infraestructuras, protocolos, servicios, dispositivos, aplicaciones, las cuales al no ser atendidas con suficiencia serán punto de partida para los atacantes que aprovecharan esas falencias que puedan hallar, a través del uso de metodologías de ataque, personas no autorizadas puede extraer información o comprometer a un usuario, debido a la forma como se establecen nuevos modelos de trabajo, comunicación, comercialización, vigilancia a través de Internet, permite que información sensible se comparta a través de los canales de Internet, quedando expuestos a terceros, si no se empieza asegurar la pirámide desde su base es decir, el fortalecimiento de los dispositivos o cosas como se denomina en IoT, muchos serán los sistemas comprometidos, lo que puede conllevar a pérdidas económicas, desastres o algo aún más preocupante la pérdida de la privacidad y confiabilidad de la información**.** (A. Pinto, 2012).

El avance de la tecnología está permitiendo que muchos dispositivos que en un principio no se pensaba que pudieran conectarse a la internet, hoy en día tengan la posibilidad de hacerlo, televisores, sensores, smartwatch, cámaras, celulares, adicional a los dispositivos que tradicionalmente ya tenían conexión a internet como computadoras, router, puntos de acceso, cambiando la forma de comunicación y transformando el uso de la Internet, esto ha producido un aumento en la asignación de direcciones que ya no puede soportar el protocolo IPV4, el cual agoto la asignación de direcciones a partir de la año 2011, así que desde ese momento los proveedores de servicio empezaron a desplegar direccionamiento basado en un nuevo protocolo ya que la cantidad de dispositivos conectados por usuario estaba en aumento, así que esta situación está ofreciendo la interoperabilidad de dos protocolos ya que muchos dispositivos están conectados bajo el protocolo anterior y nuevos dispositivos se conectan con el nuevo protocolo, esto requiere que las infraestructuras de red cuenten con equipos especializados, protocolos, elementos específicos para cada uno de los protocolos, pero que estos puedan también comunicarse entre sí, así que adoptando esta situación en la coexistencia pueden generar una serie de falencias o debilidades en los sistemas, dispositivos que

pueden ser aprovechados por terceros para comprometer la información de los usuarios, debido a que todo estos procesos al ser nuevos presentan una serie de errores, que son base para así mejorar los procesos de aseguramiento (Y. Castillo, 2016)

Por consiguiente IPV6 surge como un nuevo protocolo que soporta esa gigantesca asignación de direcciones para millones de dispositivos que quieren acceder a internet brindando un aumento en la interconexión de dispositivos usados por persona en el mundo, pero que a su vez permite que sean muchos más los objetivos para delincuentes informáticos, estos se puedan aprovechar de las múltiples vulnerabilidades y así basar sus metodologías en ataques informáticos aprovechando la falta de vigilancia, ocasionando perdida de privacidad de la información, debido a que los millones de dispositivos que se van conectando a través de Internet, reunirán una serie de datos basados en comportamientos, actividades, inclinaciones, costumbres, generando una serie de interrogantes acerca de las consideraciones de seguridad a tener en cuenta en los dispositivos en el momento de implementar IoT y este no altere o afecte los 3 principios de la seguridad de la información, disponibilidad, integridad y confidencialidad (D. Evans, 2011).

2. JUSTIFICACION

Actualmente con la aparición del IoT internet de las cosas, donde cada dispositivo que pueda imaginarse, tendrá la capacidad de conectarse a internet para cumplir una serie de actividades o procesos, millones de dispositivos generando una serie de información que en un alto porcentaje es considerada como sensible, estará viajando a través de la internet por medio de canales no seguros, de allí la importancia de analizar la seguridad en los dispositivos o cosas, ya que son la primera línea con las que un ciberdelincuentes se va a encontrar y es aquí donde estarán enfocados los diversos ataques que se pueden efectuar, así que si en estos dispositivos no se detectan cuáles son las vulnerabilidades que trae consigo las cuales se presentan en diferentes niveles, los controles que se efectúen no podrán ser efectivos, así que determinar una serie de procesos o guías que permitan al usuario establecer cuáles son las vulnerabilidades concurrentes, adicional identificar cuáles son los ataques a los que se está expuesto, serán de gran utilidad a la hora de minimizar los riesgos asociados que conlleva el uso esta nueva tecnología, a través de la interconexión de miles de dispositivos a Internet.(O. Gasquez, 2015)

Los procesos de comunicación siempre han tenido como fundamento la información, debido a la gran evolución tecnológica que ha sufrido las telecomunicaciones a lo largo de los años, el mundo ha venido cambiado la forma en que se comunica, en un principio tan solo utilizaba unos intérpretes, canales, lenguaje mensajes (información), a medida que estos procesos fueron evolucionando, aparecieron nuevos dispositivos que simplifican la manera de comunicación. Las redes de datos, internet, televisión, radio, satélites, telefonía, cada una de estas tecnologías comunican y gestionan diferentes tipos de información, voz, datos, imágenes, video (J. Moya, 2005).

Así mismo la información que se compartía en un principio, se hacía de manera local este rango se fue ampliando con la aparición de la Internet, creando nuevos modelos de negocio, educación, comercialización, investigación, entretenimiento, permitiendo la globalización de las comunicaciones, pero a su vez a ocasionar una serie de inconvenientes, en la pérdida de control sobre la información, debido a que esta pasaba por diferentes canales y redes que se consideran inseguras (R. Stair, 2000).

Es así que empezaron aparecer nuevos desafíos encaminados a establecer estándares y normas que protegieran la información que circula por los diferentes canales comunicativos, conllevando a establecer una serie de buenas prácticas encaminadas a 3 principios básicos, disponibilidad donde la información debe ser aprovechable en cualquier momento, a cualquier hora, en cualquier lugar por quien lo requiera, confidencialidad indica que solo personas autorizadas a través de unos parámetros de seguridad específicos son las únicas que pueden acceder a la información, evitando el acceso a personas no autorizadas, integridad indica que se protege la información de alteraciones o modificaciones en el camino de un origen a un destino (V. Canal, 2004)

Por tal razón es de mucha importancia establecer una adecuada gestión de la información, que involucra una serie de fases entre las que destacan, fortalecimiento de dispositivos, infraestructura, servicios, aplicaciones, sistemas de seguridad donde se establecen vulnerabilidades, amenazas y riesgos a los que se está expuesto, con el fin de establecer una serie de contingencias y planes de seguridad minimizando la pérdida de privacidad de la información (J. Bertolin, 2008)

3. OBJETIVOS

3.1 GENERAL

Analizar los aspectos de seguridad relacionado con las vulnerabilidades y ataques más frecuentes que se presentan en 4 dispositivos IoT (cámaras de seguridad, smartwatch, router, punto de acceso), estableciendo una ruta de buenas prácticas en el aseguramiento de los dispositivos.

3.2 ESPECIFICOS

Conocer las características de la arquitectura IoT.

Consultar los fallos de seguridad generales, más frecuentes e importantes que se presentan en los dispositivos IoT

Identificar los fallos de seguridad específicos más frecuentes e importantes que se presentan en los 4 dispositivos IoT seleccionados

Establecer a través de una matriz DOFA los diferentes aspectos de IoT, relacionados con seguridad en los 4 dispositivos IoT seleccionados.

Elaborar una guía que detalle una ruta de buenas prácticas en el aseguramiento de los 4 dispositivos IoT seleccionados.

4. MARCO REFERENCIAL

A partir del siglo XX, la aparición de diversas redes de comunicación, a través de sistemas de telefonía, radio, televisión, buscaban el uso de las tecnologías para procesar, distribuir la información a gran escala, también es el nacimiento de la industria de la computación, generando un nuevo cambio tecnológico, el cual establecía la fusión de computadoras con las comunicaciones, creando nuevos sistemas informáticos, dotados de diversas computadoras conectadas de manera centralizada, con la función de recolectar, procesar, transportar, almacenar la información de una manera ágil y confiable, este es el nacimiento de las redes de datos (A. tanenbaum, 2003).

Las redes de datos nacen con la necesidad de compartir recursos, servicios a través de sistemas informáticos con el fin de procesar la información de un manera más adecuada, de allí se determina que cuando una red de computadoras comparten un espacio local, de no mucha extensión, se conoce como LAN (Red de área local), cuando comparte un espacio geográfico un poco más amplio pero sin exceder una extensión mayor se conocen como PAN (Red de área panamericana), cuando su extensión es mayor conectado varias extensiones geográficas, se conoce como WAN(red de área extensa), lo que se conoce como Internet (A. tanenbaum, 2003).

La conexión de varias redes informáticas fue lo que fundamento la creación de la Internet , generando una revolución en la forma de comunicación de los seres humanos, a través de unos protocolos o reglas estandarizadas, su principal función era la de compartir información entre dispositivos, ubicados en extensiones geográficas diferentes, Internet ha evolucionado constantemente, agregando servicios, aplicaciones, generando que millones de personas establezcan comunicación a través de diferentes plataformas, Internet se ha convertido en la conjunción de todas las tecnologías, radio, televisión, telefonía, eso ha conllevado a crear un nuevo lenguaje donde se establecen una serie de términos, ciberespacio, ciberciudadano, que han generado un cambio cultural en las sociedades.

Pero todo este cambio cultural ha influenciado la parte negativa de la sociedad, donde personas inescrupulosas ven al internet como una fuente de aprovechamiento de vulnerabilidades, buscando la manera de sacar provecho, a través del robo de información, violentar la privacidad de la información de las organizaciones o personas del común aumentando los delitos informáticos cada día, es importante definir que la Internet es un espacio de mucha importancia en el mundo actual, ya que establece una nueva forma de comunicación sin limitantes, ni barreras, pero en la otra arista encontramos que es un espacio de poca confiabilidad y que se debe tener muchas precauciones de seguridad al momento de colocar un dispositivo, servicio o información, ya que esto va estar expuesto a terceros.

Los dispositivos conectados a internet deben basar su comunicación en el protocolo IPV4, es un protocolo que asigna un identificador numérico, para que pueda interconectarse con otros dispositivos, utiliza direcciones numéricas de 32 bits (4 Bytes), teniendo una capacidad limitante de asignación de direcciones de 4.294.967.295, de este total algunas direcciones son de uso privado para conectar equipos a través de redes locales, direcciones de uso público asignadas por los proveedores de servicio y son las direcciones con las cuales podemos navegar por Internet, otras direcciones que tiene usos específicos.

Debido al avance de la tecnología y la conexión de millones de usuarios, el protocolo IPV4 ha agotado la asignación de direcciones públicas, así que aquellos nuevos usuarios que quieran conectarse a Internet no pueden hacerlos, a partir de allí viendo la necesidad de ampliar la asignación de direcciones, aparece un nuevo protocolo conocido como IPV6 el cual establece 128 bits, 8 bloques numéricos de 16 bits, para un total de 340.282.366.920.938.463.463.374.607.431.768.211.456 (340 sextillones), es decir que cada usuario puede conectar muchos dispositivos a Internet (S. Deering, 2017).

A partir de este volumen de direcciones empiezan a crearse una serie de plataformas donde la conectividad de red está basada en dispositivos diferentes a los que comúnmente se conectan a internet como equipos de cómputo, en estas plataformas sobresalen los sensores, electrodomésticos, dispositivos domoticos, permitiendo el control y automatización de manera remota de diferentes procesos, esto es lo que se conoce como Internet of things (IoT), donde miles de dispositivos están conectados a Internet y se estima que en los años venideros millones de dispositivos estén conectados a Internet.

Aparece una nueva evolución de la internet, ya que al estar miles de dispositivos conectados a internet, existirá un cambio en la manera que lo seres humanos, viven, aprenden, trabajan, entretienen, comunican. Internet de las cosas está permitiendo que se puedan abarcar otras variables que no se habían tenido en cuenta como la temperatura, luz, humedad, con la capacidad de expandirse a lugares que en otros momentos se veían como inalcanzables, ahora podemos contar con un sin número de datos flotantes en la internet, proveniente de los millones de dispositivos que empiezan a conectarse, módulos con sensores que permitan validar una serie de comportamientos, dispositivos que controlan, ubican y emiten alertas, casas inteligentes que dispones de una serie de dispositivos, sensores que operan conjuntamente en la toma de decisiones para realizar una serie de operaciones programadas lo que se conoce como automatización, esto ha brindado la creación de un sin número de aplicaciones asociadas a todos estos dispositivos. Estos datos flotantes si se organizan de una manera adecuada generan información, lo cual permite generar una serie de comportamientos y tendencias, lo cual desencadena en el conocimiento y si este a su vez va de la mano de la experiencia pues estamos generando sabiduría, por lo cual el ser humano empieza a evolucionar y transforma su mundo (D. Evans, 2011).

El IoT, aparece como un término que relaciono Kevin Ashton, la interconexión de millones de dispositivos donde el ser humano ya no tiene tanta interacción, debido al control que este ejercía sobre las maquinas o dispositivos que se conectaban a Internet, tenía debilidades ante el tiempo, la exactitud y los tiempos de respuesta, eso ahora esta cambiado y el IoT, busca que esos nuevos dispositivos los cuales se interconectan entre si de una manera más acelerada, permitiendo generar comportamientos basados en reacciones ante una serie de eventos que estén controlando, realizando acciones que no requieren de la participación directa de un ser humano, los dispositivos son los actores activos de esta tecnología, los dominios que abarca esta nueva tecnología están enfocados en la industria, medio ambiente y la sociedad.

En el año 2005 la ITU, declara que hay un cambio en el uso de las tecnologías de la información, es posible establecer canales de comunicación en cualquier momento, en cualquier lugar, permitiendo que millones de dispositivos que jamás se pensarían que estuvieran conectado a Internet tendrán la capacidad de hacerlo, lo que genera una red dinámica con un poder de decisión propio, multiplicando las conexiones creando un Internet de las cosas (Bankinter, 2011).

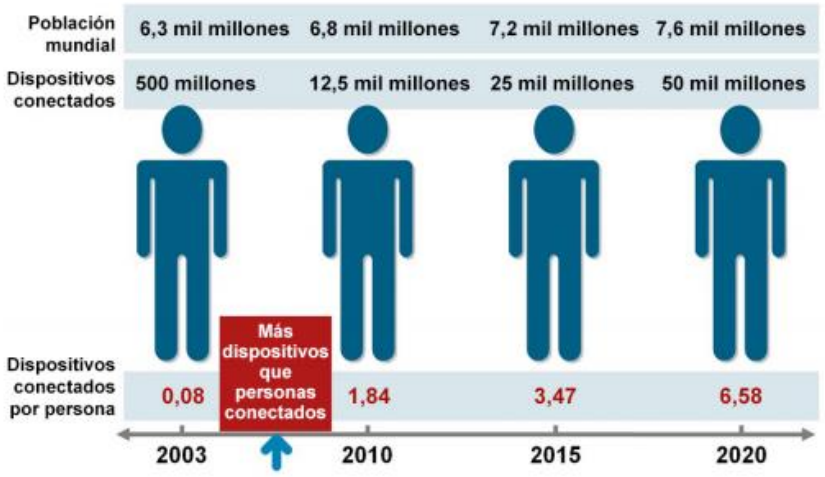
Paulatinamente el aumento de dispositivas se ha estado dando, es allí donde el internet de las cosas toma fuerza, generando la primera revolución del Internet logrando esta evolución que el Internet sea más sensorial, este basada en la comunicación de dispositivos con el fin de que sean ellos los que determinen una serie de comportamientos y permitan ejercer un control, sin tener que tener la intervención del usuario, en la búsqueda de llegar a lugares a los que nunca antes se había llegado a través de la comunicación, pero este avance aún necesita de tener un parámetros claros y estandarizados en cuanto a la seguridad, privacidad, arquitectura, la IEEE es una de la organizaciones que trabaja fuertemente para permitir que los paquetes IP puedan ser entendibles en los diferentes tipos de redes que atraviesa y esta comunicación no sea interrumpida (Dave Evans, 2011).

La tendencia indica que su implementación está acelerándose día a día, en el presente ya se cuenta con unos dispositivos controlando una serie de dispositivos de manera inteligente, en varias áreas creando su propio lenguaje y así determinando una serie de comportamientos, se espera que en el futuro esto se expanda y se aplique al término de ciudades inteligentes, industrias inteligentes, comercio inteligente, donde cada uno de los dispositivos cuenten con mucha más inteligencia, versatilidad y toma de decisiones, lo que va a generar la aceleración de las comunicación y forma de vivir de los seres humanos (Telefonica, 2011).

5. INTERNET DE LAS COSAS (IoT)

Es un término que cobra fuerza cada día, es un concepto tecnológico que busca conectar una serie de objetos a internet con el fin de automatizar una serie de procedimientos, utilizando un intercambio de información de manera sistematizada e inteligente, una gran parte de los objetos que están presentes en el Internet de las cosas son sensores que se entrelazan y conectan a través de redes inalámbricas, en la **ilustración 1** se evidencia el crecimiento de dispositivos conectados para los años 2010, 2015, estimando un aumento muy significativo para el año 2020 de aproximadamente 50 mil millones de dispositivos conectados, de igual manera el crecimiento de dispositivos que se conectan por persona (A. Everlet, J. Pastor, 2013).

Ilustración 1 Proyección dispositivos conectados



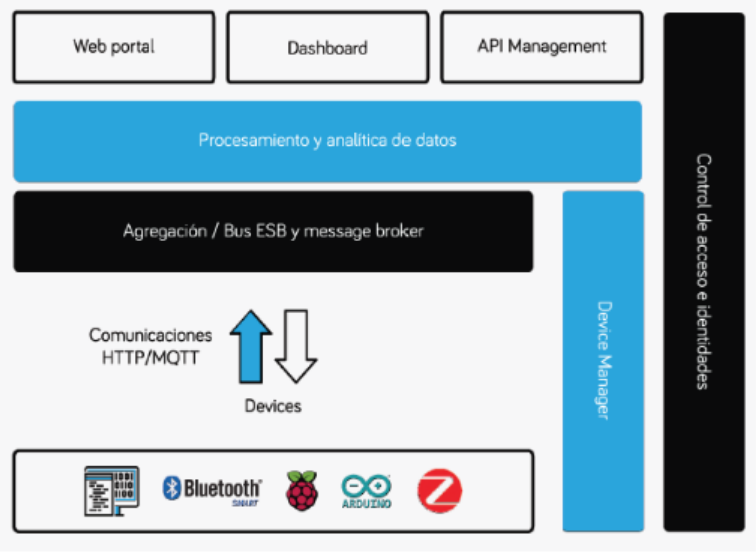
Fuente: Cisco IBSG, abril de 2011

Es así que toda esta conexión de diversos dispositivos, será la nueva generación del internet, ya que tendrá la capacidad de establecer nuevas formas para que los seres humanos establezcan comunicación, logrando impactos sensoriales a través de una serie de variables como temperatura, humedad, luz. Adicional con el Internet de las cosas se pueden llegar a una serie de lugares que en otras épocas se veían inalcanzables, esto permite que se creen sin números de aplicaciones

6. ESTRUCTURA

El Internet de las cosas es un concepto naciente por tal razón aún no hay una tecnología definida, pero su estructura está basada en varios componentes importantes que definen su implementación, un componente son los sensores, dispositivos, actuadores que son conocidos como cosas que se conectan a internet, otro componente son los buses o canales por donde las cosas conectadas envían y reciben información, el otro componente son las pasarelas que sirven de puente de conexión entre las cosas, los buses o canales, para que estos puedan interactuar en la internet debido a que esta red de redes requiere de un protocolo o lenguaje de vital importancia para que se entiendan las comunicaciones, es así que las pasarelas realizan la comunicación utilizando el protocolo de internet obteniendo conectividad y tasa de computo según el requerimiento de la cosa, la **ilustración 2** se puede observar una serie de capas de IoT, desde una inferior donde inicia el proceso con los dispositivos generando información, pasando por una capas intermedias que permiten la intercomunicación de dispositivos con protocolos, procesamiento de los datos, hasta una superior donde se brinda información ya estructurada al usuario de lo que genero el dispositivo por medio de aplicaciones (L. Jurado, A. Velásquez, F. Escobar, 2014).

Ilustración 2 Arquitectura IoT

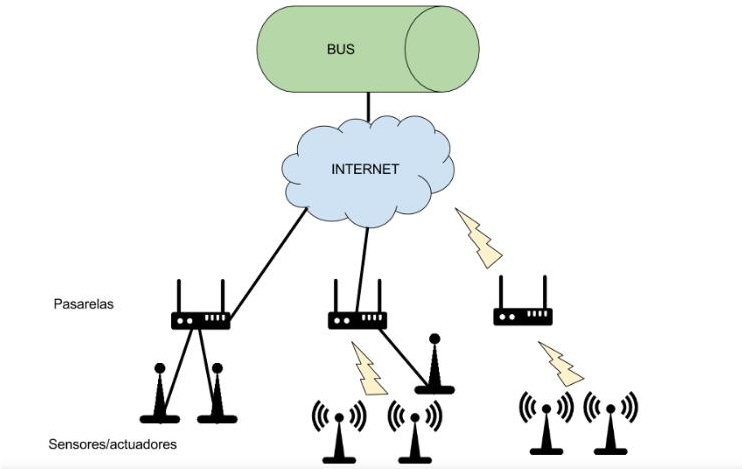


Fuente: Zemsania Tech Services & Solutions Draft Arquitectura referencia IoT

6.1 CAPA DISPOSITIVOS / COSAS

Cuando se abarca esta terminología, está basada en una serie de elementos de hardware que tiene una serie de funcionalidades que permiten la automatización de una serie de procesos, es así que cuando se refiere el concepto de cosa en el internet de las cosas, se está haciendo un énfasis a elementos como sensores, actuadores, dispositivos como tarjetas programables, la **ilustración 3** muestra la manera en que los dispositivos se conectan a pasarelas, a través de medio alambricos o inalámbricos para que se les permita la salida a Internet.

Ilustración 3 Sensores y actuadores IoT



Fuente: https://labs.beeva.com/arquitectura-de-internet-de-las-cosas-455b15ebe72c

6.1.1 Sensores

con el Internet de las cosas se busca realizar una serie de procesos inteligentes que permitan automatizar una serie de actividades como monitoreo, mediciones, todo esto genera un información que se debe recolectar, es así que se puede sintetizar que un sensor es un elemento de hardware que capta una serie de magnitudes físicas del medio como la temperatura, la humedad, aceleración, fuerza, movimiento, con el objetivo de analizar los cambios en las propiedades que en estas se presentan, para luego ser transformada a una señal eléctrica u óptica, y que un dispositivo pueda leer esa información y mostrarla a través de un aplicación, se encuentran dos tipos de sensores a tener en cuenta en el internet de las cosas como los son (R. Carreras, 2016).

- Sensor Smart
- Sensor inteligente
- Sensor de temperatura

Algunas características a tener en cuenta en los sensores son:

- La precisión
- Las condiciones ambientales del sitio
- La decisión o sensibilidad
- El alcance que pueda establecer
- Que permitan ser calibrados debido al uso

6.1.2 Actuadores son dispositivos que tiene la capacidad de recibir las señales electicas u ópticas que emiten los sensores, estableciendo una serie de parámetros con el fin de que al superar un límite que se establece con anterioridad, realicen funciones asociadas a la hidráulica, neumática, eléctrica de forma que active un elemento automatizando así un determinado proceso, los actuadores se dividen en los siguientes tipos:

- Hidráulicos – encargados de utilizar presión de un líquido para realizar una serie de movimientos mecánicos
- Eléctricos - encargado de convertir la energía eléctrica para realizar movimientos mecatronicos
- Neumático – encargados de utilizar aire para realizar movimientos mecánicos

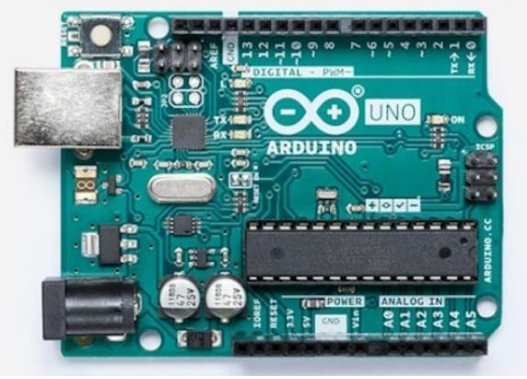
6.1.3 Tarjetas programables son dispositivos electrónicos modulares basados en hardware y software de código libre, cuentan con un microcontrolador, puertos de entrada, salida, comunicación, su funcionalidad está basada en la creación de objetos o entornos interactivos que permitan realizar y controlar una serie de procesos automatizados, a través del uso de sensores, actuadores, previa configuración realizada en el dispositivo.

Uno de los dispositivos de tarjeta programable más utilizados en el Internet de las cosas son los Arduino, esta es la plataforma más utilizada en la actualidad para desarrollar dispositivos que tenga autonomía o interactuar con otros dispositivos o aplicaciones, su funcionalidad está basada en controlar elementos a través de una serie de instrucciones programadas.

Para el desarrollo del Internet de las cosas se manejan 3 tipos de dispositivos en cuanto a plataformas electrónicas entre las que se destacan:

- Dispositivos pequeños con ciertas funciones que no cuentan con un sistema operativo, entre estos dispositivos destaca el arduino uno es un controlador que trabaja con una arquitectura de 8 bits, como se puede observar en la **ilustración 4** se detalla la tarjeta programable arduino uno, con sus controladores, puertos de conexión, una de las más utilizadas.
- Dispositivos medianos que poseen muchas más funciones, pueden contar con sistemas operativos embebidos basados en Linux, trabaja con arquitectura de 32 bits, usan chipset atheros para establecer comunicaciones inalámbricas, entre estos dispositivos destacan el arduino yun
- Dispositivos grandes que poseen gran capacidad y funcionalidad, trabajan bajo arquitecturas de 32 y 64 bits, tiene la capacidad de correr varios sistemas operativos entres los que se destacan Linux y android, su gran particularidad es que cumplen la función de Gateway para que dispositivos pequeños o medianos puedan conectarse a internet (S. Soriano, 2015).

Ilustración 4 Tarjeta programable Arduino



Fuente: https://www.xataka.com/makers/empezar-con-arduino-genuino-como-elegir-la-placa-modelos-compatibles-y-kits-de-iniciacion

Cada uno de estos dispositivos cuenta con una serie de buses que permiten la conexión de la tarjeta con elementos electrónicos con el fin de que estos elementos ejecuten una serie de instrucciones automatizadas, entres lo buses más destacados están:

- SPI – Es un bus de comunicación, que nace en 1980 lanzado por Motorola, trabaja con el establecimiento de comunicación serial, con un método síncrono, permite el envío y recepción de información de manera simultánea en modo full dúplex, se establece una topología de maestro y esclavo donde el maestro se encarga de trasmitir información a sus esclavos y los esclavos se encargan de recibir y enviar información al maestro, a través del uso de frecuencia de reloj, lo que permite una alta velocidad de trasmisión cuando l comunicación de equipos es a corta distancia (J. Garcia, 2015)

- UART – Es un bus que traduce los datos paralelos a serial, para que estos puedan ser trasmitidos, utiliza un método asíncrono entre receptor y trasmisor, para codificación de datos, estableciendo prioridad en él envió de bits, otra funcionalidad es la señalización handshaking para el estándar Rs-232 la cual permite que ambos extremos estén sincronizados a la misma velocidad, su topología es punto a punto, soportado por sistemas operativos Windows y Linux (E. Dominguez, 2005).

- I2C – Es un bus bidireccional que utiliza dos líneas, una línea para los datos la otra línea para la frecuencia de reloj, la topología está basada en maestros o esclavos, el maestro se encarga de la frecuencia de reloj, los esclavos responden al maestro, tanto maestros, esclavos pueden enviar y recibir datos, pero solo los maestros pueden iniciar una comunicación

6.1.4 Protocolos de comunicaciones entre dispositivos

- Wifi – Nace a través de la alianza de varias empresas con el propósito de suministrar una conexión inalámbrica para conectar dispositivos electrónicos a través de puntos intermedios conocidos como puntos de acceso, este punto tiene un alcance en cuanto a distancia y establece una serie de canales para la comunicación, se basa en el estándar 802.11 para comunicaciones inalámbricas LAN, los dispositivos electrónicos requieren de un tarjeta de red inalámbrica para acceder a la señal que emiten los puntos de acceso, están en la mayoría de los casos viene integradas con el dispositivos, en otras se tiene que instalar y configurar. Esta comunicación a través de su nacimiento a contado con una serie de estándares que especifican frecuencias de 2.4, 5 GHz y la velocidad de 54 a 600 Mbps, entre los que destacan 802.11a, 802.11b, 802.11g, 802.11h, 802.11n.

- Zigbee - Nace como Zigbbe Alliance, su propósito es suministrar una conexión inalámbrica para conectar dispositivos electrónicos a un computador central, especial para redes domóticas, se basa en el estándar 802.15.4 para comunicaciones de inalámbricas PAN, que requieren envió de paquetes pequeños de información, bajo consumo de energía dado para dispositivos electrónicos que tiene bajan potencia, Zigbbe estipula 3 tipos de topología en estrella, árbol, malla. Se utiliza en la banda libre de 2.4GHz, la distancia que alcanza en exteriores a través de antenas dipolos es de 100m, en interiores suele estar en los 30m, los dispositivos que podemos encontrar en Zigbee para el control de las comunicaciones son, coordinadores controlan la red y los caminos a seguir por los dispositivos electrónicos, router controla la interconexión de dispositivos de una red con otra red, finales son encargados de comunicarse con los coordinadores y router para envió de información, puede manejar de 1 a 16 canales.

- NFC – Nace en 2003, su propósito suministrar conexión inalámbrica de corto alcance, trabaja en la banda de los 13.56 MHz, su radio de distancia es máximo de 20 cm, obteniendo una transferencia o velocidad de hasta 424 Kbits, obteniendo grandes volúmenes de datos para comunicaciones que requieran establecer comunicación lazos instantáneos, aunque fue pensada para dispositivos móviles, hoy en día se está utilizando mucho en el etiquetado RFID quien ha venido reemplazado los códigos de barras, puede actuar en dos modos activo cuando dos dispositivos generan un campo

electromagnético logrado así que entre ellos puedan intercambiar información, en modo pasivo en el que un dispositivo es el encargado de producir el campo electromagnético para que el otro dispositivo se una a él y así puedan empezar el intercambio de información.

- RFID - Es una tecnología que se basa en la identificación de elementos a través del uso de radiofrecuencia, permite la lectura de etiquetas aun cuando no se cuenta con visión directa, la etiqueta está formada por un chip el cual tiene conexión directa con una antena, luego un dispositivo lee la etiqueta para la captura de información, dos tipos de etiquetas se pueden encontrar las activas están necesitan disponer de una fuente de energía interna su ventaja es que permiten la portabilidad y las pasivas necesitan estar cerca de una fuente de energía que proporcione el trasmisor su ventaja es la durabilidad. Adicional se pueden encontrar 3 categorías de etiquetas RFID, las de solo lectura, la de una sola escritura muchas lecturas y las regrabables.

- Bluetooth – Es una tecnología que se basa en la conexión inalámbrica de dispositivos con un alcance mínimo de 1 metro hasta un máximo de 100 metros, soportado bajo le estándar 802.15.1, consta de dos partes, una encargada de modular y trasmitir la señal, el otro un controlador digital que procesa los enlaces, existen diferentes versiones de Bluetooth las cuales tiene estipuladas diferentes capacidades en la transferencia de datos, es así como aparecen las versiones 1 hasta la 4, teniendo tasas de transferencia de 4 Mb para la versión 3 y llegando hasta 25 Mb para la versión 4.

- Ethernet – Es una tecnología que se basa en la conexión de dispositivos a través de medios alambricos, diseñado inicialmente para conectar a través de cables coaxiales, en la actualidad se utilizan cables trenzados de cobre o fibra óptica, soportado bajo el estándar 802.3, su funcionalidad es la conexión de dispositivos a través de segmentos centralizados a través de un conmutador, como los dispositivos comparten un mismo medio, utilizan un protocolo que permite el acceso múltiple por detección de colisión, entre los sistemas Ethernet más destacados están 100base Tx, 100base Fx, 1000base T, 1000base Sx, 1000base Lx, obteniendo velocidades de hasta 250 Mbps y distancias en cable de cobre de hasta 100 metros y en fibra de hasta 500 metros. (S. Borondo, 2015)

6.2 CAPA DE COMUNICACIONES

Es la encargada de soportar la conectividad entre los diversos dispositivos que están presente en el internet de las cosas, los protocolos que más son utilizados son:

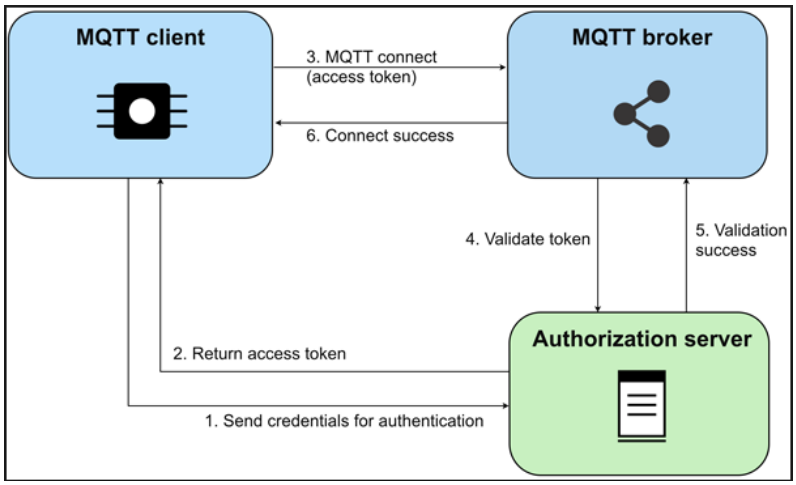
- TCP/IP – Es un protocolo de comunicación entre dispositivos, estableciendo una serie de reglas de comunicación para internet, controlando las trasmisiones, basado en direcciones ip o identificadores de red, soportado en un modelo de capas en donde cada módulo está orientado a tareas específicas ejecutando las tareas de forma secuencial de una capa a otra, sus capa inferior es la capa de interfaz de red encargada de enviar y recibir los paquetes dentro y fuera de la red, conectando tecnologías LAN y WAN, la siguiente capa es la de internet encargada de enrutar, direccionar los paquetes en esta capa se destacan protocolos como IP, ARP, ICMP, IGMP, la siguiente capa es la de transporte que tiene como función proporcionarle servicios a través de sesiones y establecer las comunicaciones a la capa subsiguiente cuenta con dos protocolos TCP, UDP, la siguiente capa es la de aplicación y su función es proporcionar servicios a las demás capas con el propósito fundamental del intercambio de información, sus protocolos destacados son HTTP, FTP, SMTP, DNS, RIP.

- MQTT - Es un protocolo abierto construido sobre TCP/IP, es uno de los estándares más utilizados para las comunicaciones que tiene que ver con sensores, objetos, cosas, lo que se conoce como Internet de las cosas, es básicamente un servicio de mensajería con comunicación asíncrona entre los pares, es liviano permitiendo que dispositivos de hardware básico que requieran anchos de banda no tan elevados puedan conectarse, también se adapta a cualquier tipo de escenario en el que estén presentes dispositivos y aplicaciones que requieran compartir información.

  Su arquitectura está basada en dos tipos de entidades como se observa en la **ilustración 5** un intermediario y los clientes, el intermediario no es más que un punto central que se encarga de recepcionar los mensajes de los clientes y redireccionarlos a destinos específicos, en el Internet de las cosas un cliente sería una cosa como un sensor o un aplicación, el cual se comunica a través de mensajes con el intermediario para así definir él envió y recepción de mensajes, el establecimiento o conexión entre los clientes y el intermediario se puede llevar a cabo a través de una conexión TCP/IP o a través de una conexión cifrada como la que lleva a cabo TLS, una vez se

realiza la conexión el cliente envía un mensaje con un tema específico al intermediario, este a su vez lo que hace es redireccionar este mensaje a todos los clientes que estén suscritos al tema específico, en el protocolo MQTT todos los mensajes deben estar organizados por temas, los desarrolladores de aplicaciones tienen la potestad de limitar la interacción con ciertos mensajes para algunos clientes. Estas aplicaciones pueden usar diversos tipos de formatos como JSON, XML, BASE64 (F. Moreno, 2018).

Ilustración 5 Protocolos de comunicación



Fuente: https://www.ibm.com/developerworks/ssa/library/iot-trs-secure-iot-solutions1/index.html

- CoAP – Es un protocolo de aplicación basado en el uso de software, su función es permite la comunicación de dispositivos en internet, especialmente dispositivos como sensores de baja potencia, implementa para la comunicación un modelo basado en el REST de HTTP, utilizando parámetros como GET, POST, PUT, DELETE, el formato de las cabeceras de este protocolo son reducidas, tiene una limitante en el intercambio de mensajes, su arquitectura está basada en servicios web utilizando dos tipos de mensajes petición y respuesta, algunas de sus características son el uso de comunicación multicast y soporte para protocolo UDP, CoAP es esencialmente utilizado en dispositivos de borde y dado el caso que el uso de HTTP demande demasiado ancho de banda (S. Molinero, 2018)

- RESTful – Es un protocolo basado en un arquitectura web que utiliza el protocolo HTTP con el objetivo de mejorar la comunicación entre cliente y servidor, su arquitectura se basa en unos principios específicos, el primer principio que todo lo que viaja en una comunicación web se define como recurso y tiene un formato especifico según el tipo de contenido, el segundo principio es que cada recurso necesita contar con un identificador único el cual se brinda a través de una URL, el tercer principio es que debe usar acciones conocidas de HTTP como GET, PUT, POST, DELETE, HEAD, CONNECT, el cuarto principio indica que cada recurso debe tener múltiples formatos de presentación, el quinto principio es tratar comunicaciones sin estado con el fin de que cada petición que reciba el servidor sea tramitada de manera independiente. Sus características principales son separación de recursos según su modelo de presentación, visibilidad, simplicidad, escalable para el aumento de peticiones que el servidor pueda atender, rendimiento en el tiempo para procesar las peticiones en el servidor y dar respuesta a los clientes (D. Gonzales, 2015).

- XMPP – Es un protocolo de mensajería abierto, a través de este protocolo se pueden diseñar una red de servidores independientes que no tiene un servidor central, cada usuario dentro de esta red debe tener un identificador el cual consta de los siguientes parámetros, nombre de usuario y una dirección DNS para identificar el servidor donde está almacenado el usuario, estos se encuentran separados por el signo @, una de sus características es que permite el uso de pasarelas, las cuales permiten que usuarios se conecten a otras redes que cuentan con otros protocolos de mensajería, otra característica indica que es un protocolo flexible ya que ha tenido una extensión a herramientas de colaboración, administración de redes, juegos, monitoreos remotos, adicional cualquier servidor XMPP puede ser aislado de la Internet, quedando como un servidor de intranet (J. Romero, 2015).

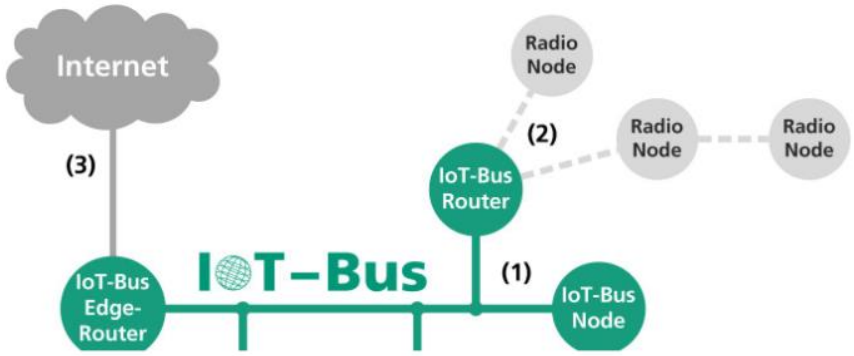
6.3 CAPA DE AGREGACIÓN / BUS

Esta capa cumple la función de traductor de borde entre las cosas (dispositivos) y la nube o internet, es muy importante ya que permite dar soporte a las comunicaciones entre el protocolo HTTP y un comunicador MQTT, lo que brinda que el lenguaje pueda hablar con los dispositivos que están generando diversos tipos de información, así que sirve de puente para escuchar los dispositivos

adecuando o trasformando los protocolos y que estos sean entendible por otros dispositivos que trabajen otros protocolos o hablen otro lenguaje, otra capacidad que provee esta capa es la interconexión de diversos dispositivos enrutando o guiando la comunicación hacia un destino específico, la **ilustración 6** presenta los buses que conectan con los dispositivos finales, buses que interconectan con un bus principal y buses de borde que son los que comunican con Internet, por medio de la utilización de Gateway o pasarelas de borde.

Otra característica de esta capa es que sirve de filtro, ya que debe validar que el cada portador tenga asociado un token o identificador, para luego a través de este identificador le permita el acceso a los recursos que está solicitando, a partir de allí le establezca una serie de políticas o permisos para el tiempo de acceso al dispositivo (L. Nieto, 2016).

Ilustración 6 Bus IoT



Fuente: https://www.iis.fraunhofer.de/en/ff/lv/net/tech/iot-bus.html

6.4 CAPA DE ANALÍTICA

Una vez la capa de agregación / bus, brinda a los dispositivos el acceso a los recursos, se empieza a generar un alto tráfico de datos el cual debe almacenarse en una base de datos, que soporte grandes volúmenes de información, es así que lo más recomendable es utilizar una plataforma de big data analytics, ya que adicional al almacenamiento de esta información, esta debe procesarse con el fin de analizar y determinar una serie de comportamientos que controlan los dispositivos en tareas automatizadas, la **ilustración 7** presenta como todos los dispositivos conectados generan información, esta debe ser estructurada generando una serie de eventos o reportes en tiempo real, las cuales modifican una serie de actividades que están controladas por los objetos o cosas

Ilustración 7 Analítica de datos

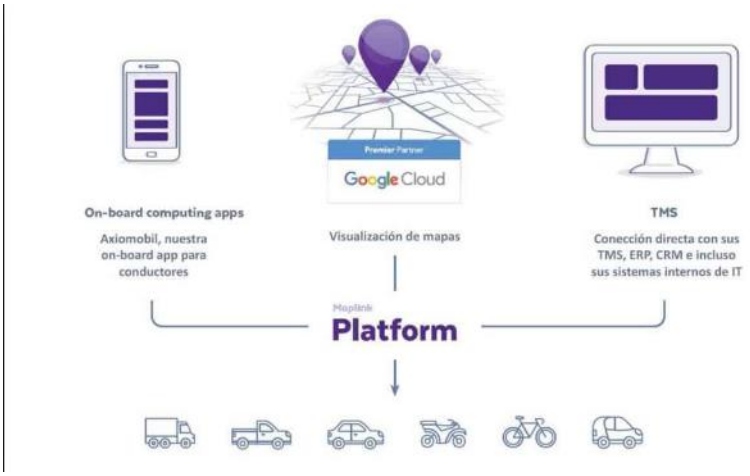
Fuente: http://www.5dias.com.py/big-data-y-como-revolucionar-la-empresa-con-el-manejo-de-la-informacion/

6.5 CAPA COMUNICACIONES EXTERNAS

Esta capa proporciona una serie de caminos de comunicación para los diferentes dispositivos que son externo al sistema o que se pueden catalogar como clientes, es así que estos dispositivos requieren de una plataforma que les permita estar en contacto con los dispositivos internos del sistema y así tener acceso a los múltiples eventos que estos van generando, como se observa en la **ilustración 8** diversos dispositivos generan información pero debe existir una plataforma que permita gestionar esa información, para que a través de aplicaciones los clientes puedan ser alertados de lo que informan sus dispositivos.

A partir de esta situación esta capa debe generar API´s, que no es más que una plataforma o portal que sirve de integrador de aplicaciones, para la comunicación de dispositivos, lo que facilita la gestión de dispositivos desde cualquier lugar a través del uso de una interfaz, adicional cuando un dispositivo en IoT, está operando no actúa de manera solitaria requiere de la comunicación con otros dispositivos, así que a través de esta plataforma se integra la adaptabilidad e integraciones abiertas para infinidad de dispositivos (J. Diaz, 2017).

Ilustración 8 Plataformas de gestión



Fuente: http://www.5dias.com.py/big-data-y-como-revolucionar-la-empresa-con-el-manejo-de-la-informacion/

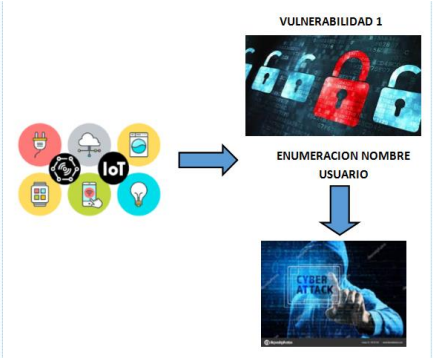
7. VULNERABILIDADES IoT

En el internet de las cosas cada día miles de dispositivos se empiezan a conectar a internet, es la evolución que se vivencia, esto genera que se puedan automatizar muchos procesos, de igual manera la economía empieza a girar de otra manera, la comodidad para usuarios es cada vez mayor, el análisis de la información toma otros rumbos, pero todo este desbordamiento de dispositivos conectados a internet, tiene consigo una serie de aspectos de seguridad que se tienen que abordar con mucho cuidado, es así como se han creado organizaciones para identificar una serie de falencias en diferentes aspectos de la tecnología, el grupo OWASP una comunidad abierta, es uno de estos quien se encarga de establecer información acerca de las vulnerabilidades en aplicaciones, pero como las tecnologías avanzan este grupo mira otras vulnerabilidades, en este caso realiza un listado de las vulnerabilidades más frecuentes que se están evidenciando en el Internet de las cosas, las cuales sirven de referencia a la hora de aplicar seguridad tanto en dispositivos, aplicaciones, protocolos, para el desarrollo de este informe se han extractado 10 ítem que se detallan a continuación en cada una de las ilustraciones que describen cada vulnerabilidad.

Algo que causa mucha curiosidad es que estas vulnerabilidades presentadas en los dispositivos, están dadas en muchas de las situaciones por fallos tan sencillos como contraseñas por defecto, utilización de usuarios o contraseñas sumamente sencillas, uso de protocolos o versiones que ya están obsoletas o fuera del mercado, también hay que comentar que otras se presentan en aspectos de programación o actualizaciones de firmware, implementación de protocolos, lo que es primordial es que están puedan ser verificadas antes de poner un dispositivos en un entorno productivo, por más de que este sea un producto de hogar y que parezca insignificante (OWASP, 2018)

La ilustración 9 relaciona la vulnerabilidad relacionada con la manera de cómo algunos dispositivos tienen carencias con la implementación de usuarios en los métodos de autenticación, razón por la cual se pueden utilizar diferentes herramientas para validar o recopilar una serie de usuarios básicos y así vulnerar el dispositivo

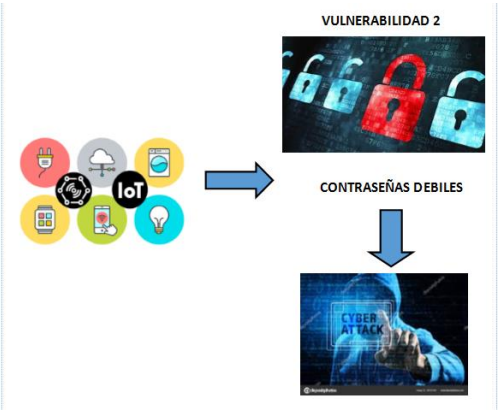
Ilustración 9 Vulnerabilidad 1 IoT



Fuente: Elaboración propia

La ilustración 10 relaciona la vulnerabilidad relacionada con el uso de contraseñas débiles que no cumplen con las políticas de complejidad de una longitud de 10 caracteres, palabras simples o contraseñas que se utilizan por defecto

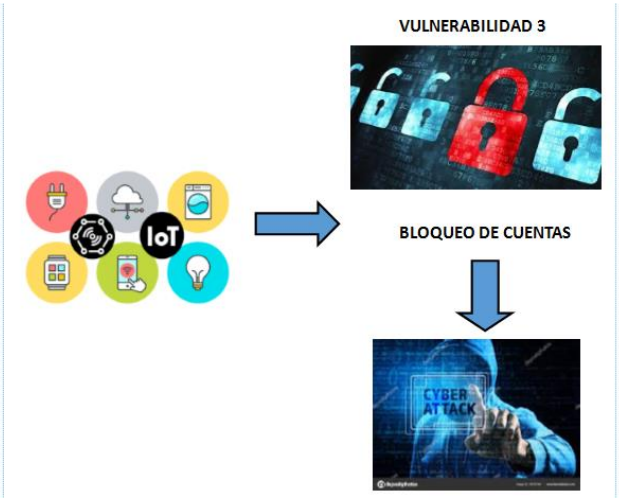
Ilustración 10 Vulnerabilidad 2 IoT



Fuente: Elaboración propia

La ilustración 11 relaciona la vulnerabilidad relacionada con los bloqueos de cuenta, es decir se permite que una persona intente autenticarse sin tener un límite de intentos a un dispositivo

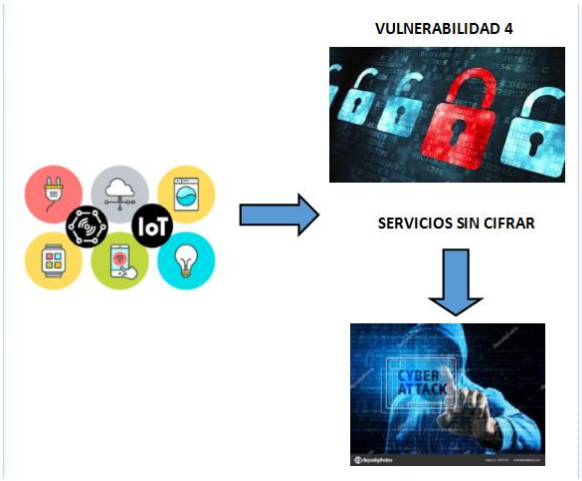
Ilustración 11 Vulnerabilidad 3 IoT



Fuente: Elaboración propia

La ilustración 12 relaciona la vulnerabilidad de servicios sin cifrar, es decir que muchos de los servicios no establecen canales de conexión seguros lo que no garantiza la fiabilidad en las comunicaciones

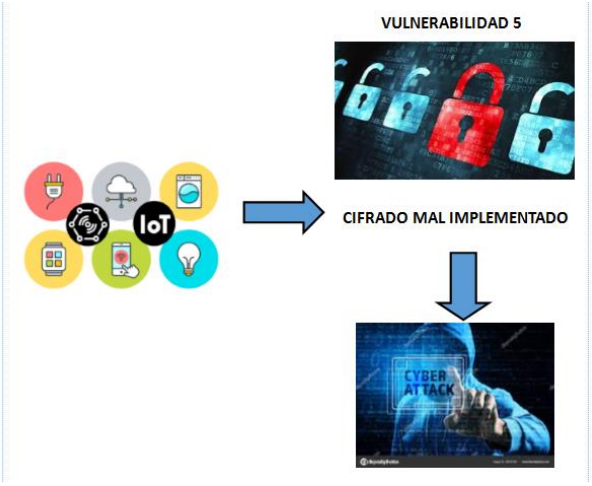
Ilustración 12 Ilustración Vulnerabilidad 4 IoT



Fuente: Elaboración propia

La ilustración 13 relaciona la vulnerabilidad de cifrado mal implementado, es decir que aunque se utilizan algoritmos para cifrar las comunicaciones o información, se aplican de mala manera al emplear versiones que ya no dan garantía como SSL v2, MD5, SHA1.

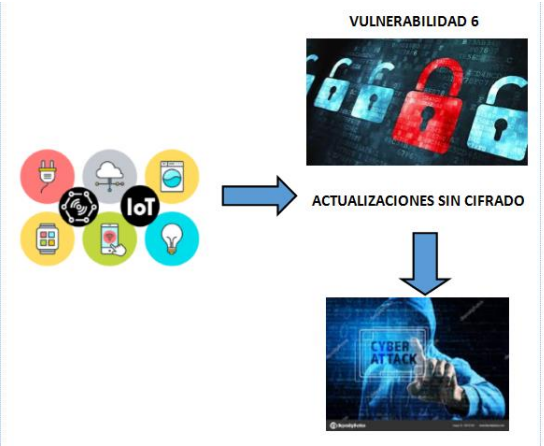
Ilustración 13 Vulnerabilidad 5 IoT



Fuente: Elaboración propia

La ilustración 14 relaciona la vulnerabilidad de actualizaciones sin cifrado, es decir se envían estas a través de canales no seguros pero no se protegen con TLS, o el archivo no se le aplica algoritmos de cifrado, para que llegue sin contratiempos al dispositivo

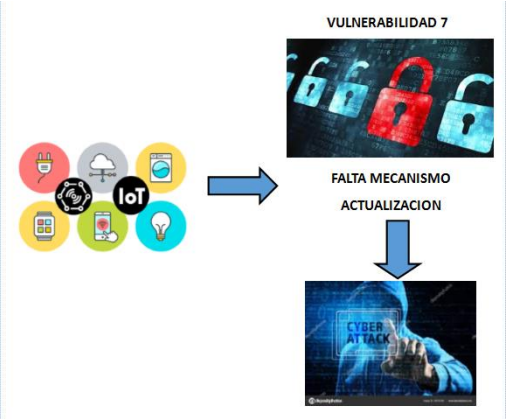
Ilustración 14 Vulnerabilidad 6 IoT



Fuente: Elaboración propia

La ilustración 15 relaciona la vulnerabilidad faltas de mecanismos de actualización, es decir que los dispositivos no reciben actualizaciones periódicas, quedando con versiones desactualizadas y sin protección, ni soporte.

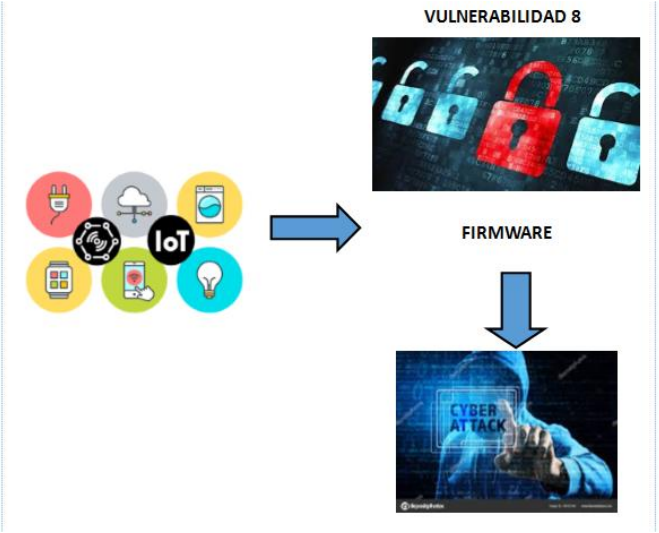
Ilustración 15 Vulnerabilidad 7 IoT



Fuente: Elaboración propia

La ilustración 16 relaciona la vulnerabilidad firmware, es decir que no se tiene conocimiento de que versión se está aplicando y si es la más adecuada para el dispositivo, del firmware se puede extraer información valiosa del dispositivo

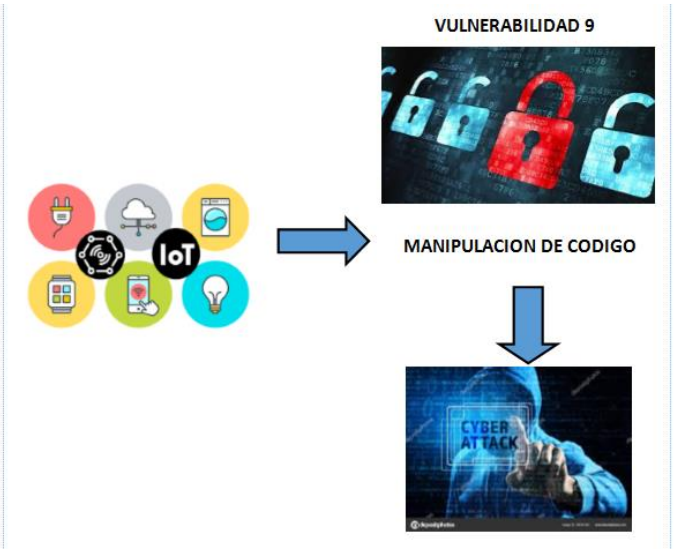
Ilustración 16 Vulnerabilidad 8 IoT



Fuente: Elaboración propia

La ilustración 17 relaciona la vulnerabilidad manipulación de código, es decir cambiar parámetros de ejecución del firmware del dispositivo evitando controles, o accediendo para verificar información que gestione el dispositivo

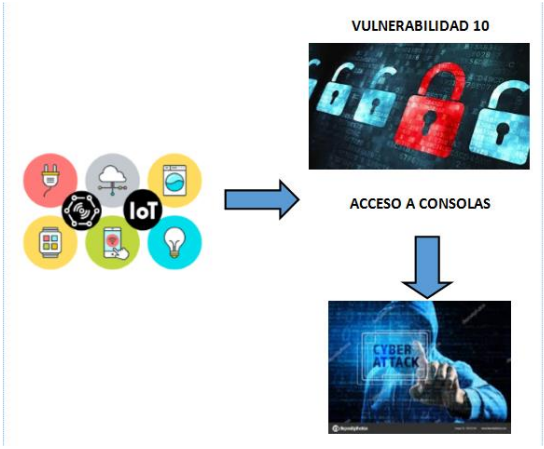
Ilustración 17 Vulnerabilidad 9 IoT



Fuente: Elaboración propia

La ilustración 18 relaciona la vulnerabilidad acceso a consolas, es decir obtener acceso al dispositivo por medio de conexiones seriales omitiendo los parámetros de autenticación establecidos

Ilustración 18 Vulnerabilidad 10 IoT



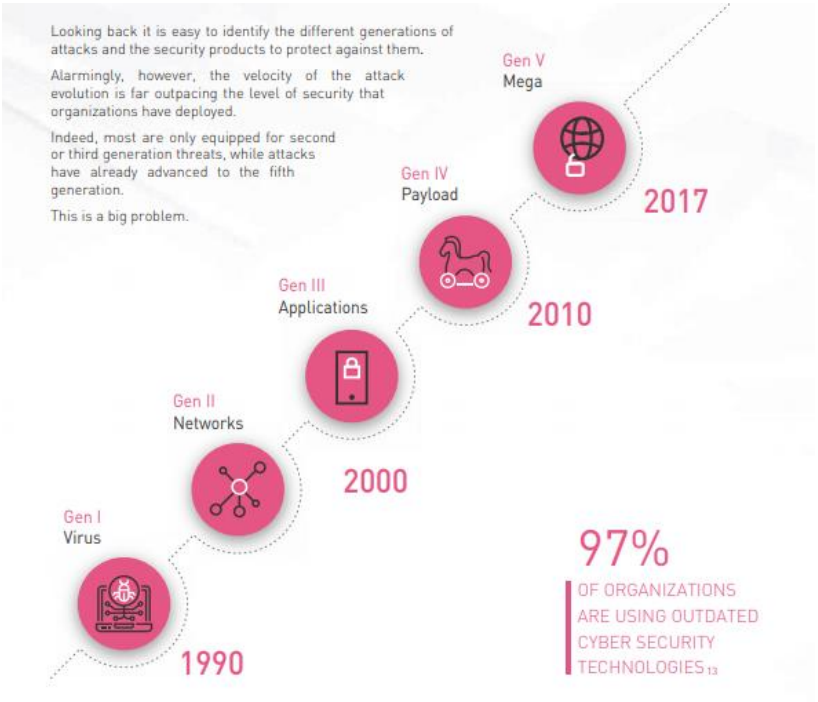
Fuente: Elaboración propia

8. ATAQUES EN IoT

Los ataques cibernéticos ha tenido una evolución, y estos cada día se vuelven más complejos, tecnificados, se han vivenciado diversas generaciones como lo indica el reporte realizado para 2018 por Check Point una de las organizaciones más importantes dedicadas a proveer soluciones de seguridad TI, los ataques tuvieron una primera generación basada en virus informáticos que buscaban infectar dispositivos, una segunda generación ya buscaba expandirse por muchos dispositivos a través de la red, una tercera generación empezó la búsqueda de otras posibilidades de ataque para este caso teniendo como foco las aplicaciones, hasta esta generación se ha tenido control, pero en la 4 generación a través del uso de exploits se empezaron a tecnificar estos ataques que ya no son tan controlables, que decir con la 5 generación que es la que se está llevando a cabo ya los atacantes buscan la afectación de tipo industrial, redes empresariales, móviles sistemas cloud y no podría escapar el Internet de las cosas.

Dentro de esta 5 generación, estos ataques se presentan de manera planeada, tecnificada, complejos, con mayores alcances y grandes repercusiones, teniendo así una mayor afectación, los ataques se presentan por malware a diferentes niveles, el ransonware, los ataques de denegación de servicios distribuida, fuerza bruta, algo que está incrementando y que asombra por su capacidad de reclutar dispositivos volviéndolos bots, zombies o reclutas, haciendo que estos sean manipulados o controlados por un delincuente informático de manera remota, provocando se puedan utilizar estos equipos reclutas para lanzar ataques de mayor fuerza a un objetivo específico , conllevando impactos negativos importantes en las organizaciones, que decir en el IoT, donde pueden manipular equipos que controlen algún tipo de equipamiento, o comprometiendo la privacidad de la información, en la **ilustración 19** se observa como ha sido la evolución por generaciones de los ataques cibernéticos (CHECK POINT, 2018).

Ilustración 19 Evolución de ataques informáticos



Fuente: 2018 Security Report Check Point Research

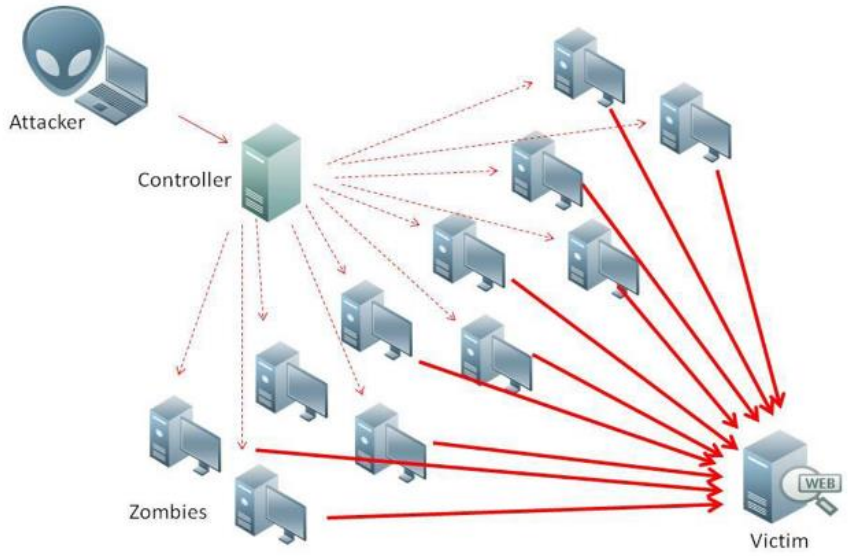
Así como la tecnología evoluciona, de igual manera lo hacen los ataques, hace unos años el mundo se veía atacado por virus, programas que buscaban infectar dispositivos de manera aislada para afectar su rendimiento, pero estos han tenido una evolución y se han convertido en una fuente esencial para los ciberdelicuentes, de igual manera los ataque de denegación de servicio, ahora presentan una evolución volviéndose ataques de denegación distribuida es decir desde varios puntos atacan de manera sincronizada para saturar un dispositivo o servicio.

Para empezar se puede indicar que uno de los primeros ataques realizados al Internet de las cosas (IoT), fue precisamente un ataque de denegación de servicio distribuida (DDoS) el más grande de este tipo efectuado el 26 de octubre de 2016, este ataque aprovecho la vulnerabilidad de los miles de dispositivos electrónicos que empezaban a constituir el IoT, la conexión a Internet era su principio básico, pero debido a la poca legislación internacional en cuanto a leyes que estipulen conceptos básicos de estándares de seguridad que deben cumplir los fabricantes

de dispositivos para ellos no es relevante el tema de la seguridad, lo importante es la cantidad de ventas que obtenga el dispositivo, adicional teniendo en cuenta la falta de cuidado de los usuarios que al comprar los dispositivos no tiene en cuenta hacer cosas tan sencillas como el cambio de los parámetros por defecto de las contraseñas, además la responsabilidad al lanzar estos dispositivos al mundo de la Internet de manera insegura, aprovechando estas vulnerabilidades el ataque lanzado a través de un script que infecto y comprometió a miles de dispositivos IoT, estos dispositivos comprometidos eran controlados remotamente por una atacante haciendo parte de un ejército zombie listo a escuchar órdenes para atacar lo que se conoce en términos de seguridad como una botnet, a partir de allí generaron una serie de scripts, que de manera distribuida y sincronizada debían enviarse para comprometer los sitios web que estaban conectados a Dyn Managed DNS dejándolos temporalmente fuera de servicio, Dyn una organización encargada de la gestión de rendimiento basado en la nube, proveedor DNS, entre los clientes afectados se encontraban Amazon, Twitter, Spotify, PayPal (Rafael Bucio, 2016).

En la **ilustración 20** se puede observar cómo es la estructura de un ataque DDoS, partiendo de un atacante, pasa a un controlador el cual infecta dispositivos volviéndolos zombies, para luego tener el control y ejecutar acciones distribuidas a una víctima especifica

Ilustración 20 Esquema Ataque DDoS



Fuente: https://www.xataka.com/basics/que-es-un-ataque-ddos-y-como-puede-afectarte

Por otro lado están los malware, uno de los más representativos en IoT, es el conocido como malware Mirai, tiene como propósitos la infección masiva de dispositivos para reclutarlos y organizarlos en una botnet, que no es más que un ejército de dispositivos que se controlan remotamente, ejecutando ordenes que son enviadas a través de un de un servidor que comanda las operaciones, otro propósito es ampliar su ejército para a partir de allí lanzar ataques de denegación de servicio distribuida comprometiendo la mayor cantidad de servicios, aplicaciones, dispositivos, pero como es el funcionamiento del malware Mirai, trabaja con una serie de listas que contienen usuarios y contraseñas por defecto las cuales se pueden observar en la **ilustración 21** y han sido identificadas en muchos de los dispositivos que están conectados a Internet, así que genera un script que es lanzado a través de diversos medios como archivos maliciosos, vulnerabilidades en sistemas operativos, infección de páginas web, vulnerabilidades en los navegadores, a la espera que al ejecutarlo en cualquier dispositivo este contenga esos usuarios o contraseñas por defecto y así pueda abrir un puerta trasera, para que sea controlado remotamente y reclutado por el ejército de botnet, de igual manera desde los dispositivos comprometidos se hace un escaneo de otros dispositivos escaneando las direcciones ip que están asociadas al puerto 48101TCP, indicando que son accesibles a través del protocolo Telnet el cual no ofrece seguridad, una vez la botnet tenga fuerza, lanzara ataques con instrucciones dadas desde el punto central a través de inundación de mensajes HTTP, GRE IP, SYN, ACK (Di Monte, E., & Solís, D., 2017)

Ilustración 21 Usuarios y contraseñas más comunes

root	xc3511	admin	1111	root	zlxx.
root	vizxv	root	666666	root	7ujMko0vizxv
root	admin	root	password	root	7ujMko0admin
admin	admin	root	1234	root	system
root	888888	root	klv123	root	ikwb
root	xmhdipc	Administrator	admin	root	dreambox
root	default	service	service	root	user
root	juantech	supervisor	supervisor	root	realtek
root	123456	guest	guest	root	00000000
root	54321	guest	12345	admin	1111111
support	support	guest	12345	admin	1234
root	(none)	admin1	password	admin	12345
admin	password	administrator	1234	admin	54321
root	root	666666	666666	admin	123456
root	12345	888888	888888	admin	7ujMko0admin
user	user	ubnt	ubnt	admin	1234
admin	(none)	root	klv1234	admin	pass
root	pass	root	zte521	admin	meinsm
admin	admin1234	root	hi3518	tech	tech
root	1111	root	jvbzd	mother	fucker
admin	smcadmin	root	anko		

Fuente: https://www.cert.gov.py/index.php/noticias/botnet-mirai-y-otras-amenazas-dispositivos-conectados-internet-iot

A partir del malware Mirai, han evolucionado nuevas versiones que buscan apropiar más propiedades y fortalecer el modo de infección, buscando otras alternativas, entre las que se destacan.

8.1 MORA

Surgido en diciembre de 2017, está basado en el uso de scripts de credenciales de autenticación comunes, pero en adición involucro dos vulnerabilidades más relacionadas con el puerto 37215 a través de un fallo detectado en la ejecución remota de código en los routers de Huawey, puerto 52869 a través de un fallo detectado con la ejecución de código en el servicio miniigd SOAP de dispositivos REALTEK, para la infección de dispositivos móviles como tablets, Smartphone (Y. Larin, 2017).

8.2 JENX

Utiliza la misma base de scripts de credenciales de Mirai, pero su enfoque principal es la de realizar ataques de DDoS, contra los dispositivos de jugadores del videojuego Grand Theft Auto San Andreas.

8.3 OMG

También basa su ejecución a través de ejecución de scripts de credenciales de autenticación, para acceder remotamente a dispositivos, pero adicional a involucrado el uso de tres servidores proxy, los cuales facilitan que puedan establecer un proxy SOCKS, HTTP, en el dispositivo que ya es controlado, esto permite que cualquier tipo de tráfico que pase por el dispositivo infectado pueda ser redirigido a elección de atacante, de igual manera sirve para atraer otras redes para que puedan tener salida de tráfico a través del dispositivo que está controlado (Ramírez García, A., 2018).

8.4 WICKED

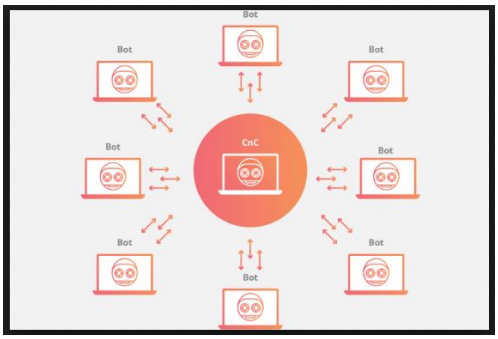
También utiliza la metodología de ofuscación que se utilizó en anteriores versiones, cambio el escaneo de credenciales por un propio escáner generado denominado RCE, su búsqueda se basa en la ubicación de enrutadores Netgear que presenten vulnerabilidades, al igual que dispositivos de circuito de televisión cerrada, cámaras, una vez han sido comprometidos descargan y ejecutan malware que reproduce nuevas botnets.

8.5 SORA

Detectado a principios del 2018, basado en Mirai busca dispositivos compatibles para ejecutar la infección a través de scripts de autenticación comunes, utilizando protocolos de conexión remota como SSH, busca a través de ataques de fuerza bruta ganar acceso a los dispositivos que encuentre vulnerables, accede remotamente y tiene la capacidad de ejecutar comandos que le permiten descargar y gestionar el binario óptimo de acuerdo a la plataforma que esté utilizando (Ruben Velasco, 2018).

En la **ilustración 22** se observa de manera gráfica como los dispositivos que han sido reclutados por un punto central se vuelven zombies, es decir están a la merced de lo que ordene el punto central, ejemplificando una botnet.

Ilustración 22 Estructura de una botnet



Fuente: https://hackerslatinos.com/como-se-pueden-lucrar-los-cibercriminales-con-una-botnet/

Asimismo se encuentran otros tipos de ataques como POODLE, este ataque aprovecha la vulnerabilidad del servicio SSL versión 3 el cual todavía es implementado aunque está demostrado que es inseguro, es utilizado por muchas plataformas en IoT, utilizado para establecer conexiones seguras en navegadores, servidores web, servidores de correo, en la cual se basa en una característica que cuando un intento de conexión falla, se podría forzar a un nuevo intento pero a través de un protocolo menos seguro, para poder realizar este tipos de ataques el primer paso es hacer un ataque de hombre en el medio ubicándose en una red para interceptar comunicaciones, a partir de allí efectúa la revisión y fuerza la falla de conexiones, para que le permita probar con una conexión SSL 3, si esta se permite aprovecha la vulnerabilidad, obteniendo el secuestro de cookies de una sesión o el registro en diferentes servicios online si tener que autenticarse con un usuario o contraseña (Cañon Miranda, D. A., 2016).

Además los tradicionales ataques por fuerza bruta o por diccionario también son predominantes en IoT, debido a la mala administración de dispositivos al dejar usuarios y contraseñas por defecto, en otros casos al hacer cambios en los usuarios y contraseñas, pero que aún no cuentan con parámetros mínimos de seguridad, se evidencia que en la masificación de dispositivos que ha traído IoT, la mayoría son utilizados por usuarios que no tienen conocimientos básicos en seguridad, simplemente les importa la funcionalidad de sus dispositivos, pero no saben a lo que pueden estar expuestos al conectarlos en la plataforma del Internet de las cosas. Estos ataque utilizan una serie de herramientas como Hydra, Medusa, que permiten la inyección de código validando una serie de combinaciones de caracteres usuales o comunes, para establecer una coincidencia, otros más sofisticados utilizan la creación de listados que contienen combinaciones de números, letras, caracteres, minúsculas, mayúsculas con unas características mínimas y máximas de longitud conocidos como diccionarios los cuales se pueden generar a través de herramienta como Crunch, o se pueden encontrar en sitios de Internet (Moreno Guataquira, N., Morón Castro, S., & Vega Torres, A. F. , 2017).

9. AMENAZA PERSISTENTE AVANZADA (Apt´s)

En un conjunto de procesos de piratería informática, dado que está dirigido en vulnerar dispositivos, servicios, aplicaciones de organizaciones o naciones, utilizan una serie de tareas avanzadas basadas en el uso de Malware, la idea de su terminología persistente consiste en una monitorización y control externo para acceder a información sensible, que se efectúa a un objetivo que está determinado específicamente y este se lleva de manera continua, guardando su visibilidad por el mayor tiempo posible, se determina que es amenaza ya que cuenta con la participación de personas (Jordi Medina, 2014)

Para crear una Apt´s se debe tener en cuenta los siguientes aspectos:

Los desarrolladores deben buscar información acerca de su objetivo, destacando los siguientes puntos:

- Sistemas informáticos
- Bases de datos utilizadas
- Dispositivos
- Sistemas de seguridad en la red perimetral
- Sistemas de seguridad puestos de trabajo
- Socios estratégicos

A partir de la recolección de esta información se identifican diferentes vulnerabilidades, los desarrolladores realizan software malicioso que permita atacar esas vulnerabilidades, una vez generado este malware buscan la manera de inyectarla en el objetivo esta es la parte compleja, pero debido a que este tipo de códigos tiene su primera instancia en la parte más vulnerable de cualquier organización el usuario final, el cual no cuenta con las capacidades de interpretar las características de seguridad que deben tenerse en cuenta, a través de ganarse la confianza para luego engañarlos o por la ingenuidad de algunos, es por allí que se rompe la cadena.

Esto llevado al mundo del Internet de las cosas se está acrecentando, debido a las vulnerabilidades encontradas en los dispositivos que cada día se conectan a Internet buscando mejorar la forma de comunicación de las personas. Algunas de las técnicas que tienen las Apt´s en IoT son (Jianpeng Mo, 2018):

9.1 Técnica de Evasión

Las Apt´s están diseñadas para evitar la detección, a través de la ofuscación de código esto trata de realizar cambios en el código fuente de manera que el código se enmascara de manera inversa para ocultar su funcionalidad, detección de entornos virtuales.

9.2 Técnica de ocultación

Busca la forma de ocultar el Malware que se instale en un dispositivo, evitando su fácil ubicación dentro del sistema.

9.3 Técnica de auto-propagación

Buscan la manera de permanecer ocultos durante mucho tiempo actuando de manera silenciosa, pero adicional buscan la manera de infectar otros dispositivos

9.4 Técnica de eficiencia de recursos

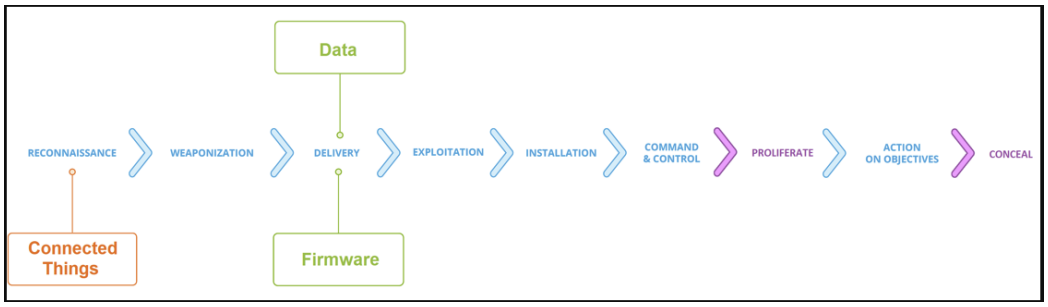
Es un factor que separa las Apt´s tradicionales de las de IoT, las Apt´s de IoT solo necesitan de menos de un 5% de la potencia de cómputo de los dispositivos para funcionar, pero el malware tiene la capacidad de adecuarse a la mínima tasa después de hacer una detección de la capacidad del dispositivo.

La estructura de ataque de un Apt´s de IoT sigue los siguientes ítems:

- Se realiza un reconocimiento a los dispositivos o cosas
- Se realiza un armamento basado en las vulnerabilidades encontradas en los dispositivos
- Se realiza la entrega del armamento a través de datos o firmware del dispositivo
- Una vez se entregue el armamento, inmediatamente se inicia la explotación del dispositivo
- Luego de hacer explosión el armamento se instala como huésped en el dispositivo
- Como huésped empieza a tomar control del dispositivo
- Teniendo control del dispositivo empieza a proliferar el armamento hacia otros dispositivos
- Cuando su cargamento se ha instalado con éxito en otros dispositivos, planea objetivos concretos y específicos
- Una vez realiza los ataques distribuidos se encubre para que nos sea detectado

En la ilustración 23 se puede observar de manera gráfica los pasos de la estructura de una Apt´s, de manera secuencial.

Ilustración 23 Metodología de las Apt´s de IoT



Fuente: https://www.opswat.com/blog/why-advanced-persistent-threats-are-targeting-internet-things

10. VULNERABILIDADES Y ATAQUES PRESENTADOS EN 4 DISPOSITIVOS IoT

Cada día es más frecuente el uso de dispositivos que se conectan a internet, buscando que diferentes sectores implementen estos servicios, para que una serie de tareas puedan ser optimizadas y automatizadas, desde cualquier lugar, pero esto se está generando sin tener algo importante en cuenta y es la seguridad que deben tener estos dispositivos, debido al auge y el comportamiento del mercado que solicita que cada elemento de la vida cotidiana esté conectado a la red enviando información sensible que permite tomar una serie de decisiones, esta tendencia del mundo globalizado hace que cada día compañías diseñen y saquen al mercado en tiempos muy cortos dispositivos tecnológicos que no cuentan con medidas de seguridad avanzadas, aun mas los usuarios que compran o implementan estos dispositivos no toma en cuenta las medidas de seguridad con las que debe contar, generando que estos dispositivos sean flanco rápidamente de los atacantes cibernéticos. Conclusiones que se dieron en el foro internacional de mecanismos contra el cibercrimen realizado por Digicert y Certicamaras en la ciudad de Bogotá, el día 29 de agosto de 2018 (Fernando Mejia, 2018).

A partir de allí se va a realizar un análisis de cuáles son los dispositivos más inseguros, cuáles son sus vulnerabilidades y cuáles son los ataques más frecuentes que se presentan en estos dispositivos, basados en páginas especializadas de seguridad encargadas de publicar las vulnerabilidades, entre las que destacan checkpoint, CVE, Embedi, Kaspersky, para ello se realizara el análisis a 10 dispositivos, cuya información estará organizada en una serie de tablas las cuales estarán listadas de la **tabla 1 a la tabla 4**, cada una de estas tablas brindaran una serie de detalles de seguridad encontrados como modelos, características, vulnerabilidades, ataques, para cámaras de seguridad, smartwatch, DVR, dron, router, aspiradora, acces point, almacenamiento NAS, estas se detallan a continuación.

Tabla 1 Detalles seguridad cámara de seguridad

Dispositivo Cámara de seguridad			
Modelos	Características	Vulnerabilidades	Ataques frecuentes
- Flir FX - Foscam - Geutebruck G-Cam/EFD-2250 - AXIS P1354 - Netwawe	- Comunicación Wifi - Video HD - Uso en exteriores - Protocolo H.264. - Grabación en la nube - Sensor infrarrojo pasivo - Conexión a servidor web	- Comunicación con casa matriz en texto plano y sin autenticación - Inyección código - Inyección SQL - Asignación incorrecta de permisos para control de recursos - Funciones ocultas - Controles de acceso inadecuado - No hay control en el consumo de recursos - Credenciales inseguras - Autenticación por defecto - Bloqueo a través de solicitudes POST - Autenticación HTTP básica - Corrupción de memoria - Acceso por Telnet - Firmware actualizable sin firmas digitales (Maria Korolov, 2016)	- MITM Hombre en el medio, que permiten verificar la comunicación entre dos dispositivos y así redireccionar trafico - Ataques de fuerza bruta, buscan encontrar contraseñas a través de combinación de caracteres básicos - Sniffing, olfatea y visualiza el tráfico en la búsqueda de vulnerabilidades.
Fuente: Elaboración propia			

Tabla 2 Detalles seguridad smartwatch

Dispositivo Smartwatch			
Modelos	Características	Vulnerabilidades	Ataques frecuentes
- Todos	- Cámara - Brújula - GPS - Wifi - Bluetooth - GPS Galileo, A-GPS - Sensores acelerómetro, luz, ritmo cardiaco	- Problemas de autenticación no se utiliza el doble factor - No soportan actualizaciones automáticas - Cifrado de datos, aunque utilizan protocolo SSL utilizan la versión 2 la cual tiene varias fallas de seguridad y la 3 que ha sido comprometida. - Se recoge información personal como nombre, fecha de nacimiento, dirección residencia - No hay protección de actualizaciones de firmware - El login vía web permite intentos ilimitados para la contraseña (Segu-info, 2015)	- Poodle funciona como exploit de hombre en el medio a través de inyección de comandos, se obtienen datos en texto plano - Harvesting de cuentas efectúa un ataque de fuerza bruta a los directorios de cuentas de usuario para obtener credenciales de acceso (Juan Ranchal, 2015)
Fuente: Elaboración propia			

Tabla 3 Detalle seguridad router

Dispositivo Router			
Modelos	Características	Vulnerabilidades	Ataques frecuentes
- D-link DSL 2750 – 816 - Linksys -	- Wifi wirelles N - ADSL2 - 4 puertos Ethernet - Velocidad fastethernet - 2 antenas externas - NAT - DDNS	- Firmware desactualizado - Credenciales por defecto - Enumeración de usuario - Omisión de autenticación - Control de acceso inadecuado - Inyección de código - No soportan actualizaciones automáticas - Contraseña administrativa en texto plano ruta /tmp/csman/0 - Parámetros de solicitud HTTP en la ruta /goform/diagnosis - Parámetros dest_host en solicitud diag_action = ping - Parámetros dentro de la configuración de ruta /goform/DDNS (Luis del Barco, 2018) -	- VPN Filter es un malware que aprovecha las vulnerabilidades de los router, para realizar el monitoreo del tráfico de los clientes del router - Inyección de comandos - Virus Mirai es una malware de tipo botnet el cual busca generar una red de robots para de allí realizar ataques programados a los clientes del router - DDoS es un ataque que busca denegar servicios a diferentes destinos realizando ataques de varios puntos de manera distribuida, va de la mano con los botnet ya que se vale de esa red para lanzar los ataques distribuidamente - Inyección de comandos que provocan desbordamiento de buffer o recuperación de resultados (Margolis, J., Oh, T. T., Jadhav, S., Kim, Y. H., & Kim, J. N, 2017)
Fuente: Elaboración propia			

Tabla 4 Detalle seguridad acces point

Dispositivo Punto de acceso			
Modelos	Características	Vulnerabilidades	Ataques frecuentes
- WatchGuard AP 100 - 102	- Comunicación wifi 802.11 a.b.n.g - Frecuencia 2.4 Ghz, 5 Ghz - Seguridad WPA2 TKIP-AES - 2 antenas omnidireccionales	- Credenciales por defecto alojadas en el fichero **/etc/passwd** - Método de autenticación oculto en la interfaz web parámetros de cabecera **AUTH_USER, AUTH_PASS** - Permitir subida de archivos a la raíz a través de la interfaz web - Error en la implementación de validación de contraseña, fallos de programación - Fallos con el firmware - Inyección de código	- Exploit que accede una cuenta codificada para una conexión SSH con un shell **/bin/false** - Ataque de acceso al permitir la autenticación mediante cuenta local y no la cuenta exclusiva de acceso web - Inyección de código aprovechando la subida de archivos a la raíz web y desde allí que se ejecute el código malicioso. - Exploit que permite que un atacante omita la comprobación del campo contraseña anterior en un formulario de cambio de contraseña (Juan Jose Ruiz, 2018)
Fuente: Elaboración propia			

11. ANALISIS MATRIZ DOFA

La herramienta de análisis DOFA permite establecer un análisis externo e interno de una variable, en este caso se tomara para analizar los 4 dispositivos IoT seleccionados, con la matriz se analizara cuáles con las fortalezas esto quiere decir que factores le dan ventajas de estos dispositivos ante otros en el mundo IoT, cuáles son las debilidades es decir las vulnerabilidades o desventajas de estos dispositivos, cuáles son las amenazas es decir todos esos ataques que pueden afectar al dispositivo, cuáles son las oportunidades es decir esos aspectos que nos pueden ayudar a fortalecer los dispositivos ante las diferentes debilidades y amenazas a las que están expuestos (Acero, L. C. P., 2010).

Es así que DOFA se define como:

- D = Debilidades
- O = Oportunidades
- F = Fortalezas
- A = Amenazas

Algo que se puede destacar con el análisis a través de la matriz DOFA, es que tanto las fortalezas y debilidades son internas viene con el dispositivo, las amenazas y oportunidades son externas así que los dispositivos deben estar preparados o atentos a reaccionar ante cualquier situación, esta matriz se presenta de la siguiente manera.

Tabla 5 Descripción campos Matriz DOFA

Matriz DOFA		
	Fortalezas	Debilidades
Oportunidades	(FO)	(DO)
Amenazas	(FA)	(DA)
Fuente: Elaboración propia		

Cada fila con su respectiva columna tiene su intersección de allí se establece lo siguiente. Fortalezas – oportunidades (FO), debilidades – oportunidades (DO), fortalezas – amenazas (FA), debilidades – amenazas (DA), cada una de estas combinaciones establece los siguientes aspectos:

- FO = Permite usar las ventajas para aprovechar las oportunidades
- FA = Permite usar las fortalezas para evitar las amenazas
- DO = Aprovechar oportunidades para minimizar las debilidades encontradas
- DA = Minimizar debilidades con el fin de prevenir amenazas

11.1 MATRIZ DOFA DISPOSITIVO CAMARA DE SEGURIDAD

Tabla 6 Matriz cámara seguridad

Matriz DOFA para Cámara seguridad		
	Fortalezas - Vigilancia en tiempo real 24x7 - Detección de intrusos - Puede estar conectadas con entes de seguridad - Sistema de grabación y almacenamiento en la nube - Se accede de manera remota - Usa medios alambricos e inalámbricos - Calidad de video en HD - Fácil instalación	**Debilidades** - Comunicación con casa matriz en texto plano y sin autenticación - Asignación incorrecta de permisos para control de recursos - Funciones ocultas - Controles de acceso inadecuado - Credenciales inseguras - Autenticación por defecto - Bloqueo a través de solicitudes POST - Autenticación HTTP básica - Acceso por Telnet
Oportunidades - Deshabilitar o cambiar credenciales por defecto - Deshabilitar Telnet - Utilizar protocolos de cifrado para la comunicación - Revisar antes de implementar los usuarios y permisos asignados para la configuración y administración de la cámara - Establecer seguridad en autenticación HTTP	- Acceder de manera remota al servidor para establecer procesos de vigilancia, utilizando usuarios con contraseñas previamente establecidas - Se puede utilizar medios alambricos e inalámbricos, utilizando métodos de cifrado de la comunicación - Sistemas de grabación en la nube se pueden proteger a través de establecer autenticación o certificados de seguridad en el sitio web	- Deshabilitar credenciales por defecto, permite crear nuevos usuarios y fortalecer las credenciales, evitando el acceso a funciones ocultas - Deshabilitar Telnet evita la comunicación en texto plano y si autenticación - Establecer seguridad en aplicaciones web, robustece la autenticación y el cifrado de las comunicaciones entre cliente y servidor, evitando inyecciones de código

Matriz DOFA para Cámara seguridad		
	Fortalezas - Vigilancia en tiempo real 24x7 - Detección de intrusos - Puede estar conectadas con entes de seguridad - Sistema de grabación y almacenamiento en la nube - Se accede de manera remota - Usa medios alambricos e inalámbricos - Calidad de video en HD - Fácil instalación	**Debilidades** - Comunicación con casa matriz en texto plano y sin autenticación - Asignación incorrecta de permisos para control de recursos - Funciones ocultas - Controles de acceso inadecuado - Credenciales inseguras - Autenticación por defecto - Bloqueo a través de solicitudes POST - Autenticación HTTP básica - Acceso por Telnet
Amenazas - MITM Hombre en el medio, que permiten verificar la comunicación entre dos dispositivos y así redireccionar trafico - Ataques de fuerza bruta, buscan encontrar contraseñas a través de combinación de caracteres básicos - Sniffing, olfatea y visualiza el tráfico en la búsqueda de vulnerabilidades. - Inyección SQL	- Se utilizan medios alámbricos e inalámbricos, lo que permite identificar que dispositivos están en escucha en la red - Al estar con entes de seguridad, se pueden guardar registros de actividad, para que sirva como evidencia en procesos jurídicos	- Deshabilitar protocolos de conexión remota inseguros como Telnet, proveer acceso a través de SSH - Fortalecer la seguridad en las bases de datos y variables en la programación de las páginas a través de los lenguajes, evitando inyecciones de código SQL - Establecer credenciales complejas y cifradas para evitar ataques para robo de contraseñas - Cifrar las comunicaciones entre cliente y servidor evita que terceros puedan ponerse en el medio para escuchar la comunicación y olfatear la red
Fuente: Elaboración propia		

11.2 MATRIZ DOFA DISPOSITIVO SMARTWATCH

Tabla 7 Matriz Smartwatch

Matriz DOFA para Smartwatch		
	Fortalezas - Cámara - Brújula - GPS - Wifi - Bluetooth - GPS Galileo, A-GPS - Sensores acelerómetro, luz, ritmo cardiaco - Acceso a Internet - Recepción y envió de emails	**Debilidades** - Problemas de autenticación no se utiliza el doble factor - No soportan actualizaciones automáticas - Cifrado de datos, aunque utilizan protocolo SSL utilizan la versión 2 la cual tiene varias fallas de seguridad y la 3 que ha sido comprometida. - Se recoge información personal como nombre, fecha de nacimiento, dirección residencia - No hay protección de actualizaciones de firmware - El login vía web permite intentos ilimitados para la contraseña
Oportunidades - Autenticación de doble factor - Cifrado con protocolo TLS - Utilizar cifrado de datos 3DES AES para información personal - Establecer intentos máximos de logueo y bloqueo de acceso vía web	- Con el acceso a Internet se puede establecer cifrado de la comunicación a través de TLS - La información que envían los sensores puede usar algoritmos de cifrado - Como se puede realizar consulta de datos a través web se puede establecer parámetros de tiempos de espera e intentos máximos de logueo a su vez bloqueo de la conexión.	- Utilizar autenticación de doble factor, evita la recopilación de datos personales a terceros - Utilizar protocolos TLS permite el uso de certificados para evitar actualizaciones de firmware falsas, adicional es más seguro que SSL - Establecer mecanismos de intentos, bloqueos de login en las conexiones, evita intentos de conexión ilimitados.

Matriz DOFA para Smartwatch		
	Fortalezas - Cámara - Brújula - GPS - Wifi - Bluetooth - GPS Galileo, A-GPS - Sensores acelerómetro, luz, ritmo cardiaco - Acceso a Internet - Recepción y envió de emails	**Debilidades** - Problemas de autenticación no se utiliza el doble factor - No soportan actualizaciones automáticas - Cifrado de datos, aunque utilizan protocolo SSL utilizan la versión 2 la cual tiene varias fallas de seguridad y la 3 que ha sido comprometida. - Se recoge información personal como nombre, fecha de nacimiento, dirección residencia - No hay protección de actualizaciones de firmware - El login vía web permite intentos ilimitados para la contraseña
Amenazas - Poodle funciona como exploit de hombre en el medio a través de inyección de comandos, se obtienen datos en texto plano - Harvesting de cuentas efectúa un ataque de fuerza bruta a los directorios de cuentas de usuario para obtener credenciales de acceso	- Como tiene acceso a internet, se puede establecer conexiones cifradas utilizando protocolos TLS, para evitar la obtención de datos en texto plano - Como utiliza conexión wifi establecer protocolos de seguridad como WPA2, con algoritmos AES y limitar los intentos de conexión fallidos - Se puede utilizar sensores como medios de autenticación biométricos	- Utilizar métodos de autenticación de doble factor, evita ataques de fuerza bruta - Utilizar canales seguros a través de TLS, evita el envió de datos en texto plano - Proteger el dispositivo de actualizaciones engañosas, evita el uso de exploit - Fortalecer los mecanismos de autenticación e intentos de conexión vía web, evita ataques por fuerza bruta
Fuente: Elaboración propia		

11.3 MATRIZ DOFA DISPOSITIVO ROUTER

Tabla 8 Matriz router

Matriz DOFA para Router		
	Fortalezas - Permite alcanzar otras redes - Utiliza medios alambricos e inalámbricos - Muy utilizado - Cortafuego interno - Conexión a internet de alta velocidad - Control de acceso usuarios - Seguridad wifi WPA2 - Filtrado direcciones MAC - Soporte conexión IPV6	**Debilidades** - Firmware desactualizado - Credenciales por defecto - Enumeración de usuario - Omisión de autenticación - Control de acceso inadecuado WPS - Inyección de código - No soportan actualizaciones automáticas - Contraseña administrativa en texto plano ruta /tmp/csman/0 - Parámetros de solicitud HTTP en la ruta /goform/diagnosis - Parámetros dest_host en solicitud diag_action = ping - Parámetros dentro de la configuración de ruta /goform/DDNS
Oportunidades - Actualización firmware - Autenticación de doble factor - Algoritmos de cifrado - Corrección de errores de programación - Acceso web seguro HTTPS - Control de acceso	- - Filtrar con las direcciones MAC de los dispositivos que se conectan al router - Conexión de alta velocidad, permite actualizaciones de firmware - Permite el control de acceso con el cual se puede establecer usuarios y contraseñas robustas - Al utilizar seguridad WPA2, se cifra las contraseñas que están en texto plano - Como es un dispositivo muy utilizado corregir problemas de programación - Deshabilitar el acceso remoto al equipo, con el fin de filtrar direcciones que se conectan al equipo	- - Con la corrección de errores de programación se limita la inyección de código. - Al utilizar autenticación de doble factor, se cierra la puerta al uso de credenciales por defecto - Utilizar algoritmos de cifrado evita que las contraseñas viajen en texto plano - Establecer un control de acceso adecuado evita la omisión de autenticación - Utilizar conexiones TLS cifradas de acceso web con certificados HTTPS, evita información en texto plano

Matriz DOFA para Router		
	Fortalezas - Permite alcanzar otras redes - Utiliza medios alambricos e inalámbricos - Muy utilizado - Cortafuego interno - Conexión a internet de alta velocidad - Control de acceso usuarios - Seguridad wifi WPA2 - Filtrado direcciones MAC - Soporte conexión IPV6	**Debilidades** - Firmware desactualizado - Credenciales por defecto - Enumeración de usuario - Omisión de autenticación - Control de acceso inadecuado WPS - Inyección de código - No soportan actualizaciones automáticas - Contraseña administrativa en texto plano ruta /tmp/csman/0 - Parámetros de solicitud HTTP en la ruta /goform/diagnosis - Parámetros dest_host en solicitud diag_action = ping - Parámetros dentro de la configuración de ruta /goform/DDNS
Amenazas - VPN Filter es un malware que aprovecha las vulnerabilidades de los router, para realizar el monitoreo del tráfico de los clientes del router - Virus Mirai es una malware de tipo botnet el cual busca generar una red de robots para de allí realizar ataques programados a los clientes del router - DDoS es un ataque que busca denegar servicios a diferentes destinos realizando ataques de varios puntos de manera distribuida, va de la mano con los botnet ya que se vale de esa red para lanzar los ataques distribuidamente -	- Establecer un control de acceso más fuerte, cambiando contraseñas por defecto que trae consigo el router de fábrica - Como utiliza medios de conexión alambricos fortalecer el acceso y cifrado de claves a través de seguridad WPA2- Algoritmo AES - Monitorear los accesos y tráfico del equipo - Como posee un cortafuegos interno deshabilitar opciones que no usadas - Como permite conexiones de alta velocidad actualizar periódicamente el dispositivo - Como permite el filtrado MAC configurar los dispositivos que se conectan	- Actualizar periódicamente el firmware del dispositivo cierra puertas traseras - Establecer contraseñas robustas con algoritmos de encrypcion evita accesos no autorizados - Revisar los parámetros de programación web en las solicitudes, por parte del fabricante para evitar la inyección de código - Se debe establecer autenticación de doble factor para evitar que el router sea parte de una Botnet - Evitar controles de acceso inadecuado como la administración remota, para evitar que el dispositivo sea controlado por un delincuente - Como en dados casos el router permite la autenticación sin contraseña como WPS deshabilitarla y ocultar el SSID
Fuente: Elaboración propia		

11.4 MATRIZ DOFA DISPOSITIVO PUNTO DE ACCESO

Tabla 9 Matriz punto de acceso

Matriz DOFA para Punto de acceso		
	Fortalezas - Comunicación inalámbrica wifi 802.11 a.b.n.g - Usa de ondas de radio - Administración vía Web - Frecuencia 2.4 Ghz, 5 Ghz - Seguridad WPA2 TKIP-AES - 2 antenas omnidireccionales - Filtrado MAC - Estándar LAN Gigabit Ethernet	**Debilidades** - Credenciales por defecto alojadas en el fichero /etc/passwd - Método de autenticación oculto en la interfaz web parámetros de cabecera AUTH_USER, AUTH_PASS - Permitir subida de archivos a la raíz a través de la interfaz web - Error en la implementación de validación de contraseña, fallos de programación - Fallos con el firmware - Inyección de código
Oportunidades - Actualización de firmware - Corregir fallos de programación aplicación web - Limitar el acceso a la ruta /etc/passwd - Denegar la subida de archivos a la raíz del sistema - Usar pruebas de autenticación en aplicaciones web para diferenciar máquinas de humanos - Utilizar métodos de consulta POST	- Filtrar con las direcciones MAC de los dispositivos que se conectan al acces point - Acceso a internet permite actualizaciones de firmware periódicas - Permite el control de acceso con el cual se puede establecer usuarios y contraseñas robustas - Al utilizar seguridad WPA2, se cifra las contraseñas que están en texto plano - Como es un dispositivo que permite la administración web, debe corregir problemas de programación y autenticación	- Actualización de firmware, corrige vulnerabilidades halladas - Corregir fallos de programación evita el acceso a ficheros del sistema - Usar Captcha para validar peticiones de usuario, evita los métodos de autenticación ocultos o errores en la validación de contraseñas - Utilizar métodos de consulta POST, en la aplicación web, evita la subida de archivos y la inyección de código

Matriz DOFA para Punto de acceso		
	Fortalezas - Comunicación inalámbrica wifi 802.11 a.b.n.g - Usa de ondas de radio - Administración vía Web - Frecuencia 2.4 Ghz, 5 Ghz - Seguridad WPA2 TKIP-AES - 2 antenas omnidireccionales - Filtrado MAC - Estándar LAN Gigabit Ethernet	**Debilidades** - Credenciales por defecto alojadas en el fichero /etc/passwd - Método de autenticación oculto en la interfaz web parámetros de cabecera AUTH_USER, AUTH_PASS - Permitir subida de archivos a la raíz a través de la interfaz web - Error en la implementación de validación de contraseña, fallos de programación - Fallos con el firmware - Inyección de código
Amenazas - Exploit que accede una cuenta codificada para una conexión SSH con un shell /bin/false - Ataque de acceso al permitir la autenticación mediante cuenta local y no la cuenta exclusiva de acceso web - Inyección de código aprovechando la subida de archivos a la raíz web y desde allí que se ejecute el código malicioso. - Exploit que permite que un atacante omita la comprobación del campo contraseña anterior en un formulario de cambio de contraseña	- Como utiliza medios de conexión alambricos fortalecer el acceso y cifrado de claves a través de seguridad WPA2- Algoritmo AES - Monitorear los accesos y tráfico del equipo a través de la administración web - Como permite acceso a internet actualizar periódicamente el firmware del dispositivo - Como permite el filtrado MAC configurar los dispositivos que se conectan - Como posee administración web, se debe corregir problemas de programación de la aplicación - Solo permitir autenticación con credenciales de acceso web	- Actualizar periódicamente el firmware del dispositivo limita las vulnerabilidades - Revisar los parámetros de programación web en las solicitudes, por parte del fabricante para evitar la inyección de código - Deshabilitar acceso a root para acceso remoto, previene la conexión a una Shell - Deshabilitar conexiones Root SSH - Denegar el acceso a cuenta locales alojadas, establecer autenticación de doble factor para cuentas de acceso web - Para reducir la inyección de código en la aplicación web, se debe reemplazar caracteres especiales por su equivalencia textual
Fuente: Elaboración propia		

12. GUIA DE BUENAS PRACTICAS DE ASEGURAMIENTO EN 4 DISPOSITIVOS IoT

Luego de establecer una serie de aspectos de seguridad, en 4 dispositivos de IoT, es adecuado presentar una guía, donde se establezcan una serie de buenas prácticas a tener en cuenta a la hora de hacer un aseguramiento de los 4 dispositivos que va a estar comunicados a través de Internet, para ello lo primero es definir cuáles son las vulnerabilidades, amenazas más recurrentes que afectan estos dispositivos y son frecuentemente utilizados por los atacantes, sacando provecho y así obteniendo una serie de accesos que facilitan el robo de información o servir de puente para lanzar otros ataques.

En esta primera parte se establecerán las vulnerabilidades y amenazas que más afectan a estos 4 dispositivos IoT seleccionados, una segunda parte estará relacionada a la guía de buenas prácticas que se deben tener en cuenta a la hora de evitar que los dispositivos seleccionados sean vulnerables, tocando varios aspectos buscando que su aseguramiento sea de mejor manera para así evitar que sean afectados por las diversas amenazas que día a día aparecen, por esta razón la guía de buenas prácticas abordara dos ítems importantes una guía para usuarios finales quienes son los que finalmente interactúan con los dispositivos, la otra para configuraciones específicas de los equipos.

Se detallan las vulnerabilidades encontradas en los 4 dispositivos seleccionados, cámaras de seguridad, smartwatch, router, punto de acceso, las cuales estarán asociadas a un código identificado con la letra V seguido de un numero ejemplo V1

Tabla 10 Resumen Vulnerabilidades 4 dispositivos IoT

Vulnerabilidades 4 dispositivos IoT	
Descripción	Código
- Comunicación en texto plano y sin autenticación	V1
- Controles de acceso inadecuado	V2
- Credenciales inseguras	V3
- Autenticación por defecto	V4
- Asignación incorrecta de permisos para control de recursos	V5
- Inyección código	V6
- Bloqueo a través de solicitudes POST	V7
- Bloqueo a través de solicitudes POST	V8
- El login vía web permite intentos ilimitados para la contraseña	V9
- Método de autenticación oculto en la interfaz web parámetros de cabecera AUTH_USER, AUTH_PASS	V10
- Enumeración de usuario	V11
- Cifrado de datos y canales de comunicación	V12
- Error en la implementación de validación de contraseña, fallos de programación	V13

Vulnerabilidades 4 dispositivos IoT	
Descripción	Código
- Permitir subida de archivos a la raíz a través de la interfaz web	V14
- No hay control en el consumo de recursos	V15
- Corrupción de memoria	V16
- Acceso por Telnet	V17
- No soportan actualizaciones automáticas	V18
- Fallos con el firmware	V19
Fuente: Elaboración propia	

Se detallan las amenazas más frecuentes encontradas en los 4 dispositivos seleccionados, cámaras de seguridad, smartwatch, router, punto de acceso, las cuales estarán asociadas a un código, identificado con la letra A seguido de un numero ejemplo A1

Tabla 11 Resumen Amenazas 4 dispositivos IoT

Amenazas 4 dispositivos IoT	
Descripción	Código
- Inyección SQL	A1
- MITM Hombre en el medio, que permiten verificar la comunicación entre dos dispositivos y así redireccionar trafico	A2
- Ataques de fuerza bruta, buscan encontrar contraseñas a través de combinación de caracteres básicos	A3
- Sniffing, olfatea y visualiza el tráfico en la búsqueda de vulnerabilidades	A4
- Poodle funciona como exploit de hombre en el medio a través de inyección de comandos, se obtienen datos en texto plano	A5
- Harvesting de cuentas efectúa un ataque de fuerza bruta a los directorios de cuentas de usuario para obtener credenciales de acceso	A6
- VPN Filter es un malware que aprovecha las vulnerabilidades de los router, para realizar el monitoreo del tráfico de los clientes del router	A7
- Inyección de comandos	A8

Amenazas 4 dispositivos IoT	
Descripción	Código
- Virus Mirai es una malware de tipo botnet el cual busca generar una red de robots para de allí realizar ataques programados a los clientes del router	A9
- DDoS es un ataque que busca denegar servicios a diferentes destinos realizando ataques de varios puntos de manera distribuida, va de la mano con los botnet ya que se vale de esa red para lanzar los ataques distribuidamente	A10
- Exploit que accede una cuenta codificada para una conexión SSH con un shell **/bin/false**	A11
- Ataque de acceso al permitir la autenticación mediante cuenta local y no la cuenta exclusiva de acceso web	A12
- Inyección de código aprovechando la subida de archivos a la raíz web y desde allí que se ejecute el código malicioso.	A13
- Exploit que permite que un atacante omita la comprobación del campo contraseña anterior en un formulario de cambio de contraseña.	A14
Fuente: Elaboración propia	

12.1 CREDENCIALES DE ACCESO DISPOSITIVOS

Tabla 12 Buenas practicas credenciales

Credenciales de acceso	
Recomendación	Prevención Vulnerabilidad / Amenaza
- Contraseña debe estar compuesta por mínimo 10 caracteres - Contraseña debe estar compuesta por letras minúsculas, mayúsculas, números, caracteres especiales - Contraseña no debe contener fechas, ni nombres personales, ni palabras comunes - Contraseña debe cambiarse cada 3 meses - Contraseña es de carácter personal y no se debe compartir con terceros - Si utiliza administración web, no guardar las contraseñas en el navegador - Cambie o deshabilite las credenciales de usuario y contraseña que se establcen por defecto en los dispositivos	- V3, V2 A3, A6, A12 - V3, V2 A3, A6, A12 - V3, V2 A3, A6, A12 - V3, V2 A3, A6, A12 - V3, V2 A3, A6, A12 - V3, V2 A3, A6, A12 - V4, V3, V2 A3, A6, A12
Fuente: Elaboración propia	

12.2 CONTROL DE ACCESO LOGICO A LOS DISPOSITIVOS

Tabla 13 Buenas practicas control de acceso

Control de acceso	
Recomendación	Prevención Vulnerabilidad / Amenaza
- Limitar los intentos fallidos de conexión al dispositivo a máximo 2 - Bloquear la sesión al sobrepasar los intentos de conexión permitidos - Bloquear las sesiones cuando estas se encuentren inactivas - Cambiar usuarios y contraseñas por defecto - - Utilizar autenticación de doble factor, con el uso de token o pines - Asignar permisos para que los usuarios solo puedan hacer configuraciones específicas que no comprometan el sistema - Revisar periódicamente los eventos que se registran o establecer un sistema que permita validar los registros de actividad determinando quien está accediendo al dispositivo -	- V2, V4, V9, V11 A3, A6, A7, A12 - V2, V4, V9, V11 A3, A6, A7, A12 - V2, V4, V9, V11 A3, A6, A7, A12 - V2, V4, V9, V11 A3, A6, A7, A12 - V2, V4, V9, V11 A3, A6, A7, A12 - V2, V4, V5, V6, V10, V14 A3, A6, A7, A8, A12, A13 - V1, V2, V3, V4, V9, V10, V11, V14, A10, A12
Fuente: Elaboración propia	

12.3 COMUNICACIÓN CON DISPOSITIVOS

Tabla 14 Buenas prácticas de comunicación

Comunicacion	
Recomendación	Prevención Vulnerabilidad / Amenaza
- No utilizar protocolos obsoletos e inseguros de conexión remota como Telnet - Deshabilitar el protocolo Telnet en los dispositivos - Establecer conexiones remotas a través del uso de protocolo SSH versión 2 - - Utilizar para la autenticación de la conexión algoritmos asimétricos como RSA, con tamaño mínimo de clave de 1024 - Limitar los intentos de conexión - - Bloquear la conexión cuando se superan los intentos - Bloquear la sesión cuando se presenta inactividad - Cambiar los puertos por defecto de protocolos o servicios web - No utilizar las versiones de SSL protocolo de conexión para la comunicación web - En lo posible garantizar la conexión para la comunicación vía web a través de protocolo TLS en sus versiones 1.2, 1.3	- V1, V2, V3, V17, A3, A4, A11, A12 - V1, V2, V3, V17, A3, A4, A11, A12 - V1, V2, V3, V12, V17, A2, A3, A4, A5, A11, A12 - V1, V2, V3, V12, V17, A2, A3, A4, A5, A11, A12 - V2, V9, V11, A3, A5, A6, A11, A12 - V2, V9, V11, A3, A5, A6, A11, A12 - V2, V9, V11, A3, A5, A6, A11, A12 - V2, A4, A12 - S - V1, V3, V11, V12, A2, A4, A5 - V1, V3, V11, V12, A2, A4, A5
Fuente: Elaboración propia	

12.4 CONFIGURACION REDES INALAMBRICAS WIFI DISPOSITIVOS

Tabla 15 Buenas practicas configuración Wifi

Comunicación Wifi	
Recomendación	Prevención Vulnerabilidad / Amenaza
- Cambiar el SSID que viene por defecto con los dispositivos - Ocultar el SSID para que la red no sea visible a terceros - Desactivar el modo ad-hoc - - Utilizar protocolo 802.1x con autenticación EAP, Radius - Realice un filtrado de direcciones MAC, para que solo se conecten dispositivos de confianza - Realizar actualizaciones periódicas del firmware - - Evitar uso de dispositivo, si no se cuenta con firmware actualizado - - No utilizar métodos de encriptación como WEP o WPA - Utilizar métodos de encriptación como WPA2 - Desactivar el mecanismo WPS, que permite la conexión a través de un PIN	- V2, V3, V4, A2, A3, A4, A6 - V2, V3, V4, A2, A3, A4, A6 - V2, V3, V4, A2, A3, A4, A6 - V2, V3, V4, V15, A2, A3, A5, A6, A7 - V1, V2, A2, A7 - - - V1, V6, V13, V15, V16, V17, V19, A7, A9, A11 - V1, V6, V13, V15, V16, V17, V19, A7, A9, A11 - V1, V2, V12, A3, A6, A9, A10, A11 - V1, V2, V12, A3, A6, A9, A10, A11 - V1, V2, V3, A2, A4, A7, A9, A10
Fuente: Elaboración propia	

12.5 APLICACIONES WEB DE ADMINISTRACION DE DISPOSITIVOS

Tabla 16 Buenas practicas aplicaciones web

Aplicaciones web	
Recomendación	Prevención Vulnerabilidad / Amenaza
- Implementar autenticación multifactor - Establecer políticas de longitud - Complejidad y continua rotación de contraseñas - Limite los intentos fallidos de inicio de sesión de usuarios - Registrar todos los fallos que ocurran al inicio de sesión, control de acceso y validación de entradas - No almacenar datos sensibles innecesariamente - Separar datos de comandos y consultas - Utilizar API segura - Evite el uso de intérpretes por completo - Realizar validaciones de entrada de datos utilizando listas blancas - Utilizar controles SQL como LIMIT, evitando fuga masiva de registros	- V2, V3, V4, V9, V11, V13, A3, A5, A6, A11, A12, A14 - V2, V3, V4, V9, V11, V13, A3, A5, A6, A11, A12, A14 - V2, V3, V4, V9, V11, V13, A3, A5, A6, A11, A12, A14 - V2, V3, V4, V9, V11, V13, A3, A5, A6, A11, A12, A14 - V5, V9, V11, V15, V16, A2, A3, A4, A6 - V6, A1, A4, A5, A6, A8 - V6, V7, V8, V14, A1, A5, A7, A8, A12, A13, A14 - V6, V7, V8, V14, A1, A5, A7, A8, A12, A13, A14 - V6, V7, V8, V14, A1, A5, A7, A8, A12, A13, A14 - V6, V7, V8, V14, A1, A5, A7, A8, A12, A13, A14

- - Utilice métodos de cifrado para datos almacenados cuando estos sean sensibles - Cifre los datos en tránsito a través del uso de canales seguros con protocolo TLS - Deshabilitar el almacenamiento en cache de datos sensibles - Almacene contraseñas aplicándoles hash Argon2, bcrypt, sha512 - No utilice hash para almacenar contraseñas como MD5, SHA1 - Usar plataformas sin funcionalidades innecesarias, no instale frameworks	- V6, V7, V8, V14, A1, A5, A7, A8, A12, A13, A14 - V1, V12, A2, A4, A7 - - V1, V12, A2, A4, A7 - - V6, V7, V8, V14, A1, A5, A7, A8, A12 - V1, V3, V12, A1, A2, A3, A5, A6, A14 - V1, V3, V12, A1, A2, A3, A5, A6, A14 - V6, V7, V8, V14, A1, A5, A7, A8, A12, A13, A14
Fuente: Elaboración propia	

13. CONCLUSIONES

Al término de esta investigación las conclusiones que se plantean son las siguientes

- La arquitectura IoT, está basada en una serie de capas que permiten entender el funcionamiento de los dispositivos desde el momento que empiezan a generar información, hasta el momento en que se puede consultar esa información desde un cliente en cualquier lugar solo contando con un acceso a Internet.

- Debido al auge de IoT, cada vez mas dispositivos se conectan a la red, pero muchos de ellos no cuentan con medidas esenciales de seguridad, evidenciando una serie de vulnerabilidades relacionadas con los controles de acceso y el cifrado de la información, lo que conlleva a una serie de ataques relacionados con denegación de servicios, accesos no autorizados, por medio del uso de exploits sofisticados

- En los 4 dispositivos IoT, seleccionados se evidencia vulnerabilidades frecuentes relacionadas con autenticaciones por defecto, debilidad en contraseñas, fallas en controles de acceso, inyección de código en las plataformas web, desactualización de firmware

- Las amenazas más frecuentes evidenciadas en los 4 dispositivos IoT, seleccionados están basados en malware, exploits, denegación de servicios, fuerza bruta, aprovechando las vulnerabilidades que trae consigo cada dispositivo

- EL uso de la matriz DOFA, estableció una serie de fortalezas y debilidades para los 4 dispositivos IoT, aprovechando las oportunidades con que cuenta cada uno para minimizar las debilidades encontradas, usando las fortalezas con que cuenta cada uno para evitar las amenazas concurrentes, y minimizar las debilidades a través de medidas de aseguramiento

- Se establece una guía de buenas prácticas, las cuales se recomiendan aplicar en los 4 dispositivos IoT seleccionados, para que sean tenidos en cuenta por el proveedor del dispositivo y para el usuario final del dispositivo

- Los fallos de seguridad evidenciados en el análisis realizado en la investigación, basado en los 4 dispositivos IoT, en la mayoría de las situaciones son presentados por el pobre aseguramiento que hace el proveedor del dispositivo en su afán de venta y la falta de conocimiento del usuario final quien confían en los que su proveedor le vende.

14. RECOMENDACIONES

Una vez finalizada la investigación se consideran las siguientes recomendaciones:

- Extender la investigación de los fallos más frecuentes en dispositivos IoT, abordando cada una de las capas que componen la estructura IoT, brindando un análisis más específico de las causales de vulnerabilidad

- Considerar un análisis de seguridad basado en vulnerabilidades y ataques que cubra a más dispositivos IoT, los cuales estén asociados a diferentes servicios

- Detallar las técnicas y metodologías que se usan en los ataques realizados a dispositivos IoT, verificando como aprovechan las vulnerabilidades encontradas

- Analizar los derechos y responsabilidades que tiene la industria, los proveedores y el consumidor final en garantizar que los dispositivos IoT cuenten con un aseguramiento adecuado

- Trabajar en los procesos de socialización y sensibilización a través de estas metodologías de investigación, con el fin de masificar la importancia de establecer una serie de aspectos que deben considerarse antes de conectar un dispositivo a Internet

BIBLIOGRAFIA

EVERLET, Alvaro; PASTOR, Javier. Introducción al Internet de las cosas. *Construyendo un proyecto de IOT. España: Universidad Rey Juan Carlos*, 2013.

CAMA-PINTO, Alejandro; DE LA HOZ, Emiro; CAMA-PINTO, Dora. Las redes de sensores inalámbricos y el internet de las cosas. 2012.

TANENBAUM, Andrew. *Redes de computadoras*. Pearson educación, 2003.

ACERO, Luis. *Dirección estratégica*. Ecoe Ediciones, 2010.

BANKINTER, Fundación. El Internet de las cosas. *Sl: Fundación de La Innovación Bankinter*, 2011C. Narvaez. (2004).

MIRANDA, David, et al. *Seguridad de la información en la internet de las cosas*. 2016. Tesis de Licenciatura. Universidad Piloto de Colombia.

CHECK POINT. *2018 Security report.* Tel Aviv: Check point research. 2018.

EVANS, Dave. Internet de las cosas. *Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG*, 2011, vol. 11, no 1, p. 4-11.

GONZÁLEZ, Daniel; TRINH, Anthanh. Análisis, diseño e implementación de un SDK híbrido basado en tecnologías web para la integración de clientes contra una plataforma de servicios RESTFul/JSON. 2015.

SOSA, Eduardo; GODOY, Diego. Internet del futuro. Desafíos y perspectivas. *Revista de Ciencia y Tecnología*, 2014, vol. 16, no 21, p. 40-46.

EVANS, Dave. Internet de las cosas. *Cómo la próxima evolución de Internet lo cambia todo. Cisco Internet Bussiness Solutions Group-IBSG*, 2011, vol. 11, no 1, p. 4-11.

USECHE, David. Cyberintelligence for IoT. 2018.

DI MONTE, Eduardo; SOLÍS, Daniel. Aquae Security: Un paso por delante de los ciberataques dirigidos. *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, 2017, vol. 26, no 126, p. 68-70.

DOMÍNGUEZ, Enrique; MARRERO, Francisco. Diseño y desarrollo de la Interfaz de Comunicación del Sistema Diramic. *Revista CENIC. Ciencias Biológicas*, 2005, vol. 36.

MORENO, Francesc. *Demostrador arquitectura publish/subscribe con MQTT*. 2018. Tesis de Licenciatura. Universitat Politècnica de Catalunya.

MEJIA, Fernando. El internet de las cosas es algo genial, pero sumamente peligroso. *Enter*. 2018.

SUÁREZ, Isabella, et al. Monografía primer módulo maestría en territorio y ciudad. 2018.

GARCÍA, Jonathan. Sistema prototipo Fly-by-Wire. 2005.

BERTOLÍN, Javier, et al. *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo, 2008.

DÍAZ, Joaquín. Modelado de comunicaciones entre servicios internos y aplicaciones entre servicios internos y aplicaciones externas mediante APIS en el entorno bancario. 2017.

MOYA, José, TEJEDOR, Ramón; MARTÍNEZ, David. *Tecnologías de telecomunicaciones*. Creaciones Copyright, 2005.

ROMERO, Jose, et al. Prueba de plataformas para el desarrollo de aplicaciones de la Internet de las cosas. 2015.

MO, Jianpeng. *OPSWAT*. {En linea}. {9 de Enero de 2019}. disponible en: (https://www.opswat.com/blog/why-advanced-persistent-threats-are-targeting-internet-things)

MEDINA, Jordi. *IBM*. {En linea}. {24 de Febrero de 2019}. disponible en: (https://www.ibm.com/blogs/think/es-es/2015/02/24/cuidado-con-las-apts/)

ANABALON, Juan. Internet of Threats (IoT): Una visión de la arquitectura, aplicaciones, riesgos y desafíos futuros. 2016.

RUIZ, Juan. *Hispasec.* {En linea}. {5 de Mayo de 2019}. disponible en: (https://unaaldia.hispasec.com/2018/05/multiples-vulnerabilidades-en-puntos-de-acceso-watchguard.html)

RANCHAL, Juan. *Myseguridad.net.* {En linea}. {29 de Julio de 2019}. disponible en: (https://www.muyseguridad.net/2015/07/29/smartwatches-seguridad/)

NIETO, Luis. *Desarrollo de una plataforma abierta para el almacenamiento y gestión de información de nodos móviles para internet de las cosas de la célula inteligente de la Universidad Politécnica Salesiana*. 2016. Tesis de Licenciatura.

LARIN, Yeisson, et al. *El internet de las cosas y sus riesgos para la privacidad*. 2017. Tesis de Licenciatura. Universidad Piloto de Colombia.

DEL BARCO, Luis.. *Hipertextual - Uno de los 'routers' más usados cuenta con una vulnerabilidad que pone tus datos en peligro.* {En linea}. {22 de Junio de 2019}. disponible en: (https://hipertextual.com/2018/06/router-dlink-vulnerabilidad-satori-botnet)

MARGOLIS, Joel, et al. An In-Depth Analysis of the Mirai Botnet. En *2017 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2017. p. 6-12.

KOROLOV, Maria. *CSO Report: Surveillance cameras most dangerous IoT devices in enterprise. {En linea}. {*17 de Noviembre de 2019}. disponible en: (https://www.csoonline.com/article/3142484/internet-of-things/report-surveillance-cameras-most-dangerous-iot-devices-in-enterprise.html)

MORENO, Nicolas; MORÓN, Stefany; TORRES, Andrés. Seguridad para IoT: solución para la gestión de eventos de seguridad en arquitecturas de Internet de las cosas. 2017.

GÁSQUEZ, Oriol; CHECA, José. Si hay Internet de las cosas (IoT) habrá “seguridad de las cosas”. *Revista SIC: ciberseguridad, seguridad de la información y privacidad*, 2015, no 114, p. 86-88.

OWASP. *OWASP Internet of Things Project.* {En linea}. {16 de Noviembre de 2019}. disponible en: (https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=ICS_2FSCADA)

CARRERAS, Ramón. *Retos tecnológicos en la iot en el ámbito de las redes de sensores*. 2017. Tesis Doctoral. Universidad Politécnica de Cartagena.

STAIR, Ralph; REYNOLDS, George. *Principios de sistemas de información: enfoque administrativo*. International Thomson, 2000.

BUCIO, Rafael.*TPX*. {En linea} {24 de Octubre de 2019}. disponible en: (https://tpx.mx/blog/2016/iot-la-herramienta-de-ataques-distribuidos-mas-grande-conocida.html)

RAMÍREZ, García. *Sistemas multi agentes para la defensa de redes IoT.* 2018. Escuela Colombiana de Ingenieria Julio Garavito.

VELASCO, Ruben. *Movil Experto.* {En linea}. {24 de Agosto de 2019}. disponible en: (http://www.movilexperto.com/sora-la-variante-de-mirai-que-convierte-dispositivos-iot-en-una-botnet-da-el-salto-a-otras-plataformas/)

MOLINERO, Sergi. *Internet of Things (IoT) implementación con nodos Zolertia RE-Mote*. 2018. Tesis de Licenciatura. Universitat Politècnica de Catalunya.

BORONDO, Sonia, et al. *Implementación de una solución internet of things base para futuros desarrollos de aplicaciones verticales enfocadas a hacer eficientes, optimizar y gestionar ámbitos o negocios concretos*. 2015. Tesis de Maestría. Universidad Autonoma de Madrid

DEERING, Steve. *Internet protocol, version 6 (IPv6) specification.* California. 2017.

SORIANO, Saúl. *Internet de las cosas: Desarrollo de un servidor Domótico*. 2015. Tesis Doctoral.

SEGU-INFO. *Noticias sobre seguridad de la informacion.* {En linea}. {28 de Julio de 2019}. disponible en: (https://blog.segu-info.com.ar/2015/07/100-de-los-smartwatches-son-vulnerables.html)

TELEFÓNICA, Fundación. *Smart Cities: un primer paso hacia la Internet de las Cosas*. Fundación Telefónica, 2011.

CANAL, Vicente. *Seguridad de la información: Expectativas, riesgos y técnicas de protección: Incluye ejemplos de normativas de seguridad y referencias*. Creaciones copyright, 2004.

JURADO, Luis; VELÁSQUEZ, Adrian; ESCOBAR, fernando. Estado del arte de las arquitecturas de internet de las cosas (iot). Escuela Técnica Superior de Ingenieros de Telecomunicación. 2014.

CASTILLO, Yarisol. Agotamiendo IPv4 en la región latinoamericana. *Revista Prisma Tecnológico*, 2014, vol. 5, no 1, p. 26-28.