RETOS DE CIBERSEGURIDAD EN LA IMPLEMENTACIÓN DE DISPOSITIVOS IOT

CAMILO ALBERTO VELASQUEZ GOMEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2023

RETOS DE CIBERSEGURIDAD EN LA IMPLEMENTACIÓN DE DISPOSITIVOS IOT

CAMILO ALBERTO VELASQUEZ GOMEZ

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

EDGAR DULCE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Medellín, Fecha sustentación

DEDICATORIA

Dedico este proyecto de grado a Dios por permitirme tomar las decisiones correctas respecto a mi crecimiento personal y laboral. A mi familia y seres queridos por el apoyo incondicional brindado durante toda esta etapa de aprendizaje, los sacrificios que tanto ellos como yo, hemos asumido para que el día de hoy pueda estar realizando los sueños que tanto anhelamos.

AGRADECIMIENTOS

Agradezco a la empresa Redesistemas donde actualmente laboro por el espacio brindado para llevar a cabo cada una de las actividades académicas. Igualmente, agradezco a los profesores y compañeros de la Universidad Nacional Abierta y a Distancia por los conocimientos compartidos y brindados durante esta etapa de aprendizaje.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ATAQUE: En informática ataque hace referencia al intento de tomar control, alterar o destruir algún sistema sin tener ningún tipo de autorización para hacerse. Entre sus principales objetivos es el robo o secuestro de la información o espionaje.

BONET: Bonet hace referencia a una red de equipos que fueron vulnerados y que están bajo el control de un delincuente informático. Los Bonets son usados principalmente para realzar ataques sincronizados como ataques DDoS (Distributed Denial of Service).

DELINCUENTE: Individuo que realiza actos ilegales. El delincuente es la persona que realiza los ataques informáticos y hace uso de los botnet para su beneficio.

FIRMWARE: Software o programa que se encarga de controlar los circuitos electrónicos de un dispositivo. Está presente en los dispositivos como computadoras, dispositivos móviles, electrodomésticos, dispositivos de entretenimiento, entre otros.

INFORMACIÓN: Son el conjunto de datos que se envían y/o procesan para que sean interpretados por el receptor.[1] Es uno de los activos más valiosos en la actualidad por la relevancia que esta tiene en la gestión y funcionamiento de las organizaciones.

INTERNET: Es la interconexión de las redes en el mundo con el fin de proporcionar intercambio de información utilizando múltiples protocolos, proporcionando los recursos y servicios para que las computadoras y usuarios puedan estar conectados entre ellos.

MALWARE: Es usado para referirse al software intrusivo que se encarga de realizar tareas o acciones de sabotaje, espionaje, encriptación o destrucción de la información.

---

[1]VEGA PALACIO, David Alfonso. Análisis del nivel de exposición y privacidad de información personal en fuentes abiertas a través de la metodología open source intelligence (OSINT) [En linea]. Proyecto de Grado. Riohacha. UNAD. Escuela de ciencias básicas, tecnología e ingeniería – ECBTI, 2021. 83 p. [Consultado el 5 de mayo del 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/48313/davegap.pdf?sequence=1&isAllowed=y

PROTOCOLO: Es un sistema de normas que permiten la regulación de comunicación entre varios sistemas, que reciben y transmiten información a través de diversos medios. Algunos ejemplos de protocolo son FTP,SSH DNS,HTTP.[2]

RIESGO: Es a todo lo que los sistemas de la información están expuestos por la presencia de amenazas y vulnerabilidades[3].

SEGURIDAD: Conjunto de procedimientos, herramientas y estrategias que tienen como finalidad poder garantizar disponibilidad, integridad y confidencialidad de la información.[4]

SERVIDOR: Sistema que se encarga de brindar recursos a otras computadoras. Es utilizado para almacenar información, gestión de software, mensajería, controles de acceso, entre otros.

VULNERABILIDAD: Se refiere a la debilidad presente en un sistema la cual puede ser aprovechada para realizar ataques o robo de información.[5]

[2] CONCEPTO. Protocolo informatico. [Pagina Web] .[Consultado el 8 de mayo de 2022]. Disponible en : https://concepto.de/protocolo-informatico/

[3]RICO MACIAS, Victor Hugo. Modelo de defensa ante ataques a equipos IoI aplicado a smart tv basado en vulnerabilidades identificadas con OSSTMM [en línea]. Proyecto de grado especialización. Cali: UNAD, 2020 [consultado el 4, mayo, 2022]. 116 p. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/41520/vhricom.pdf?sequence=3&isAllowed=y

[4]MENDOZA DOMINGUEZ, Esly Lorena. La seguridad de la información en el internet de las cosas (IoT) [en línea]. Proyecto de grado especialización. Cali: UNAD, 2021 [consultado el 4, mayo, 2022]. 82 p. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/47752/32584013LaSeguridadDeLaInformacionEnElInternetDeLasCosasIoT.pdf?sequence=1&isAllowed=y

[5]MOLINA SANCHEZ, Edwin Alfredo. Análisis de seguridad de vulnerabilidades presentes en redes sin hilos corporativas [en línea]. Proyecto de grado especialización. Bogota: UNAD, 2020 [consultado el 4, mayo, 2022]. 104 p. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/37512/eamolinas.pdf?sequence=1&isAllowed=y

RESUMEN

El avance tecnológico ha permitido que miles de dispositivos y aplicaciones estén presentes en cada una de las actividades que realizan los seres humanos frecuentemente. Esto permite mejorar la calidad de vida de las personas, brindarles una mejor seguridad y un mejor confort, conectando miles de dispositivos a la red que se encargan de monitorear, controlar, medir y ejecutar actividades sin la necesidad que exista alguna intervención del ser humano.

El uso de los dispositivos IoT implica una cantidad importante de información que debe ser procesada y que a su vez se le debe brindar la seguridad suficiente para que esta no sea alterada o manipulada por personas no autorizadas. De allí, surge la necesidad de que la seguridad informática esté involucrada en el desarrollo, crecimiento e implementación de estas nuevas tecnologías, garantizando que su uso sea benéfico y seguro para la humanidad.

Al interconectar los dispositivos IoT a la red se generan grandes retos a nivel de seguridad de la información, los cuales son importantes conocer e identificar para mejorar continuamente en la implementación de este tipo de tecnología. Estos retos se convierten en piezas importantes para el avance de nuevas tecnologías y la implementación de nuevas técnicas y controles de seguridad.

Existen múltiples falencias en el internet de las cosas y OWASP las lista en su Top Ten para que tanto usuarios y fabricantes puedan tener precauciones con respecto a estas. Las vulnerabilidades presentes en estos dispositivos han hecho que estos sean blanco de ataques como DDoS y malware como el Mirai. Múltiples organizaciones en el mundo buscan hacer del internet de las cosas, una tecnología más segura por medio de buenas prácticas y marcos de referencia que se actualizan y se brindan de manera libre para fabricantes y consumidores.

ABSTRACT

Technological progress has allowed thousands of devices and applications to be present in each of the activities that human beings carry out frequently. This allows improving people's quality of life, providing them with better security and comfort, connecting thousands of devices to the network that are responsible for monitoring, controlling, measuring and executing activities without the need for any human intervention.

The use of IoT devices implies a significant amount of information that must be processed and that, in turn, must be provided with sufficient security so that it is not altered or manipulated by unauthorized persons. Hence, the need arises for information security to be involved in the development, growth and implementation of these new technologies, guaranteeing that their use is beneficial and safe for humanity.

When interconnecting IoT devices to the network, great challenges are generated at the level of information security, which are important to know and identify in order to continuously improve the implementation of this type of technology. These challenges become important pieces for the advancement of new technologies and the implementation of new techniques and security controls.

There are multiple shortcomings in the internet of things and OWASP lists them in its Top Ten so that both users and manufacturers can take precautions regarding them. The vulnerabilities present in these devices have made them the target of attacks such as DDoS and malware such as Mirai. Multiple organizations in the world seek to make the Internet of Things a more secure technology through good practices and reference frameworks that are updated and provided freely to manufacturers and consumers.

INTRODUCCIÓN

Los dispositivos IoT en la actualidad son implementados y utilizados en diversos campos como son la salud, el hogar, la industria, ciudades inteligentes, haciendo más fácil y cómoda la vida a sus consumidores gracias a su fácil implementación y uso. La gran acogida de estos dispositivos por parte de la humanidad ha impulsado a los delincuentes informáticos a realizar ataques continuos a estos dispositivos como Malware, DDoS gracias a las múltiples vulnerabilidades presentes en el proceso de diseño, fabricación e instalación de IoT.

Organizaciones como OWASP han demostrado y han publicado las principales vulnerabilidades en estos dispositivos, que han ayudado a que tanto fabricantes como consumidores de IoT, logren detectar y corregir de manera oportuna las deficiencias de seguridad. Igualmente, se enumeran algunos de los ataques más conocidos en el mundo en donde el internet de las cosas ha sido epicentro, debido a los riesgos, amenazas y vulnerabilidades que existen actualmente,

De acuerdo con el panorama de uso y vulnerabilidades en el internet de las cosas, la investigación de retos de ciberseguridad en los dispositivos IoT se enfoca en determinar las metas y objetivos que estos dispositivos deben garantizar para mejorar su seguridad en cuanto a la protección del dispositivo, de la información y de los consumidores finales. Pero cumplir estos retos, trae algunos problemas o inconvenientes que es necesario que se evalúen y corrijan para lograr las metas que se desean en materia de seguridad de la información.

Teniendo claros los retos es necesario que los fabricantes y organizaciones se apoyen en marcos de referencia como lo son el NIST (National Institute of Standards and Technology), IoTSF (Internet of Things Security Foundation), IEC (International Electrotechnical Commission) y ENISA (European Union Agency for Cybersecurity) que tienen en común la búsqueda de la seguridad en dispositivos IoT en aspectos como lo es las comunicaciones, seguridad de la información, protección de las interfaces y mecanismos de actualización. La implementación de estos marcos y buenas prácticas ayudarán a cumplir las metas deseadas, aumentando la confianza de uso de este tipo de dispositivos por organizaciones y en nuevos sectores que no se han explorado adecuadamente debido a temores de ataques informáticos.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La aceleración que se vive con el uso y la implementación del internet de las cosas en la actualidad provoca que existan grandes cantidades de deficiencias en materia de seguridad. Los ataques de denegación de servicio distribuido (DDoS) son ejecutados constantemente por los delincuentes informáticos utilizando dispositivos IoT ubicados en todo el mundo, tal y como ocurrió en el año 2016 donde el malware Mirai infectó miles de dispositivos que no se protegieron correctamente formando un Bonet que posteriormente fue utilizado para atacar Dyn una empresa de servicios DNS en todo el mundo.[6]

El diseño y fabricación de dispositivos IoT se realiza de manera acelerada y no contempla las suficientes medidas de seguridad, no realizando actualización constante de firmware que puedan brindar una mejor experiencia y seguridad a los usuarios como tampoco el cifrado de datos que conserven la privacidad de la información. Gran parte de estos dispositivos son de bajo costo llevando a que gran parte de los fabricantes se vean en la necesidad de omitir elementos de seguridad para garantizar bajos precios, de igual forma, existen muchas más limitantes como falta de experiencia y control que pueden provocar que los riesgos en materia de ciberseguridad se sigan presentando con el uso del internet de las cosas.

1.2 FORMULACIÓN DEL PROBLEMA

El desarrollo tecnológico le permite a la humanidad contar con una cantidad importante de beneficios en materia de salud, conectividad, comodidad entre otros. Los dispositivos IoT son uno de estos dispositivos y su implementación es cada día más común y fácil de realizar en los hogares, automóviles, y ciudades.

Al implementar y adoptar estos nuevos dispositivos es necesario que ellos constantemente ejecuten tareas y envíen o reciban información para su correcto funcionamiento y operación. Es de allí, que surge la inquietud ¿Cuáles son los retos de ciberseguridad con la implementación de dispositivos IoT?, puesto que al estar

[6] MCAFEE. Proteja los dispositivos IoT para prevenir ataques. [página web]. Madrid: (2017). [Consultado el 1, abril, 2022]. Archivo pdf. Disponible en Internet: https://www.mcafee.com/enterprise/es-es/assets/solution-briefs/sb-quarterly-threats-mar-2017-1.pdf

conectados a la red pueden estar expuestos a posibles ataques o manipulación de personas no autorizadas.

2 JUSTIFICACIÓN

El uso de dispositivos IoT es cada día más común en el siglo XXI debido a los múltiples beneficios y oportunidades que estos pueden brindar al desarrollo y mejora de la calidad humana de las personas. Estos dispositivos utilizan el internet para intercambiar datos entre ellos o con otros dispositivos, realizar validaciones, alimentar bases de datos y un sin número de tareas automatizadas.

Una de las principales bondades de IoT es su capacidad de operar con la poca interacción del ser humano, realizando tareas como monitorear, grabar y ajustar de manera automática. A medida que se aumenta la cantidad de dispositivos de igual forma se incrementa el valor y la cantidad de información que estos equipos transmiten y procesan.

La ciberseguridad como herramienta para la protección de la información se hace cada vez más importante en el crecimiento del uso de este tipo de dispositivos, puesto que crece la necesidad de garantizar que dicha información y dispositivos no sean manipulados por delincuentes informáticos. Al acelerado crecimiento del uso de este tipo de dispositivos y con ello la digitalización de grandes cantidades de información, se incrementan el número de amenazas y los retos de ciberseguridad que esto acarrea.

Es de allí, donde los retos de ciberseguridad son cada vez más complejos y más comunes en el diseño, fabricación, instalación, configuración y mantenimiento, dando como resultado que cada una de las etapas desde que se planea y diseña los dispositivos IoT deben estar pensadas en brindar la seguridad necesaria para la integridad, confidencialidad y disponibilidad de la información que estos dispositivos procesan.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Explicar los retos de ciberseguridad implícitos en la implementación de dispositivos IoT, investigando cuales son los ataques, debilidades, marcos de referencia y buenas prácticas en la fabricación y uso del internet de las cosas.

3.2 OBJETIVOS ESPECÍFICOS

Establecer cuáles son los principales campos de aplicación de los dispositivos IoT, describiendo sus principales usos y encontrando cómo interactúan en la actualidad con la humanidad.

Investigar las principales vulnerabilidades de seguridad presentes en dispositivos IoT, teniendo como referencia OWASP Top 10 para determinar las principales causas de ataques a estos dispositivos.

Identificar los retos de ciberseguridad de los dispositivos IoT de acuerdo con las buenas prácticas recomendadas por las principales organizaciones de ciberseguridad para estos dispositivos.

Analizar algunos marcos de referencia de dispositivos IoT en búsqueda de mejores prácticas y características de ciberseguridad para este tipo de dispositivos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

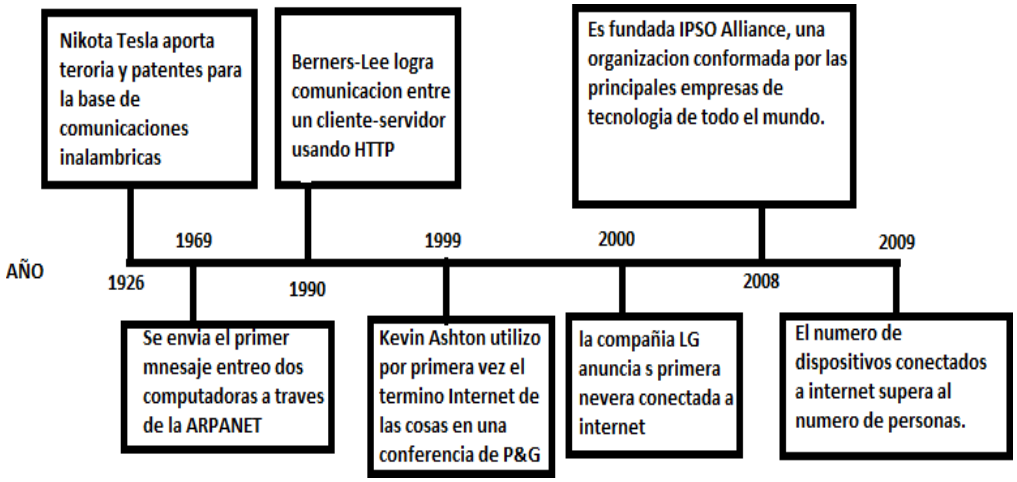
En muchas ocasiones se asocia el surgimiento del internet de las cosas con los avances y desarrollos realizados por Nikola Tesla en materia de comunicaciones inalámbricas y de radio, también es común encontrar que surge en el año 1969 con la conexión y envío por primera vez de mensajes entre computadoras usando ARPANET. Sin embargo, el término de internet de las cosas fue usado por primera vez por Kevin Ashton en el año 1999 cuando realizaba una presentación en P&G. En ese mismo año en el instituto de tecnología de Massachusetts (MIT) se funda el grupo Auto-ID Center con el fin de realizar investigación en identificación por radiofrecuencia en red (RFID) con el fin de generar nuevas tecnologías y formar el internet de las cosas.[7]

En la Figura 1 se muestran los eventos más relevantes que llevaron al surgimiento del internet de las cosas iniciado en el año 1926 hasta el año 2009 donde el número de dispositivos supera el número de personas en el planeta.[8]

[7] EVANS, Dave. Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo [En linea]. Cisco IBSG: 2011. p.2. [Consultado el 1 de abril del 2022]. Disponible en https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

[8] RAMIREZ MADRID, David Andres; RODRIGUEZ HERNANDEZ, Erika Dennis. Diseño de un método para identificar necesidades y oportunidades para la implementación de Internet de las cosas (IoT) aplicable a oficinas de trabajo donde permanezcan entre 30 y 70 personas y planteamiento de un caso práctico de solución en las oficinas de la Agencia Nacional del Espectro. [En línea]. Trabajo de grado. Bogotá: Universidad distrital Francisco Jose de Caldas, 2016.p.25-27. [Consultado 1 de abril del 2022]. Disponible en https://repository.udistrital.edu.co/bitstream/handle/11349/5343/RamirezMadridDavidAndres2017.pdf;jsessionid=5E8A531A628066293E16AA6FCEC78285?sequence=1

Figura 1. Línea de tiempo del surgimiento del internet de las cosas



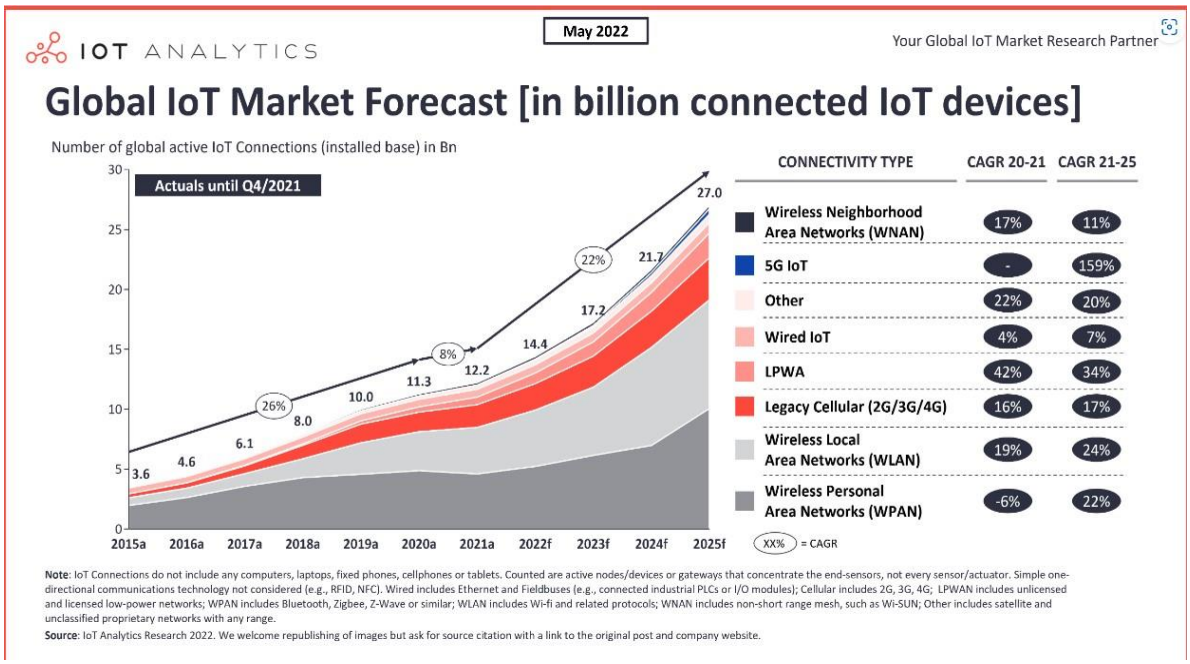
Fuente: Elaboración Propia

Después del surgimiento del internet de las cosas y su acogida a nivel mundial tanto por los fabricantes como por los consumidores, el número de dispositivos ha estado en constante crecimiento llegando en el año 2020 a superar el número de dispositivos IoT conectados a la red.[9] Estas cifras demuestran el acelerado auge de la humanidad por la implementación y aceptación de este tipo de tecnología, encontrándose dispositivos para automatización del hogar, robots para realizar la limpieza, control por voz, cerraduras inteligentes, cámaras de seguridad y nuevos dispositivos que puedan usar la red para compartir y recibir información.

En la Figura 2 se encuentra el número de dispositivos conectados a la red desde el año 2015 hasta el año 2025 y como es su crecimiento en billones como lo muestra IoT analytic en su publicación de mayo del 2022, en donde se toma en cuenta los retos de la pandemia del COVID-19 y la escasez de chips actual que hace que la recuperación del mercado de IoT sea más lenta.

[9] LASSE LUETH, Knud. State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. IoT Analytics [página web]. (19, noviembre, 2020). [Consultado el 1, abril, 2022]. Disponible en Internet: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Figura 2. Número de dispositivos conectados



Fuente: HASAN, Mohammad. State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally [página web]. (18, mayo, 2022). [Consultado el 12, junio, 2022]. Disponible en Internet: https://iot-analytics.com/number-connected-iot-devices/

Para que el desarrollo y crecimiento exponencial del internet de las cosas fuera posible, otras tecnologías necesarias en el IoT se unieron y avanzaron en simultaneo como lo son[10]:

- **Conectividad**. La evolución de la velocidad de conexión en la actualidad, brindan mejores velocidades a los dispositivos y usuarios con la posibilidad de transmitir grandes cantidades de datos a la nube y millones de dispositivos.
- **Sensores**. La creciente demanda de dispositivos IoT en conjunto con su innovación provoco que este tipo de sensores utilizados por el internet de las cosas mejorara sus precios y producción, haciendo que estos sean más funcionales y a su vez económicos.
- **Poder informático**. El uso y procesamiento de los datos y el almacenamiento digital de los mismos, ha generado que los consumidores demanden dispositivos IoT con mejores capacidades de procesamiento y

[10]¿Qué es IoT y cómo funciona? [Anónimo]. SAP [página web]. [Consultado el 2, abril, 2022]. Disponible en Internet: https://www.sap.com/latinamerica/insights/what-is-iot-internet-of-things.html.

memoria, impulsando que los fabricantes fabriquen mejores dispositivos con mejor capacidad y aplicabilidad.

- **BigData**. Con la cantidad de datos generados diariamente el almacenamiento y procesamiento ha mejorado sustancialmente gracias a BigData y las herramientas de análisis de grandes volúmenes de datos en tiempo real. El uso de estos datos y de su velocidad de procesamiento es vital para el funcionamiento y aplicacion del internet de las cosas.
- **Computación en la nube**. Con la evolución de la computación en la nube y su acogida con el pasar de los años, ha permitido que el internet de las cosas pueda utilizar sus servicios para recopilar y transmitir gran cantidad de información para ser procesada.
- **Inteligencia Artificial (IA)**. La inteligencia artificial aprovechando la gran cantidad de datos suministrados de dispositivos IoT, logra analizar de manera avanzada la información recopilada para toma de decisiones de manera autónoma y precisa.

Dicho crecimiento no viene acompañado solamente de digitalización y automatización, es también la gran oportunidad para que delincuentes informáticos puedan realizar todo tipo de ataques informáticos. Con la conexión de miles de dispositivos a la red surgen grandes cantidades de riesgos y retos en materia de seguridad puesto que su gran demanda, potencializa y atrae la atención de los delincuentes llevando a que los intentos de infecciones con malware sean cada vez más comunes.

Kaspersky uno de los principales desarrolladores de software de seguridad del mundo manifiesta que, de acuerdo con los últimos datos obtenidos en el primer semestre del 2021, los ataques informáticos a dispositivos IoT se duplicaron en el último año. Dichos ataques tienen como finalidad robar datos personales, realizar ataques de denegación de servicio utilizando estos dispositivos e incluso ser usados para minería de criptomonedas. Una de las principales armas que usan los ciberdelincuentes son los exploits aprovechando que los usuarios no prestan atención a la seguridad de sus dispositivos y para algunas personas no son tan importantes como para que un hacker se interese en ellos.[11]

[11] KASPERSKY. El número de ataques a dispositivos IoT se duplica en un año [Sitio Web]. [Consultado el 2 de abril de 2022]. Disponible en: https://www.kaspersky.es/about/press-releases/2021_el-numero-de-ataques-a-dispositivos-iot-se-duplica-en-un-ano

4.2 MARCO CONCEPTUAL

4.2.1 IoT (Internet de las cosas). Internet de las cosas son todos aquellos dispositivos que tienen la capacidad de conectarse a internet y que se utilizan cotidianamente. Estos dispositivos tienen como finalidad monitorear y/o sistematizar procesos de manera automática haciendo que la intervención del ser humano sea la menor posible. El internet de las cosas se caracteriza por ser comúnmente un hardware de bajo costo y puede ser usado para brindarle conectividad a otros objetos, permitiendo que estos cuenten con la capacidad de monitoreo y configuración remota que antes no poseía. Adicionalmente IoT es usado para transferir gran cantidad de información a centros de análisis de manera que esta pueda ser procesada con el fin de tomar decisiones a futuro, incluso ayudando a prevenir eventos.[12]

4.2.2 BigData. BigData es usado para hablar de las grandes cantidades de datos que no pueden ser procesados de manera adecuada por las herramientas que comúnmente se usan. Se caracteriza por ser datos de gran volumen y variedad debido a que provienen de múltiples fuentes haciendo que esta información se le dé un tratamiento especial. Otra de sus características es la velocidad en que la información debe ser procesada de manera que se obtenga respuestas rápidas para tomar decisiones de manera precisa y en el momento oportuno.

Con la cantidad de dispositivos IoT interconectados enviando y recibiendo información todo el tiempo, BigData es la solución adecuada para que la información enviada por este tipo de dispositivos pueda ser usada de manera efectiva con la finalidad de que este sea usado para ejecutar o prevenir eventos.[13]

4.2.3 Seguridad informática. La seguridad informática son los diferentes métodos o técnicas encargadas de garantizar que los sistemas informáticos se encuentren protegidos, eliminando amenazas que puedan ocasionar daños, alteraciones o pérdida de información. La seguridad informática se fundamenta en tres pilares los cuales deben cumplirse con la finalidad de lograr seguridad en la información.

---

[12] BOECKL,Katie, et al. Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT). [En linea]. Departamento de Comercio de los EE. UU, 2019.p.4 [Consultado el 2 de abril del 2022]. Disponible en https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932207

[13] PISANO, Ariel. Internet de las Cosas. [En linea]. Tesis maestría. Buenos Aires. Universidad de San Andres, 2018. 94 p. [Consultado el 02 de abril del 2022]. Disponible en https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16159/1/%5BP%5D%5BW%5D%20T.%20M.%20Ges.%20Pisano%2C%20Ariel.pdf

- **Confidencialidad**: Su objetivo principal es garantizar que la información conserve su privacidad y no sea robada por terceros, estableciendo procesos de encriptación, autenticación de usuarios y controles de acceso que solo permita la gestión a las personas autorizadas.
- **Integridad**: Hace referencia a la manera como la información se transporta y se almacena, esta debe conservarse igual a como fue creada sin sufrir afectaciones o manipulación. La implementación de sistemas de autenticación facilita que no se realicen modificaciones no deseadas.
- **Disponibilidad**: Con este pilar se garantiza que la información podrá ser consultada o manipulada por los usuarios autorizados en todo momento. Con la implementación de copias de seguridad y sistemas redundantes los datos podrán estar disponibles o se podrán recuperar ante cualquier incidente.

A continuación, se presenta en la figura 3 las bases para lograr la correcta implementación de la seguridad informática:

Figura 3. Pilares seguridad informática

Fuente: MACIAS MENDEZ, Xiomara Mayerli; DUEÑAS JUEZ, Jose Luis. Implementación de un modelo de seguridad informática en un sistema de monitoreo para los canales de comunicaciones y Datacenter en la empresa Atento SA [En línea]. Monografía. Bogotá. Universidad distrital Francisco Jose de Caldas, 2015. p .8 [Consultado 4 de abril del 2022]. Disponible en https://repository.udistrital.edu.co/bitstream/handle/11349/4258/MaciasMendezXiomaraMayerli2015.pdf?sequence=9&isAllowed=y

4.2.4 IIoT (Internet Industrial de las Cosas). El internet industrial de las cosas es un término para referirse al IoT de la industria y que consiste en la conexión de equipos industriales a la red para realizar procesamiento de datos. El uso de dispositivos IoT trae consigo beneficios de gran valor como lo es el mejoramiento en la eficiencia de la línea de producción, mejor gestión en cadenas de suministro gracias al control de inventario, gestión de ambientes industriales mediante el uso de sensores para medición de temperatura y fuentes de riesgo.[14]

4.2.5 DDoS (Distributed Denial of Service). Este tipo de ataque es un arma con la cual los ciberdelincuentes pueden llegar a interrumpir el servicio de alguna organización. este tipo de ataques se realiza de manera coordinada entre miles de dispositivos para crear una red y posteriormente enviar grandes cantidades de tráfico que llevan a sobrecargar los servidores y en ocasiones hasta infraestructuras completas.[15]

Los ataques DDoS se pueden clasificar en tres tipos[16]:

- **Ataques DDoS volumétricos**: Son los más comunes y tienen como objetivo inhabilitar un servidor, o una infraestructura generando grandes cantidades de peticiones saturando los recursos disponibles. Para ejecutar este tipo de ataques se usan dispositivos IoT que fueron comprometidos como cámaras, entre otros.
- **Ataques de protocolo**: Este ataque se caracteriza por aprovecharse de los puntos débiles de los servicios de red, enviando mensajes broadcast con direcciones IP falsificadas, saturando de tráfico a la víctima.
- **Ataques de aplicación**: Son ataques que requieren menos recursos y van dirigidos específicamente a las aplicaciones, donde muchos de los firewall o sistemas de protección no detectan el ataque. Su objetivo es hacer que la conexión sea inestable y fallida dejando una mala experiencia a los usuarios.

[14] HPE. ¿qué es el internet de las cosas industrial (IIoT)? [Sitio Web]. [Consultado el 10 de abril de 2022]. Disponible en: https://www.hpe.com/lamerica/es/what-is/industrial-iot.html
[15] IBM. Manejo de los ataques de tipo DDoS (Distributed Denial of Service) [Sitio Web]. (25 de junio de 2019). [Consultado el 5 de mayo de 2022]. Disponible en: https://cloud.ibm.com/docs/cis?topic=cis-distributed-denial-of-service-ddos-attack-concepts&locale=es
[16] OVHCLOUD. ¿Qué es un ataque DDoS? [Sitio Web]. [Consultado el 5 de mayo de 2022]. Disponible en:https://www.ovhcloud.com/es/security/anti-ddos/ddos-definition/

4.2.6 Ransonware. Es un malware que se encarga de impedir que los usuarios puedan acceder a sus archivos mediante técnicas de cifrado. Los atacantes suelen dejar mensajes solicitando pagos por el rescate de la información y dispositivos.

Existen 3 tipos de Ransonware según malwarebytes los cuales son[17]:

- **Scareware**: Inunda su dispositivo de mensajes emergentes indicando que necesita soporte técnico o que su dispositivo no se encuentra a salvo y la forma para que desaparezcan es realizar pagos a los delincuentes.
- **Bloqueadores de pantalla**: Consiste en bloquear las pantallas de los ordenadores con un mensaje que se ha detectado actividades ilegales y que debe pagar alguna multa.
- **Ransonware de cifrado**: Es el más temido, debido a que cifra los archivos, exigiendo el pago para recuperar sus archivos y descifrarlos. En caso de no realizar el pago es muy probable perder la información.

[17] MALWAREBYTES. Ransonware [Sitio Web]. [Consultado el 8 de mayo de 2022]. Disponible en: https://es.malwarebytes.com/ransomware/

5 DESARROLLO DE LOS OBJETIVOS

A continuación, se presentan los desarrollos de los objetivos en busca de dar respuesta al planteamiento del problema.

5.1 ESTABLECER CUÁLES SON LOS PRINCIPALES CAMPOS DE APLICACIÓN DE LOS DISPOSITIVOS IOT, DESCRIBIENDO SUS PRINCIPALES USOS Y ENCONTRANDO CÓMO INTERACTÚAN EN LA ACTUALIDAD CON LA HUMANIDAD.

El internet de las cosas ha generado grandes oportunidades para el desarrollo de nuevos equipos y líneas de negocio, conceptos que sirven como fundamento para que el día de hoy se hable de ciudades inteligentes o industria 4.0. El internet ya no solo está conformado por computadoras o dispositivos móviles como celulares, la posibilidad de conectar otro tipo de dispositivos a la red desde sensores, objetos, electrodomésticos ha generado gran impacto en la calidad de vida de los seres humanos y su desarrollo económico.

La evolución tecnológica y las mejoras significativas en las redes inalámbricas y comunicación móvil en los últimos años, ha permitido la expansión de IoT en múltiples campos, haciendo que estos se encuentren tanto en la vida cotidiana y en sector industrial. Los campos en los cuales más sobresale este tipo de tecnología es transporte, hogar, salud, industria[18].

La Figura 4 muestra un breve panorama de los campos más relevantes en donde el internet de las cosas está presente en la actualidad, permitiendo el despliegue de aplicaciones por cada uno de estos campos resaltando los más usados en la actualidad.

[18] PINZON NIÑO, David Leonardo. Panorama de aplicación de internet de las cosas (IoT) [En línea]. Monografía. Bogotá. Universidad Santo Tomas, 2015. 82 p. [Consultado 5 de abril del 2022]. Disponible en https://repository.usta.edu.co/bitstream/handle/11634/672/Panorama%20de%20aplicacion%20de%20internet%20de%20las%20cosas.pdf?sequence=1&isAllowed=y

Figura 4. Campos de aplicación de internet de las cosas

Fuente: VERGARA, Carolina; OCAMPO VILLAN, Maria. El internet de las cosas (IoT) y la cuarta revolución Industrial [Pagina web]. Noviembre,2017. [Consultado el 15 de abril del 2022]. Disponible en https://energub.com/el-internet-de-las-cosas-iot-y-la-cuarta-revolucion-industrial/

En la anterior figura se evidencia los diferentes campos de aplicación donde se involucran el internet de las cosas. Estos campos están compuestos por los objetos que se pueden conectar a la red en búsqueda de formar entornos más automatizados e inteligentes como lo son hogares, ciudades inteligentes, medicina, consumo de energía, monitoreo de objetos o individuos, sensores, agricultura y dispositivos móviles. Las aplicaciones y el uso del internet de las cosas son múltiples, por lo que a continuación se resaltan algunas de las más comunes en la actualidad.

5.1.1 Domótica. La domótica es sin duda una de las aplicaciones más conocidas e implementadas a nivel mundial debido a la automatización que permite realizar a los hogares, brindando mejoras en cuanto a la calidad de vida de estos. Los electrodomésticos en la actualidad cuentan con mejoras significativas a los tradicionales, incluyendo sensores para la recepción y envío de datos por medio de dispositivos integrados. La Domótica ofrece ventajas como la de poder automatizar y controlar procesos gracias a que gran cantidad de los dispositivos del hogar se encuentran conectados a la red, logrando que de manera remota se pueda ejecutar

órdenes brindando múltiples beneficios[19]. Los principales beneficios o ventajas de la domótica son:

- **Ahorro de energía**: La posibilidad de incorporar sensores y controles a los dispositivos entre los que se encuentran aires acondicionados, sistema de iluminación, electrodomésticos, persianas eléctricas, supone un ahorro energético importante dado que con la información recolectada el sistema estará en capacidad de encender o apagar dispositivos, abrir o cerrar cuando sea oportuno y otras acciones que busquen optimizar el consumo de energía.
- **Seguridad**: Comúnmente se realiza la instalación de equipos de seguridad como cámaras, alarmas y cerraduras electrónicas en hogares y edificios, IoT hace posible conectar estos equipos a la red permitiendo que desde los dispositivos móviles se logren gestionar, teniendo en tiempo real de manera remota la gestión de su vivienda, oficina y hogar.
- **Confort**: Poder controlar temperatura, iluminación, el sistema de entretenimiento desde un solo lugar y de manera sencilla, hace esta una de las ventajas que más impulsa el uso de la domótica, haciendo que los ambientes de hogar y oficina sean más cómodos y confortables.

5.1.2 Ciudades inteligentes: Las ciudades inteligentes integran la tecnología, sus recursos y la innovación con el fin de lograr sostenibilidad y elevar considerablemente la calidad de vida de sus ciudadanos.[20] En este orden de ideas, el internet de las cosas es el mejor aliado a nivel tecnológico para permitir que se pueda regular el tráfico, determinar niveles de contaminación, recolección de basuras por demanda, sistemas de alumbrado público y seguridad.

IoT permite que semáforos puedan estar interconectados con otros dispositivos como cámaras para lograr gestionar de manera eficiente el tráfico de las ciudades de acuerdo con el flujo vehicular. Las ciudades inteligentes han logrado su implementación gracias a que hoy en día los diferentes sensores ambientales, cámaras, servicios públicos y demás objetos que se encuentren conectados puedan

[19] VASQUEZ RODRIGUEZ, Romel. Aplicaciones y tecnologías para el desarrollo de la internet de las cosas: *Revista metropolitana de ciencias aplicadas* [En línea]. Ecuador: Universidad metropolitana de Ecuador, diciembre 2018. Vol. 1. nro. 3. [Consultado el 04 de abril del 2022]. ISSN: 2631-2662 Disponible en: https://remca.umet.edu.ec/index.php/REMCA/article/download/58/162

[20] CARAZO ALCALDE, Ciudad inteligente [página web]. Economipedia. (7 de abril de 2017). [Consultado el 6 de abril de 2022]. Disponible en Internet: https://economipedia.com/definiciones/ciudad-inteligente-smart-city.html

ser usados para conseguir que las ciudades del futuro sean sostenibles y logren mejorar la calidad de vida de sus habitantes.

5.1.3 Sector salud. Las soluciones de internet de las cosas para el sector prometen brindar a las organizaciones de este sector ser más eficientes en sus procesos promoviendo una mejor atención, mejorar los resultados y reducir los costos. Entre los ejemplos más relevantes de las soluciones ofrecidas de IoT para este sector son:

- Dispositivos médicos que puedan estar conectados tales como tomógrafos y resonancia, de manera que la información se encuentre computarizada para su análisis y visualización.
- Dispositivos médicos que sean portátiles que logren realizar monitorización remota de los pacientes y que ayuden con su recuperación y tratamiento, promoviendo que la atención sea más efectiva sin la necesidad de que el paciente se encuentre en centro hospitalario.
- Equipos de seguridad y control de acceso que garanticen la identificación y aumenten la seguridad en los establecimientos de salud.
- Control de los dispositivos médicos mediante etiquetas conectadas a la red por medio de tecnología inalámbrica, facilitando su localización.[21]

5.1.4 Sector automotriz y transporte. En la actualidad es bastante común el uso de dispositivos como sensores en medios de transporte como aviones, automóviles, trenes, bicicletas. Estos sensores permiten recolectar información como la velocidad, ubicación y el estado actual de las partes del vehículo.[22] El internet de las cosas ocasiona que los fabricantes busquen revolucionar sus modelos buscando que estos sean cada vez más inteligentes, tecnológicos y conectados.

Con el despliegue de nuevas tecnologías móviles como el 5G los automóviles equipados con sensores podrán realizar reconocimiento y podrán comunicarse con otros vehículos, realizar conducción autónoma de manera segura, elegir las mejores rutas y mejorar en la eficiencia de combustible.

Las aplicaciones que se pueden lograr con la incorporación del internet de las cosas en este sector pueden ser múltiples, en donde la alta tecnología y la competitividad

[21] ALCATEL LUCENT ENTERPRISE. [En línea]. Internet de las Cosas en sanidad. (Diciembre 2019). [Consultado el 7 de abril de 2022]. Archivo pdf. Disponible en: https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-healthcare-solutionbrief-es.pdf
[22] PINZON NIÑO, Op.cit., p.63.

del mundo actual generan que los fabricantes deban mejorar cada día sus productos y servicios. Entre los factores que más impulsan el uso del IoT en el sector automotriz resaltan los siguientes:

- **Sensores y consumo eléctrico**: Con el paso de los años el costo de fabricación de sensores ha disminuido considerablemente por lo que su implementación en la industria ha permitido mejor recolección de datos en tiempo real, con consumos eléctricos más reducidos y eficientes.
- **Conectividad**: La recolección de datos por parte de los sensores ya puede ser recolectada de manera rápida a través de los diferentes canales de comunicación inalámbricos como WiFi y redes móviles, facilitando a los fabricantes y usuarios tener control y gestión de sus automóviles.
- **Alertas en tiempo real**: La conectividad y los sensores permite que se comparta información sobre el estado de los vehículos, rutas, patrones de manejo, consumo de combustible, accidentes y fallas de componentes.

5.1.4 Industria. Las industrias al igual que las ciudades inteligentes y otros sectores, han evolucionado al uso de dispositivos IoT en sus procesos con el fin de automatización y control de sus procesos. Este tipo de tecnología ha permitido que en la actualidad se hable de nuevos conceptos como lo son el IIoT (Internet industrial de las cosas) por sus siglas en inglés y de industria 4.0. Esta cuarta revolución genera mayor valor y desarrollo a las líneas de producción con la ayuda de la robótica y el intercambio constante de datos.[23]

Las fábricas en la actualidad desean mejorar sus cadenas de producción y hacer de estas mucho más inteligentes y eficientes, para ello, el uso de sensores que se encuentran conectados a sus equipos permite tener un mejor panorama de cómo se encuentran sus equipos, mejoramiento de la eficiencia de operación mediante el análisis en tiempo real de los datos recopilados y que posteriormente son analizados en la nube gracias a BigData. De igual forma, los servicios energéticos emplean el internet de las cosas para conocer y supervisar el estado de las redes eléctricas, medir el flujo de las tuberías y controlar emisiones sin importar que tan alejadas se encuentren los recursos. [24]

[23] KOVÁCS MATÍNEZ, Pablo. IoT: Internet de las cosas en el modelo de Industria 4.0 [En línea]. Trabajo de grado. Sevilla. Universidad de Sevilla, 2018. 79 p. [Consultado 5 de abril del 2022]. Disponible en https://biblus.us.es/bibing/proyectos/abreproy/91965/fichero/TFG-1965-KOVACS.pdf

[24] REDHAT: ¿Qué es el Internet industrial de las cosas? [Página web]. (7 de mayo de 2021) [Consultado el 6 de abril de 2022]. Disponible en: https://www.redhat.com/es/topics/internet-of-things/what-is-iiot

La llegada de esta nueva forma de conectar las cosas entre ellas y sus diferentes campos de aplicación ha llevado que la sociedad, fabricantes y sectores industriales evolucionen en el desarrollo de sus actividades y productos, buscando cada día optimizar y automatizar sus entornos y espacios. En la tabla 1 se presenta en resumen los principales campos de aplicación del internet de las cosas y que objetos hacen parte de esta.

Tabla 1. Principales escenarios IoT

Campo de aplicación	Elementos IoT	Descripción
Hogar	Electrodomésticos Iluminación Sistema de entretenimiento Sistema de seguridad	Todos los sistemas pueden ser gestionados desde un solo dispositivo y desde cualquier lugar por medio de internet.
Ciudades Inteligentes	Semáforos Sistemas de iluminación Sistemas de seguridad Monitores de contaminación Estacionamiento inteligente Monitores de ruido ambiental	Las ciudades inteligentes integran diferentes elementos para controlar de manera inteligente y autónoma los diferentes sistemas que la componen.
Salud	Vigilancia de pacientes Equipos especializados Telemedicina	La integración de equipos sanitarios a la red permite a las instituciones realizar un mejor seguimiento de sus pacientes, recopilando información de pacientes y prestando servicios médicos a distancia.

Continuación Tabla 1

Campo de aplicación	Elementos IoT	Descripción
Automotriz Transporte	Sistema de navegación Sensores Conducción autónoma Piezas del motor	IoT permite a la industria automotriz realizar seguimiento del estado de los vehículos, implementar conducción autónoma, mejorar la seguridad mediante ubicación en tiempo real y sensores ubicados en el vehículo.
Industria	Robots Sistema de almacenamiento Sistemas de seguridad Sensores Control de temperatura	IIoT integra toda la cadena de producción de las compañías para elevar eficiencia y avanzar en la automatización de procesos.

Fuente: Elaboración Propia

5.2 INVESTIGAR LAS PRINCIPALES VULNERABILIDADES DE SEGURIDAD PRESENTES EN DISPOSITIVOS IOT, TENIENDO COMO REFERENCIA OWASP TOP 10 PARA DETERMINAR LAS PRINCIPALES CAUSAS DE ATAQUES A ESTOS DISPOSITIVOS

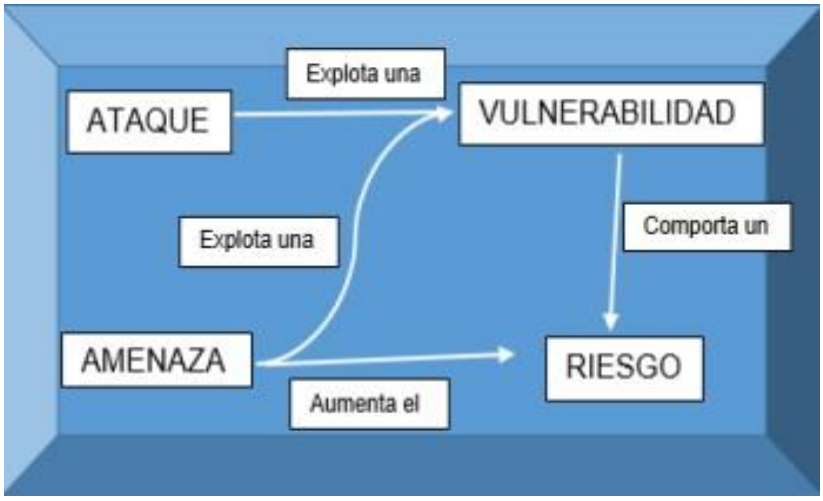
Los campos de aplicación e implementación del internet de las cosas son cada vez mayores identificando dentro de los principales o más relevantes a el hogar, ciudades inteligentes, salud, sector transporte e industria. Este crecimiento y mayor conectividad de dispositivos además de suponer mejoras en materias de seguridad, calidad de vida, bienestar y confort, es también una oportunidad para que los ciberdelincuentes puedan obtener un beneficio propio.[25]

[25] INCIBE: Seguridad en la instalación y uso de dispositivos IoT: Una guía de aproximación para el empresario. [Página web]. (2020) [Consultado el 26 abril de 2022]. Archivo pdf. Disponible en: Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario (incibe.es)

En los sistemas informáticos las vulnerabilidades hacen referencia a las debilidades o puntos débiles que estos pueden tener debido a la falta de protecciones, fallos en la implementación y diseño, que algún agente externo puede llegar a utilizar para poner en riesgo los pilares de la seguridad informática y así causar algún tipo de daño o robo de información.[26] Con la existencia de las vulnerabilidades en los diferentes sistemas existe los riesgos que se pueden presentar por medio de ataques. Los dispositivos IoT no son ajenos a esta realidad y la existencia de vulnerabilidades es bastante común, los ataques son cada vez mayores debido a la efectividad de estos por parte de los ciberdelincuentes.

La Figura 5 se observa la relación que existe entre los conceptos de ataques, vulnerabilidades y el riesgo en entornos informáticos, en donde la existencia de las vulnerabilidades hace posible que un ataque o una amenaza pueda aumentar los riesgos.

Figura 5. Relación ataque, vulnerabilidad y riesgo

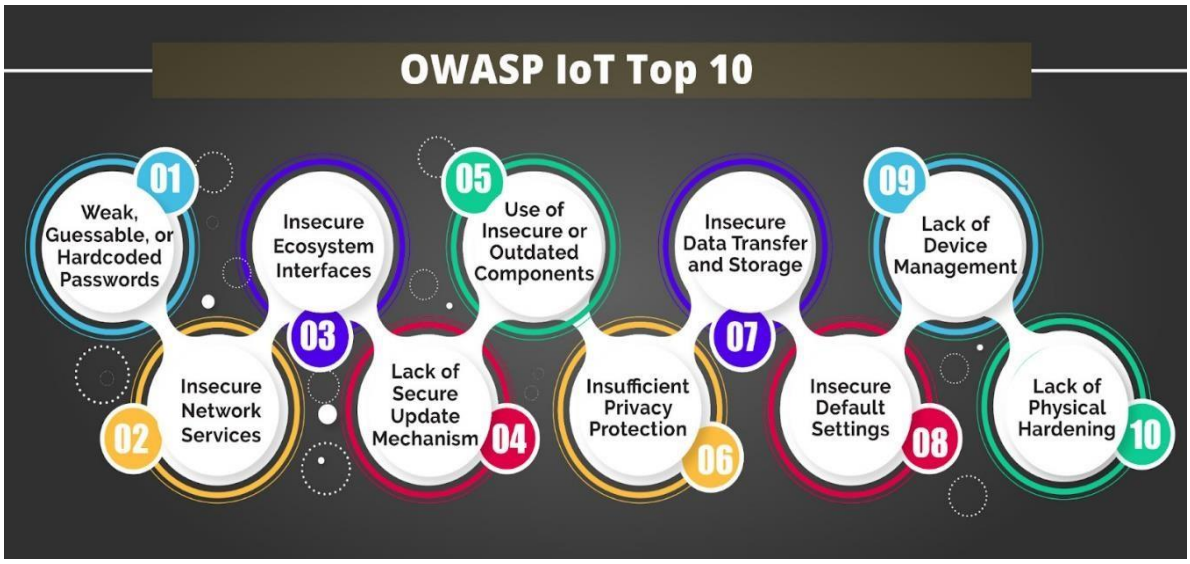


Fuente: SANCHEZ GAMBOA, Hilbert Leonardo. Identificación de vulnerabilidades y riesgos en los activos de ti de energitel. [En línea]. Proyecto de Grado especialización. Ibagué. UNAD. Escuela de ciencias básicas, tecnología e ingeniería – ECBTI, 2018. p 28. [Consultado el 27 de abril del 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28221/93405573.pdf?sequence=1&isAllowed=y

[26] MENDOZA DOMINGUEZ, Op.cit., p.56.

5.2.1 Principales vulnerabilidades IoT. OWASP es una fundación que busca y trabaja por mejorar la seguridad mediante la utilización de proyectos de software de código abierto. Durante su existencia con ayuda de los miembros que la conforman, ha desarrollado herramientas y recursos que han permitido mejorar continuamente la seguridad de la información. Esta fundación cuenta con un proyecto llamado OWASP IoT Top 10 desarrollado para que los fabricantes, consumidores y programadores puedan comprender los fallos de seguridad de este tipo de dispositivos, tomando decisiones en pro de mejorar la seguridad de estos. En su última publicación en el año 2018, OWASP describe las 10 principales vulnerabilidades de internet de las cosas como se muestra en la siguiente figura.

Figura 6 Listado de Vulnerabilidades OWASP IoT



Fuente: BASATWAR, Govindraj. Guide to OWASP IoT Top 10 for proactive security - AppSealing. AppSealing [página web]. (17, septiembre, 2021). [Consultado el 1, mayo, 2022]. Disponible en Internet: https://www.appsealing.com/owasp-iot-top-10/.

Basados en la Figura 6 se observan las 10 vulnerabilidades que OWASP resalta como las más relevantes para el internet de las cosas, a continuación, se realiza la descripción de cada una de estas.

5.2.1.1 Contraseñas débiles o comunes. Cuando se habla de IoT se asocia con dispositivos fáciles y sencillos de instalar por lo que la mayoría de los usuarios no contemplan configuración y cambio de contraseña dentro de su implementación. Gran cantidad de estos dispositivos conservan su contraseña por defecto debido a

que en muchas ocasiones los usuarios no tienen conocimiento para realizar su cambio o el dispositivo no se lo exige, generando una vulnerabilidad de las más comunes y aprovechadas por los ciberdelincuentes.

Gran mayoría de los dispositivos IoT se distribuyen con los nombres de usuario y contraseña como lo son admin y admin respectivamente, a la espera que el usuario realice el cambio, lo cual ha generado grandes problemas en materia de seguridad en el internet de las cosas.[27]

5.2.1.2 Servicios y redes inseguras. Los servicios de red expuestos sin la debida protección hacen más probable que las debilidades de los dispositivos sean explotadas con éxito, en donde los datos que viajan desde los dispositivos a los servidores pueden ser vulnerados de manera que se vea afectada la confidencialidad de los usuarios. La mala gestión de la red y los servicios permite que ataques como los de *man-in-the-iddle* (MITM), puedan tomar credenciales y tomar el control de dispositivos IoT para ataques sincronizados.[28]

5.2.1.3 Interfaces inseguras. El uso de herramientas Web, las interfaces de programación de aplicaciones (API), permite que los delincuentes informáticos puedan tomar control de los dispositivos debido a la carencia o poca gestión de seguridad de estas interfaces. La ausencia de controles y el no encriptado de las comunicaciones permiten que se presente este tipo de vulnerabilidad en el internet de las cosas.[29]

5.2.1.4 Mecanismos inseguros de actualización. Los procesos de actualización de dispositivos IoT están expuestos a que se instale código o firmware maliciosos, debido a que no cuentan con canales cifrados que permitan que el software sea validado y aprobado, evitando la filtración por parte de un agente externo.[30]

5.2.1.5 Componentes obsoletos e inseguros. La gran aceleración de IoT lleva a que gran cantidad de estos dispositivos compartan hardware que ya han sido explotados y vulnerados anteriormente. Igualmente, el uso software de código abierto y ampliamente distribuido incrementa los riesgos y las posibilidades que

[27] OWASP top 10 internet of things [En linea]. (2018) [Consultado el 01 mayo de 2022]. Disponible en: https://owasp.org/www-pdf-archive//OWASP-IoT-Top-10-2018-final.pdf
[28] Ibíd., p.1.
[29] Ibíd., p.1.
[30] Ibíd., p.1

tienen los atacantes para vulnerar de manera exitosa la seguridad de los dispositivos.[31]

5.2.1.6 Poca protección de privacidad. Es frecuente que los dispositivos de internet de las cosas almacenen información de los usuarios como lo son datos personales, métodos de pago, ubicación y otra información que en muchas ocasiones no se realiza bajo el consentimiento de los usuarios ni la seguridad que dicha información requiere.[32]

5.2.1.7 Almacenamiento y transferencia inseguros. Para el procesamiento de los datos obtenidos por medio de dispositivos IoT, estos deben procesar, almacenar, enviar y recibir información que en muchas ocasiones no se protege o se restringe de manera adecuada, permitiendo que usuarios externos tengan acceso y puedan manipular y disponer de ella.[33]

5.2.1.8 Falta de gestión. No se cuenta con las políticas y controles necesarios y adecuados que permitan tener la gestión de los dispositivos, inventario, actualizaciones, borrado adecuado y tiempo de vida de estos.

5.2.1.9 Configuración de fábrica insegura. En muchos casos la configuración inicial o por defecto de los dispositivos IoT no cuentan con la seguridad suficiente para brindar protección a la información y al dispositivo en sí, abriendo una vulnerabilidad y oportunidad para los ciberdelincuentes.[34]

5.2.1.10 Seguridad física inadecuada. El internet de las cosas goza del privilegio de poder ser ágil y fácil de desplegar en ambientes remotos, sin embargo, al estar en estos entornos dificulta los controles y tareas de seguridad apropiadas, permitiendo que sea vulnerable para ataques informáticos.

5.2.2 Ataques relacionados con dispositivos IoT. Las vulnerabilidades impulsan de gran manera el actuar de los ciberdelincuentes que con gran éxito van obteniendo gran resultado en materia de explotación y materialización de ataques a los diferentes dispositivos IoT. De acuerdo con el informe de amenazas IoT del año 2020 realizado por Paloalto Networks el 98% del tráfico de los dispositivos IoT no está cifrado y pone en riesgo los datos de los usuarios, igualmente el 57% de

[31] Ibíd., p.1.
[32] Ibíd., p.1.
[33] Ibíd., p.1.
[34] Ibíd., p.1.

estos dispositivos son vulnerables a ataques con una gravedad media o alta, convirtiéndolos en una oportunidad para los ciberdelincuentes[35]. De acuerdo con los datos suministrados por paloalto Networks y teniendo en cuenta las vulnerabilidades descritas por OWASP, los ataques a los cuales más comunes que se presentan en IoT se presentan a continuación:

5.2.2.1 Malware. Los ataques de malware apoyados del impulso del uso del internet de las cosas, permitió a los atacantes explorar nuevas opciones con el fin de alcanzar sus objetivos y aprovechar las potenciales vulnerabilidades de los dispositivos IoT. Los ataques con Ransonware son ahora una amenaza para las organizaciones y sus infraestructuras críticas, generando efectos en cascada que afectan de manera directa las operaciones bloqueando dispositivos claves en cadenas de suministro y operación. Ransonware como Darkside ahora centran sus objetivos IoT en busca de obligar a empresas a pagar rescates por recuperar sus dispositivos.[36]

Las organizaciones no son las únicas comprometidas con malware, los ataques a router y dispositivos como televisores inteligentes, sistemas de calefacción y máquinas de café han sido víctimas de este tipo de ataques, en donde no solo se busca tener un beneficio económico, sino también, generar redes de dispositivos para ataques sincronizados. A continuación, se describen algunos malware comunes en el internet de las cosas.

- **Mirai**. Es un malware que corresponde a la familia de los botnets en busca de infectar dispositivos IoT a nivel mundial con el objetivo de utilizarlos para fines de ataques sincronizados como DDOS. Este malware es de código abierto generando que aparezcan nuevas variantes en busca de nuevos objetivos y su método de ataque principal se realiza mediante el escaneo y telnet habilitado en IoT. Con el paso del tiempo este malware se ha debilitado, pero su código fuente ha sido usado para la creación de nuevos malware o variantes como Okiru, Satori,Masuta y PureMasuta.[37]

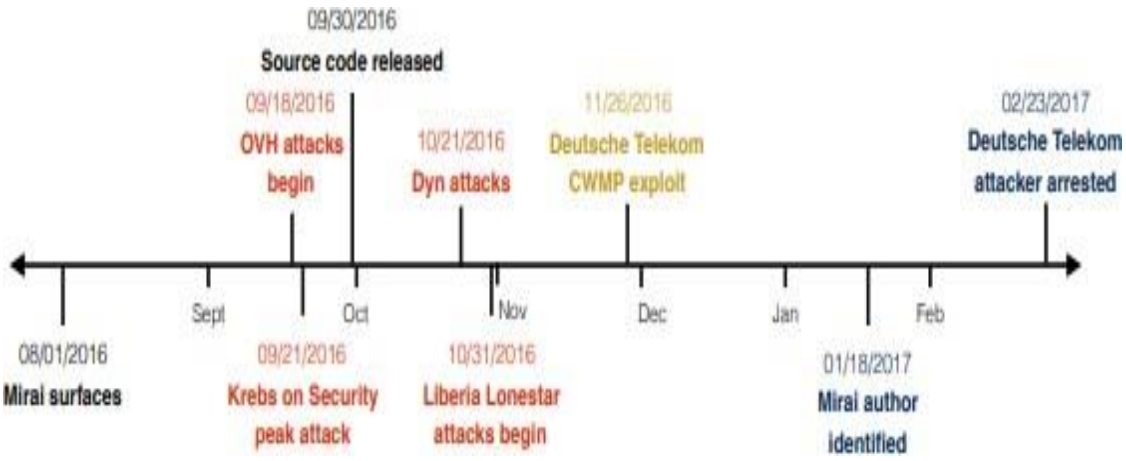
[35] PALOALTO NETWORKS. Informe de amenazas IoT 2020 de Unit 42 [en línea]. 2020 [consultado el 28, septiembre, 2022]. 24 p. Disponible en Internet: https://info.smartekh.com/hubfs/IoT/Informe%20de%20Amenazas%20IoT%202020.pdf.

[36] TRENDMICRO: IoT and Ransomware: A Recipe for Disruption [Página web]. (28 de septiembre del 2021). [Consultado el 02 de mayo de 2022]. Disponible en: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-and-ransomware-a-recipe-for-disruption

[37] CLOUDFLARE: ¿Qué es la botnet Mirai? [Página web]. Cloudflare. [Consultado el 02 de mayo de 2022]. Disponible en: https://www.cloudflare.com/es-es/learning/ddos/glossary/mirai-botnet/

Los creadores de Mirai fueron Paras Jha y Josiah White, quienes eran cofundadores de una empresa que ofrecía servicios de mitigación de DDoS a las mismas organizaciones que ellos atacaban usando su malware. En la figura 7 se muestran algunos de los eventos más relevantes de este tipo de malware entre los cuales se encuentran ataques a OVH, Dyn y la identificación del autor de Mirai.

Figura 7. Eventos relacionados con Mirai Bonet



Fuente: ANTONAKAKIS, Manos, *et al.* Understanding the Mirai Botnet [en línea]. Vancouver, Canadá. 16, agosto, 2017 [consultado el 2, mayo, 2022]. Disponible en Internet: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

- **Mozi**. Es una amenaza que combina 3 malware de los cuales ya se conocían anteriormente como lo son Gafgyt, IoT Reaper y Mirai. Su principal objetivo son los dispositivos IoT con lo cual se busca recopilar y robar información, realizar ataques de DDoS.[38] Mozi utiliza el protocolo peer-to-peer para infectar diferentes dispositivos mediante la explotación de contraseñas por medio de telnet, además de la explotación de vulnerabilidades que no han sido parcheadas en especial en los enrutadores de la marca Netgear, ZTE,

[38] CERT-PY: "Mozi" nueva familia de Malware que afecta a dispositivos IoT combinando 3 malwares en 1 [Página web]. [Consultado el 03 de mayo de 2022]. Disponible en: https://www.cert.gov.py/noticias/mozi-nueva-familia-de-malware-que-afecta-dispositivos-iot-combinando-3-malwares-en-1

Huawei, permitiendo la entrada de nuevos malware y ataques en otro tipo de dispositivos.[39]

El flujo de ataque de Mozi es el siguiente:

- Escaneos en internet en busca de dispositivos.
- Identificación de objetivos.
- Explotación de vulnerabilidades.
- Infección de dispositivos.
- Ejecución de scripts que le permitan permanecer en el dispositivo después de reinicios.
- Atacante evita acceso al dispositivo.
- Redirección de peticiones de usuario a sitios maliciosos.
- Infección de dispositivos de Ransonware.

5.2.2.2 Fuerza bruta. Este tipo de ataque uno de los más usados consiste en la utilización de contraseñas más comunes para intentar acceder a los dispositivos para posteriormente comprometerlos. Pero tomar el control de un dispositivo IoT puede ir más allá, cuando se desea hacer este tipo de ataque en objetivos con claves cifradas puede tomar bastante tiempo. Los dispositivos de internet de las cosas pueden ser usados de manera colectiva, el descifrado de claves conlleva múltiples operaciones matemáticas y con la ayuda de grandes cantidades de estos dispositivos puede provocar ataques más rápidos y exitosos.[40]

5.2.2.3 Spam. Este tipo de ataques consiste en el envío de información no solicitada de manera masiva a diferentes destinatarios. Se realiza a través de correo electrónico y aunque existen muchos métodos de detección para estos, el uso de miles de dispositivos IoT en todo el mundo pueden pasar por alto para estos sistemas. En el año 2014 se conocieron los primeros ataques usando este método,

[39] ATCH, David; REGEV,Gil y BEVINGTON,Ross. How to proactively defend against Mozi IoT botnet [Página web]. Microsoft. (19 de agosto de 2021). [Consultado el 04 de mayo de 2022]. Disponible en: https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/

[40] CAÑAS CUEVAS, Javier Alexander; PATIÑO DORADO, Lucas Alejandro. Modelo informático aplicado a la ciberseguridad de dispositivos IoT. [En línea]. Proyecto de Grado. Bogotá. Universidad EAN. Facultad de ingenierías, 2021. 50 p. [Consultado el 04 de abril del 2022]. Disponible en: https://repository.ean.edu.co/bitstream/handle/10882/10773/PatinoLucas2021.pdf?sequence=1

en donde más de 100 mil dispositivos IoT (televisores, enrutadores, refrigeradores) enviaron más de 300 mil correos electrónicos por día.[41]

5.2.2.4 Espionaje o robo de información. En cada actividad de la vida cotidiana es muy común estar relacionado con un dispositivo IoT, en el hogar, en el transporte, en el trabajo, para hacer deporte y demás usos. En dispositivos como pulseras es recurrente que se procesen y almacene información personal como ubicación, horarios y estado de salud; En dispositivos como televisores se encuentra información de contraseñas, métodos de pago. Toda esta información puede verse comprometida y puede ser robada por delincuentes para beneficio económico o espionaje, incluso puede llegar a comprometer la seguridad de otros dispositivos conectados a la misma red. [42]

5.2.2.5 Ataques DDoS. Los ataques DDoS utilizan la superficie de dispositivos IoT como principal arma mediante la creación de Botnets y ejecución de ataques masivos. La denegación de servicio afecta no solo a los dispositivos IoT mediante la implantación de malware, también afecta a organizaciones que se ven comprometidas por ataques realizados utilizando este mecanismo. Las principales razones que hace de internet de las cosas un blanco atractivo para los delincuentes son las siguientes[43]:

- **Operación continua**: Los dispositivos IoT como cámaras, routers, funcionan las 24 horas del día, permitiendo al atacante analizar y explotar vulnerabilidades continuamente.
- **Mala protección**: Desarrollos de dispositivos por parte de fabricantes con protecciones débiles, permitiendo fácil acceso.

[41] ACOSTA MOLINA, Cesar Mauricio. El estado del arte sobre el internet de las cosas. amenazas y vulnerabilidades de seguridad informática evidenciadas desde la domótica. [En línea]. Proyecto de Grado especializacion. Bogotá. UNAD, Escuela de Ciencias Básicas, Ingeniería, Tecnología e Ingeniería – ECBTI, 2019. 81 p. [Consultado el 04 de abril del 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28446/Monografia.pdf?sequence=1&isAllowed=y

[42] MUYSEGURIDAD. IoT: así se resiente la seguridad del Internet de las Cosas. [Página web]. (13 de septiembre de 2019). [Consultado el 14 de mayo del 2022]. Disponible en: https://www.muyseguridad.net/2019/09/13/iot-seguridad-cosas/

[43] FERNANDES SILVEIRA, Frederico augusto. Smart-IoT: um sistema de proteção contra DDoS para rede de Internet das Coisas. [En línea]. Tesis de Maestria. Natal. Universidade federal do rio grande do norte, 2020. 84 p. [Consultado el 04 de abril del 2022]. Disponible en: https://repositorio.ufrn.br/bitstream/123456789/30831/1/SmartIoTsistema_Silveira_2020.pdf

- **Mantenimiento nulo**: Los usuarios no supervisan el funcionamiento y actualizaciones de sus dispositivos a menos que estos dejen de funcionar.
- **Tráfico considerable**: Los dispositivos IoT poseen capacidades de tráfico potentes, adecuadas para realizar ataques de tipo DDoS.
- **Interfaces de usuario poco interactivas**: No se cuenta con interfaces que permitan detectar de manera sencilla y oportuna alguna anomalía en el dispositivo, la mayoría de los ataques pasan desapercibidos para los usuarios.

5.3 IDENTIFICAR LOS RETOS DE CIBERSEGURIDAD DE LOS DISPOSITIVOS IOT DE ACUERDO CON LOS BUENAS PRÁCTICAS RECOMENDADAS POR LAS PRINCIPALES ORGANIZACIONES DE CIBERSEGURIDAD PARA ESTOS DISPOSITIVOS.

Para la implementación de dispositivos de IoT en sus diferentes campos de aplicación es necesario considerar los retos que esto implica en materia de ciberseguridad tanto para los dispositivos como para los usuarios y organizaciones. La Figura 8 muestra las principales metas a mitigar en el internet de las cosas de acuerdo con el instituto nacional de estándares y tecnología.

Figura 8 Metas de ciberseguridad IoT de acuerdo el NIST

Fuente: BOECKL,Katie, et al. Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT). [En línea]. Departamento de Comercio de los EE. UU, 2019.p.23 [Consultado el 2 de abril del 2022]. Disponible en https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932207

La figura anterior resalta los retos de protección del dispositivo, datos y la seguridad de los usuarios. Estos retos se describen a continuación con cada una de sus características más relevantes[44]:

5.3.1 Protección del dispositivo. Este reto es de vital importancia para prevenir que los dispositivos IoT puedan ser tomados o manipulados por terceros, para la ejecución de ataques como lo son los DDoS, interceptación del tráfico o servir de salto a otros dispositivos que se encuentren en la red. Dentro de las áreas a tener en cuenta para alcanzar este reto se encuentra.

- **Gestionar los activos**: Realizar inventario de manera periódica de los dispositivos IoT, sus características técnicas, de manera que se logre tener control y gestión de cada uno de ellos.
- **Gestionar las vulnerabilidades**: Identificar cuáles de los dispositivos cuentan con vulnerabilidades conocidas en su hardware o software, realizando actualizaciones y lograr reducir las probabilidades de ataques.
- **Gestionar el acceso**: Proteger el acceso lógico y físico del dispositivo a personas que no cuenten con los permisos para hacerlo.
- **Detectar incidentes de seguridad en el dispositivo**: Vigilar de manera constante los dispositivos IoT en busca de ataques o manipulaciones que logren comprometer su seguridad.

5.3.2 Protección de los datos. Gran parte de los dispositivos IoT tanto de uso personal como en organizaciones realizan la recolección, procesamiento y trasmisión de datos. Este reto implica proteger los tres pilares de la seguridad informática como lo son la confidencialidad, disponibilidad e integridad de la información. Las áreas que componen este reto son las siguientes:

- **Protección de los datos**: Proteger los datos que se encuentran almacenados del dispositivo o que se transportan de manera que se preserve la confidencialidad, evitando que sufra alguna manipulación de externos.
- **Detectar incidentes de seguridad de datos**: Al igual que se vigila el dispositivo, es importante analizar y verificar que los datos no tengan señales de manipulación que ponga en riesgo la seguridad de estos.

[44] BOECKL,Katie, et al, Op Cit, p23.

5.3.3 Protección de la privacidad de los usuarios. No solo basta con proteger el dispositivo y los datos, se hace necesario proteger a los usuarios de los riesgos de seguridad que puedan sufrir por la utilización de dispositivos IoT. Este reto se compone de las siguientes áreas:

- **Gestionar el flujo de la información**: Realizar una correcta administración de los datos, el flujo y ciclo de vida que se está procesando en el dispositivo.
- **Gestión de permisos**: Gestionar los permisos para el debido procesamiento de la información con la autorización de los usuarios.
- **Decisiones informadas**: Hacer que los usuarios hagan parte de las decisiones y los efectos del procesamiento de la información por parte de dispositivos IoT.
- **Datos desasociados**: Minimizar en la medida de lo posible la información y los dispositivos IoT.
- **Detectar vulnerabilidades de privacidad**: Realizar el análisis y vigilancia en búsqueda de posibles ataques que puedan poner en riesgo la privacidad de los usuarios.

De acuerdo con el informe Interinstitucional o internet 8228 del NIST, alcanzar las metas de ciberseguridad y mitigación de los riesgos en dispositivos IoT implica una serie de problemas relacionados con los retos anteriormente descritos. Los problemas de los cuales se habla en el documento se muestran en la siguiente tabla.

Tabla 2. Problemas para alcanzar metas de ciberseguridad en IoT

Reto	Problemas
Protección del dispositivo	– Dispositivos en las organizaciones sin identificador único para gestión de activos. – Dispositivos IoT que no se pueden gestionar de manera centralizada. – Dispositivo IoT no proporciona información de firmware, software y hardware. – Fabricante del dispositivo IoT no proporciona parches de seguridad y actualizaciones. – Dispositivo no cuenta con la posibilidad de aplicar actualizaciones o parches. – El dispositivo no ofrece la posibilidad de configurar el software de acuerdo con las necesidades de los usuarios.

Continuación Tabla 2

Reto	Problemas
Protección del dispositivo	– No se puede ejecutar detección de vulnerabilidades en el dispositivo IoT. – El dispositivo no oculta los caracteres de la contraseña al momento de ingresarla. – No es compatible el dispositivo IoT con contraseñas robustas o mecanismos de múltiple factor. – El software no registra los eventos que suceden en el dispositivo con detalle.
Protección de los datos	– El dispositivo IoT no realiza cifrado sólido de los datos que se encuentran almacenados. – No se proporciona mecanismos de restauración de datos o creación de copias de seguridad. – No se cifran los datos confidenciales a través de las comunicaciones de red. – El dispositivo IoT no realiza validación de dispositivo de otros dispositivos antes de enviar o recibir información.
Protección de la privacidad de los usuarios	– El dispositivo no cuenta con interfaces para que el usuario pueda interactuar con él, permitiendo que el usuario pueda tomar decisiones o leer avisos de privacidad. – Dispositivo recolecta o analiza información sin los requerimientos del usuario previos. – El dispositivo no tiene la capacidad de ajustar la configuración para denegar activaciones remotas.

Fuente: Elaboración Propia

Teniendo en cuenta los inconvenientes que se presentan con el amplio crecimiento y los desafíos en materia de ciberseguridad se han desarrollado modelos de buenas prácticas para la implementación de dispositivos IoT. Entre las herramientas y buenas prácticas de seguridad para este tipo de dispositivos se encuentran las siguientes:

5.3.4 European Union Agency for Cybersecurity (ENISA). Esta agencia de ciberseguridad de la unión europea contribuye a que los países miembros logren mejorar conjuntamente en sus esquemas de seguridad informática. ENISA ha desarrollado una guía con el fin de proteger los dispositivos IoT y las infraestructuras inteligentes de diferentes amenazas, por medio de la implementación de buenas

prácticas de seguridad tanto para fabricantes, operadores y encargados de tomar las decisiones. Esta guía está compuesta por una serie de factores relevantes como se listan a continuación[45]:

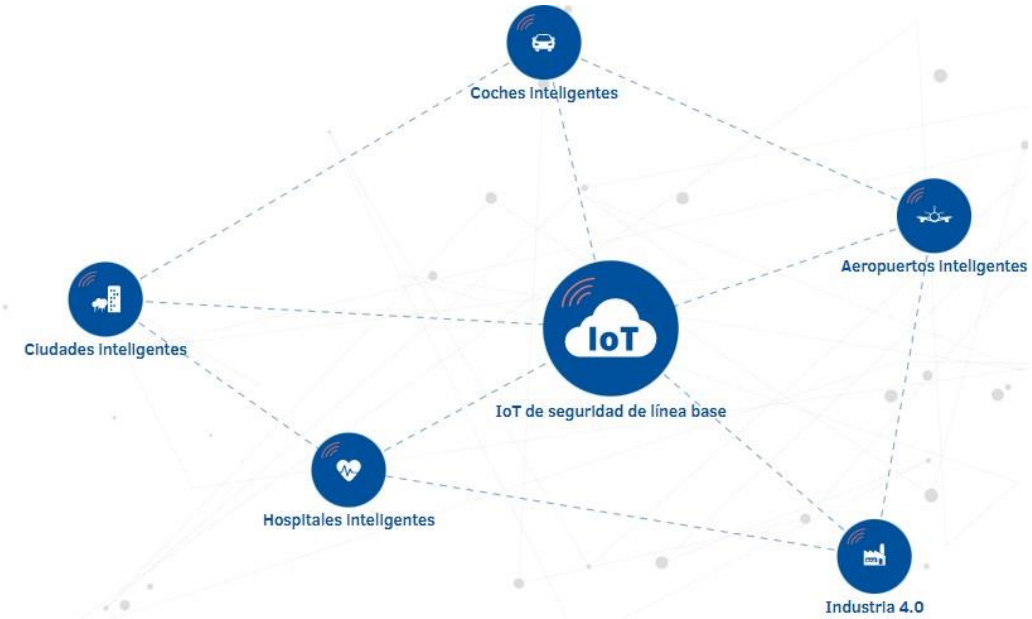
- **Fase conceptual**: En esta fase se realiza el diseño conceptual del dispositivo, su posible hardware, software, servicios y donde es importante tener aspectos de seguridad de los dispositivos IoT, como son los costos de producción evitando que se cometan errores que puedan desencadenar en fallas de seguridad del producto final.
- **Fase de desarrollo**: Al igual que la fase conceptual es importante tener en cuenta aspectos con el hardware y software, agregando la fabricación del dispositivo y de sus componentes como fundamentales puesto que implica proveedores, firmware, servicios, que no dependen solamente de la marca del dispositivo IoT.
- **Fase de producción**: La producción en masa de dispositivos IoT abarca desafíos de miles de proveedores de componentes, verificación de productos en mal estado que puedan ocasionar fallas de seguridad. Esta fase también implica un correcto almacenamiento, gestión de inventario y empaque de estos.
- **Fase de utilización**: Comprende una correcta entrega al usuario final, instalación del dispositivo, configuración inicial, asignación de credenciales por parte del usuario, conexión con otros dispositivos, entre otros. Esta fase es altamente compleja y donde el factor humano juega un papel importante.
- **Fase de apoyo**: En esta fase es importante dar soporte a los usuarios y a los dispositivos por medio de reemplazo de dispositivos con fallas y actualizaciones de seguridad durante su ciclo de vida, garantizando parches de seguridad a nivel de software, firmware y librerías.
- **Fase de retiro**: Después que los dispositivos cumplen su ciclo de vida se debe garantizar su correcta eliminación y destrucción, ayudando en materia de reciclaje de componentes y en la seguridad de la información que se encuentra en el dispositivo.

La Figura 9 hace referencia a los diferentes escenarios donde la agencia europea de seguridad de las redes y la información cuenta con publicaciones de buenas

[45] GUIDELINES FOR SECURING THE INTERNET OF THINGS [Anónimo]. ENISA [página web]. (noviembre, 2020). [Consultado el 13, septiembre, 2022]. Disponible en Internet: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport.

prácticas para los dispositivos IoT, y donde se muestran campos de aplicación como ciudades inteligentes, hospitales, coches e industria.

Figura 9. Escenarios de buenas prácticas para IoT suministrados por ENISA



Fuente: Enisa good practices for IoT and Smart Infrastructures Tool [Anónimo]. ENISA [página web]. [Consultado el 13, septiembre, 2022]. Disponible en Internet: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool.

5.3.5 IoT Security Foundation (IoTSF). Es una organización mundial sin ánimo de lucro que busca una mejor ciberseguridad de los dispositivos IoT, haciendo frente a los constantes desafíos que se generan con la expansión y el uso de estos dispositivos. Esta organización está conformada por fabricantes, operadores de red, distribuidores, instituciones académicas y personas que se encuentren relacionadas con la seguridad y la privacidad de la información. IoTSF ha publicado marcos de seguridad, guías de buenas prácticas para el diseño seguro, guía de buenas prácticas para divulgación de vulnerabilidades y principios de seguridad para el internet de las cosas como se muestra a continuación[46].

[46] ESTABLISHING PRINCIPLES FOR INTERNET OF THINGS SECURITY [Anónimo]. IoT Security Foundation [página web]. (septiembre, 2015). [Consultado el 13, septiembre, 2022]. Disponible en Internet: https://www.iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf.

- Ofrecer seguridad sobre los demás equipos de la red local donde se encuentra conectado el dispositivo.
- Mantener informado a los usuarios de los datos personales que se requiere para el funcionamiento del dispositivo.
- Brindar la posibilidad que los usuarios revisen sus datos para verificar su privacidad y confidencialidad.
- Realizar cifrado seguro de las claves.
- Verificación de la integridad del software.
- Protección y autenticación de los datos personales.
- Identificación de los equipos que se encuentren averiados o comprometidos en materia de ciberseguridad.
- Aislamientos de los datos de otros sistemas.
- Monitoreo de las fallas y estado de los dispositivos.
- Identificación de los dispositivos en la red de manera segura.
- Información oportuna a los usuarios de la funcionalidad y restricciones del dispositivo.
- Diseños seguros evitando la piratería.
- Cumplimiento de estándares de codificación y test de penetración.
- La gestión del dispositivo se realiza a través de canales autenticados.
- Suministro y actualizaciones seguras y oportunas.
- Verificación de la fuente de actualizaciones o parches de seguridad.
- Manejo de datos confidenciales en caso de transferencia de propiedad del dispositivo.
- Control de políticas para habilitar y deshabilitar funciones no deseadas.

IoTSF cuenta con una serie de herramientas y materiales de apoyo de manera gratuita en su sitio, entre los más relevantes en los últimos años se encuentra el marco de ciberseguridad, mejores prácticas de diseño, cuestionario de cumplimiento como se muestra en la siguiente figura.

Figura 10. Herramientas publicadas por IoT Security Foundation

Fuente: LACNIC [página web]. (2, mayo, 2022). [Consultado el 14, septiembre, 2022]. Disponible en Internet: https://www.lacnic.net/innovaportal/file/5959/1/presentacion_ftl2022-oscar-giudice.pdf.

5.3.6 Código de buenas prácticas del consumidor del Reino Unido. El ministerio de cultura, comunicaciones y deporte del reino unido realiza la publicación de un código de buenas prácticas para que los consumidores logren la seguridad en el internet de las cosas. El documento está construido con ayuda del centro nacional de seguridad cibernética y se compone por las siguientes 13 pautas[47]:

- Los dispositivos IoT no deben contar con contraseñas predeterminadas o por defecto, haciendo necesario que el consumidor sea la persona quien asigne el usuario y la contraseña para lograr activar y utilizar el dispositivo.
- Las compañías que venden dispositivos IoT deben hacer público las vulnerabilidades de los dispositivos, permitiendo que los consumidores y

[47] Code of Practice for consumer IoT security [Anónimo]. Department for Digital, Culture, Media & Sport [página web]. (octubre, 2018). [Consultado el 14, septiembre, 2022]. Disponible en Internet: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.

profesionales de la seguridad puedan informarse de los problemas de manera oportuna.

- La actualización del dispositivo IoT debe realizarse de manera segura sin afectar el dispositivo, informando al usuario de su vida útil como también el tiempo que recibirá software por parte del fabricante.
- Las credenciales deben almacenarse de manera segura en los dispositivos y servicios, evitando que estas se encuentren codificadas dentro del software.
- La información privada o sensible debe ser cifrada mientras se encuentra en tránsito a otros dispositivos, de acuerdo con la tecnología y el uso que se le esté dando.
- Se debe realizar el cierre de los puertos y servicios que no se estén usando o no sean necesarios en el dispositivo, el software solo se ejecuta con los privilegios adecuados minimizando la superficie de los ataques en que se encuentra expuesto el dispositivo.
- Es necesario el arranque seguro que verifique la integridad del software, generando alertas al consumidor, restringiendo conexiones a redes donde pueda afectar otros usuarios o equipos.
- La protección de los datos personales se debe realizar acorde a las leyes de protección de datos, informando al consumidor de qué manera se usan los datos, los fines y porque servicio.
- Los sistemas que componen el internet de las cosas deben soportar interrupciones de servicios de conectividad y energía, recuperándose de manera ordenada, conservando la información y funcionalidad.
- Gran cantidad de electrodomésticos y otros dispositivos IoT realizan el envío de datos de telemetría para detectar fallas en el mismo, el usuario debe ser consciente de que datos se recopilan, reduciendo al máximo el procesamiento de datos personales.
- Facilitar a los consumidores el poder realizar el borrado de los datos personales cuando lo deseen o cuando se realice el traslado de propiedad a otros usuarios. Los fabricantes deben incluir instrucciones claras sobre la realización de este tipo de procedimientos.
- Una buena guía o acompañamiento para la instalación y mantenimiento de los dispositivos, empleando buenas prácticas no solo de uso sino también de seguridad.
- Realizar validación de los datos ingresados y transmitidos por medio de API, disminuyendo la probabilidad de que puedan aparecer brechas de seguridad que puedan ser explotadas.

Los retos de ciberseguridad tanto para proveedores, fabricantes, implementadores y consumidores de dispositivos IoT hace que cada día se consoliden mejores prácticas y políticas de manera conjunta, haciendo que los desafíos en cuanto a la expansión del uso de estos dispositivos, vaya de la mano con mayor seguridad y privacidad de la información. Las iniciativas anteriormente descritas hacen parte de una gran cantidad de proyectos que pretenden conseguir hacer del internet de las cosas, un entorno seguro y que su uso no implique una amenaza para las organizaciones o usuarios finales.

5.4 ANALIZAR ALGUNOS MARCOS DE REFERENCIA DE DISPOSITIVOS IOT EN BÚSQUEDA DE MEJORES PRÁCTICAS Y CARACTERÍSTICAS DE CIBERSEGURIDAD PARA ESTE TIPO DE DISPOSTIVOS.

El marco de referencia permite que las organizaciones mejoren sus políticas de seguridad y puedan tomar correctivos para mitigar y reducir las vulnerabilidades de sus entornos informáticos. El internet de las cosas no es ajeno a estos marcos y algunas entidades dedicadas a la ciberseguridad han creado framework con controles que permiten maximizar la adopción y los beneficios en la implementación del internet de las cosas en empresas, hogares, ciudades inteligentes y campos de aplicación de este tipo de dispositivos.

El NIST en su informe interinstitucional 8259A indica las capacidades de ciberseguridad básicas que los dispositivos IoT deben cumplir de acuerdo con los marcos de referencia más importantes. Algunos de los marcos de referencia para IoT mencionados en este documento son el IoT Security Foundation, Internet Society/Online Trust Alliance (OTA), agencia europea de seguridad de redes de la información (ENISA), la comisión electrónica internacional (IEC) y el instituto nacional de estándares y tecnología (NIST) [48]. En la siguiente figura se observan algunas características técnicas de algunos de los marcos de ciberseguridad para los dispositivos IoT.

[48] FAGAN, Michael, et al. Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT [en línea]. [s.l.]: [s.n.], 2020 [consultado el 25, septiembre, 2022]. 24 p. Informe interinstitucional o interno 8259A del NIST. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259Aes.pdf.

Figura 11 principales características técnicas de algunos marcos de ciberseguridad

ALGUNAS CARACTERÍSTICAS TÉCNICAS DE LOS MARCOS DE CIBERSEGURIDAD PARA IOT

Características	IoT SF	ISOC - OTA	NIST	ENISA
Seguridad	*	*	*	*
Privacidad	*	*	*	*
Sustentabilidad a largo plazo	*	*	---	*
Confianza por diseño	*	*	*	*
Dispositivos/sensores	---	*	*	*
Comunicaciones	*	*	*	*
Servicios de backend	*	*	*	*
Aplicaciones	*	*	*	*
Múltiples iniciativas (distintos campos)	---	*	*	*

Fuente: LACNIC [página web]. (2, mayo, 2022). [Consultado el 14, septiembre, 2022]. Disponible en Internet: https://www.lacnic.net/innovaportal/file/5959/1/presentacion_ftl2022-oscar-giudice.pdf.

La Figura 11 muestra algunas de las características técnicas de algunos de los marcos de referencia, hallándose que gran parte de ellos son similares en aspectos de ciberseguridad para el internet de las cosas como lo son la privacidad, comunicaciones, dispositivos capa de aplicación, entre otros. A continuación de presentan algunos de los marcos de referencias con sus principales características de seguridad para dispositivos IoT.

5.4.1 Marco de referencia IoTSF. Este framework de seguridad detalla de manera correcta y minuciosa cada una de las sesiones y requerimientos que los dispositivos IoT deben cumplir para contar con una seguridad óptima desde su proceso de diseño hasta la transferencia final al consumidor. Se compone de 14 garantías de aplicabilidad donde cada una de ellas se compone de múltiples requerimientos necesarios para su cumplimiento. A continuación, se listan cada de las aplicaciones de seguridad que se abarcan en este marco[49].

- Políticas, procesos y responsabilidades de seguridad empresarial.
- Seguridad del dispositivo y del hardware.

[49] IoT security Assurance Framework [Anónimo]. IoT Security Foundation – The Global Home of IoT Cybersecurity [página web]. (noviembre, 2021). [Consultado el 20, septiembre, 2022]. Disponible en Internet: https://www.iotsecurityfoundation.org/best-practice-guidelines.

- Seguridad del software del dispositivo.
- Seguridad del sistema operativo.
- Interfaces cableadas e inalámbricas.
- Autenticación y autorización.
- Encriptación y gestión de claves.
- Interfaz de usuario.
- Aplicaciones móviles.
- Protección de datos y privacidad de estos.
- Elementos de red y la nube.
- Producción y cadena de suministro.
- Configuración del dispositivo.
- Transferencia de propiedad al usuario.

Este marco está dirigido para administradores de ciberseguridad en organizaciones que deseen gestionar y adoptar mejores prácticas en los proyectos que se vayan a implementar o ya estén en curso. Igualmente, este marco se dirige a los ingenieros, desarrolladores y personal encargado de fabricar los diferentes dispositivos y componentes que hacen parte del internet de las cosas, buscando que los procesos se encuentren bajo lineamientos y se tenga evidencia del aseguramiento tanto de la integridad, confidencialidad y disponibilidad[50].

De acuerdo con la aplicación del dispositivo IoT y el mercado en que este se encuentre es probable que el nivel de seguridad pueda variar, es por esto, que el marco de seguridad de IoTSF ofrece 5 nivel de protección como lo son[51]:

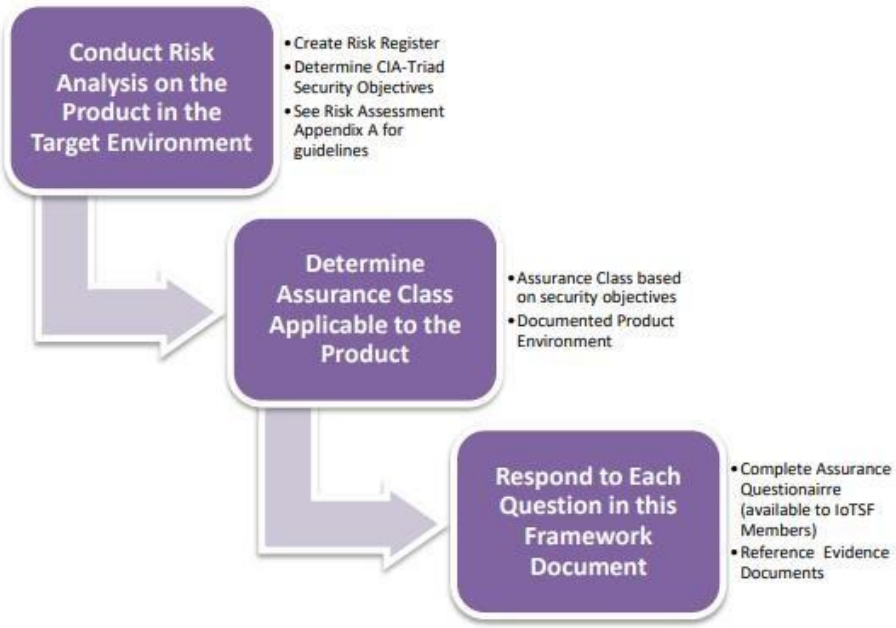
- **Clase 0**: Los datos o su perdida no producen un impacto importante para las organizaciones o consumidores.
- **Clase 1**: La pérdida o el compromiso de los datos resulta en un impacto leve o solo afecta a un individuo u organización. El ETSI (instituto europeo de normas de telecomunicaciones) exige que se cumpla como mínimo esta clase.
- **Clase 2**: El dispositivo IoT es capaz de cumplir con lo establecido en la clase 1 y además es robusto para garantizar la disponibilidad de la infraestructura donde está conectado.
- **Clase 3**: Se cumple las clases anteriores y se protege los datos confidenciales que se encuentran almacenados en el dispositivo IoT.

[50] Ibíd., p.5.
[51] Ibíd., p.9.

- **Clase 4**: Máxima protección de la seguridad de la información, debido a que la perdida de datos o de control del dispositivo puede afectar infraestructuras críticas o afectar a personas.

La siguiente Figura ilustra el proceso que el marco IoTSF indicia que se debe seguir para ley aseguramiento del internet de las cosas.

Figura 12 Pasos para el aseguramiento de los dispositivos IoT



Fuente: IoT security Assurance Framework [Anónimo]. IoT Security Foundation – The Global Home of IoT Cybersecurity [página web]. (noviembre, 2021). [Consultado el 20, septiembre, 2022]. Disponible en Internet: https://www.iotsecurityfoundation.org/best-practice-guidelines.

De acuerdo a la Figura 12 el proceso de aseguramiento se compone de tres pasos como lo son análisis del dispositivo por medio de una evaluación de riesgos de acuerdo a el entorno donde se encuentra o va a ser instalado, seguido a esto se determina el nivel de aseguramiento que se le va a aplicar al dispositivo y por último realizar el cuestionario de garantía de acuerdo a las pautas indicas por IoTSF.

El marco de Ciberseguridad de IoTSF es uno de los marcos más completos para el internet de las cosas en cada una de las aplicaciones de seguridad que se abarcan en el documento, detallando uno a uno los requisitos que son necesarios para

cumplirlos y el nivel de aseguramiento y la aplicabilidad que se puede tener para cada uno de ellos.

5.4.2 Marco de seguridad OTA. El marco de confianza para IoT de esta organización busca aumentar la seguridad de los dispositivos IoT y la confianza por parte de los consumidores para el uso de este tipo de tecnologías. Este marco se caracteriza por tener en cuenta aspectos importantes como lo son el ciclo de vida de los dispositivos y ecosistemas que muchas veces no se contemplan como lo son los servicios backend y aplicaciones móviles.

El marco OTA se basa en principios que se dividen en 8 categorías de manera que, si se cumplen los principios de cada una de ellas, es muy probable elevar la confianza y seguridad en el internet de las cosas. Las categorías incluidas en este marco son las siguientes[52]:

- **Autenticación**: Es necesario realizar autenticación tanto de dispositivos como de usuarios para evitar accesos no deseados.
- **Encriptación**: Realizar la encriptación para evitar filtración de datos e información delicada.
- **Seguridad**: Se abarca la seguridad en aplicaciones, dispositivos, backend y actualizaciones.
- **Actualizaciones**: Ofrecer actualizaciones fáciles y seguras con poca intervención de los usuarios.
- **Privacidad**: Informar a los usuarios las políticas de privacidad, recolección y si se va a compartir alguno de sus datos.
- **Divulgaciones**: Informar sobre parches de seguridad y políticas claras de manera que los usuarios puedan tomar decisiones.
- **Control**: Los usuarios pueden borrar o transferir información cuando ellos lo deseen.
- **Comunicaciones**: Comunicar de manera oportuna al consumidor la información real del dispositivo, sus capacidades, mejores prácticas, reduciendo los ataques de ingeniería social.

El marco de confianza de IoT de OTA se encuentra en la versión 2.5 se compone de 4 principios que facilitan que los desarrolladores de internet de las cosas puedan

[52] IoT confianza por diseño - Internet Society [Anónimo]. Internet Society [página web]. (22, mayo, 2018). [Consultado el 20, septiembre, 2022]. Disponible en Internet: https://www.internetsociety.org/es/resources/doc/2018/iot-trust-by-design.

establecer bases de certificación de este tipo de dispositivos en el futuro, y a su vez permita ayudar que las organizaciones y consumidores logren identificar dispositivos más seguros y confiables. Los principios en los cuales se divide el marco son[53]:

- **Principio de seguridad**: Se aplica a cualquier dispositivo IoT y abarca de manera rigurosa la seguridad del software, datos almacenados, datos trasmitidos, pruebas de penetración y reportes de vulnerabilidades.
- **Acceso y credenciales de usuario**: Este principio busca que la información cumpla con los requisitos de encriptación de las credenciales, se otorgue contraseñas únicas a cada dispositivo, restablecimiento de contraseñas seguros y se prevenga ataques que puedan acceder al dispositivo mediante fuerza fruta.
- **Privacidad, transparencia y divulgaciones**: Busca que se cumpla con políticas de privacidad, dándole la capacidad a los usuarios de poder restablecer configuración de fábrica.
- **Notificaciones y mejores prácticas**: Este principio garantiza que los usuarios logren recibir notificaciones de manera oportuna sobre posibles amenazas o si se requiere una acción de su parte. se exige notificaciones por correo electrónico de manera clara y que el envasado del producto sea seguro.

El marco de ciberseguridad de OTA abarca de manera acertada las diferentes áreas y categorías que componen la seguridad de los dispositivos IoT, con una amplia cantidad de controles a implementar indicando si estos son obligatorios o son voluntarios. Igualmente, el marco de ciberseguridad y algunos de los controles cuentan con el respaldo de recursos y enlaces para implementar de manera correcta la seguridad.

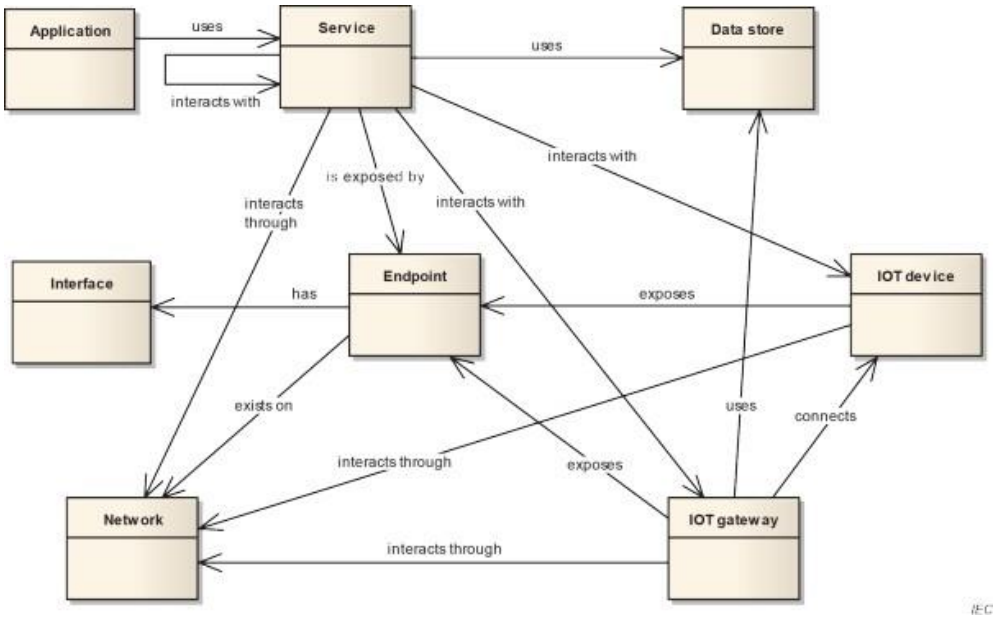
5.4.3 IEC 30141. En el año 2018 nace el primer estándar internacional desarrollado por IEC e ISO con el fin de proporcionar una referencia en cuanto a la arquitectura de los dispositivos IoT. Este estándar brinda los conceptos necesarios para que los fabricantes de este tipo de tecnologías logren realizarlos más confiables, seguros y de acuerdo con los más altos estándares de seguridad de la información. el estándar abarca las siguientes características en la arquitectura.

[53] OTA. “IoT Trust Framework” Marco de confianza y confidencialidad de IoT v2.5 [en línea]. 14, octubre, 2017 [consultado el 21, septiembre, 2022]. Disponible en Internet: https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_ES.pdf.

- Características de confiabilidad del sistema IoT.
- Conectividad de red.
- Modularidad.
- Escalabilidad.
- Identificación única.
- Autoconfiguración.
- Manejabilidad.
- Flexibilidad.
- Administración de red.
- Integridad.
- Separar capacidad funcional de la de gestión.

La figura 13 muestra el modelo conceptual del estándar IEC30141 para la relación entre los servicios, redes, IoT Gateway y el dispositivo IoT. Esta arquitectura busca garantizar la seguridad de cada uno de los componentes que hacen parte del internet de las cosas.

Figura 13 Concepto de relación entre Servicios, IoT Gateway redes y dispositivo



Fuente: INTERNATIONAL ELECTROTECHNICAL COMMISSION. Internet of Things (IoT) – Reference architecture [en línea]. ISO/IEC 30141. Geneva, Suiza: [s.n.], 2018 [consultado el 20, octubre, 2022]. 88 p. Disponible en Internet: https://standards.iso.org/ittf/PubliclyAvailableStandards/c065695_ISO_IEC_30141_2018(E).zip.

Este marco de referencia a diferencia de los marcos anteriores, está diseñado especialmente para diseñadores y fabricantes de dispositivos IoT, desglosando de manera detallada cada una de las características para lograr elevar la seguridad de este tipo de dispositivos. La ISO/IEC 30141 promueve que se utilice un lenguaje universal en la industria y se recupere la confianza de seguridad de IoT por parte de las organizaciones y los consumidores.

En la siguiente tabla se muestran las capacidades de ciberseguridad de los dispositivos IoT que son protegibles[54].

Tabla 3 Capacidades de seguridad de IoT con base a marcos de referencia

Capacidad del dispositivo	**Descripción**	**Marcos de referencia**
Identificación del dispositivo	Los dispositivos deben contar con un identificador único ya sea físico o lógico, que permita a los usuarios distinguirlos de los demás dispositivos IoT de la red. El identificador único permite que se logre realizar gestión centralizada del dispositivo al igual que autenticación de estos.	IoTSF ENISA IEC OTA
Configuración del dispositivo	Tiene la capacidad de modificar las opciones de configuración del software. Permite que los usuarios u organizaciones realicen cambios de la configuración. Restauración de la configuración en caso de ser necesario.	IoTSF ENISA IEC OTA
Protección de datos	El dispositivo tiene la capacidad de ejecutar algoritmos criptográficos de la información como hash, cifrado y firmas digitales.	IoTSF ENISA IEC OTA

[54] FAGAN, Michael, et al, Op.cit., p.12

Continuación tabla 3

Capacidad del dispositivo	Descripción	Marcos de referencia
Protección de datos	Se logra controlar el acceso a la información del dispositivo para los usuarios que se encuentren o no autorizados.	IoTSF ENISA IEC OTA
Acceso lógico a las interfaces	Se permite deshabilitar o habilitar las interfaces de red de acuerdo con su uso por parte de los usuarios. Se restringe el uso de las interfaces solo a los servicios o usuarios autenticados. Permite configurar las interfaces, sus capacidades, medidas de seguridad o intentos fallidos de autenticación.	IoTSF ENISA IEC OTA
Actualización de software	Se permite la actualización del dispositivo de manera remota. Verificación de actualizaciones antes de instalarla. Posibilidad de revertir las actualizaciones del software. Capacidad para limitar las actualizaciones. Restricción de quien puede ejecutar actualizaciones en el dispositivo.	IoTSF ENISA IEC OTA
Información del estado de ciberseguridad	Informa el estado de la seguridad del dispositivo. Solo los usuarios autorizados pueden observar el estado o logs del dispositivo. Permite enviar información del estado a otros servidores de eventos o estados.	IoTSF ENISA IEC OTA

Fuente: Elaboración Propia

Las capacidades expuestas en la tabla 3, se observa como los marcos de referencia cuentan con grandes similitudes en la forma como abarcan la seguridad de estos dispositivos, buscando que estos puedan cumplir con las exigencias de seguridad suficientes y así de esta manera su implementación no ponga en riesgo la información y privacidad de las organizaciones y consumidores del internet de las cosas. Los marcos de referencia son el camino que tanto fabricantes como consumidores deben seguir para lograr que los retos de ciberseguridad presentes en el internet de las cosas puedan superarse, elevando la confianza en el uso de estos dispositivos y que el esperado crecimiento de conectividad en los próximos años esté al nivel de seguridad esperada.

6 CONCLUSIONES

Las conclusiones que se logran obtener del desarrollo de esta investigación son las siguientes:

El acogimiento del internet de las cosas con el paso de los años ha sido muy positivo llevando a que su uso se extienda a múltiples campos como lo son la medicina, hogar, ciudades inteligentes, transporte, industria y otros. El uso de estos dispositivos IoT beneficia a la humanidad brindándole una mejor conectividad, confort, seguridad y comunicación que hace unos años no era posible sin la implementación de este tipo de tecnologías. De acuerdo con esto, se concluye como el internet de las cosas ha revolucionado el mundo con dispositivos económicos, de fácil instalación y acceso tanto para las personas como para los diferentes sectores de la industria.

Se evidenció como el internet de las cosas ha sido blanco de ataques informáticos como también pueden ser usados para generar ataques sincronizados a gran escala, impulsados principalmente por las múltiples vulnerabilidades y debilidades que presentan los dispositivos IoT y que OWASP manifiesta y describe en su Top Ten. OWASP manifestó como el internet de las cosas presenta fallas desde su parte de diseño con el uso de componentes poco seguros y obsoletos, malas gestiones del dispositivo en cuanto a actualizaciones y uso de software inseguro, haciendo que los ciberdelincuentes centren su atención a este tipo de dispositivos debido a la alta probabilidad de tener éxito a la hora de efectuar un ataque informático.

Se identificaron cuáles son los principales retos en materia de ciberseguridad que existen en el diseño, fabricación e implementación de los dispositivos IoT, en donde se resaltan tres principales retos como lo son la protección del dispositivo, protección de los datos y por último la protección de la privacidad de los usuarios. Estos retos van alineados y de la mano de las diferentes guías y buenas prácticas que las organizaciones de seguridad como NIST, IoTSF, ENISA han publicado con respecto al desarrollo e implementación del internet de las cosas tanto para organizaciones como para su uso común, en búsqueda que este tipo de tecnologías cuenten con la seguridad necesaria para los dispositivos como para sus consumidores.

Debido a la necesidad de garantizar la seguridad de la información y de los dispositivos IoT, diferentes organizaciones a nivel mundial desarrollaron marcos de

referencia en búsqueda de brindar guías de referencia para lograr una mejor ciberseguridad en el internet de las cosas. Se encontró como los marcos de referencia cuentan con características similares y abarcan temas de seguridad, privacidad, confianza, diseño, comunicación, aplicaciones y actualizaciones que permitan elevar el nivel de confianza por parte de los distribuidores y consumidores de dispositivos IoT.

7 RECOMENDACIONES

Con el desarrollo de los objetivos se han obtenido resultados con respeto a los retos de ciberseguridad en IoT, sin embargo, se realizan las siguientes recomendaciones al respecto:

Realizar análisis adecuados en materia de seguridad de la información a los dispositivos IoT que se desean implementar en organizaciones, hogares u otros sectores de manera que su uso brinde los beneficios adecuados a los consumidores de estos productos, pero también brinden la privacidad y seguridad suficiente de la información y de los datos de los usuarios.

Diseñar, construir y distribuir dispositivos IoT que cuenten con mejores sistemas de seguridad de la información, priorizando aspectos como el diseño, mejores materiales, aplicaciones seguras, actualizaciones recurrentes que superen las vulnerabilidades expuestas en el OWASP Top Ten y permita una mejor experiencia de ciberseguridad para los consumidores.

Ejecutar mejores prácticas de ciberseguridad al momento de instalar y administrar dispositivos de internet de las cosas, estableciendo contraseñas fuertes, monitoreo constante de los logs, seguridad física adecuada, actualizaciones periódicas que ayuden a que este tipo de tecnologías no sean la entrada a ataques informáticos o robo de información en organizaciones u otras infraestructuras donde se encuentren operando.

Ajustar las políticas de ciberseguridad que los diferentes fabricantes de dispositivos IoT usan para el diseño y fabricación de estos, de manera que se logren alinear con las buenas prácticas que las organizaciones en el mundo presentan para el internet de las cosas. El desarrollo de estas prácticas ayudará a que el internet de las cosas pueda alcanzar las metas contempladas en este documento en protección de los dispositivos, protección de los datos y privacidad de los usuarios.

Implementar normativa robusta para que tanto los diseñadores, fabricantes y distribuidores de dispositivos IoT puedan apoyarse en su fabricación, evitando que el uso de los marcos de referencia y buenas prácticas publicadas en la actualidad no sean solo material de apoyo, garantizando que el internet de las cosas pueda cumplir con los requerimientos mínimos de seguridad que se requiere a nivel de trazabilidad, autenticidad, privacidad e integridad de la información.

BIBLIOGRAFÍA

ACOSTA MOLINA, Cesar Mauricio. El estado del arte sobre el internet de las cosas. amenazas y vulnerabilidades de seguridad informática evidenciadas desde la domótica. [En línea]. Proyecto de Grado especialización. Bogotá. UNAD, Escuela de Ciencias Básicas, Ingeniería, Tecnología e Ingeniería – ECBTI, 2019. 81 p. [Consultado el 04 de abril del 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28446/Monografia.pdf?sequence=1&isAllowed=y

ALCATEL LUCENT ENTERPRISE. [En línea]. Internet de las Cosas en sanidad. (Diciembre 2019). [Consultado el 7 de abril de 2022]. Archivo pdf. Disponible en: https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-healthcare-solutionbrief-es.pdf

ANTONAKAKIS, Manos, et al. Understanding the Mirai Botnet [en línea]. Vancouver, Canadá. 16, agosto, 2017 [consultado el 2, mayo, 2022]. Disponible en Internet: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

ARIAS SILVA, Nino Alexander. análisis de seguridad de vulnerabilidades y ataques presentados en 4 dispositivos de internet de las cosas [En línea]. Trabajo de grado. UNAD, 2019. [Consultado 13 de abril del 2022]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/33326/naariass.pdf?sequence=1&isAllowed=y

ATCH, David; REGEV,Gil y BEVINGTON,Ross. How to proactively defend against Mozi IoT botnet [Página web]. Microsoft. (19 de agosto de 2021). [Consultado el 04 de mayo de 2022]. Disponible en: https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/

BOECKL,Katie, et al. Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT). [En linea]. Departamento de Comercio de los EE. UU, 2019.p.4 [Consultado el 2 de abril del 2022]. Disponible en https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932207

CAÑAS CUEVAS, Javier Alexander; PATIÑO DORADO, Lucas Alejandro. Modelo informático aplicado a la ciberseguridad de dispositivos IoT. [En línea]. Proyecto de Grado. Bogotá. Universidad EAN. Facultad de ingenierías, 2021. 50 p. [Consultado el 04 de abril del 2022]. Disponible en: https://repository.ean.edu.co/bitstream/handle/10882/10773/PatinoLucas2021.pdf?sequence=1

CARAZO ALCALDE, Ciudad inteligente [página web]. Economipedia. (7 de abril de 2017). [Consultado el 6 de abril de 2022]. Disponible en Internet: https://economipedia.com/definiciones/ciudad-inteligente-smart-city.html

CERT-PY: “Mozi” nueva familia de Malware que afecta a dispositivos IoT combinando 3 malwares en 1 [Página web]. [Consultado el 03 de mayo de 2022]. Disponible en: https://www.cert.gov.py/noticias/mozi-nueva-familia-de-malware-que-afecta-dispositivos-iot-combinando-3-malwares-en-1

CLOUDFLARE: ¿Qué es la botnet Mirai? [Página web]. Cloudflare. [Consultado el 02 de mayo de 2022]. Disponible en: https://www.cloudflare.com/es-es/learning/ddos/glossary/mirai-botnet/

Code of Practice for consumer IoT security [Anónimo]. Department for Digital, Culture, Media & Sport [página web]. (octubre, 2018). [Consultado el 14, septiembre, 2022]. Disponible en Internet: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.

CONCEPTO. Protocolo informatico. [Pagina Web] .[Consultado el 8 de mayo de 2022]. Disponible en : https://concepto.de/protocolo-informatico/

DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT: Code of Practice for Consumer IoT Security. [Página web]. (octubre 2018) [Consultado el 27 abril de 2022]. Archivo pdf. Disponible en:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

Enisa good practices for IoT and Smart Infrastructures Tool [Anónimo]. ENISA [página web]. [Consultado el 13, septiembre, 2022]. Disponible en Internet: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

ESTABLISHING PRINCIPLES FOR INTERNET OF THINGS SECURITY [Anónimo]. IoT Security Foundation [página web]. (septiembre, 2015). [Consultado el 13, septiembre, 2022]. Disponible en Internet: https://www.iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf.

EVANS, Dave. Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo [En linea]. Cisco IBSG: 2011. p.2. [Consultado el 1 de abril del 2022]. Disponible en

https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

FAGAN, Michael, et al. Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT [en línea]. [s.l.]: [s.n.], 2020 [consultado el 15, septiembre, 2022]. 24 p. Informe interinstitucional o interno 8259A del NIST. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259Aes.pdf.

FERNANDES SILVEIRA, Frederico augusto. Smart-IoT: um sistema de proteção contra DDoS para rede de Internet das Coisas. [En línea]. Tesis de Maestria. Natal. Universidade federal do rio grande do norte, 2020. 84 p. [Consultado el 04 de abril del 2022]. Disponible en: https://repositorio.ufrn.br/bitstream/123456789/30831/1/SmartIoTsistema_Silveira_2020.pdf

FORTINET: What Is an IoT Device Vulnerability? [Página web]. [Consultado el 29 de abril de 2022]. Disponible en: Principales vulnerabilidades de dispositivos IoT: cómo proteger dispositivos IoT | Fortinet

GUIDELINES FOR SECURING THE INTERNET OF THINGS [Anónimo]. ENISA [página web]. (noviembre, 2020). [Consultado el 13, septiembre, 2022]. Disponible en Internet: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport

HASAN, Mohammad. State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally [página web]. (18, Mayo, 2022). [Consultado el 12, junio, 2022]. Disponible en Internet: https://iot-analytics.com/number-connected-iot-devices/

HPE. ¿qué es el internet de las cosas industrial (IIoT)? [Sitio Web]. [Consultado el 10 de abril de 2022]. Disponible en: https://www.hpe.com/lamerica/es/what-is/industrial-iot.html

IBM. Manejo de los ataques de tipo DDoS (Distributed Denial of Service) [Sitio Web]. (25 de junio de 2019). [Consultado el 5 de mayo de 2022]. Disponible en: https://cloud.ibm.com/docs/cis?topic=cis-distributed-denial-of-service-ddos-attack-concepts&locale=es

INCIBE: Seguridad en la instalación y uso de dispositivos IoT: Una guía de aproximación para el empresario. [Página web]. (2020) [Consultado el 26 abril de 2022]. Archivo pdf. Disponible en: Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario (incibe.es)

KASPERSKY. El número de ataques a dispositivos IoT se duplica en un año [Sitio Web]. [Consultado el 2 de abril de 2022]. Disponible en:

https://www.kaspersky.es/about/press-releases/2021_el-numero-de-ataques-a-dispositivos-iot-se-duplica-en-un-ano

KOVÁCS MATÍNEZ, Pablo. IoT: Internet de las cosas en el modelo de Industria 4.0 [En línea]. Trabajo de grado. Sevilla. Universidad de Sevilla, 2018. 79 p. [Consultado 5 de abril del 2022]. Disponible en https://biblus.us.es/bibing/proyectos/abreproy/91965/fichero/TFG-1965-KOVACS.pdf

LACNIC [página web]. (2, mayo, 2022). [Consultado el 14, septiembre, 2022]. Disponible en Internet: https://www.lacnic.net/innovaportal/file/5959/1/presentacion_ftl2022-oscar-giudice.pdf

LASSE LUETH, Knud. State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. IoT Analytics [página web]. (19, noviembre, 2020). [Consultado el 1, abril, 2022]. Disponible en Internet: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

MACIAS MENDEZ, Xiomara Mayerli; DUEÑAS JUEZ, Jose Luis. Implementación de un modelo de seguridad informática en un sistema de monitoreo para los canales de comunicaciones y Datacenter en la empresa Atento SA [En línea]. Monografía. Bogotá. Universidad distrital Francisco Jose de Caldas, 2015. p .8 [Consultado 4 de abril del 2022]. Disponible en https://repository.udistrital.edu.co/bitstream/handle/11349/4258/MaciasMendezXiomaraMayerli2015.pdf?sequence=9&isAllowed=y

MALWAREBYTES. Ransonware [Sitio Web]. [Consultado el 8 de mayo de 2022]. Disponible en: https://es.malwarebytes.com/ransomware/

MCAFEE. Proteja los dispositivos IoT para prevenir ataques. [página web]. Madrid: (2017). [Consultado el 1, abril, 2022]. Archivo pdf. Disponible en Internet: https://www.mcafee.com/enterprise/es-es/assets/solution-briefs/sb-quarterly-threats-mar-2017-1.pdf

MENDOZA DOMINGUEZ, Esly Lorena. La seguridad de la información en el internet de las cosas (IoT) [en línea]. Proyecto de grado especialización. Cali: UNAD, 2021 [consultado el 4, mayo, 2022]. 82 p. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/47752/32584013LaSeguridaddDeLaInformacionEnElInternetDeLasCosasIoT.pdf?sequence=1&isAllowed=y

MOLINA SANCHEZ, Edwin Alfredo. Análisis de seguridad de vulnerabilidades presentes en redes sin hilos corporativas [en línea]. Proyecto de grado especialización. Bogotá: UNAD, 2020 [consultado el 4, mayo, 2022]. 104 p. Disponible en Internet:

https://repository.unad.edu.co/bitstream/handle/10596/37512/eamolinas.pdf?sequence=1&isAllowed=y

MUYSEGURIDAD. IoT: así se resiente la seguridad del Internet de las Cosas. [Página web]. (13 de septiembre de 2019). [Consultado el 14 de mayo del 2022]. Disponible en: https://www.muyseguridad.net/2019/09/13/iot-seguridad-cosas/

ORACLE. ¿Qué es el IoT?. [Sitio Web]. [Consultado el 12 de abril de 2022]. Disponible en: https://www.oracle.com/co/internet-of-things/what-is-iot/

OVHCLOUD. ¿Qué es un ataque DDoS? [Sitio Web]. [Consultado el 5 de mayo de 2022]. Disponible en:https://www.ovhcloud.com/es/security/anti-ddos/ddos-definition/

OWASP top 10 internet of things [En linea]. (2018) [Consultado el 01 abril de 2022]. Disponible en: https://owasp.org/www-pdf-archive//OWASP-IoT-Top-10-2018-final.pdf

PALOALTO NETWORKS. Informe de amenazas IoT 2020 de Unit 42 [en línea]. 2020 [consultado el 28, septiembre, 2022]. 24 p. Disponible en Internet: https://info.smartekh.com/hubfs/IoT/Informe%20de%20Amenazas%20IoT%202020.pdf.

PARRA JIMENEZ, Jhon Alexander. Un método para la identificación y prevención temprana de incidentes de ciberseguridad en dispositivos del Internet de las Cosas. [En linea]. Tesis maestria. Medellin. Universidad nacional de Colombia, 2021. [Consultado el 01 de abril del 2022]. Disponible en https://repositorio.unal.edu.co/bitstream/handle/unal/81148/1030660760.2021.pdf?sequence=1&isAllowed=y

PINZON NIÑO, David Leonardo. Panorama de aplicación de internet de las cosas (IoT) [En línea]. Monografía. Bogotá. Universidad Santo Tomas, 2015. 82 p. [Consultado 5 de abril del 2022]. Disponible en https://repository.usta.edu.co/bitstream/handle/11634/672/Panorama%20de%20aplicacion%20de%20internet%20de%20las%20cosas.pdf?sequence=1&isAllowed=y

PISANO, Ariel. Internet de las Cosas. [En linea]. Tesis maestría. Buenos Aires. Universidad de San Andres, 2018. 94 p. [Consultado el 02 de abril del 2022]. Disponible en https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16159/1/%5BP%5D%5BW%5D%20T.%20M.%20Ges.%20Pisano%2C%20Ariel.pdf

RAMIREZ MADRID, David Andres; RODRIGUEZ HERNANDEZ, Erika Dennis. Diseño de un método para identificar necesidades y oportunidades para la implementación de Internet de las cosas (IoT) aplicable a oficinas de trabajo donde

permanezcan entre 30 y 70 personas y planteamiento de un caso práctico de solución en las oficinas de la Agencia Nacional del Espectro. [En línea]. Trabajo de grado. Bogotá: Universidad distrital Francisco Jose de Caldas, 2016.p.25-27. [Consultado 1 de abril del 2022]. Disponible en https://repository.udistrital.edu.co/bitstream/handle/11349/5343/RamirezMadridDavidAndres2017.pdf;jsessionid=5E8A531A628066293E16AA6FCEC78285?sequence=1

REDHAT: ¿Qué es el Internet industrial de las cosas? [Página web]. (7 de mayo de 2021) [Consultado el 6 de abril de 2022]. Disponible en: https://www.redhat.com/es/topics/internet-of-things/what-is-iiot

RICO MACIAS, Victor Hugo. Modelo de defensa ante ataques a equipos IoT aplicado a smart tv basado en vulnerabilidades identificadas con OSSTMM [en línea]. Proyecto de grado especialización. Cali: UNAD, 2020 [consultado el 4, mayo, 2022]. 116 p. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/41520/vhricom.pdf?sequence=3&isAllowed=y

SANCHEZ GAMBOA, Hilbert Leonardo. Identificación de vulnerabilidades y riesgos en los activos de ti de energitel. [En línea]. Proyecto de Grado especialización. Ibagué. UNAD. Escuela de ciencias básicas, tecnología e ingeniería – ECBTI, 2018. p 28. [Consultado el 27 de abril del 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28221/93405573.pdf?sequence=1&isAllowed=y

TRENDMICRO: IoT and Ransomware: A Recipe for Disruption [Página web]. (28 de septiembre del 2021). [Consultado el 02 de mayo de 2022]. Disponible en: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-and-ransomware-a-recipe-for-disruption

URIBE CASTRO, Alejandro. Análisis del nivel de seguridad presente en los dispositivos que componen el internet de las cosas. [En línea]. Proyecto de Grado especialización. Cali. UNAD. Escuela de ciencias básicas, tecnología e ingeniería – ECBTI, 2019. 67 p. [Consultado el 30 de abril del 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/35363/auribeca.pdf?sequence=1&isAllowed=y

VASQUEZ RODRIGUEZ, Romel. Aplicaciones y tecnologías para el desarrollo de la internet de las cosas: *Revista metropolitana de ciencias aplicadas* [En línea]. Ecuador: Universidad metropolitana de Ecuador, diciembre 2018. Vol. 1. nro. 3. [Consultado el 04 de abril del 2022]. ISSN: 2631-2662 Disponible en: https://remca.umet.edu.ec/index.php/REMCA/article/download/58/162

VEGA PALACIO, David Alfonso. Análisis del nivel de exposición y privacidad de información personal en fuentes abiertas a través de la metodología open source intelligence (OSINT) [En linea]. Proyecto de Grado. Riohacha. UNAD. Escuela de ciencias básicas, tecnología e ingeniería – ECBTI, 2021. 83 p. [Consultado el 5 de mayo del 2022]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/48313/davegap.pdf?sequence=1&isAllowed=y

VERGARA, Carolina; OCAMPO VILLAN, Maria. El internet de las cosas (IoT) y la cuarta revolución Industrial [Pagina web]. Noviembre,2017. [Consultado el 15 de abril del 2022]. Disponible en https://energub.com/el-internet-de-las-cosas-iot-y-la-cuarta-revolucion-industrial/