# SEGURIDAD EN DISPOSITIVOS IOT EN ORGANIZACIONES INDUSTRIALES EN COLOMBIA

Oscar Giovanny González Cruz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C

2023

# SEGURIDAD EN DISPOSITIVOS IOT EN ORGANIZACIONES INDUSTRIALES EN COLOMBIA

Oscar Giovanny Gonzalez Cruz

Proyecto de Grado – Monografía presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Hernando José Peña

Director de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

2023

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C. Diciembre del 2023

## DEDICATORIA

Dedico esta monografía a mi familia puntualmente mamá, hermana y amigos que he encontrado en el camino y que pese a las adversidades se encuentran a mi lado brindando apoyo incondicional para realizar esta especialización y también a Dios por permitirme hacer este sueño realidad.

## AGRADECIMIENTOS

Quiero agradecerle a la Universidad Nacional Abierta y a Distancia (UNAD) por contar con el modelo de educación virtual que permite a las personas trabajar y estudiar para así mismo superarse de manera profesional obteniendo conocimiento, habilidades que permiten tener una mejor calidad de vida. También agradecer a mi familia, amigos y conocidos que directa o indirectamente me han apoyado en este proyecto.

CONTENIDO

Pág.

## LISTA DE ILUSTRACIONES

## LISTA DE TABLAS

## GLOSARIO

**Actualizaciones:** Hace referencia a que todo sistema tecnológico requiere de ser actualizado constantemente debido a que el proveedor suministra nuevas funcionalidades para corregir errores y fallas de seguridad**.**

**Amenaza:** Una amenaza es una probable y potencial violación de la seguridad de un sistema, que podría causar un efectivo negativo en los activos que lo componen.[1]

**API:** Hace referencia a cualquier tipo de software que brinda una interfaz para administrar, realizar ajustes, configuraciones. Es un componente fundamental para el funcionamiento actual en aplicaciones y cualquier tipo de servicio web.

**Atacante:** Es un individuo u organización el cual su objetivo es tener el control de un sistema informático con la finalidad de generar actividades maliciosas y en algunos casos cobrar un rescate por la información obtenida ilegalmente.[2]

***Backdoor:*** Termino de seguridad informático también conocido como puerta trasera.

***Bróker*:** Hace referencia a un programa que actúa como intermediario entre 2 sistemas.

***Backend:*** Es un componente fundamental del desarrollo web es el encargado de la lógica de un sitio web.

---

[1] Instituto Nacional de Ciberseguridad. [Sitio web]. Bogotá: INCIBE. [consultado el 18 de septiembre del 2023] . Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[2] Computer security art and science 2nd edition [Libro]. Bogotá [consultado el 18 de septiembre del 2023] . Disponible en: https://ptgmedia.pearsoncmg.com/images/9780321712332/samplepages/9780321712332_Sample.pdf

**Ciberdelincuente:** Se denomina a las personas que buscan algún beneficio ingresando de manera ilegal a plataformas o sitios web aprovechando de las fallas de seguridad.

**DTLS:** Protocolo de seguridad de capa transporté de diagrama proporciona capacidad brinda proporcionar privacidad a las comunicaciones UDP.

**FLOSS:** Hace referencia a las herramientas que están bajo la licencia de *software* libre y/o código abierto.

***Hardware*:** Es el conjunto de componentes físicos que se encuentra en los dispositivos tecnológicos, es decir, son la parte tangible, por ejemplo: baterías, teclado, audífonos, pantalla, torre.[3]

**Encriptación:** Es una forma de cifrar los datos por medio de algoritmos que esconden la información de forma no entendible y para acceder a este se necesita usar un sistema de claves.[4]

**Incidente de seguridad:** Hace referencia a cualquier tipo de suceso que interfiera sobre los activos de información en una organización.

**Ingeniería Social:** Es un tipo ataque en el cual se utilizan diferentes técnicas psicológicas para conseguir que los usuarios brindan información confidencial de una organización e inclusive cuentas bancarias para después beneficiarse.[5]

---

[3] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia [Sitio web]. Bogotá: Mintic. [consultado el 18 de septiembre del 2023] . Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

[4] Centro Criptológico Nacional [Sitio web]. Bogotá: CCN-CERT. [consultado el 18 de septiembre del 2023] . Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=1965.html

[5] idric. [Sitio web]. Bogotá: idric.com.mx. [consultado el 24 de septiembre del 2023] . Disponible en: https://www.idric.com.mx/blog/post/glosario-de-seguridad-informatica

**OWASP:** Proyecto sin ánimo de lucro a nivel mundial que tiene la finalidad de mejorar la seguridad del software y todo lo relacionado directo e indirecto al mismo.

**Políticas de seguridad:** Una política en seguridad es la definición de lo que está y no está permitido realizar dentro de un sistema de información.[6]

**Protocolo:** Son un conjunto de reglas y estándares conformados por ciertas restricciones y definidos para el intercambio de paquetes de información con la finalidad de permitir una comunicación entre 2 o más servicios o dispositivos en una red.

**SOAP:** El protocolo de acceso a objetos simples funciona para aplicaciones basadas en XML y para implementar servicios web dentro de arquitectura orientada a servicios.

***Software:*** Se trata de aquellos elementos intangibles que conforman un dispositivo tecnológico y, a su vez, son fundamentales para el funcionamiento. En el caso de un computador, este se compone de un sistema operativo y programas.

**XML:** Es un lenguaje estructurado basado en etiquetas que permite definir y comprender en una máquina sobre el contenido del documento.

**Vulnerabilidad:** Es una debilidad que se presenta en un activo o en un control y que puede ser explotada.

**Zombis:** Se define a los ordenadores que se encuentran controlados de manera remota por un ciberdelincuente usando software malicioso y son utilizados para realizar actividades ilícitas a través de una red.

---

[6] Computer security art and science 2nd edition [Libro]. Bogotá [consultado el 18 de septiembre del 2023] . Disponible en: https://ptgmedia.pearsoncmg.com/images/9780321712332/samplepages/9780321712332_Sample.pdf

## RESUMEN

La tecnología IoT, conocida como Internet de las cosas, se refiere a aquellos dispositivos físicos que se encuentran conectados en la red de redes que posibilitan la recolección y transmisión de información automáticamente. No obstante, es una tecnología en desarrollo que presenta diversos problemas de seguridad en sus protocolos y transmisión de información, y actualmente no cuentan con normas globales sobre las obligaciones para los proveedores que deben cumplir para vender productos o servicios en un país.

La tecnología actual se encuentra en un auge debido a su capacidad para generar un amplio volumen de datos que pueden ser almacenados y explorados por cualquier dispositivo que se encuentre en la red. Este ecosistema permite a una compañía estar al tanto de todos los eventos que se encuentren en una red local y ser consultados en tiempo real. Por consiguiente, cada vez más entidades están empleando estos dispositivos y monitoreando su infraestructura con el fin de optimizar sus procesos industriales y empresariales.

En los últimos años, las compañías han ampliado su gama de tecnología IoT, a través de la utilización de códigos de barras, la identificación de radiofrecuencias, el sistema de posicionamiento global y sensores, en algunos sectores empresariales que requieren el seguimiento y comunicación de dispositivos físicos, lo que ha ocasionado una reducción significativa de los problemas en su infraestructura.

Esta tecnología se ha convertido en un protagonista debido a su simplicidad de conexión, no requiere cables, es completamente inalámbrica. Han sido adoptados para diferentes sectores que han permitido automatizar, mejorar de manera eficiente varias tareas y/o necesidades que se encuentren en la vida cotidiana.

Los dispositivos de IoT se convertirían en una parte integral de la ciudad inteligente y, actualmente, muchas empresas de telecomunicaciones se encuentran enfocadas en ofrecer aplicaciones para diferentes sectores públicos y privados.

## *ABSTRACT*

*IoT technology, known as the Internet of Things, refers to those physical devices that are connected in the network of networks that enable the collection and transmission of information automatically. However, it is a developing technology that presents various security problems in its protocols and information transmission, and currently do not have global rules on the obligations for suppliers who must comply to sell products or services in a country.*

*Today's technology is booming due to its ability to generate a large volume of data that can be stored and explored by any device on the network. This ecosystem allows a company to be aware of all events in a local network and be consulted in real time. Consequently, more and more entities are using these devices and monitoring their infrastructure to optimize their industrial and business processes.*

*In recent years, companies have expanded their range of IoT technology, using barcodes, radio frequency identification, global positioning system and sensors, in some business sectors that require the tracking and communication of physical devices, which has led to a significant reduction of problems in their infrastructure.*

*This technology has become a protagonist due to its simplicity of connection, requires no cables, is completely wireless. They have been adopted for different sectors that have allowed to automate, efficiently improve various tasks and/or needs that are in daily life.*

*IoT devices would become an integral part of the smart city and many telecom companies are currently focused on delivering applications for different public and private sectors.*

# 1. INTRODUCCIÓN

El Internet de las Cosas (IoT) hace referencia a todo el conjunto de dispositivos, sensores, aparatos electrónicos que cuentan con la capacidad de proporcionar y recibir información que será transmitida e interpretada y utilizada para los diferentes servicios y usuarios finales. Sin embargo, ese tipo de tecnología ha planteado varios desafíos que permita garantizar la adopción segura y eficiente.

Estos dispositivos actualmente se encuentran en riesgo debido a que la gran mayoría no dispone de la capacidad de procesamiento y almacenamiento suficiente para realizar la instalación de un sistema de seguridad o implementar alguna medida que permita asegurarlos.

Debido a que todos los sensores que recolectan la información y la almacenan mediante un canal sin cifrar, pueden ser detectados por los ciberdelincuentes para identificar la forma en que se almacenan los datos y la intercepten con el fin de recuperarla.

En lo que respecta a la privacidad, los dispositivos IoT almacenan una gran cantidad de información que son compartidos o vendidos para terceros. Esta situación se encuentra en las condiciones de servicio, donde la mayoría de los usuarios carecen de atención adecuada y, en ocasiones, no se logra identificar clara esta información. Además, existen regulaciones para los consumidores que obligan a que los fabricantes cumplan con ciertas normas para comercializar sus productos.

Actualmente, existen organizaciones privadas y sin ánimo de lucro que brindan herramientas, metodologías para evaluar la seguridad que se encuentre implementada en un dispositivo IoT, permitiendo así que posteriormente realizar una evaluación que permite asegurarlo.

# 2. DESCRIPCIÓN DEL PROBLEMA

## 2.1. ANTECEDENTES DEL PROBLEMA

Durante los últimos años, se ha incrementado la adquisición de los dispositivos IoT, uno de los motivos radica en su asequible precio, además de la posibilidad de llevar a cabo tareas diarias de manera automatizada, lo que ha evidenciado un gran empleo en hogares. Según un experto que participó en el evento SaferNet Day 2023 existen actualmente 7000 millones de estos a nivel mundial y que se prevé para el 2025 alcanzarían a 22.000 millones de productos conectados.[7]

En Colombia se encuentra actualmente en diferentes cambios de economía política, tecnología, el gobierno colombiano tiene como objetivo alcanzar un 85% de la conectividad en todo el país, lo cual ha permitido la apropiación del internet de las cosas IoT y la inteligencia artificial en las actividades de monitoreo, control y análisis de dispositivos remotos.[8]

Estos dispositivos cuentan con la capacidad que permite la interconectividad entre los sistemas microelectrónicos de manera inalámbrica y conexión a internet para ser monitoreados y operados remotamente. Generando nuevos desafíos ante la denominada cuarta revolución industrial.

A causa de la gran cantidad de información y sus respectivos usuarios que están en peligro de ser interceptados por cibercriminales, la tecnología IoT se encuentra en su fase de desarrollo. Uno de los principales motivos radica en la falta de atención de los fabricantes para considerar el aspecto de la seguridad presente en sus productos, lo que desde su creación son inseguros.

---

[7] hdplnews.com [Sitio web]. Bogotá: dplnews. [consultado el 18 de septiembre del 2023] . Disponible en: https://dplnews.com/numero-de-dispositivos-iot-conectados-alcanzara-22-mil-millones-para-2025/

[8] avilatinoamerica. [Sitio web]. Bogotá: avilatinoamerica.com [consultado el 23 de octubre del 2023] . Disponible en: https://www.avilatinoamerica.com/2023042122931/noticias/empresas/colombia-esta-a-la-vanguardia-del-iot-en-america-latina.html

## 2.2. FORMULACIÓN DEL PROBLEMA

Los dispositivos IoT, a pesar de ser una tecnología reciente, se han diseñado por un hardware esencial y software embebido que se ejecuta en los servicios que ofrecen en los puertos TCP y UDP. Actualmente, existen aproximadamente 13 protocolos compatibles con determinadas funciones, una de ellas es la de recolección de información a través de sensores que realizan la recepción y envió de datos, entre otros utilizando internet. [9]

Los datos son transmitidos sin ningún mecanismo de seguridad, y los paneles de administración se encuentran empleando HTTP (Hypertext Transfer Protocol) que puede ser capaz de capturar credenciales, mediante un analizador de protocolos que captura toda la información transmitida.

Dado que estos dispositivos son tan económicos, fueron diseñados por diferentes fabricantes que han creado sus protocolos y aplicaciones sin ningún tipo de normativa, por lo cual es difícil identificar qué servicios y puertos están asociados, lo que ocasionó la distribución de mirai una botnet que fue creada con el objetivo de distribuir software malicioso en routers, grabadoras digitales y cámaras. La propagación del contenido se llevó a cabo mediante la utilización de credenciales de defecto.[10]

La incógnita qué se presenta en la presente monografía es:

El internet de las cosas brinda muchos beneficios para las compañías y ciudades, sin embargo, ¿Qué normatividad y leyes a nivel de ciberseguridad se encuentren actualmente para los dispositivos IoT?

---

[9] ucol.mx. [Sitio web]. Bogotá: ucol.mx. [consultado el 09 de noviembre del 2023] . http://ww.ucol.mx/content/publicacionesenlinea/adjuntos/Internet-de-las-cosas-DIG_533.pdf

[10] Instituto Nacional de Ciberseguridad. [Sitio web]. Bogotá: INCIBE. [consultado el 19 de septiembre del 2023] . Disponible en: https://www.incibe.es/ciudadania/servicio-antibotnet/info/mirai

# 3. JUSTIFICACIÓN

El uso de dispositivos IoT en la actualidad han mejorado la calidad de vida, automatizando procesos, monitoreando servicios en tiempo real, dicha tecnología se encuentra aplicada en todas las ramas, utilizando aplicaciones que permiten realizar el salto hacia la transformación digital, permitiendo responder a los desafíos e innovación tecnológica.

En consecuencia, resulta crucial tener en cuenta el aspecto de seguridad, en el cual las investigaciones llevadas a cabo han constatado que se ha convertido en el objetivo novedoso para los ciberdelincuentes. La nueva era permite la hiperconexión con todos los dispositivos que se interconectan hacia internet y generan datos.

El propósito de esta monografía consiste en identificar las diversas metodologías y regulaciones que se encuentran en curso, con el fin de evaluar y asegurar los dispositivos IoT, así como también adquirir una perspectiva global acerca del uso de estos dispositivos.

Por último, identificar qué políticas o normativas se encuentran en Colombia sobre el uso de estos dispositivos y la regulación acerca de los proveedores que brindan sus productos. Además de concientizar que esta tecnología está presente y requiere atención debido a que en los siguientes años hará parte de cualquier red organizativa, por lo tanto, una organización debe contar con personal capacitado para administrarlos y auditarlos.

# OBJETIVO

## 4.1. OBJETIVO GENERAL

Evaluar las amenazas de seguridad en dispositivos IoT del sector industrial en Colombia mediante revisión bibliográfica que permita recomendar posibles medidas de mitigación a vectores de ataque.

## 4.2. OBJETIVO ESPECÍFICOS

- Examinar los principales ataques actuales en dispositivos IoT a partir de la información pública en los boletines de organismos especializados en seguridad para el reconocimiento de amenazas**.**

- Identificar las diferentes organizaciones que han creado metodologías y/o guías de buenas prácticas referentes a la auditoría de seguridad sobre los dispositivos y tecnologías IoT.

- Proponer acciones de mejora a la seguridad en arquitecturas IoT en sectores industriales en Colombia a partir de estándares que permita reducir el riesgo.

- Inspeccionar las iniciativas para la gestión de seguridad en arquitecturas IoT a partir de legislaciones existentes para sugerir a las organizaciones colombianas.

# MARCO TEÓRICO

El ámbito de la digitalización de dispositivos electrónicos y objetos comunes se enfoca en la digitalización de diversos dispositivos electrónicos y objetos comunes, tales como vehículos, seguridad física, cámaras IP, luces y sensores, implantes médicos, ropa, hogares, electrodomésticos (lavadoras, neveras y aspiradoras), electrodomésticos, domótica.

La transformación digital es una realidad, y el uso de la tecnología digital de las cosas ha dado lugar a una innovación y adaptación tanto para entidades como para empresas. Según la empresa, se estima que 27.000 millones de dispositivos conectados, hiperconectados con tecnología 5G e inteligencia artificial, y soluciones en la nube, otorgando una mayor eficiencia en los negocios, servicios 100% disponibles.

## 4.3. CONCEPTO DE IOT

Se define como una red de objetos físicos que incluyen sensores, software y tecnología que permiten la interacción con otros dispositivos y sistemas a través de la red. Los últimos años, se han convertido en un gadget doméstico y para uso de herramientas industriales modernas. En la actualidad, según los expertos, se estima que en el año 2025 se estimarían aproximadamente 22,000 millones de dólares.[11]

En la actualidad, esta tecnología se ha convertido en uno de los más relevantes del siglo XXI, que permite conectar objetos cotidianos, electrodomésticos e industriales hacia internet, lo que permite una comunicación fluida entre personas, procesos y dispositivos. [12]

[11] Oracle. [Sitio web]. Bogotá: aws.amazon.com. [consultado el 19 de septiembre del 2023] . Disponible en: https://www.oracle.com/co/internet-of-things/what-is-iot/

[12] incibe. [Sitio web]. Bogotá: incibe.es. [consultado el 05 de octubre del 2023] . Disponible en: https://www.incibe.es/empresas/blog/tematicas-internet-things-luces-y-sombras-las-cosas-conectadas

La informática de bajo costo que se utiliza en la nube, Big Data, analítica y tecnología móvil permite compartir y recopilar todos los datos con muy poca intervención humana.[13]

Todo se sugiere que el mundo interconectado sea un entorno interconectado en el que los sistemas digitales poseen la habilidad de grabar, supervisar y ajustar mediante la interacción entre los dispositivos interconectados.

En lo que respecta a la ciberseguridad, los dispositivos IoT han convertido en un vínculo entre el mundo físico y digital, lo que implica la posibilidad de generar daños que amenacen a la vida humana. En la actualidad, existe una complejidad de estos sistemas debido a que son elaborados por diversos agentes y cada uno de ellos ha implementado diferentes estándares.

El mayor ataque DDoS de la historia fue ejecutado en septiembre de 2016 mediante la botnet mirai, la cual estaba formada por miles de millones de dispositivos tecnológicos, entre ellos conformados por IoT a nivel mundial. Se coordinaron diversos ciberdelincuentes que utilizaron un sistema de vigilancia, electrodomésticos inteligentes, routers y granjas de servidores que los piratas informáticos que alquilaban para cualquier persona u organización mediante un pago en el que brindaban servicios como spam, denegación de servicio y fuerza bruta.[14]

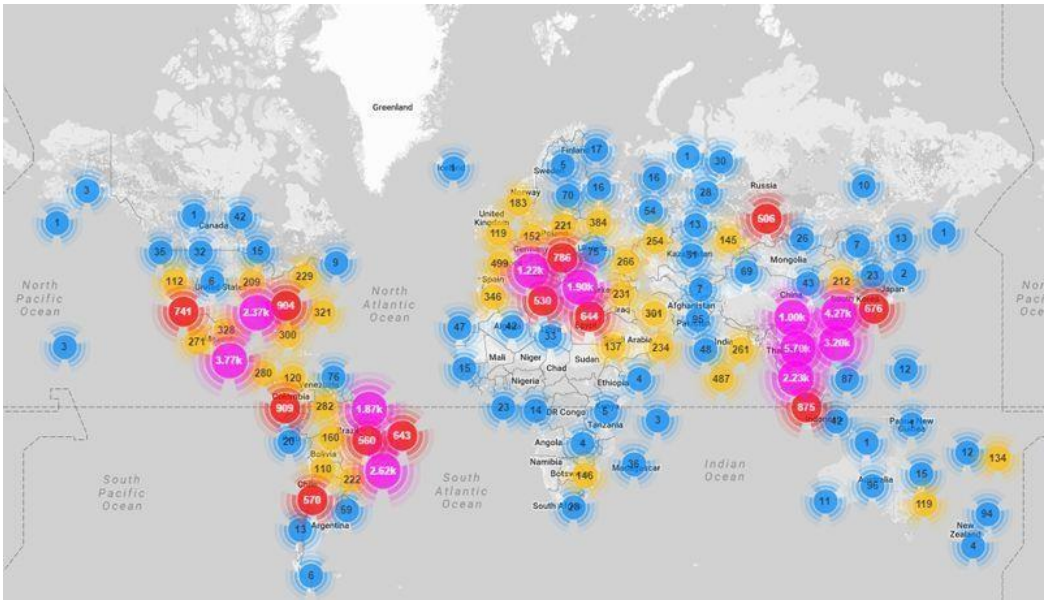
En la Ilustración 1 se puede observar de forma gráfica cómo el Botnet mirai se expandió mediante la utilización de dispositivos IoT, lo que lo convirtió en el ataque de ataques DDoS más vasto de la historia.

---

[13] redhat.com. [Sitio web]. Bogotá: redhat.com. [consultado el 09 de noviembre del 2023] . https://www.redhat.com/es/topics/internet-of-things/what-is-iot

[14] Kaspersky. [Sitio web]. Bogotá: latam.kaspersky.com. [consultado el 19 de septiembre del 2023] . Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security

**Ilustración 1. Mapa de dispositivos usados en la Botnet Mirai**




Fuente: blogs. protegerse, blogs.protegerse.com. mirai botnet ataques DDoS desde el internet de las cosas. [En línea]. 2021. [Consultado el 23 de septiembre de 2023]. Disponible en internet: https://blogs.protegerse.com/2016/10/17/mirai-botnet-ataques-ddos-desde-el-internet-de-las-cosas/

Los expertos en investigación descubrieron que los piratas informáticos crearon esta *botnet* a través de un procedimiento automático que detectó que los dispositivos IoT utilizaban credenciales defectuosas, ingresaron y tomaron el control de los dispositivos IoT, reclutando y reclutando a medida que se intercomunicaban entre sí.

La denegación de servicio sobre la empresa Dyn, que es la encargada de Proveer y gestionar la resolución de nombres, provocó una interrupción temporal de servicios y sitios web, como: Twitter, Netflix, Spotify, PlayStation, entre otros. Afortunadamente, este ataque fue minimizado debido a la implementación de planes de contingencia que posibilitaron la resolución rápida del inconveniente.[15]

[15] cloudflare.com [Sitio web]. Bogotá: cloudflare.com. [consultado el 19 de septiembre del 2023] . Disponible en: https://www.cloudflare.com/es-es/learning/ddos/glossary/mirai-botnet/

Debido a la gran magnitud y a tantos dispositivos comprometidos, un equipo de inteligencia de amenazas ha identificado que actualmente existen 7 nuevas variantes de Mirai. Se investigó utilizando ciber inteligencia y el creador de esta botnet rentaba servicios para otros cibercriminales, permitiendo la modificación del código fuente original y distribuirlo.[16]

El creador 'Anna-Senpai' lanzó el código fuente de Mirai convirtiéndose en el marco de referencia y una plantilla para cualquier cibercriminal, esto permitió que en el 2018 aparecieran más variantes y cuentan con las siguientes características:

**Combinación de credenciales:** Los usuarios y contraseñas originales se encontraban por defecto en un diccionario, pero en las variantes se determinó qué se trataba a través de un *Bot*, el cual se encargaba de realizar un ataque de fuerza bruta mediante una lista de credenciales aún más amplia.

**Arquitecturas:** Fue posible determinar que las variantes de Mirai fueron desarrollados sobre la misma, Sin embargo, esto no significa que funcionen de igual manera varios malware pueden muy perjudiciales y se desconocen puertas traseras para comunicarse con más dispositivos para recopilar información.

Los investigadores recalcan que es importante realizar regularmente el cambio de contraseña por defecto, aplicar todas las actualizaciones qué el proveedor suministre o lo indique.

Cómo buena práctica se sugiere deshabilitar la administración remota, Si observa un comportamiento inadecuado o que su dispositivo se encuentra infectado se recomienda restablecerlo. Pero en algunos casos otros actores maliciosos se basaron en este tipo de software malicioso creando:

**Mēris**: El malware presentado en el año 2021 ha impactado en una multitud de dispositivos, siendo la mayoría de los dispositivos conectados a una red para

[16] avast [Sitio web]. Bogotá: avast.com. [consultado el 19 de septiembre del 2023] . Disponible en: https://www.avast.com/es-es/c-mirai.

generar ataques de DDoS. En que se alcanzó a 21,8 millones de solicitudes por segundo y atacó a varias empresas financieras y tecnológicas rusas.[17]

**OMG:** Este malware posee ciertos atributos de mirai, no obstante, el autor amplió el código, incluyendo un servidor Proxy que habilitó protocolos HTTP en el dispositivo infectado.

En la ilustración 2 se pueden observar los múltiples intentos de ciberataques que se presentan en el año 2021. Brasil experimentó 289.000 millones de amenazas cibernéticas, mientras que México lideró el número de ataques informáticos con 85.000 millones. En el segundo lugar se ubicaron Brasil con 289.000 millones, mientras que Colombia con 11.300 millones. [18]

**Ilustración 2. Ataques registrados en América latina año 2021**


**Fuente:** esemanal, esemanal.mx. Fortinet registró 85 mil millones de intentos de ciberataques en México, es el país más atacado de la región. [En línea]. 2022. [Consultado el 20 de https://esemanal.mx/2022/08/fortinet-registro-85-mil-millones-de-intentos-de-ciberataques-en-mexico-es-el-pais-mas-atacado-de-la-region/

[17] Kaspersky [Sitio web]. Bogotá: kaspersky.es. [consultado el 20 de septiembre del 2023] . Disponible en: https://www.kaspersky.es/blog/router-malware/27267/

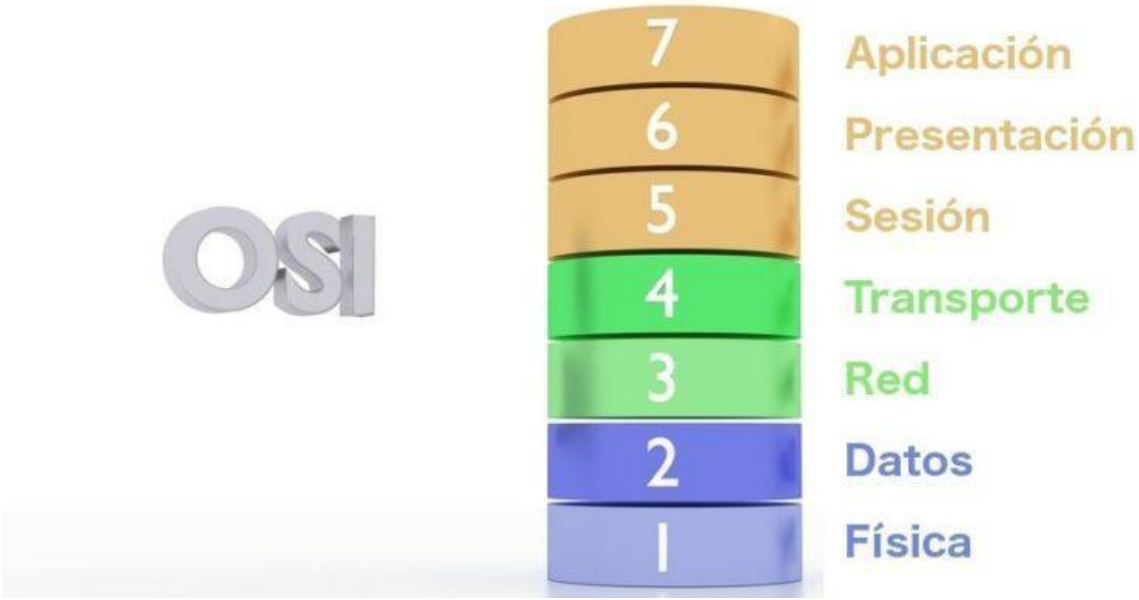
[18] esemanal. [Sitio web]. Bogotá: esemanal.mx. [consultado el 20 de septiembre del 2023] . Disponible en: https://esemanal.mx/2022/08/fortinet-registro-85-mil-millones-de-intentos-de-ciberataques-en-mexico-es-el-pais-mas-atacado-de-la-region/

## 4.4. MODELO OSI

La organización internacional de normas (ISO) fue concebida con el propósito de establecer un estándar de protocolos a nivel internacional mediante capas en 1995, denominado *Open System Interconnection* OSI (Sistema abierto de interconexión), también conocido como interconexión de sistemas abiertos. Este proyecto fue concebido con el propósito principal de establecer una conexión entre diversos sistemas de comunicaciones.[19]

Se encuentra dividido en 7 capas que dependen una de otra y cumple una función específica como se puede observar en la Ilustración 3:

**Ilustración 3 . Modelo OSI**




**Fuente**: concepto, concepto.de. Modelo OSI. [En línea]. 2020. [Consultado el 20 de septiembre de 2023]. Disponible en internet: https://concepto.de/modelo-osi/

[19] Concepto.de [Sitio web]. Bogotá: concepto.de. [consultado el 20 de septiembre del 2023] . Disponible en: https://concepto.de/modelo-osi/

### 4.4.1. MODELO TCP/IP

El modelo TCP/IP, que se refiere al conjunto de protocolos y normas para los formatos de mensaje que permiten la comunicación entre las máquinas y los diferentes sistemas para transmitir un mensaje, está conformado por cuatro capas, las cuales se describen en la ilustración 4:

**Ilustración 4. Modelo TCP / IP**


**Fuente**: elprofealegria, elprofealegria.com. Modelo TCP/IP [En línea]. 2020. [Consultado el 20 de septiembre de 2023]. Disponible en internet: https://elprofealegria.com/redes/modelo-tcp-ip/

### 5.2.2. ARQUITECTURA IOT

La recolección de datos mediante dispositivos interconectados ha propiciado el desarrollo de tecnologías innovadoras aplicadas a diversos sectores y que en la actualidad forman parte de la vida cotidiana. La arquitectura IoT es la responsable de la creación y la integración de sistemas, donde se procesa la información que se desplaza hacia la red o nube. Se ejecutan instrucciones que posibilitan la activación de características o una acción concreta.

En el contexto de la industria 4.0, esta arquitectura puede ofrecer soluciones a la recepción de datos que cualquier entidad necesita. La tecnología ha contribuido en la optimización de los procesos de producción, la disminución de costos y el tiempo, y una mayor capacidad de respuesta a las exigencias actuales.

La arquitectura requiere de un proceso integrado fundamental dividido en fases o etapas:

#### 5.2.2.1. CAPA FÍSICA

La mayoría de los dispositivos sensores y controladores están conformados por el entorno IoT, todo equipo inteligente que se conecte de manera cableada o inalámbrica forma parte del internet de las cosas.

#### 5.2.2.2. CAPA INFORMÁTICA

Se compone de la tarea de almacenamiento y procesamiento de los datos sobre los dispositivos, además de la aplicación de protocolos de comunicación utilizados para la conectividad.

### 4.4.2. CAPA DE APLICACIÓN

Se hace referencia al conjunto de servicios y protocolos que se encuentran integrados y son proporcionados por el fabricante mediante la nube del internet de las cosas, en la que se recopila información necesaria para su funcionamiento, además de brindar soporte y actualización en el *firmware*.[20]

### 4.4.3. PROTOCOLOS DE COMUNICACIÓN IOT

Los dispositivos IoT comparten la misma arquitectura a partir del kernel de Linux o *Windows* embebidos, que utilizan un servicio de bajo nivel y su comunicación es sumamente distinta.[21]

El protocolo TCP/IP es uno de los más utilizados para la transmisión, navegación, descarga y subida de archivos, así como la comunicación entre los dispositivos

[20] guinea.pe. [Sitio web]. Bogotá: guinea.pe. [consultado el 09 de noviembre del 2023] . https://guinea.pe/blog/arquitectura-iot/

[21] incibe [Sitio web]. Bogotá: incibe.es. [consultado el 20 de septiembre del 2023] . Disponible en: https://www.incibe.es/incibe-cert/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones

mediante paquetes bajo un esquema de direccionamiento. La tecnología IoT, gracias a su arquitectura, puede transmitir de manera inalámbrica mediante la utilización de dispositivos como wifi, Bluetooth, red 3G, 4G y actualmente la 5G.

La tecnología IoT se originó a partir de la industria 4.0, en la cual se puede definir como una parte de la implementación e integración de diversas tecnologías que procesan datos e información mediante un software inteligente. Estos dispositivos poseen sensores que permiten la comunicación entre sí y el exterior mediante cualquiera de los protocolos establecidos.

#### 5.2.3.1. AMQP

Se utiliza en el sector financiero para la comunicación punto a punto, tipo, publicación y suscripción. Este modelo se encuentra presente en el ámbito de la tecnología de la Información, siendo capaz de preservar las transacciones, asegurando la seguridad en la comunicación.

#### 5.2.3.2. *BLUETOOTH*

Se trata de un tipo de tecnología concebida para el uso de tecnologías de corto alcance que se encuentran en la plataforma 2,4 GHz. Se presentan dos tipos de comunicación tradicionales que se emplean para transmitir audio inalámbricamente, y energía baja orientada para dispositivos que requieren menos información, y se emplean en el rastreo de salud y aparatos domésticos inteligentes.

#### 5.2.3.3. CoAP

Este protocolo fue concebido por IETF, el cual posibilita la aplicación de un método de compatibilidad en HTTP (Protocolo de transferencia de hipertexto), aplicable tanto al cliente como al servidor. Al usar UDP (protocolo de comunicación de la capa de transporte) usando multicast para ser reemplazado por HTTP y simplificar su encabezado, se reduce el tamaño de cada solicitud. Como medida de seguridad, DTLS (Protocolo de Seguridad de Capa de Transporte) funciona en la capa de transporte y protege las comunicaciones.[22]

[22] uniandes [Sitio web]. Bogotá: uniandes.edu.co. [consultado el 20 de septiembre del 2023] . Disponible en: https://repositorio.uniandes.edu.co/bitstream/handle/1992/53720/24727.pdf?sequence=1

#### 5.2.3.4 DDS

Este tipo de protocolo funciona de manera similar a un publicador/suscriptor en tiempo-real mediante un estándar abierto, lo que posibilita la comunicación desde un punto a otro mediante multicast. Esta solución requiere intercambiar información, controlar el tráfico aéreo y vehicular, gestionar redes inteligentes, vehículos con autonomía, robótica, transporte y electricidad.[23]

#### 5.2.3.5 HTTP

Se trata de un protocolo que se utiliza para servicios web que funciona como cliente/servidor y que se utiliza para diferentes tecnologías de código abierto. Su principal característica es el envío de una gran cantidad de datos, una de ellas es la lectura de sensores en tiempo real, generando estadística obtenida. Viaja sin ningún tipo de cifrado, por lo cual es recomendable utilizar un protocolo criptográfico SSL/TLS en HTTP.[24]

#### 5.2.3.6 LPWAN

Se trata de un protocolo de transporte inalámbrico denominado redes de áreas amplias y de baja potencia, en el cual la información viaja a través de pequeños paquetes de datos y un consumo bajo. Se emplea en proyectos de IoT, a través de sensores que se encuentran diseñados para conectar a usuarios y organizaciones.[25]

#### 5.2.3.7 LoRaWAN

La tecnología, que se conecta con cualquier tipo de tecnología inalámbrica de larga distancia, ofrece un costo reducido para transmitir información de manera segura y segura en las aplicaciones de IoT y M2M. La estructura de la radiofrecuencia fue concebida con el fin de estructurar las frecuencias radiofrecuencias.

---

[23] iotcolombia. [Sitio web]. Bogotá: iotcolombia.org. [consultado el 05 de octubre del 2023] . Disponible en: https://iotcolombia.org/protocolos/iot-protocolos-de-comunicacion/

[24] incibe [Sitio web]. Bogotá: incibe.es. [consultado el 20 de septiembre del 2023] . Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[25] pandorafms. [Sitio web]. Bogotá: pandorafms.com. [consultado el 05 de octubre del 2023] . Disponible en: https://pandorafms.com/blog/es/que-es-lpwan/

LoRa este protocolo es de uso abierto para ser utilizado en la nube, intercomunicarse con otros dispositivos.

#### 5.2.3.8 LWM2M

Un protocolo concebido para la gestión de redes y sensores en entornos M2M utilizados en telemetría, posibilitando la administración remota. Utilizando la aplicación M2M, fue creado como una opción para los dispositivos de bajo consumo con capacidad limitada tanto a nivel de procesamiento y almacenamiento.

#### 5.2.3.9 MIPv6

El protocolo de comunicación móvil de la versión 6 está basado en la tecnología IoT. Su utilidad es apoyar las conexiones móviles y está diseñado para autenticarse sobre esta tecnología IoT**.**

#### 5.2.3.10 MQTT

El protocolo MQTT-SN es un protocolo que permite conectar a una máquina de manera inalámbrica, utilizando la función de publicador/suscriptor que funciona sobre la capa de aplicación. Este protocolo está implementado en dispositivos IoT, OT, la generación de electricidad en fuentes renovables. Toda esta información es enviada en texto claro sin ninguna medida de seguridad.

#### 5.2.3.11 NFC

Es un campo de comunicación cercano, se utiliza tecnología de alta frecuencia. La radiofrecuencia de alta frecuencia se emplea en una distancia de 10 a 15 cm del dispositivo para comunicarse.

#### 5.2.3.12 RFID

La identificación por radiofrecuencia es un protocolo de IoT que se emplea de manera inalámbrica y en campos electromagnéticos. Este protocolo permite la identificación de objetos y las etiquetas de lectura, almacenando información y no requiere energía. Estos dispositivos son frecuentemente empleados en tiendas peajes y autopistas que permiten acceso a edificios.

#### 5.2.3.13 SigFox

Es una red de conectividad móvil enfocada en internet de las cosas, diseñada para la comunicación, la velocidad que reduce costos y el consumo de energía. Se utiliza a una baja velocidad y la intercomunicación es muy pequeña, se implementa en el sector urbano debido a su corto espacio.

#### 5.2.3.14 STOMP

Se trata de un protocolo simplificado que se emplea para llevar a cabo la comunicación de los clientes acerca de cualquier mensaje *Bróker*. Se utiliza para las comunicaciones de tipo texto (XML, JSON, entre otros) de programas desarrollados para diferentes lenguajes.

#### 5.2.3.15 *THREAD*

Se trata de una radiofrecuencia inalámbrica de baja potencia utilizada para hogares inteligentes que permite hablar o comunicarse directamente entre sí, crea una red de malla estableciéndose como punto de acceso**.**

#### 5.2.3.16 WAMP

Se trata de un protocolo de mensajes para aplicaciones web, el cual está abierto y se puede ejecutar en el *socket* web.

#### 5.2.3.17 WIFI

Se trata de un protocolo de comunicación que se basa en el estándar 802.11, que se aplica tanto en redes locales como en áreas inalámbricas. En la actualidad, se encuentra en la versión 802.11 b/g/n/, la cual ha sido corregida por problemas en la frecuencia y ha posibilitado la transmisión de información adicional mediante su velocidad.

#### 5.2.3.18 WMQ

El protocolo de propiedad de IBM proporciona conectividad a los dispositivos y puede ser utilizado de manera autónoma para otros integrantes de la misma solución. Se brinda la posibilidad de establecer conexiones desde dispositivos de escritorio hasta microcomputadores, y se dispone de la habilidad de incorporar aproximadamente 35 plataformas distintas.

#### 5.2.3.19 *ZIGBEE*

Se trata de un protocolo de red malla concebido para la automatización de edificios y hogares. Este protocolo es uno de los más utilizados en entornos IoT de corto alcance y bajo consumo.

Se caracteriza por su capacidad para transmitir comunicación a diversos dispositivos, así como por su flexible capacidad de energía ultra bajá y biblioteca de aplicaciones.

#### 5.2.3.20 *Z-Wave*

Se trata de un protocolo de comunicación de red malla inalámbrica concebido para tecnologías de radiofrecuencia baja potencia, a la vez que se pueden comunicar los dispositivos inteligentes mediante un cifrado, lo que proporciona un nivel de seguridad al ser implementado.

La utilización de este instrumento en sistemas de seguridad tanto en residencias como en entidades agrícolas se encuentra aplicada en radiofrecuencias de 908,42 MHz en los Estados Unidos, no obstante, en cada nación se encuentra distinto.

## 4.5. MARCO CONCEPTUAL

### 4.5.1. APLICACIONES

Se trata de un programa informático que fue concebido para resolver o completar una tarea de manera más rápida.

### 4.5.2. AUTOMATIZACIÓN

Se trata de un sistema en el que se generan tareas automáticas que suelen ser llevadas a cabo por recursos humanos y un sistema tecnológico.

### 4.5.3. *Big DATA*

Se refiere al procedimiento que se utiliza para recopilar datos y el proceso de análisis de los mismos, identificar patrones que permitan identificar y realizar estadísticas basándose en la información obtenida previamente.

### 4.5.4. CHIP

Se trata de un dispositivo de hardware de gran tamaño que se compone de un material semiconductor, que se utiliza en ordenadores de índole reducida y dispositivos electrónicos.

### 4.5.5. CRYPTOMINING

Se trata de un método para insertar malware que está concebido para extraer monedas digitales por ciberdelincuentes, después de utilizar equipos como víctimas que son infectadas mediante un sitio web**.**

### 4.5.6. CÓDIGOS QR

El Código de respuesta rápida es un módulo que posibilita el almacenamiento de información en una matriz de puntos o código de barras, que realiza una lectura sobre un dispositivo móvil y, de manera inmediata, redirige a la red de internet. [26]

### 4.5.7. CONECTIVIDAD

Se hace referencia a los diversos tipos de redes y elementos que se encuentran involucrados para conectar un dispositivo hacia la red, lo cual posibilita la recopilación de datos, actualizaciones y soporte que se encuentran enviado a la nube.

### 4.5.8. DOMÓTICA

Se hace referencia a las residencias inteligentes que se vuelven cada vez más populares, lo que posibilita a los usuarios automatizar múltiples procedimientos diarios, tales como la iluminación, la calefacción y la gestión remota de los mismos.[27]

---

[26] Wikipedia [Sitio web]. Bogotá: wikipedia.org. [consultado el 20 de septiembre del 2023] . Disponible en: https://es.wikipedia.org/wiki/C%C3%B3digo_QR

[27] incibe [Sitio web]. Bogotá: incibe.es. [consultado el 20 de septiembre del 2023] . Disponible en:https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

### 4.5.9. DISPOSITIVOS INTELIGENTES

Se refiere a diversos tipos de dispositivos, tales como televisores, sensores y cámara de seguridad. La aplicación IoT alberga información acerca de su entorno, incluyendo dispositivos de entrada y salida, patrones de usuario, y toda esta información se transmite a través de la red y la aplicación de Internet de Tecnologías de la Información.

### 4.5.10. *FIRMWARE*

Se refiere a un sistema concebido con el propósito de establecer la interacción entre *hardware* y *software*.

### 4.5.11. INTERFAZ DE USUARIO

Es imperativo que un usuario intervenga para controlar el sistema. Es esencial diseñar una interfaz que facilite la interacción visual e intuitiva mediante un navegador web.

### 4.5.12. MICROCONTROLADOR

Se trata de un circuito integrado que contiene una unidad central de procesamiento, CPU, memoria RAM, puertos de entrada y salida. Estas partes están interconectadas dentro del mismo y este conjunto se denomina microcomputadora.

### 4.5.13. RADIOFRECUENCIA

Son los conjuntos de dónde hacen electromagnéticas por donde se propaga el sonido a través del espacio.

### 4.5.14. *RESTful*

Se trata de un conjunto de principios arquitectónicos que permiten la creación de servicios web. Aprovechando los recursos del sistema mediante la utilización de un navegador web, y empleando diversos lenguajes de programación.

### 4.5.15. SENSOR

Se trata de un dispositivo electrónico que detecta una condición física o componente y realiza la entrega; la señal electrónica proporciona la característica identificada.

### 4.5.16. SISTEMA DE CONTROL

Los datos obtenidos o capturados son gestionados y procesados con el fin de llevar a cabo las medidas y conexiones pertinentes.

### 4.5.17. SUPERFICIE DE ATAQUE IOT

Se refiere a la identificación de todas las probabilidades que potencialmente se encuentran en el dispositivo y cómo materializarlas o explotarlas.

### 4.5.18. TECNOLOGÍA EMBEBIDA

En la actualidad, y debido a la evolución, diversos dispositivos tecnológicos, tales como relojes, sensores, celulares, puertas de entrada y salida, memorias y microprocesadores, utilizan sistemas embebidos, cuyo 99% cuenta con un sistema operativo Linux, y se encuentran disponibles en el mercado a un precio bajo.

### 4.5.19. TELE MONITORIZACIÓN

Se hace referencia a la especialidad de telemedicina, donde se emplean dispositivos para proporcionar una asistencia domiciliaria a un paciente, a través de la presencia de un monitor y un profesional, a fin de llevar a cabo un seguimiento de estos parámetros en función de las pulsaciones, la presión, entre otros aspectos.

### 4.5.20. TELEMETRÍA DE DISPOSITIVO

Se refiere a los dispositivos que contienen información sobre el sensor, lo que posibilita la medición de la velocidad, temperatura, identificación, mensajes de error o eventos de información.

### 4.5.21. TICs

La tecnología de la información y la comunicación es una variedad de tecnologías desarrolladas para la gestión de información, siendo estas tecnologías específicas que se encuentran disponibles para la gestión de información, y que ofrecen soluciones amplias, incluyendo el almacén de información, la recuperación, la mejora de la sección de información de sitio a sitio, así como la capacidad de calcular resultados y la elaboración de informes.

## 4.6. MARCO LEGAL Y NORMATIVO

La constitución de la Ley 30 establece los planes de desarrollo nacionales, en los cuales se persigue un sistema de planificación novedoso en Colombia, que posibilita la asistencia y generación de una evolución e internacionalización en el ámbito de la formación educativa superior.

### 4.6.1. CONSTITUCIÓN NACIONAL DE COLOMBIA 1991

En el año 1991, se promulgó la constitución nacional de Colombia la promulgación de la legislación educativa que fomente el desarrollo de los derechos, principios y valores. La educación se convierte en un derecho fundamental y se considera como un servicio público de carácter esencial que se debe prestar por el estado o particulares, que cada persona posee y que los ciudadanos pueden tener acceso al conocimiento a la ciencia y la tecnología, como se indica en el artículo 67 de la carta magna. [28]

La constitución política de Colombia ha incluido el derecho a la privacidad sobre los ciudadanos y se refiere a la responsabilidad del estado para protegerla.

[28] corteconstitucional [Sitio web]. Bogotá: corteconstitucional.gov.co. [consultado el 20 de septiembre del 2023] . Disponible en: https://www.corteconstitucional.gov.co/relatoria/2013/t-743-13.htm

La apertura económica se promulgó en la constitución nacional de Colombia en 1991, lo cual establece, bajo una norma fundamental, la legislación educativa que fomenta el desarrollo de los derechos, principios y valores. La educación se convierte en un derecho fundamental y se considera como un servicio público de carácter esencial que se debe prestar por el estado o particulares, que cada persona posee y que los ciudadanos pueden tener acceso al conocimiento a la ciencia y la tecnología, como se indica en el artículo 67 de la carta magna.

Todas las personas tienen derecho a la intimidad personal y familiar. El estado tiene la responsabilidad de respetarlos y hacerlos respetar de la misma manera, y puede actualizar la información recopilada sobre ellas en el banco de datos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los mismos, se evidencia la libertad y las garantías consagradas en la constitución.

La ley estatutaria 1581 del año 2012 establece que había una garantía general de protección de información personal. En dicha ley se incluye la categoría de datos sensibles, incluyendo el acceso biométrico de las personas. A través del decreto 1377 del año 2013, se otorga el derecho de efectuar consultas, modificaciones o eliminaciones. [29]

La norma establece que las personas que aporten dicha información deben hacerlo de manera expresa para permitir que estos datos se hayan utilizado y la responsabilidad que lleva a ser utilizados sin previo aviso. [30]

En Colombia, las tecnologías de la información y las comunicaciones, conocidas como TIC, son un conjunto de recursos, herramientas, equipos, software informático, aplicaciones, redes y medios que posibilitan la compilación, procesamiento, almacenamiento y transmisión de información, tales como voz

[29] funcionpublica [Sitio web]. Bogotá: funcionpublica.gov.co. [consultado el 20 de septiembre del 2023] . Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[30] sic.gov. [Sitio web]. Bogotá: sic.gov.co [consultado el 23 de octubre del 2023] . Disponible en: https://www.sic.gov.co/preguntas-frecuentes-pdp

datos, textos y multimedia, y que se encuentran claramente especificadas en el artículo 6 de la Ley 1341 del 2009.[31]

El Ministerio de las tecnologías de la información y las comunicaciones ha llevado a cabo una reducción de la pobreza y, bajo la supervisión del gobierno colombiano, la importancia de la tecnología en el país para la modernización del sector y la conectividad ha buscado alianza con empresas para la innovación que generó la creación de un laboratorio de internet de las cosas denominado (IoT LAB). Se trata de un espacio y ecosistema para la solución de cualquier emprendedor, lo que explicó la ministra de las TIC acerca de esta iniciativa de compañías como Wayra y telefónica, los emprendedores que forman parte de CEmprende. [32]

El propósito de este espacio consiste en proporcionar a los diversos actores del ecosistema emprendimiento colombiano un sitio apropiado para desarrollar aplicaciones y herramientas basadas en la tecnología IoT, así como establecer una red exclusiva con telefónica Movistar, que se encargará de atender a las necesidades planteadas en el camino. Con el propósito de transformar la sociedad mediante la tecnología y cerrar la brecha existente en Colombia.

## PRINCIPALES ATAQUES SOBRE DISPOSITIVOS IOT.

La cantidad de dispositivos IoT, dispositivos de comunicación inteligente, dispositivos de comunicación IP, cámaras IP, sensores, enrutadores y componentes inteligentes para el hogar. En la actualidad, se encuentran en un

[31] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. [Sitio web]. Bogotá: mintic.gov.co. [consultado el 9 de abril de 2023]. Disponible en: https://mintic.gov.co/portal/inicio/Glosario/T/5755:Tecnologias-de-la-Informacion-y-las-Comunicaciones-TIC

[32] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. [Sitio web]. Bogotá: mintic.gov.co. [consultado el 9 de abril de 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/106960:Primer-Laboratorio-de-Internet-de-las-Cosas-IoT-LAB-para-emprendedores-abre-sus-puertas-en-Colombia

acelerado crecimiento y se espera que, según la investigación llevada a cabo por Kaspersky, alcanzar los 29.000 millones de dólares en el año 2030.[33]

Los expertos de Kaspersky han descubierto productos y servicios de la *Darknet* vinculados al hackeo de los dispositivos IoT, en particular la delegación de servicio distribuido (DDoS), que son gestionados a través de *botnets*, cuya demanda es significativa. Asimismo, se han detectado ciertos tipos de malware que son predominantes.

## 6.1. VECTORES DE ATAQUE

Según el estudio realizado por Securelist, existen dos formas principales de infectar los dispositivos IoT, una de ellas a través de la Fuerza bruta, que algunos de ellos son susceptibles debido a las contraseñas fáciles o por defecto, y la explotación de vulnerabilidades en los servicios de red.[34]

En la ilustración 5 se puede observar el rango de países que, durante el semestre de 2022, llevando a cabo intentos de Fuerza Bruta para obtener contraseñas registradas, emplearon honeypots (sistema trampa o señuelo) que se vinculan con el protocolo Telnet (Protocolo de red) y el 2.09% correspondiente al servicio de SSH (acceso remoto a un servidor modo consola). Los principales dispositivos infectados se encontraban en China, India y Estados Unidos, y su origen se encuentra en China, India y Estados Unidos.[35]

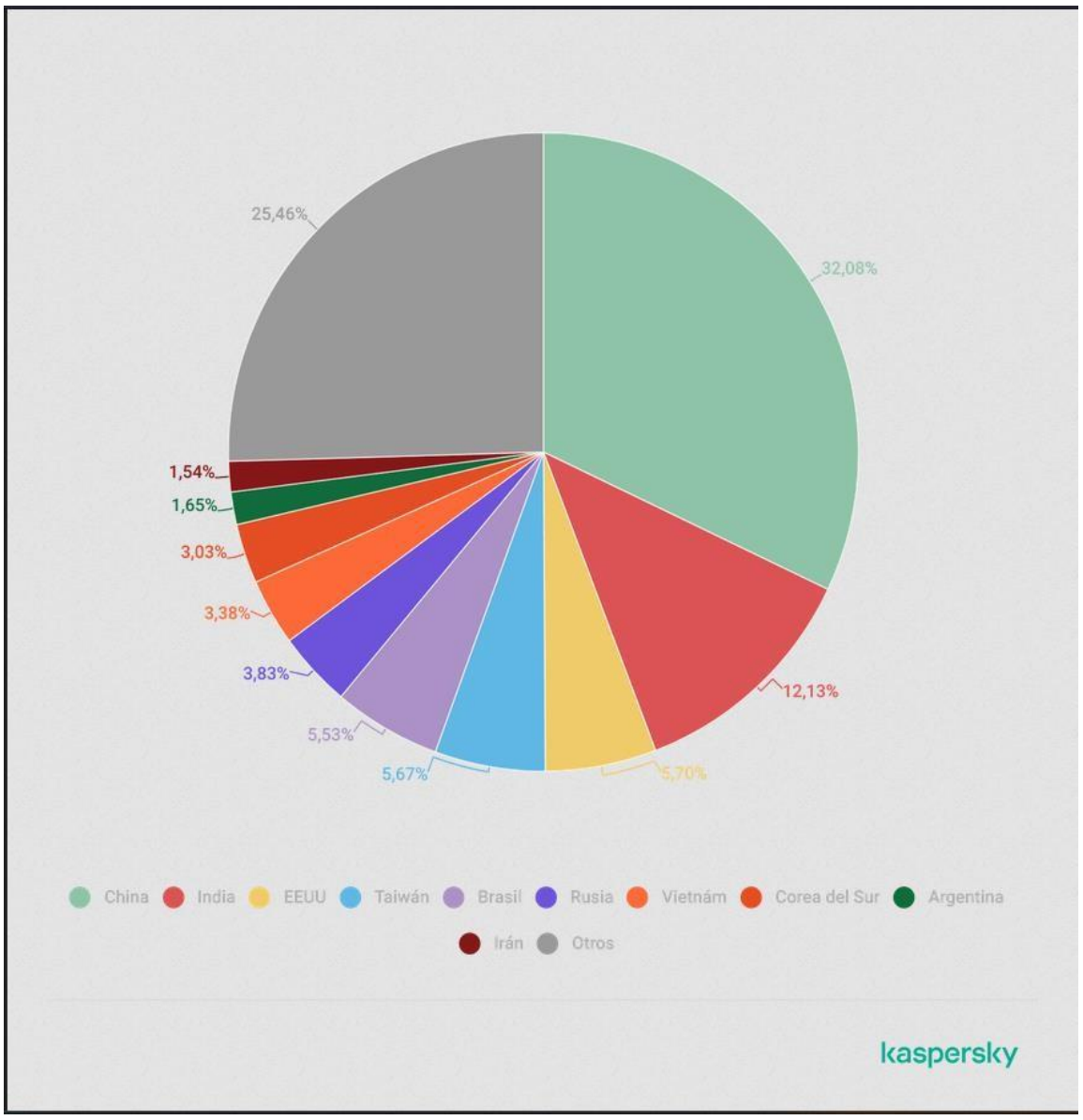
---

[33] revistaeconomia [Sitio web]. Bogotá: revistaeconomia.com. [consultado el 21 de septiembre del 2023] . Disponible en: https://www.revistaeconomia.com/kaspersky-publica-resumen-general-de-las-amenazas-relacionadas-con-iot-en-2023/

[34] securelist [Sitio web]. Bogotá: securelist.lat [consultado el 21 de septiembre del 2023] . Disponible en: https://securelist.lat/iot-threat-report-2023/98141/

[35] securelist [Sitio web]. Bogotá: securelist.lat [consultado el 21 de septiembre del 2023] . Disponible en: https://securelist.lat/iot-threat-report-2023/98141/

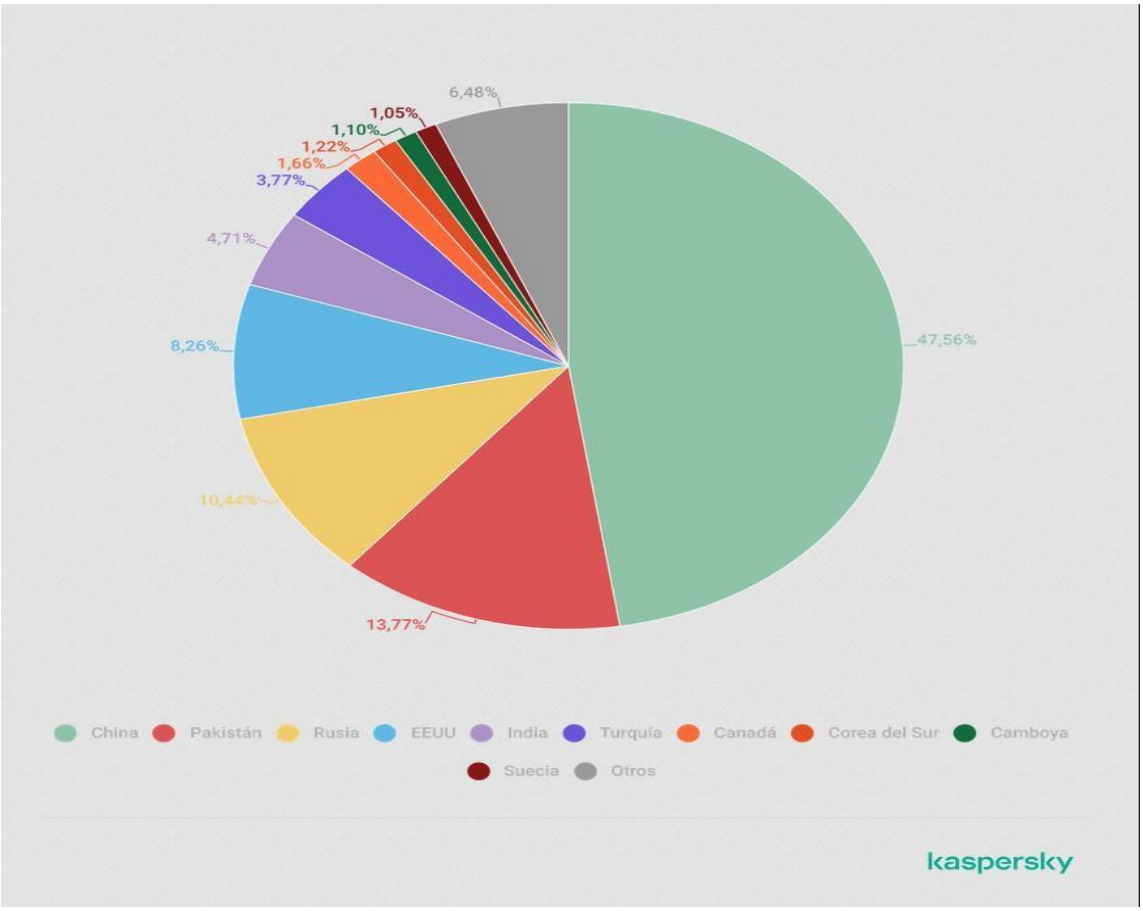
**Ilustración 5. TOP 10 de países atacados por honeypots de Kaspersky**




**Fuente:** securelist, securelist.lat. TOP 10 de países y territorios donde se encontraban los dispositivos que atacaron los honeypots de Kaspersky, primer semestre de 2023. [En línea]. 2023. [Consultado el 21 de septiembre de 2023]. Disponible en https://securelist.lat/iot-threat-report-2023/98141/.

En la ilustración 6 se puede observar el índice de países o territorios en los que los responsables de la aplicación de Honeypots implementados por Kaspersky durante el primer semestre del año 2023.

**Ilustración 6. TOP 10 países y territorios fuente de ataques a los honeypots de Kaspersky**




**Fuente:** securelist, securelist.lat. TOP 10 países y territorios fuente de ataques a los honeypots de Kaspersky, primer semestre de 2023. [Consultado el 21 de septiembre de 2023]. Disponible en https://securelist.lat/iot-threat-report-2023/98141/

En los servicios inseguros que se encuentran en un dispositivo IoT, pueden convertirse en una vulnerabilidad que se explota por ciberdelincuentes mediante la introducción de comandos maliciosos al realizar peticiones a la interfaz web, lo cual ocurrió con el malware. Se ha constatado que ciertos proveedores de internet configuraban estos aparatos en una red local, y los atacantes envían paquetes sin autenticación, lo que genera una infección en el botnet.

### 6.1.2 SERVICIOS OFRECIDOS EN LA *DARKNET*

En la plataforma de navegación de carácter oscuro, se hace referencia al conjunto de sitios web ocultos que pueden ser accesibles mediante software especializado. Se ofrecen servicios tales como ataques de denegación de servicio, redes de Bots

creadas en esta tecnología, que se han vuelto cada vez más populares y son anunciadas en diversos foros, siendo uno de los más solicitados por los atacantes.[36]

Los expertos en Kaspersky Digital Footprint Intelligence en el primer semestre del año 2023 han detectado aproximadamente 700 anuncios de servicios de ataque de delegación de servicio en diversos foros.[37]

El valor de cada servicio se encuentra en múltiples factores, y a medida que sea más sofisticado el ataque, su costo se incrementa con el fin de obtenerlo. Los ataques utilizados en concreto son ataques de tipo de exploits o vulnerabilidades de día cero que se encuentran en dispositivos IoT que hasta el momento no han sido solucionados por los proveedores.

El objetivo principal es continuar infectando dispositivos IoT y utilizarlos como herramientas de ciberataque, *bots*, proxy, cambios de DNS, enmascarar tráfico malicioso, minería de criptomonedas. Esta tecnología es susceptible a casos de Ransomware (Secuestro de información) y los ciberdelincuentes requieren un rescate para recuperar el acceso a los mismos.[38]

En la ilustración 7 se puede observar que, durante el primer semestre del año 2023, los expertos en Kaspersky Digital Footprint han recibido más de 700 anuncios de servicios de denegación en diversos foros de la plataforma de la Darknet.

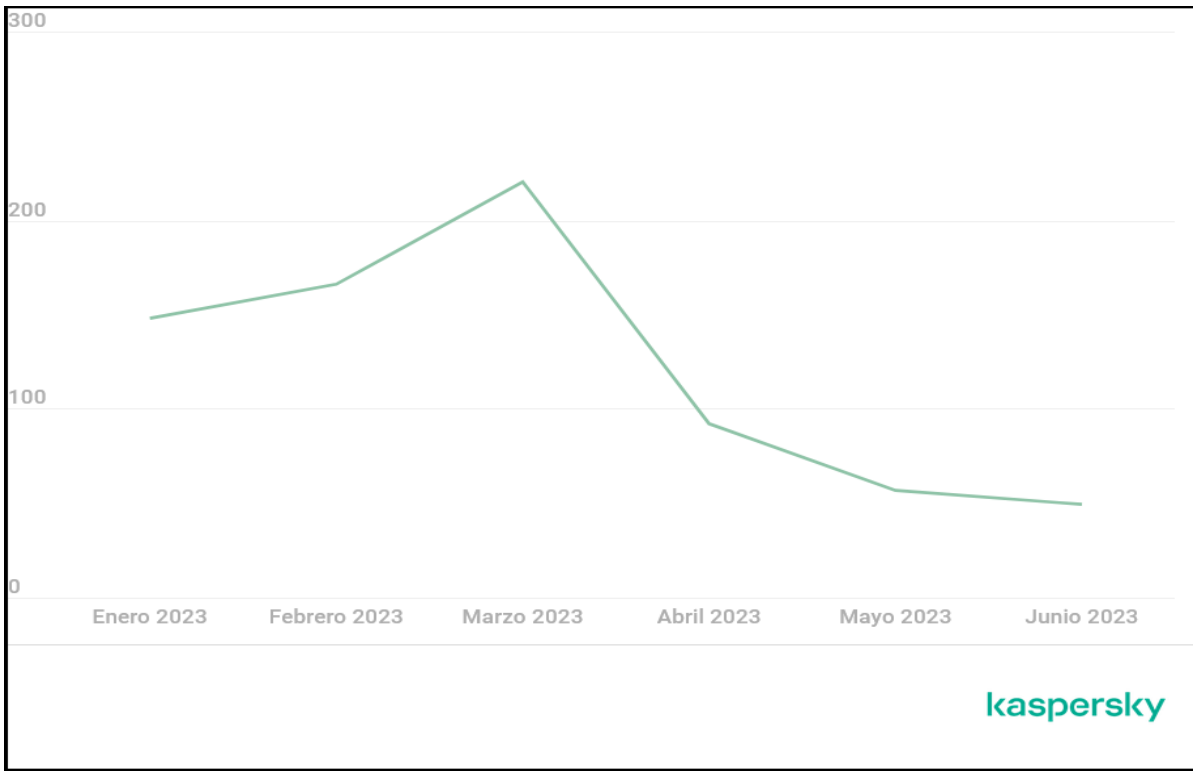
---

[36] welivesecurity. [Sitio web]. Bogotá: welivesecurity.com. [consultado el 05 de octubre del 2023] . Disponible en: https://www.welivesecurity.com/la-es/2023/07/04/dark-web-productos-servicios-ofrecen-cibercriminales/

[37] securelist [Sitio web]. Bogotá: securelist.lat [consultado el 21 de septiembre del 2023] . Disponible en: https://securelist.lat/iot-threat-report-2023/98141/

[38] revistaeconomia [Sitio web]. Bogotá: revistaeconomia.com. [consultado el 21 de septiembre del 2023] . Disponible en: https://www.revistaeconomia.com/kaspersky-publica-resumen-general-de-las-amenazas-relacionadas-con-iot-en-2023/

**Ilustración 7. Distribución del número de publicaciones relacionadas con los servicios de ataques DDoS**




**Fuente:** securelist, securelist.lat. *Distribución del número de publicaciones relacionadas con los servicios de ataques DDoS por mes, primer semestre de 2023.* [Consultado el 21 de septiembre de 2023]. Disponible en https://securelist.lat/iot-threat-report-2023/98141/

## METODOLOGÍAS PARA AUDITORIA DE DISPOSITIVOS IoT

En la actualidad, existen diversas organizaciones públicas y privadas sin ánimo de lucro que han elaborado metodologías para estos tipos de dispositivos. En el cual participan especialistas desarrolladores, investigadores y pentesters, con el propósito de crear una serie de fases o actividades con el fin de detectar amenazas y vulnerabilidades en este tipo de tecnologías, clasificarlas en función del riesgo (bajo, medio o alto) y cómo mitigarlas.

Además de informar que las tecnologías innovadoras deben progresar y no solo tener en cuenta su capacidad. Se deben cumplir ciertos requisitos o requerimientos técnicos para su salida al mercado, y es importante que los fabricantes y las organizaciones administradas por terceros implementen medidas de seguridad hacia estos dispositivos.

## 7.1 DIRECTRICES DE EVALUACIÓN EN SEGURIDAD IOT (GSMA IOT SECURITY GUIDELINES AND ASSESSMENT)

GSMA es una entidad privada de operadores de dispositivos móviles y se dedica a la asistencia y aplicación del sistema de telefonía GSM. Esta entidad se enfoca en la inclusión de aquellos dispositivos que se encuentren directa o indirectamente vinculados.

En la actualidad, está impulsando las buenas prácticas que deben aplicarse en las fases de diseño, desarrollo e implementación de servicios seguros sobre los dispositivos IoT, estableciendo mecanismos que permitan evaluar la seguridad, fiabilidad e integridad. Al fomentar la innovación en el mercado y adaptarse a las nuevas amenazas que conllevan en hogares y oficinas.

Al implementar estos dispositivos para llevar a cabo tareas diarias en las que se recopila información, se podría escalar hacia la red de una organización, identificar servicios, usuarios, contraseñas y convertirse en puertas traseras para los ciberdelincuentes. Se han establecido vínculos con diversas compañías de prestigio mundial que han adoptado sus directrices y han evaluado sus productos, generando soluciones IoT confiables al mercado.

En su metodología, se aconseja contar con medidas y/o procedimientos a nivel de seguridad para proteger los activos lógicos y físicos, además de los dispositivos IoT. Estos dispositivos se sustentan en procesos de evaluación que impactan la privacidad, los riesgos adecuados y permiten identificar las necesidades particulares de operadores, proveedores y servicios de terceros.

La finalidad de esta metodología, desde su perspectiva, es proporcionar las herramientas de seguridad y recursos acerca de los servicios y protocolos que se

encuentran implementados en el ámbito de la red de las cosas, lo que le brinda una guía para asegurar su infraestructura en el ámbito de dispositivos IoT.[39]

Brinda los siguientes lineamientos de Seguridad IoT de la GSMA:

- Se dispone de 85 recomendaciones detalladas acerca del diseño, desarrollo e implementación de dispositivos IoT seguros.
- Se abordan los aspectos vinculados a las redes de comunicación, servicios y hardware.
- Se lleva a cabo un análisis detallado de los desafíos concernientes a la seguridad, los diversos ataques y la evaluación de los riesgos.
- Se dispone de diversos casos de estudio prácticos sobre el diseño seguro de dispositivos IoT.

En el aspecto de evaluación de Seguridad IoT cuenta con:

- Proporciona un enfoque estructurado y una serie de controles de seguridad concisos.
- Se considera toda la infraestructura en cuestión.
- Se dispone de un modelo de cadena de suministros.
- Considera los diversos tipos de dispositivos que se encuentran en el mercado de la IoT.

### 7.2 OWASP FSTM

Se trata de una metodología de seguridad abierta y desarrollada por OWASP, una organización sin ánimo de lucro, en la cual se encuentran analistas,

[39] ccn-cert [Sitio web]. Bogotá: ccn-cert.cni.es [consultado el 21 de septiembre del 2023] . Disponible en: https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiv-jornadas-stic-ccn-cert/ponencias-1/5536-s19-d01-12-los-criminales-no-esperan-a-las-normas-por-eso-debemos-actuar-ya/file.html

desarrolladores e investigadores que diseñaron una guía que se encuentra actualmente en la versión 1 enfocada en el análisis de *Firmware*.

Se fundamenta en la estandarización de los procesos, herramientas, metodologías y todos los aspectos directos e indirectos. Este proceso está compuesto por una serie de fases y fue publicado para servir como guía predefinida.[40]

La metodología OWASP FSTM se compone de nueve fases concebidas por analistas, investigadores, desarrolladores, pentesters y expertos en seguridad de la información con el propósito de llevar a cabo evaluaciones a nivel de firmware.

### 7.2.1 ETAPA 1 RECONOCIMIENTO Y BÚSQUEDA DE INFORMACIÓN

Para una auditoría de seguridad en dispositivos IoT, el reconocimiento y la evaluación de vectores posibilitan la identificación de las tecnologías más utilizadas y la identificación de los diversos componentes que se encuentren en peligro, tales como los siguientes:

- Web del fabricante: La cantidad de información sobre el dispositivo puede variar debido a los diferentes fabricantes que se encuentran en el mercado. Según la mayoría de ellos, se enumeran las características técnicas, modos de uso, aplicaciones para interactuar con la tecnología y un enlace para otros recursos. Asimismo, se proporcionan datos técnicos, firmware, esquemas, fotografías del interior y componentes de los dispositivos.

  Debido a temas de regulación en diferentes regiones, muchos fabricantes están obligados a compartir más información en esos países.

- Web de otros fabricantes: Algunos artículos son concebidos por terceros o por otros profesionales, lo que posibilita la existencia de tecnología en la que se expone información sensible sobre ellos. En algunas regiones del

[40] tarlogic [Sitio web]. Bogotá: tarlogic.com [consultado el 21 de septiembre del 2023] . Disponible en: https://www.tarlogic.com/es/blog/analisis-de-seguridad-en-iot-owasp/.

mundo están obligados a proporcionar documentación acerca de los servicios prestados.

- Registro de certificación: En la actualidad, existen diversas entidades y compañías encargadas de llevar a cabo la certificación sobre un dispositivo, cumpliendo con las normas técnicas establecidas, detallados, procedimientos y materiales, con el fin de detectar deficiencias al examinar un producto.

Entre los diversos datos y características se encuentran fotografías del interior, dispositivo, información sobre el hardware, posibles prototipos, documentos de fabricantes y proveedores. Existen organizaciones en función del continente, existe una norma técnica que pueda o debe ser regulada.

- Repositorio de código: En la actualidad, numerosos dispositivos utilizados en la actualidad poseen software de código abierto. Estas licencias obligan a los fabricantes a publicarlo de manera abierta, acceso a código fuente, sitios web de fabricantes de soporte y actualizaciones de la tecnología IoT.

- Foros de fabricantes: Han sido concebidos con el propósito de solventar diversas dificultades o deficiencias en un producto. Esto permite realizar búsquedas para obtener una mayor comprensión de la composición general del firmware, soporte especializado, repositorios de drivers para descargar y actualizaciones, identificar su arquitectura de CPU, el sistema operativo, configuración del cargador de arranque, esquemático de hardware, hoja de datos sobre los componentes o líneas de código (LoC).

- Identificar los repositorios de código fuente de los fabricantes de tecnología IoT, el registro de terceros, los cambios realizados a nivel de puertos estándares y certificados e información del sistema, el diagrama de diseño, el flujo de datos y los informes realizados sobre las pruebas de penetración realizadas con su respectivo reporte de seguimiento de errores.

- En la actualidad, se encuentran programas en los que investigadores o hackers éticos identifican vulnerabilidades y las notifican directamente a los fabricantes para ser solucionadas, mediante la actualización o un procedimiento que permita la implementación de configuraciones para ser

solventadas. Es esencial llevar a cabo un análisis exhaustivo de los siguientes aspectos con el fin de documentarlos y generar un análisis posterior.

#### 7.2.1.1 ARQUITECTURAS DE CPU SOPORTADAS

Una de las tareas fundamentales consiste en llevar a cabo un análisis exhaustivo de la arquitectura que se encuentra, identificar sus particularidades y habilidades, con el fin de optimizar los procedimientos de reversing (proceso de análisis y descomposición del software o hardware), con el fin de simplificar los procesos de reversing (proceso de analizar y descomponer el software o hardware), así como de identificar posibles vulnerabilidades. La emulación nos permite comprender los posibles mecanismos y módulos criptográficos.

En la Ilustración 8 se presentan los diversos elementos que posibilitan la capacidad de funcionamiento del hardware y software que requiere un dispositivo IoT.

**Ilustración 8. Factores de un dispositivo IoT**


Fuente: algotive, algotive.ai. ¿Qué es el Internet de las cosas (IoT), cómo funciona y cuál es su importancia? [En línea]. 2022. [Consultado el 21 de septiembre de 2023]. Disponible en internet: https://www.algotive.ai/es-mx/blog/que-es-el-iot-como-funciona-y-cual-es-su-importancia

#### 7.2.1.2. PLATAFORMAS DE SISTEMAS OPERATIVOS

Previamente, se ha identificado la estructura de la computadora de computadoras (CPU) Conocer su sistema operativo que se encuentre implementado en el dispositivo. La seguridad de cualquier plataforma debe ser transparente y garantizar la seguridad, mantener cuidadosamente y solventar las vulnerabilidades que se presentan en el transcurso del tiempo.[41]

Los sistemas de código abierto pueden ser uno de los más críticos, no obstante, se corrigen de manera rápida y regular por parte de diversos investigadores, quienes reportan vulnerabilidades. Los sistemas de código cerrado o privativo requieren demasiado tiempo para corregir los errores, ya que su código fuente requiere ser corregido por terceros.

Algunas plataformas, como Amazon Web Services, GCP IoT (Google Cloud), Azure IoT y Zephyr OS, poseen sistemas embebidos que permiten llevar a cabo un proceso de test, actualización de vulnerabilidades en el sistema base y actualizaciones de los dispositivos.

#### 7.2.1.3. CONFIGURACIÓN SOBRE EL CARGADO DE DISCO

En la actualidad, existen diversas opciones de arranque sobre el sistema, que se utilizan para brindarle una capa de seguridad, en algunos dispositivos para realizar la recuperación del cargue. El disco que está protegido también permite realizar una copia de seguridad sobre el sistema operativo, credenciales y certificados de acceso.

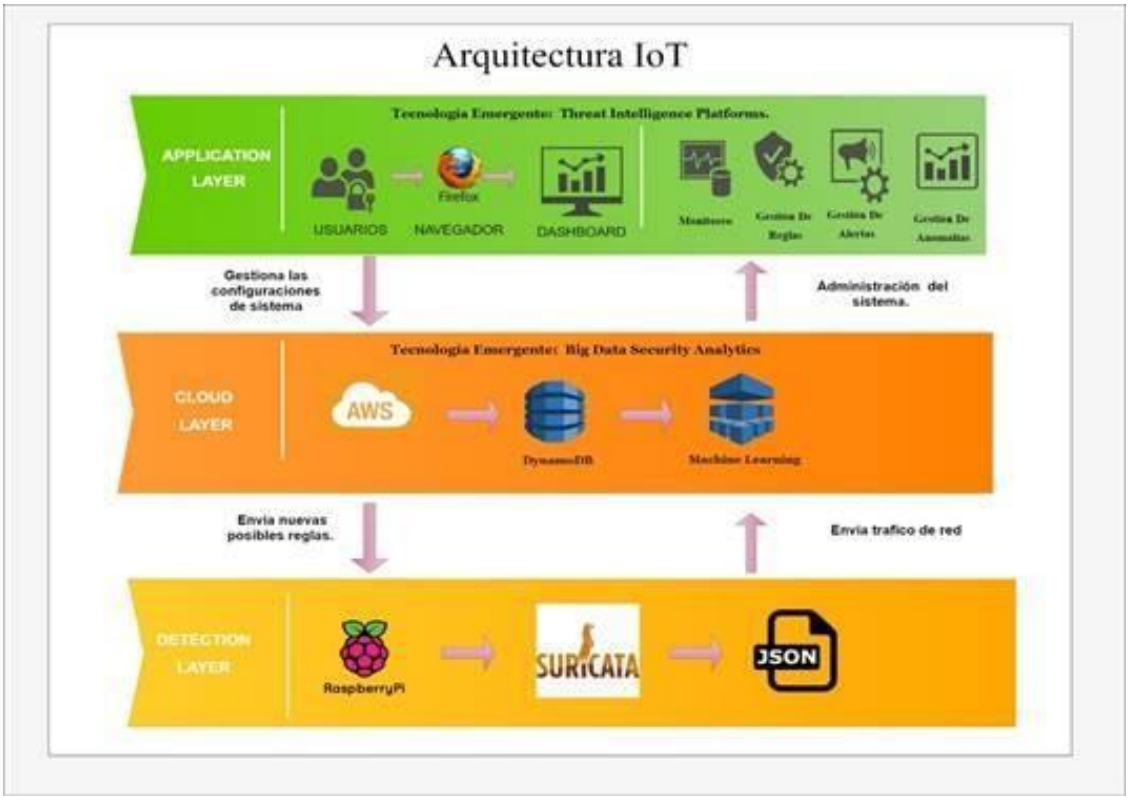
#### 7.2.1.4. ESQUEMAS DE HARDWARE

Asimismo, es posible obtener información sobre el esquema de diseño electrónico, como se muestra en la Ilustración 9, a través del uso de fuentes oficiales proporcionadas por el fabricante o ingeniería inversa, con el objetivo de que el auditor expanda la superficie de ataque para identificar los diferentes

[41] Amazon. [Sitio web]. Bogotá: aws.amazon.com. [consultado el 19 de septiembre del 2023] . Disponible en: https://aws.amazon.com/es/what-is/iot/

componentes que se encuentran en los mismos, servicios o protocolos habilitados.

**Ilustración 9. Ejemplo de un esquema de Hardware**




Fuente: revistas. unisimon, revistas.unisimon.edu.co. Arquitectura IoT. [En línea]. 2022. [Consultado el 21 de septiembre de 2023]. Disponible en internet: https://revistas.unisimon.edu.co/index.php/innovacioning/article/view/5340/6059#figures.

### 7.2.1.5. GUÍA DE LOS COMPONENTES

Después de conocer los esquemas de los dispositivos, es importante identificar los componentes de los mismos, que se encuentran sobre la placa electrónica, para reconocer el diseño y las partes físicas.

### 7.2.1.6. LÍNEAS DE CÓDIGO (LOC) ESTIMADAS

Tras analizar e identificar el dispositivo que se aproxima a identificar la cantidad de memoria disponible sobre el sistema operativo o firmware, se puede conocer la longitud del código, ejecutando diferentes herramientas y técnicas para encontrar el binario y cómo descifrarlo.

#### 7.2.1.7. REGISTRO DE CAMBIOS

Una vez que se han analizado los registros de cambios en el hardware y software, se ha obtenido una fuente de información muy fiable que permite detectar deficiencias o vulnerabilidades presentes que se han corregido en versiones posteriores. La mayoría de los dispositivos carecen de alternativas para remediarlo, pues los fallos que se presenten en el hardware solo pueden ser corregidos mediante un nuevo producto físico. En algunos casos, se emplean librerías obsoletas que permiten la autenticación o accesibilidad a los puertos sin ningún tipo de seguridad.

#### 7.2.1.8. DIAGRAMAS DE DISEÑO Y FLUJO DE DATOS

La totalidad de la información recopilada posibilita la identificación del diseño y los flujos de datos que se encuentran en un dispositivo, así como la comprensión de la lógica y la transmisión de datos. Con el propósito de obtener los índices de entrada y evitar la vulneración de este dispositivo.

#### 7.2.1.9. INFORMES DE PRUEBAS DE PENETRACIÓN PREVIAS

Es esencial llevar a cabo una investigación sobre las auditorías de seguridad realizadas para descartar caminos explorados y contemplar nuevas formas de intrusión; se recomienda llevar a cabo un análisis de vulnerabilidades para descartar o identificar vectores de ataque.

#### 7.2.1.10. *TICKETS* DE SEGUIMIENTO DE ERRORES

La totalidad de la información recopilada posibilita la identificación del diseño y los flujos de datos que se encuentran en un dispositivo, así como la comprensión de la lógica y la transmisión de datos. Con el propósito de obtener los índices de entrada y evitar la vulneración de este dispositivo.

### 7.2.2. ETAPA 2 OBTENCIÓN DEL FIRMWARE DE DISPOSITIVOS IOT

En esta fase, el propósito primordial es obtener el firmware mediante diversos procedimientos para alcanzarlo. Se centra en diferentes opciones, analizando sus pros y contras. Con el fin de determinar los puertos físicos de depuración, se

requiere la identificación de los chips de memoria. Al analizar la documentación, las herramientas, las recomendaciones y las buenas prácticas.[42]

Para la extracción del firmware, no se dispone de un solo camino, sino que se requiere de esfuerzo, conocimiento, creatividad y pensamiento lateral por parte del auditor o investigador.

#### 7.2.2.1. RECOMENDACIÓN Y BUENAS PRÁCTICAS

Es esencial disponer de uno o más dispositivos físicos o la posibilidad de emularlos, ya que existe software diseñado para la emulación de router, Switch, Firewall, sistemas operativos, entre otros.

#### 7.2.2.2. COMPROBACIÓN DEL FUNCIONAMIENTO DEL DISPOSITIVO

Se aconseja que, previo a la extracción, se verifique que el dispositivo se encuentra funcionando adecuadamente y no presenta ningún inconveniente físico o lógico que sea causado por factores como el calor, la humedad, las fallas de corriente, entre otros. Se puede observar que al llevar a cabo un análisis de manera forense y la toma de evidencias no se logra una ejecución adecuada.

#### 7.2.2.3. DESCARGAR DEL *FIRMWARE* DE LA PÁGINA DEL FABRICANTE

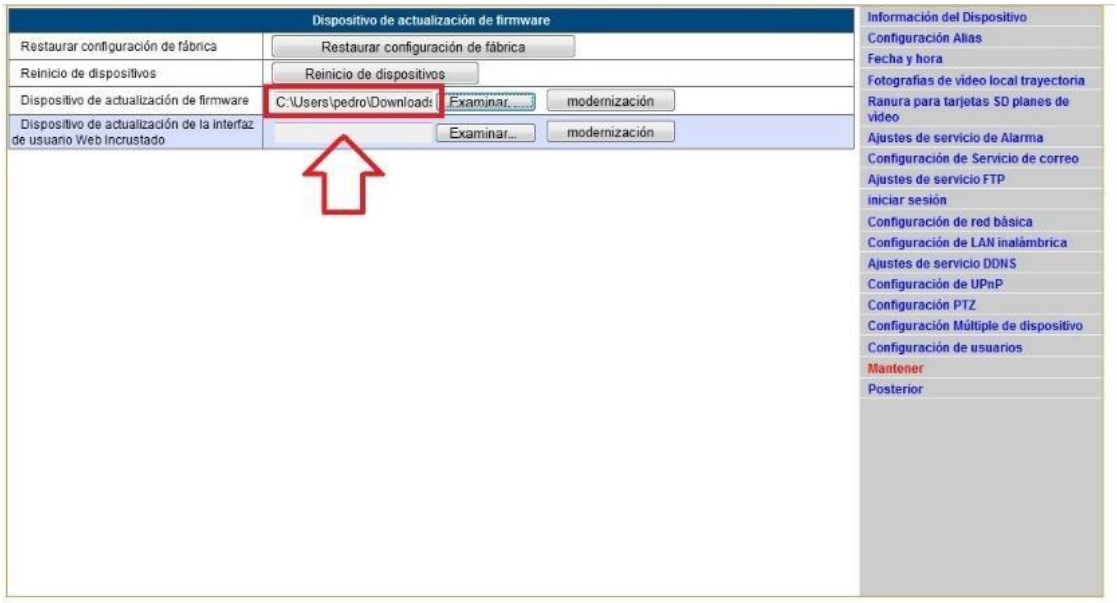
Es imperativo y de manera diligente llevar a cabo regularmente las actualizaciones de los aparatos, aprovechando y obtener el firmware mediante la página web del fabricante, donde se indica la versión y la versión posible actualizar.

Se recomienda verificar si el dispositivo tiene la opción de ser actualizado de manera remota a través de un archivo de configuración que se sube desde otro equipo, como se muestra en la ilustración 10, lo cual permite obtener una copia del software interno.

---

[42] tarlogic.com [Sitio web]. Bogotá: [consultado el 21 de septiembre del 2023] . Disponible en: https://www.tarlogic.com/es/blog/owasp-fstm-obtencion-firmware-iot/.

**Ilustración 10. Actualizar un firmware**




Fuente: tarlogic, tarlogic.com. owasp fstm obtención firmware IoT. [En línea]. 2022. [Consultado el 21 de septiembre de 2023]. Disponible en internet: https://www.tarlogic.com/es/blog/owasp-fstm-obtencion-firmware-iot/

### 7.2.2.4. INTERCEPTAR COMUNICACIONES PARA LA OBTENCIÓN DEL FIRMWARE DE DISPOSITIVOS IOT

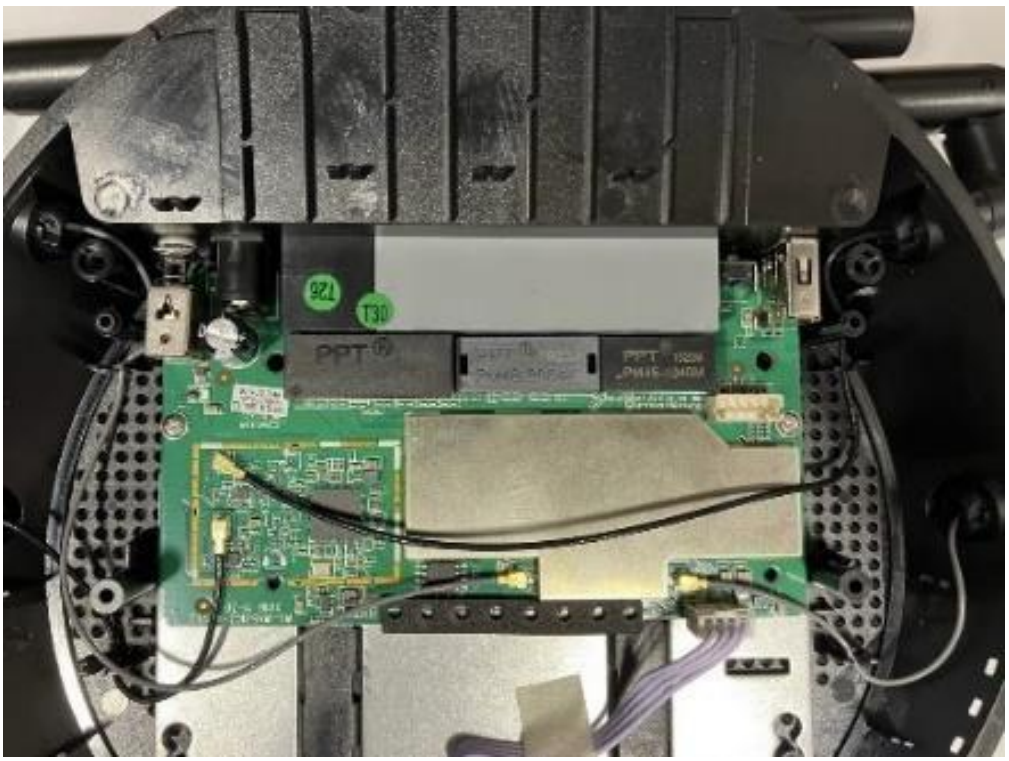
Realizar una auditoría sobre las comunicaciones capturando el tráfico a través de Wireshark, un software libre multiplataforma, herramienta creada para el análisis y solución de problemas de redes de comunicaciones, analizando protocolos que permiten volcar los datos y obtener el archivo de firmware.[43]

### 7.2.2.5. ACCESO AL HARDWARE DEL DISPOSITIVO

Una de las opciones es llevar a cabo un análisis del hardware, desmontando el dispositivo, algo similar a la ilustración 11 en la que se muestran sus componentes, identificando los conductores y circuitos integrados. Antes de ello, resulta imperativo disponer del manual que se encuentra disponible en la página principal del proveedor.

[43] futurespace.es. [Sitio web]. Bogotá: futurespace.es. [consultado el 09 de noviembre del 2023] . https://www.futurespace.es/hacking-en-iot/

**Ilustración 11. Desmontando dispositivo IoT**



Fuente: tarlogic, tarlogic.com. owasp fstm obtención firmware IoT [En línea]. 2022. [Consultado el 21 de septiembre de 2023]. Disponible en internet: https://www.tarlogic.com/es/blog/owasp-fstm-obtencion-firmware-iot/

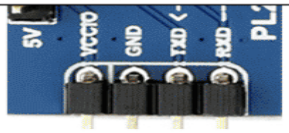
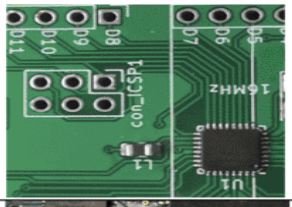
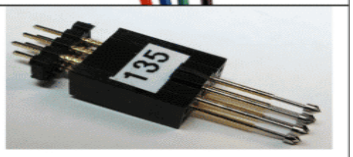
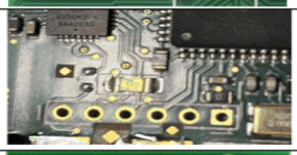
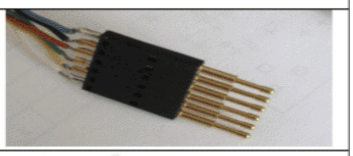
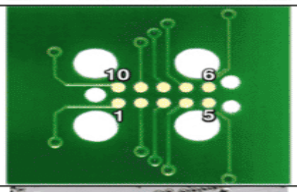
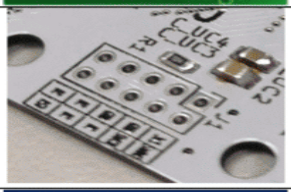
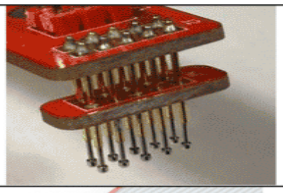
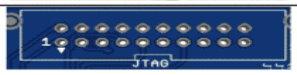
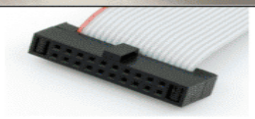
### 7.2.2.6. IDENTIFICACIÓN DE PUERTOS DE COMUNICACIÓN

En el mercado de dispositivos IoT hay varios tipos de dispositivos que se usan para dispositivos IoT, como microprocesadores, procesadores y sensores que son usados en otros dispositivos de algún fabricante.[44]

En la ilustración 12 se presentan los diferentes puertos de comunicación disponibles. Dependen de cada fabricante debido a que adoptan soluciones a sus necesidades particulares, por lo que es recomendable que se identifique previamente el tipo de protocolo que utiliza el dispositivo IoT.

[44] aprendiendoarduino.wordpress.com. [Sitio web]. Bogotá: aprendiendoarduino.wordpress.com. [consultado el 09 de noviembre del 2023] . https://aprendiendoarduino.wordpress.com/2019/10/15/dispositivos-hardware-iot-2/

**Ilustración 12. Puertos de comunicación más usados**

| Pines | Nombre | Diseño en PCB | Conector |
|---|---|---|---|
| **4**<br>Configuración<br>1x4<br>Paso<br>2,54 mm | *UART* |  |  |
| **6**<br>Configuración<br>2X3<br>Paso<br>2,54 mm | *ICSP* |  |  |
| **6**<br>Configuración<br>1x6<br>Paso<br>2,54 mm | *ICSP* |  |  |
| **10**<br>Configuración<br>2x5<br>Paso<br>1,27 mm | *J Link* |  |  |
| **10**<br>Configuración<br>2x5<br>Paso<br>2,00 mm | *JTAG* |  |  |
| **20**<br>Configuración<br>2x10<br>Paso<br>2,54 mm | *JTAG* |  |  |

Fuente tarlogic, tarlogic.com. owasp fstm obtención firmware IoT [En línea]. 2022. [Consultado el 21 de septiembre de 2023]. Disponible en internet: https://www.tarlogic.com/es/blog/owasp-fstm-obtencion-firmware-iot/

La tensión de un puerto se mide mediante el osciloscopio. Esta herramienta realiza un análisis sobre señales analógicas, identificando los voltajes de operación que se encuentran en cualquier señal o dispositivo digital.

El analizador lógico permite monitorear la evolución de una señal en tiempo real distinguir y hacer una medición directa, identificando un valor lógico debajo a alto (0 o 1).

#### 7.2.2.7. LECTURA DEL FIRMWARE A TRAVÉS DE UN COMPONENTE DEL CIRCUITO

En ocasiones, resulta imposible acceder a ningún puerto, por lo que es necesario desmontar el dispositivo y llevar a cabo un minucioso análisis de la placa con el fin de obtener el firmware correspondiente. Tras identificar cualquier tipo de memoria flash con el fin de efectuar una actualización o backup de la configuración.

### 7.2.3. ETAPA 3 ANÁLISIS DEL FIRMWARE

Esta fase lleva a cabo un análisis del firmware en función de todos los casos previamente mencionados. Una de las técnicas más utilizadas es el volcado de memoria que se realiza sobre un formato de binario estándar o mediante el uso de técnicas y/o herramientas públicas o de terceros, trucos según el fabricante y la versión del dispositivo.

#### 7.2.3.1. OBTENER MEDIANTE UN VOLCADO DE BINARIO EN BRUTO

Este tipo de volcado puede hallarse en diferentes formatos. Para realizar un análisis existen herramientas que requieren del formato o el binario en específico. Al emplear un editor de texto que permite corroborar la información, los más utilizados son los siguientes:

#### 7.2.3.2. INTEL HEX

Este es uno de los formatos más antiguos se representa el contenido de memorias. Se distingue por su estructura física que consta de una línea y dos puntos.

#### 7.2.3.3. SREC

Es un código de inicio en el que se describen los datos en un formato hexadecimal.

#### 7.2.3.4. BASE64

Se trata de uno de los formatos más utilizados para la transmisión de datos a través de un canal. Se encuentra en dispositivos embebidos para su codificación, utilizando Python o Perl.

#### 7.2.3.5. CRIBADO DE LOS DATOS DE FUERA DE BANDA Y PARIDAD

La presente tarea consiste en la eliminación de los datos que se encuentran en ausencia de banda y paridad. A continuación, se realiza un volcado de memoria, lo que produce la extracción física. Para llevar a cabo la extracción de manera automatizada, se emplean herramientas.

#### 7.2.3.6. ANÁLISIS DE ENTROPÍA

La capacidad de obtener los valores posibles mediante la utilización de una variable aleatoria, el conjunto de datos originarios y de formato indefinido o indeterminado. Se utiliza el comando binwalk que se encuentra en los sistemas operativos Linux para llevar a cabo esta tarea.

#### 7.2.3.7. IDENTIFICACIÓN DE FIRMAS

En la actualidad, existen una gran cantidad de formatos de archivos y sistemas de ficheros que cuentan con una serie de bytes para su identificación denominados números mágicos (magic números), que se identifican durante un análisis de firmware. Esto se puede realizar de manera manual o con herramientas automáticas que genera como resultado cadenas de texto referencial de sistemas, algoritmos de cifrado, entre otros.

#### 7.2.3.8. SECCIONADO DEL BINARIO

Una vez que se extrae la imagen del firmware, es posible analizar el archivo independiente, usando una herramienta de Linux llamada dd, que realiza una copia de los bytes de un archivo de entrada hacia un archivo de salida.

#### *7.2.3.9.* DISTRIBUCIÓN DE *BYTES*

Otro procedimiento de análisis puede ser llevado a cabo mediante la obtención del archivo, mediante la realización de un histograma que evalúa la distribución de los valores, y genera unos rangos que se corresponden con las distribuciones de caracteres para la tabla del código ASCII.

#### 7.2.3.10. BÚSQUEDA DE CADENAS

La técnica es uno de los más fundamentales en la cual se realiza la lista de cadenas de texto que se encuentran en el firmware, aportando información importante al momento de leer un análisis. Estos archivos binarios utilizan un string que permite identificar licencias de software, mensajes de versión, nombres y funciones para compararlos con el sitio web del fabricante.

#### 7.2.3.11. BÚSQUEDA DE OTRAS CONSTANTES

La presente técnica posibilita la identificación de sesiones cifradas mediante el empleo de un análisis de entropía que se encuentren en la distribución de los bytes. Posteriormente, al identificar el algoritmo criptográfico y el hash, un algoritmo matemático que utiliza un cifrado determinado, se detectan y corregir errores.

Esta actividad puede realizarse de forma manual a través de editores decimales, ya que permite verificar la integridad de la construcción de la imagen de firmware, identificar el formato propietario, las firmas digitales, entre otros.

### 7.2.4. ETAPA 4 EXTRACCIÓN DEL SISTEMA DE FICHEROS

En la actualidad, se encuentran numerosos dispositivos IoT ejecutados en un sistema operativo Linux embebido, debido a su económicamente más barata de crear y fácil de adquirir, a través de una imagen firmware.

Se dispone de archivos ejecutables, ficheros de configuración, script y servicios que se ejecutan directamente en el sistema para identificar las características del dispositivo. Este proceso se divide en diversas fases:

#### 7.2.4.1. IDENTIFICACIÓN DEL FORMATO DE *FIRMWARE*

Se dispone de archivos ejecutables, archivos de configuración, script y servicios que se basan directamente en el sistema con el fin de identificar las particularidades del dispositivo. Este procedimiento se estructura en múltiples fases:

#### 7.2.4.2. BÚSQUEDA DE FIRMAS Y NÚMEROS LÓGICOS

Para identificar un firmware, se utiliza una técnica denominada identificación de sesiones que permite identificar las cadenas de caracteres que se encuentran comprimidas en un archivo.

#### 7.2.4.3. ESTUDIO DE ENTROPÍA

En algunos casos, el *firmware* obtenido puede ser cifrado o comprimido, y en el día de hoy se procederá a la descodificación. La entropía es una fuente de datos que posibilita la descifrarían de una imagen de *firmware.*

#### 7.2.4.4. EXTRACCIÓN DEL SISTEMA DE FICHEROS

El objetivo de esta fase consiste en extraer el sistema de archivos mediante la utilización de herramientas automatizadas para agilizar el proceso de detección y extracción de *firmware,* obteniendo números mágicos, firmas y cadenas que identifiquen secciones dentro del *firmware*.

### 7.2.5 ETAPA 5 ANÁLISIS DEL SISTEMA DE FICHEROS

Esta etapa se fundamenta en las actividades anteriores, con el objetivo de obtener toda la información posible sobre el funcionamiento del sistema, archivos, configuraciones, credenciales y ejecutables. Identificar los procesos de iniciación, los servicios que se están llevando a cabo en el dispositivo, los usuarios por defecto y el aprovechamiento de las vulnerabilidades existentes. [45]

#### 7.2.5.1. PROCESO DE ARRANQUE

Esta fase se lleva a cabo un análisis del proceso de inicio y las tareas que se llevan a cabo a nivel de usuario y servicio que son llevados a cabo en el kernel. Existen diversos tipos de arranque en los sistemas Unix; no obstante, los más utilizados son los siguientes:

---

[45] tarlogic.com [Sitio web]. Bogotá: [consultado el 21 de septiembre del 2023] . Disponible en: https://www.tarlogic.com/es/blog/owasp-fstm-analisis-sistema-ficheros/.

#### 7.2.5.1.2. BSD

Uno de los procesos más utilizados en sistemas operativos BSD, FreeBSD y OpenBSD es el que se ejecuta sobre scripts en el directorio /etc./rc, /etc/rc.local, /etc/rc.conf, dependiendo de la versión del sistema operativo.

#### 7.2.5.1.3. SYSTEM V

Se trata de un proceso de arranque utilizado en BusyBox y otros sistemas, en el cual el contenido del fichero se encuentra en /etc/inittab o /etc/init.d según su configuración.

Una vez identificado el proceso, es posible obtenerla a través del terminal, el cual utiliza ingeniería inversa para comprobar el sistema de arranque, identificar servicios abiertos, puertos por defecto, usuarios anónimos o con privilegios altos, ejecutables.

#### 7.2.5.1.4 BÚSQUEDA DE FICHEROS

Posteriormente, a partir de los resultados previos, se procederá a llevar a cabo un análisis del proceso de inicio, considerando todos los servicios disponibles y su funcionamiento, a partir de la información previamente recopilada tras documentarse. Se procede a la identificación de ficheros de configuración, tareas automáticas, scripts y proceso de iniciación. Se aconseja emplear una lista de elementos específicos:

- Buscar servidores actualizados o inseguros.
- Identificar código fuente y scripts de inicio.
- Identificar servicios de api con configuraciones predeterminadas
- Realizar pruebas de credenciales predeterminadas o por defecto.

A partir de los elementos previamente mencionados, es factible detectar vulnerabilidades en el sistema o ataques de ejecución remota de código (RCE), intrusión al sistema y ejecución de código arbitrario.

Posteriormente, al acceder al dispositivo, se procede a efectuar una búsqueda inicial de las ubicaciones habituales de los sistemas de archivos que se encuentran en los sistemas operativos Linux y UNIX mediante búsquedas automáticas, scripts y herramientas que permitan identificar los siguientes ficheros.

- Archivos relacionados con certificados SSL y claves de certificado con extensión .crt,cert,.pem.
- Archivos o ficheros de configuración con la extensión.conf.
- Ficheros o carpetas con permisos de ejecución.
- Ficheros binarios con extensión.bin.
- Servicios ejecutables como SSH, telnet, tftp.
- Scripts almacenados en extensión.sh.
- Servidores web implementados en apache o nginx.

De manera que permitan realizar una búsqueda mediante cadenas de texto en las que se buscan palabras fundamentales como:

- Identificar funciones del lenguaje C vulnerables.
- Identificar usuarios admin, password, user.
- Identificar URLs, direcciones IP que se comuniquen remotamente.

#### 7.2.5.2. HERRAMIENTAS PARA AUTOMATIZACIÓN

Para llevar a cabo esta tarea, que suele ser un tanto difícil, existen herramientas públicas que permiten realizar un análisis de manera automatizada a los sistemas de ficheros que se encuentran en un *firmware*. Los más conocidos son los siguientes:

##### 7.2.5.2.1 . *FIRMWALKER*

*Software* libre desarrollada en *bash* (herramienta qué permite crear programas ejecutables) realizar búsquedas automatizadas sobre los sistemas de ficheros del *firmware* extraído para identificar posibles vulnerabilidades.[46]

[46] gurudelainformatica. [Sitio web]. Bogotá: gurudelainformatica.es. [consultado el 05 de octubre del 2023] . Disponible en: https://gurudelainformatica.es/test-de-penetracion-de-dispositivos-iot

#### 7.2.5.2.2. *THE FIRMWARE ANALYSIS AND COMPARISON TOOL O FACT* (ANALIZADOR Y COMPARADOR DE FIRMWARE)

Se trata de una herramienta de las más conocidas que permite al auditor automatizar la mayor parte del proceso para identificar el contenido e interpretar los sistemas de ficheros extraídos.

#### 7.2.5.3. FACT

Se trata de una herramienta que permite detectar credenciales y certificados que ya han sido implementados de manera débil, basándose en la lista de CVE (enumeración de vulnerabilidades comunes), así como también comparar versiones de los ficheros.

#### 7.2.5.4. EMBA *EMBEDDED ANALYZER* (ANALIZAR INTEGRADO)

Se trata de un *Framework* (Un conjunto de y librerías que se utilizan para el desarrollo de aplicaciones) utilizando diversas herramientas disponibles con diferentes funcionalidades para extraer el sistema de ficheros, analizar estático los ejecutables e identificar vulnerabilidades conocidas.

### 7.2.6. ETAPA 6 EMULACIÓN DEL FIRMWARE

Esta etapa permite replicar el comportamiento del dispositivo en una plataforma virtual, ejecutando diferentes pruebas para comprobar las vulnerabilidades que previamente detectadas de manera manual o utilizando herramientas automatizadas. Existen 2 tipos de emulación:

#### 7.2.6.1. EMULACIÓN PARCIAL

El cual se centra en establecer un servicio o proceso en particular.

#### 7.2.6.2. EMULACIÓN SOBRE UN ESPACIO DE USUARIO PARA UN EJECUTABLE

En este contexto, el emulador se encarga de simular un dispositivo genérico para cargar un ejecutable.

#### 7.2.6.3. EMULACIÓN SOBRE UN ESPACIO DE ARCHIVOS SIMULADOS

En algunos casos, los ejecutables requieren acceso al dispositivo y/o archivos dependen del hardware, por lo que se requiere replicar estas acciones mediante software como CUSE (dispositivos caracteres en el usuario) o FUSE (Sistema de usuarios).

#### 7.2.6.4. EMULACIÓN DE SISTEMA SIN UTILIZAR BOOTLOADER

En ciertas circunstancias, es necesario emular un kernel en relación con los procesos y/o servicios en un *firmware*. Para llevar a cabo esta tarea, se inicia el kernel en memoria, sin necesidad de utilizar un *bootloader* (carga de inicio).

#### 7.2.6.5. EMULACIÓN TOTAL

Este tipo de emulación se produce cuando los firmwares utilizan un método de comprensión y/o cifrado. Algunos de ellos están ofuscados y su documentación es insuficiente, por lo cual es una tarea demasiado difícil, ya que se requiere realizar un análisis completo del dispositivo.

La emulación del firmware posibilita al auditor llevar a cabo un análisis de los protocolos o servicios que se han implementado con el fin de detectar nuevas vulnerabilidades en los dispositivos. En las pruebas de arquitectura basadas en hardware, se requiere efectuar una emulación parcial o total, mediante la utilización de herramientas como:

#### 7.2.6.6. QEMU

La capacidad de visualizar y emular máquinas se basa en un modelo virtual de máquinas completas (CPU, Memoria RAM, Tarjeta de red) permite ejecutar un sistema totalmente emulado.

#### 7.2.6.7. UNICORN

Se utiliza para la emulación de diversas arquitecturas de CPU, es un emulador extremadamente flexible y tiene un gran rendimiento a nivel de velocidad.

#### 7.2.6.8. RENODE

Se trata de una herramienta que permite la emulación de firmware y otros sistemas, lo que permite la interacción entre múltiples procesos virtuales y la memoria visualizada entre diferentes dispositivos.

#### 7.2.6.9. FIRMADYNE

Este emulador está compuesto por un conjunto de herramientas que posibilitan al auditor automatizar y simplificar el proceso al efectuar una emulación de un dispositivo, lo que a su vez aporta diversas vulnerabilidades detectadas.

### 7.2.7. ETAPA 7 ANÁLISIS DINÁMICO

Tras la ejecución del firmware, esta fase se encarga de llevar a cabo una depuración en el hardware con el fin de localizar puertos, conectores, controles de flujo, entre otros elementos. El análisis dinámico es uno de los métodos más simples de realizar para prevenir fallos, y su propósito primordial radica en la obtención de una comprensión general acerca del funcionamiento de este sistema, lo cual permitirá corroborar los puntos débiles y los servicios vulnerables.

#### 7.2.7.1. DEPURACIÓN POR MEDIO DE EMULACIÓN

Al diseñar sobre cualquier virtualizado o emulador del dispositivo a evaluar, se emplea la técnica de la línea, la cual consiste en la ejecución de un depurado de software para identificar el estado del sistema .

En el caso de la emulación completa, estas técnicas tienden a enfocarse en las funciones del inicio y los elementos del kernel.

#### 7.2.7.2. DEPURACIÓN POR MEDIO DE EMULACIÓN

En algunos casos, algunos dispositivos disponen de puertos físicos para la depuración mediante interfaces de tipo JTAG (interfaz de hardware) o UART (interface de protocolo de datos).

Esto ocurre debido a que los desarrolladores no brindaron una debida protección sobre estos dispositivos que, a través de las interfaces, permiten la lectura y escritura de la memoria ROM (Memoria de lectura) y RAM (Memoria de Acceso aleatorio) para interactuar a través de dispositivos.

Las interfaces UART son aquellas que permiten la depuración y el acceso a la interacción mediante el uso de un terminal en la memoria para controlar el flujo de ejecución.

#### 7.2.7.3. *FUZZING*

Se trata de una técnica de búsqueda utilizada para la validación y pruebas automatizadas de software, identificando errores o deficiencias en el código fuente de los dispositivos IoT. Existen diversas técnicas en función de la necesidad o el propósito de la auditoría.

- *Fuzzing* en aplicación: La modificación de los datos de entrada se enfoca en la identificación de los fallos en el código, siendo esta una técnica de mayor utilidad para el análisis de pruebas que comprometan la integridad.
- *Fuzzing* sobre formato: Esta técnica permite modificar los datos de entrada generando paquetes y ficheros mal estructurados para detectar los errores de implementación que no cumplan con las normas.
- *Fuzzing* en protocolo: La presente técnica posibilita la creación de paquetes modificados en relación con el protocolo de comunicación particular, mediante la utilización de un proxy, en el cual se modifiquen los paquetes para reenviarlos hacia un destino específico.

#### 7.2.7.4. MODIFICACIONES SOBRE EL BOOTLOADER

Se trata de una de las tareas más utilizadas para impedir el acceso al login manager, para acceder a una terminal y, como usuario administrador, manipular los parámetros del kernel. Esta técnica es posible llevar a cabo aprovechando algún tipo de deficiencia que se encuentra en el dispositivo de arranque, modificándolo de acuerdo con el fabricante y generando una imagen de firmware.

#### 7.2.7.5. MODIFICACIONES SOBRE EL *FIRMWARE*

Esta técnica emplea la inexactitud del origen del firmware, efectuando ataques a integridad y generando una copia modificada para detectar vulnerabilidades. Mediante el uso del puerto SSH, se procede a extraer los datos del sistema y los ficheros, así como a realizar un proceso de ejecución y emisión de la imagen, ubicando el inicio del proceso.

### 7.2.8. ETAPA 8 ANÁLISIS SOBRE TIEMPO DE EJECUCIÓN

Este tipo de análisis se fundamenta en fases previas mediante diversos procedimientos para analizar el hardware original o un emulador en el cual se encuentra el firmware virtualizado. Para esta fase, se requieren herramientas depuradoras, las cuales son las siguientes:

#### 7.2.8.1. INSTRUMENTACIÓN Y DEPURACIÓN

Esta categoría dispone de depuradores que pueden inspeccionar a nivel de la memoria, identificar todos los procesos en ejecución, controlar el flujo utilizando puntos estratégicos e inyectar códigos de depuración.

#### 7.2.8.2. *TRACING*

Esta técnica se basa en registrar todos los eventos de llamada al sistema que se producen y ofrece un esquema fundamental sobre todas las operaciones realizadas.

#### 7.2.8.3. *LOGGING*

La presente técnica se lleva a cabo mediante la ejecución de registros obtenidos por el mismo ejecutable, a fin de obtener información acerca de los errores y procesos.

#### 7.2.8.4. INSTRUMENTACIÓN Y DEPURACIÓN

Se trata de un conjunto de técnicas utilizadas para supervisar, medir y modificar la ejecución de una pequeña parte del software para proporcionar información.

Se requiere examinar el comportamiento de un programa que aguarda la ejecución, efectuando una inspección del estado de memoria.

#### 7.2.8.5. DEPURADORES DE *HARDWARE*

Se utilizan diferentes herramientas de depuración según el fabricante, según los puertos estándar para las condiciones de *hardware* y *software*.[47]

#### 7.2.8.6. DEPURADORES DE *SOFTWARE*

Se trata de un depurador concebido con el propósito de detectar y evaluar la seguridad en los dispositivos de IoT.

### 7.2.9. ETAPA 9 EXPLOTACIÓN DE EJECUTABLES

La etapa final presenta evidencias de vulnerabilidades identificadas. Se llevará a cabo una prueba de concepto con el fin de aprovechar una vulnerabilidad y acceder al dispositivo. [48]Se requiere realizar una inspección de código fuente ejecutable compilada de vulnerabilidades, las más utilizadas son:

#### 7.2.9.1. *BUFFER OVERFLOW*

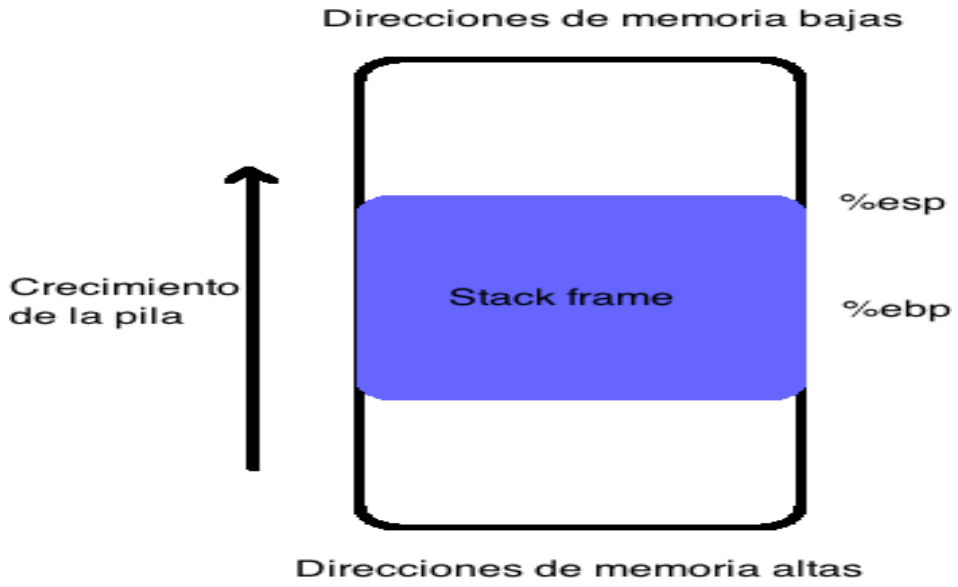
La corrupción de memoria es una de las características más habituales que se observan en el contexto de la corrupción de memoria. Como se muestra en la ilustración 13, los desbordamientos de buffer permiten la ejecución de código remoto arbitrario. Se ubican en un área de la memoria con el propósito de preservar un valor temporal en C. Estos recursos se fundamentan en los arrays (conjunto de variables) y se basan en la inyección de código malicioso en la memoria.

---

[47] onasystems [Sitio web]. Bogotá: onasystems.net [consultado el 23 de septiembre del 2023] . Disponible en: https://www.onasystems.net/glosario-de-ciberseguridad/?dir=4&name_directory_startswith=D

[48] tarlogic.com [Sitio web]. Bogotá: [consultado el 21 de septiembre del 2023] . Disponible en: https://www.tarlogic.com/es/blog/owasp-fstm-etapa-9-explotacion-de-ejecutables/

**Ilustración 13. Ejemplo de Desbordamiento de Buffer Overflow**




Fuente: byte-mind, byte-mind.net. cómo funciona un buffer overflow parte 1. [En línea]. 2022. [Consultado el 21 de septiembre de 2023]. Disponible en internet: https://byte-mind.net/como-funciona-un-buffer-overflow-parte-i/

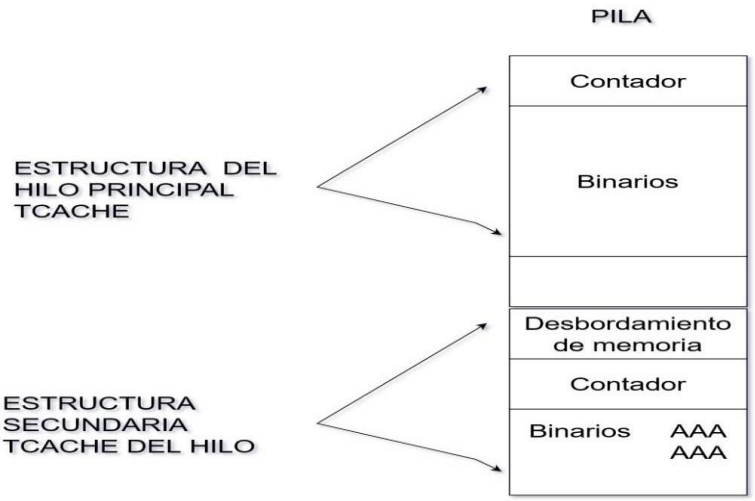
#### 7.2.9.2. FORMATO ATAQUE *STRING*

Esta es una deficiencia que se produce debido al uso incorrecto de la función *printf* en C que se encuentra sobre la cadena de formato. Esta función permite leer los valores en el *stack* (Memoria no ejecutable) y prioridad. Identificando el buffer y examinando la entrada mediante una dirección de memoria, se procede a alterar el formato %, lo que permite identificar la dirección de la memoria, proporcionando, además, el número de caracteres escritos y leer el contenido del firmware.

#### 7.2.9.3. *HEAP OVERFLOW*

Se trata de otra técnica de explotación que como lo indica la Ilustración 14 utilizando de ejecutables derivada de buffer overflow que se realiza en el espacio de la memoria dinámica en el lugar del stack, para superar estos límites, sobrescribir valores y acceder a los datos en sesiones no deseadas para tomar el control del dispositivo.

**Ilustración 14. Ejemplo de *Heap Overflow***




Fuente: Propia

### 7.2.9.3.1. PROTECCIÓN DE BINARIOS Y *HARDENING*

Al detectar una posible vulnerabilidad sobre un dispositivo, es importante evaluar el riesgo que genere una afectación del dispositivo para esta labor. Existen diversas técnicas que presentan sus respectivas medidas para llevar a cabo su ejecución, tales como las siguientes:

- ***Position Independent Executable* (Posición independiente de ejecutable)** : Esta opción de compilación genera un código que, al ejecutarse de forma independiente sobre la dirección absoluta de memoria previamente cargada, logra el direccionamiento relativo y evita el uso de referencias absolutas.
  La presente técnica posibilita la carga del binario en diversas direcciones de memoria, y cada vez saltarlo mediante rutas relativas y crear un código malicioso para salvaguardar la protección.
- **NX (*NoeXecute*)**: Esta técnica posibilita la aseguración de que el stack (área en la que se lleva a cabo el código) sea la ubicación donde se almacena los datos.
  El binario debe estar activado sobre el procesador para proteger y evitar la protección, insertando un código malicioso, lo que genera una persistencia para acceder al dispositivo.
- ***Stack Canaries***: Esta técnica busca sobrescribir los valores de compilador que se inserta la función que realiza solicitudes saltándose las protecciones

mediante un formato de cadenas y realizar lecturas en posiciones de memoria arbitrarias.

- **ASRL (Aleatorización del diseño del espacio de direcciones)**: Esta técnica se centrada en sistema operativo que es la encargada de habilitar las direcciones en el espacio de memoria. Cada vez que se ejecute un proceso el atacante aprovecha para identificar y explotar corrupciones a nivel de memoria.
- **Comprobación automática**: Esta técnica es un último recurso en caso de que no sea posible identificar vulnerabilidades sobre el *hardware* o *firmware*. Utilizando herramientas automáticas para un chequeo acerca de qué protecciones se encuentran habilitadas a nivel de binario en el dispositivo IoT.
- **Protección de evasión:** Para los dispositivos que se encuentran con una protección totalmente avanzado existen diferentes técnicas y herramientas las cuales burlan las protecciones sobre los ejecutables y a continuación se realizará la descripción de las más utilizadas actualmente:
- **Programación orientada al retorno**: Existen mecanismos de seguridad para evitar la ejecución remota. Utilizando técnicas de evasión para burlar esta protección identificando la falencia que sea capaz de explotar y acceder al dispositivo.
- **Fuga y ataques de fuerza bruta**: Este tipo de técnica permite detectar una vulnerabilidad en el formato de cadenas, para realizar un volcamiento del stack hasta encontrar un valor, ejecutar *buffer overflow* y saltar las protecciones. Posteriormente, efectuar un ataque de fuerza bruta contra el valor de protección que se encuentra en el *stack* hasta generar una colisión. Este procedimiento es arduo y diligente. Se aconseja llevar a cabo la tarea en un emulador.
- **SROP**: Más conocida por sus siglas, programación orientada a retornos que consiste en realizar una ejecución sobre *buffer overflow* sobrescribiendo el stack en el que se almacenan los estados, registros de retorno y la obtención de los registros.

  Esta técnica es capaz de simplificar exhaustivamente todos los registros y proporcionar un control completo del proceso de ejecución.

# 8. GUÍAS DE BUENAS PRACTICAS

Los datos sensibles y privados constituyen el activo más valioso para individuos naturales y entidades. En la actualidad, los dispositivos IoT almacenan información y se interconectan hacia la nube, lo que implica la administración, gestión, monitoreo de un área responsable, procedimientos, controles, actualizaciones, entre otros aspectos, entre otros.

De igual manera, existen organizaciones privadas, gubernamentales y sin ánimo de lucro, con personas expertas que proporcionan guías y herramientas para asegurar los dispositivos IoT.

## 8.1. INCIBE-CERT

Centro de respuesta sobre incidentes de seguridad que ocurran a ciudadanos, entidades públicas y privadas en España. Es el encargado de coordinar con los equipos de todo el país e internacional. Ha otorgado una mejora en la lucha contra los ciberdelitos y los sistemas de información en la seguridad pública. Han identificado las principales amenazas en estos dispositivos:

### 8.1.1. ACCESO FÍSICO

Se pretende realizar la exhibición de dispositivos IoT en exteriores sin ningún control o mecanismo que restringe el acceso no autorizado del dispositivo, lo que posibilita la hurto o destrucción del mismo, generando una amenaza baja.

### 8.1.2. ATAQUE DE AGUJERO DE GUSANO

Este tipo de ataque es uno de los más utilizados para manipular los datos y las aplicaciones en tiempo real, lo cual tiene un gran impacto en la tríada de la información.

Esta amenaza es muy alta debido a que, con frecuencia, los cibercriminales implementan puertas traseras para continuar con el acceso a estos dispositivos y

realizar un descubrimiento sobre servidores, switch y router que se encuentren en esa misma zona de red.

### 8.1.3. BLOQUEO DE RADIOFRECUENCIA (RF)

Los dispositivos de comunicación inalámbrica pueden ser bloqueados por sensores de radio que interfieren las comunicaciones inalámbricas de manera ilegal, lo que genera una amenaza media.

### 8.1.4. *BOTNET*

Este tipo de ataque fue uno de los más frecuentes en los últimos años, lo que permite acerca de la salvaguarda de la infraestructura necesaria para el hogar u oficina. Aprovechando para comprometer muchos dispositivos controlados de manera remota para que realicen muchas peticiones a un mismo objetivo, lo que permite un ataque de denegación de servicio clasificado como una amenaza media. Esto se debe a que hacer comprometido se convierte en una falla de seguridad.

### 8.1.5. HERRAMIENTAS EXTERNAS NO VERIFICABLES

La interfaz web de los dispositivos con medidas de seguridad insuficientes o bajas, que son fáciles de saltar, permite el control del dispositivo, lo que genera una amenaza alta.

### 8.1.6. INTERFACES DE ECOSISTEMAS INSEGURAS

Las interfaces web que se encuentran en el ámbito *Backend*, conocida como la arquitectura del diseño web o aplicación móvil, y servicios sobre la nube, son frecuentemente desaprobadas, lo que posibilita a los atacantes comprometer el dispositivo y sus componentes mediante las interfaces o paneles de administración, generando una amenaza baja/media.

### 8.1.7. *Firmware* y componentes desactualizados

Los dispositivos de comunicación digital de las cosas carecen de regulación, por lo que cada fabricante implementa su sistema. Diversos expertos han constatado que los dispositivos de firmware carecen de la verificación adecuada en cuanto a la criptografía. Por consiguiente, es posible que un atacante aproveche esta falta para acceder al sistema con privilegios altos y se asigne como una amenaza baja.

### 8.1.8. FUERZA BRUTA

Este es uno de los ataques más frecuentes en los dispositivos IoT, en los cuales los delincuentes intentan acceder a ellos mediante la utilización de contraseñas genéricas por defecto, con el fin de comprometer los dispositivos que se encuentran en el ámbito de la red, generando una amenaza media/alta.

### 8.1.9. FUGA DE DATOS Y/O VIOLACIÓN DE DATOS

Es posible que un usuario no autorizado implemente una puerta trasera, la información es extraída y se convierta en una amenaza crítica debido a que son datos sensibles.[49]

### 8.1.10. INUNDACIÓN DE SYN *FLOODING*

La técnica utilizada por los atacantes que llevan a cabo un ataque de denegación de servicio informático, mediante la utilización de millones de dispositivos tecnológicos, que generan repetidas consultas de diversas direcciones IPS falsas, sobrecargando e indisponiendo el sistema, lo que provoca una caída parcial o total de la plataforma tecnológica. Esta amenaza es calificada como baja.

### 8.1.11. MAL USO DE CONTRASEÑAS

La utilización de contraseñas no seguras, embebidas o que se encuentran defectuosas para todos los dispositivos, resulta efectiva para los delincuentes, quienes pueden acceder con privilegios elevados y realizar ajustes o configuraciones en las que pueden ejercer el control completo del dispositivo.

### 8.1.12. *MALWARE*

Se denomina a cualquier software malintencionado, aprovechándose de una falta en la que los ciberdelincuentes han diseñado un malicioso software, el cual infecta

[49] onasystems [Sitio web]. Bogotá: onasystems.net [consultado el 23 de septiembre del 2023] . Disponible en: https://www.onasystems.net/glosario-de-ciberseguridad/?dir=4&name_directory_startswith=F

el dispositivo y tiene la capacidad de propagarse sobre otros dispositivos, lo que genera una amenaza alta.

### 8.1.13. MANIPULACIÓN DE MEDICIONES

Se pretende tener en cuenta este tipo de ataque el servidor, basándose en la información almacenada y clasificada, ya comprometido, ejecutando órdenes incorrectas, lo que provoca una interrupción en el servicio, alertas de falsos positivos, lo que genera una amenaza media/alta.

### 8.1.14. PRIVACIDAD

Los atacantes tratan de acceder a los dispositivos, identificando la localización, la versión del dispositivo, los servicios innecesarios activos, los usuarios con privilegios altos, credenciales por defecto, bajo nivel de información y manejo de datos confidenciales, lo que genera una amenaza media/alta.

### 8.1.15. *RASONWARE OF THINGS* (ROT)

La aplicación de *software* malicioso, especialmente concebida para ocultar la información, se encuentra en una estrategia de secuestro específica, apoderarse del dispositivo y controlándolo por completo, dejando el dispositivo inoperativo con un mensaje de secuestro, solicitando que para ser utilizado debe efectuar un rescate, generalmente en criptomonedas, generando una amenaza alta.[50]

### 8.1.16. ROBO DE INFORMACIÓN

Es una de las amenazas más frecuentes en dispositivos en los que los ciberdelincuentes persiguen obtener información crítica o personal mediante diversas técnicas y la recopilación de datos confidenciales que se encuentran en el historial de navegación, datos confidenciales que se convierten en un valor monetario sobre la red oscura, generando una amenaza alta.

[50] incibe. [Sitio web]. Bogotá: incibe.es [consultado el 25 de septiembre del 2023] . Disponible en: https://www.incibe.es/ciudadania/blog/rot-ransomware-de-las-cosas-en-smarttvs

### 8.1.17. *SPAM*

Se presenta debido a las malas configuraciones en las que el puerto SMTP se encuentra habilitado, lo que permite administrar de manera remota y administración de remota, generando una red zombi que se encargan de enviar spam y otros softwares maliciosos, generando una amenaza media/alta.

### 8.1.18. RCE

Estas acciones se realizan de manera remota hacia un dispositivo de internet de las cosas, enviando paquetes maliciosos para obtener el control total, lo que genera una amenaza elevada.

#### 8.1.1.1. RECOMDENDACION DE BUENAS PRACTICAS INCIBE

A causa del arduo esfuerzo realizado por INCIBE, se ha convertido en un referente por su excelente labor, servicios, publicaciones y boletines de seguridad. Esta entidad lleva a cabo investigaciones sobre las diversas amenazas y riesgos que pueden surgir en el uso de los dispositivos IoT, y aconseja implementar las siguientes medidas de seguridad:

#### 8.1.1.2. ACTUALIZACIONES

Realizar actualizaciones periódicas sobre los dispositivos IoT, así como evaluar los servicios que sean innecesarios para desactivarlos.

#### 8.1.1.3. CONECTIVIDAD Y SERVICIOS

Se recomienda garantizar los puertos y servicios abiertos en los dispositivos IoT, integración con la infraestructura. Se debe establecer una política de cifrado en todas las plataformas de comunicación.

#### 8.1.1.4. CONTROL DE AUTENTICACIÓN Y AUTORIZACIÓN

Realizar la adopción de mecanismos seguros que establezcan conexiones entre dispositivos, servicios internos y externos.

#### 8.1.1.5. CONTRASEÑAS

Se debe realizar la implementación de contraseñas complejas mediante la utilización de letras mayúsculas y minúsculas, así como de símbolos, y se establece una política de modificación de credenciales para cada cierto.

#### 8.1.1.6. DISEÑO

Es imperativo tener en cuenta que todos los componentes, tanto hardware como software, tengan la capacidad de contar con los elementos fundamentales en cuanto a la privacidad.

#### 8.1.1.7. EVALUACIONES DE IMPACTO

Este punto se centra en los proveedores y desarrolladores, en los que es importante realizar evaluaciones sobre la privacidad (EIP) antes de lanzar cualquier aplicación IoT.

#### 8.1.1.8. INSTALACIÓN Y CONFIGURACIÓN

Implementar una lista de aseguramiento en la que se verifique la instalación, configuración de los dispositivos IoT y modificación de ajustes de seguridad previamente establecidos.

#### 8.1.1.9. OBLIGACIONES SOBRE LOS PROVEEDORES

Es fundamental asegurar que los dispositivos ofrecidos por terceros estén actualizados y parecidos, con los protocolos estándares seguros, sin ningún tipo de vulnerabilidad explotada y soporte. Se debe verificar que el individuo no empleó contraseñas embebidas o quemadas en el código fuente.

#### 8.1.1.10. PRIVACIDAD

Se sugiere la implementación de medidas de protección en los dispositivos IoT, a fin de que la información sea almacenada de manera privada y confidencial mediante un cifrado de extremo a extremo, y al ser interceptado, se requiere la interpretación de esta información mediante un conversor y políticas para la destrucción segura de datos.

#### 8.1.1.11. RASTREO DE UBICACIÓN

Este asunto se centra en los fabricantes, a fin de evitar rastrear la ubicación, a fin de evitar la utilización de huellas digitales y la identificación de las interfaces inalámbricas. Se aconseja emplear identificadores aleatorios y direcciones MAC con el fin de prevenir la identificación y rastreo de la ubicación.

## 8.2. CCN-CERT

En virtud de su identidad, el Centro criptológico Nacional, entidad gubernamental nacional de España, fue concebido en 2006 como una entidad gubernamental nacional de España. La finalidad primordial de esta entidad consiste en contribuir a la mejora de la ciberseguridad, vigilar, notificar y colaborar en la solución rápida y eficiente de los ciberataques.[51]

### 8.2.1. RELACIÓN CON LA NUBE

En la actualidad, un número considerable de dispositivos están conectados en la red, y cada vez más la tecnología IoT se encuentra interconectada para llevar a cabo actividades de uso común. Por consiguiente, es fundamental asegurar los servicios que se ofrecen, los datos que se almacenan allí y se distribuyen, proteger la privacidad al recopilar la información y los metadatos que se encuentran en él. [52]

Los dispositivos del Internet de las cosas se convertirán en una enorme red abierta para entidades y objetos virtuales que interactúan entre sí a través de un entorno

---

[51] ccn-cert [Sitio web]. Bogotá: ccn-cert.cni.es [consultado el 23 de septiembre del 2023] . Disponible en: https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html

[52] forum.huawei. [Sitio web]. Bogotá: forum.huawei.com. [consultado el 24 de septiembre del 2023] . Disponible en: https://forum.huawei.com/enterprise/es/La-computaci%C3%B3n-en-la-nube-y-su-relaci%C3%B3n-con-el-Internet-de-las-Cosas/thread/667224498274975744-667212887476809728

en el futuro. Las organizaciones establecerán políticas de gestión y riesgos para aplicar a los dispositivos que están interconectados.

La nube en la que se encuentran todos los servicios de respaldo, monitoreo y control de usuarios de manera remota mediante aplicaciones móviles y portales webs. Es de suma importancia que el producto proporcionado por un proveedor de servicio dispone de diversas fases de desarrollo y se puede verificar la seguridad de su interfaz de la siguiente manera:

- Se deben identificar los valores debido a la carencia de credenciales de acceso, para que puedan ser modificados posteriormente durante el proceso de instalación del producto.
- Realizar diversas verificaciones en las cuales se pueden detectar después de los intentos de bloquear el acceso al dispositivo.
- Asegurarse de la resistencia de la interfaz web.
- Se requiere llevar a cabo una validación acerca de los servicios que se comunican con la nube para cualquier posible vulnerabilidad que se pueda presentar en la interfaz del sistema de la nube.
- Se requiere llevar a cabo una validación acerca de la exposición de las credenciales como token de acceso que no se encuentren expuestos en el sitio web, y se aconseja utilizar siempre conexiones cifradas con autenticación SSL.
- Se recomienda que se realice una autenticación mediante 2 factores.
- Se sugiere la implementación de técnicas que detecten y bloqueen las solicitudes o intentos anómalos que se hayan efectuado, lo que permitirá la ejecución del dispositivo de manera no autorizada.

### 8.2.2. INFRAESTRUCTURAS CRITICAS

En los últimos años, la tecnología industrial y la IoT han estado presentes en cada uno de los sistemas de control industrial (ICS) y los sistemas de control distribuidos (DCS).[53]

[53] ccn-cert.cni. [Sitio web]. Bogotá: ccn-cert.cni.es. [consultado el 24 de septiembre del 2023] . Disponible en: https://www.ccn-cert.cni.es/ca/gestion-de-incidentes/lucia/23-noticias/535-infraestructuras-criticas-contenidos-minimos-de-los-pso-y-ppe.html

Los sistemas industriales reciben una gran cantidad de datos en las estaciones remotas y esto se genera de forma automática mediante acciones ejecutivas que se envían a los dispositivos. [54]

Los artefactos han sido utilizados para llevar a cabo tareas como abrir, cerrar válvulas, frenar, quitar, recoger información que se encuentra en los sensores para supervisar el entorno y establecer alarmas, entre otros.

### 8.2.3. VISIBILIDAD EN INTERNET

Internet cada día cuenta con más herramientas de alcance y una de ellas es los famosos buscadores, los cuales permiten identificar dispositivos IoT que están conectados directamente a internet, por lo cual se ha evidenciado puertos por defecto sin algún tipo de seguridad o utilizando credenciales por defecto de diferentes organizaciones que prestan servicios de medicina, telemedicina dispositivos industriales, que los atacantes han vulnerado.

El CCN-CERT ha identificado las diferentes fases para vulnerar dispositivos que se enumeran a continuación:

- El atacante, al localizar los dispositivos en la red, busca la manera de automatizar búsquedas para acceder a administrarlos remotamente con el objetivo de realizar actividades ilícitas.
- Es factible identificar los diversos dispositivos que se encuentran bajo la responsabilidad de una misma red, tales como botnet, que a su vez son conformados por *bots*.
- El individuo que accede a un dispositivo frecuentemente lleva a cabo la instalación de software malintencionado o dañino con el fin de tener un control y lanzar instrucciones simultáneas sobre los dispositivos infectados que actúen coordinadamente hacia un mismo propósito.

[54] incibe [Sitio web]. Bogotá: incibe.es. [consultado el 20 de septiembre del 2023] . Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

- Uno de los ataques más utilizados en los últimos años es la denegación de servicio, que se realiza de manera masiva y simultánea desde diferentes nodos, impidiendo un sitio en particular. Una de las razones por las que se hacen estas acciones es por temas políticos, activistas o extorsión.
- Los dispositivos IoT que se encuentran más alineados en la mayoría de las grabaciones de video y cámaras IP.

### 8.2.4. RECOMENDACIONES

Es de suma importancia informar a todas las entidades acerca de la necesidad de asegurar los dispositivos IoT mediante la implementación de las siguientes medidas:

- Realizar un cambio de la contraseña por una robusta y segura.
- Implementar opciones de cifrado.
- Si es posible, solo se conecta a un dispositivo en el que se pueda administrar los mismos.
- Se requiere activar las medidas de seguridad que se han implementado en el dispositivo IoT.
- Se requiere separar los archivos de administración de los usuarios habituales.
- Establecer controles de acceso para garantizar la conectividad entre los dispositivos IoT.
- Se requiere la utilización de elementos que permitan la separación de la red de dispositivos IoT en el resto del ámbito digital.
- Desactivar cualquier servicio que se considere que no es usado.
- Habilitar el registro de eventos de seguridad.
- Se aconseja activar alertas notificaciones para todos los usuarios en la actualidad en relación con la seguridad del dispositivo IoT.
- Cifrar los datos que se encuentran tanto en el dispositivo como en los que se transmiten.
- Contar con un registro de eventos de seguridad.
- Se debe llevar a cabo un seguro físico en el cual se garantice que solo individuos debidamente autorizados puedan acceder al mismo.
- Desactivar los puertos físicos que sean innecesarios y que no afecten el funcionamiento del dispositivo.

En la Ilustración 15 ccn-cert.cn se recomienda llevar a cabo ciertas acciones para la instalación de dispositivos IoT.

**Ilustración 15. Decálogo de Seguridad para Instalaciones IoT**

| | Decálogo de Seguridad para Instalaciones IoT |
|---|---|
| 1 | Evitar utilizar dispositivos IoT siempre que no sean estrictamente necesarios. |
| 2 | No utilizar, en la medida de lo posible, aquellos dispositivos IoT que transmiten información a servidores externos (la Nube), incluso si son los del fabricante. |
| 3 | Cambiar las contraseñas por defecto de los dispositivos y utilizar contraseñas realmente robustas, que no estén en ningún diccionario, que sean suficientemente largas y por tanto difíciles de adivinar. |
| 4 | Mantener actualizados los dispositivos con las últimas versiones disponibles de software y firmware. |
| 5 | Desactivar toda conectividad remota (con Internet) de los dispositivos cuando no sea estrictamente necesaria. |
| 6 | Mantener abiertos solo aquellos puertos de comunicación que sean realmente necesarios y modificar los puertos de escucha si es posible. |
| 7 | Si los dispositivos IoT no permiten la configuración de su seguridad, operar con ellos siempre en una red de área local (LAN) detrás de un dispositivo (enrutador) correctamente configurado que sí provea esa seguridad. |
| 8 | En la medida de lo posible, asegurar la autenticidad, confidencialidad e integridad en todas las comunicaciones locales (LAN), especialmente si estas se realizan por enlaces radio (Wi-Fi, Bluetooth, etc.). |
| 9 | Comprobar periódicamente y sin previo aviso, la configuración de seguridad de todos los elementos de la arquitectura IoT y de sus dispositivos de comunicación con el exterior. |
| 10 | Comprobar la visibilidad de los dispositivos propios en buscadores de dispositivos IoT como Shodan. |

Fuente: ccn-cert.cni, ccn-cert.cni.es. comunicados ccn cert. [En línea]. 2021. [Consultado el 23 de septiembre de 2023]. Disponible en internet: ttps://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/4691-publicado-el-ccn-cert-bp-05-16-en-la-parte-publica-de-su-portal.html

## 8.3. NIST

Se trata de un instituto fundado en Estados Unidos que permite a los negocios comprender y analizar los riesgos de seguridad que se encuentran en su plataforma e infraestructura. [55]

[55] ftc.gov [Sitio web]. Bogotá: ftc.gov.es [consultado el 23 de septiembre del 2023] . Disponible en: https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Este marco se lleva a cabo de forma voluntaria y brinda una metodología de lo que esa organización considera como guía de buenas prácticas o referente al implementar normas y recursos para la protección de ciberseguridad.

Este tipo de dispositivos poseen una habilidad de seguridad o funciones que se sustentan en sus recursos hardware y poseen una referencia fundamental. Por consiguiente, es necesario reforzar los controles y medidas para preservarlos.

Mediante el informe interinstitucional o interno 8259, se presentan actividades fundamentales de ciberseguridad para los fabricantes de dispositivos de internet, a través de las cuales se proporcionan herramientas de aseguramiento de los mismos.

Las organizaciones deben tener en cuenta la capacidad de los dispositivos, ya que son el punto de partida que permite establecer las medidas a nivel de seguridad, privacidad y mitigación de los riesgos. En este contexto, el informe interinstitucional interno 8228 emitidos por NIST se enfoca en la atención de cubrir todas las principales amenazas ciberseguridad en los dispositivos IoT, tal como se ilustra de manera resumida la Ilustración 16.

**Ilustración 16. Áreas de mitigación de riesgos basado en 8228 del NIST**


Fuente: ftc.gov, ftc.gov.es guía para negocios [En línea]. 2022. [consultado el 23 de septiembre del 2023] . Disponible en:https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

### 8.3.1. BÁSICAS SOBRE LAS CAPACIDADES DE CIBERSEGURIDAD EN LOS DISPOSITIVOS IOT

A través de una tabla con referencias sobre las capacidades de ciberseguridad para los dispositivos IoT, en las que se encuentran normas o parámetros predeterminados, se protege de manera mínima cualquiera de estos La presente tabla proporciona una tabla que permite que las entidades puedan adquirir una guía que se adapte a sus necesidades. Según el informe interinstitucional o interno 8259 de NIST, se describe que los fabricantes deben establecer diferentes mecanismos, elementos, arquitectura de seguridad, boletines de actualización y aseguramiento sobre los dispositivos IoT.

- En la primera columna se especifica la capacidad en cuanto a las áreas de mitigación y problemas que se encuentran en el informe interinstitucional o interno 8228 del NIST, que se encuentran puntualmente en consideración para la gestión de riesgos en ciberseguridad y privacidad en internet de las cosas.
- En la segunda columna se presenta una lista de diferentes elementos comunes que tienen la capacidad de identificar elementos relevantes para ser una referencia.
- La tercera columna presenta de manera exhaustiva la necesidad de incluir la capacidad y los elementos habituales que se encuentran en los dispositivos de internet de las cosas, tomando una referencia básica.
- En la última columna se hace referencia a la plataforma digital de las actividades que posibilitan la protección de la ciberseguridad de los individuos, y se especifican las capacidades que presentan similitud, empleando conceptos fundamentales y herramientas para conocer cada uno de ellos, detallando y otorgando una identificación precisa de las características más apropiadas para implementarlos.

### 8.3.2. AGELIGHT (GRUPO ASESOR DE CONFIANZA DIGITAL)

La organización ofrece una arquitectura segura y un conjunto de herramientas para evitar el riesgo en dispositivos de la red de las cosas, versión 3.1.

### 8.3.3. BITAG (GRUPO ASESOR TÉCNICO DE INTERNET DE BANDA ANCHA)

La organización en cuestión tiene una posición acerca de la recomendación para garantizar la seguridad y privacidad del dispositivo electrónico de IoT.

### 8.3.4. CSDE (CONSEJO PARA ASEGURAR LA ECONOMÍA DIGITAL)

El Consejo encargado de establecer un consenso acerca de las referencias necesarias para asegurar los dispositivos IoT.

### 8.3.5. CTIA (ASOCIACIÓN DE COMUNICACIÓN ALÁMBRICA)

Asociación que elaboró un plan de prueba para certificar la ciberseguridad en los dispositivos IoT.

### 8.3.6. ENISA (AGENCIA EUROPEA DE SEGURIDAD SOBRE RED E INFORMACIÓN)

Agencia encargada de proporcionar recomendaciones de referencia para la seguridad en internet de las cosas puntualmente en infraestructura de información crítica.

### 8.3.7. ETSI (INSTITUTO EUROPEO DE NORMAS DE TELECOMUNICACIONES)

Instituto de ciberseguridad para el internet de las cosas y los consumidores.

### 8.3.8. IEC (COMISIÓN ELECTRÓNICA INTERNACIONAL)

La Comisión encargada de proveer sistemas de automatización y control industrial.

### 8.3.9. IIC

Se trata de un consorcio de internet industrial especializado en la industria del internet de las cosas, a través de un framework o marco de seguridad.

### 8.3.10. IOTSF (FUNDACIÓN DE LA SEGURIDAD IOT)

El marco de aplicación para garantizar la seguridad en el dispositivo móvil de IoT.

### 8.3.11. ISOC/OTA (SOCIEDAD DE INTERNET ALIANZA DE CONFIANZA EN LÍNEA)

La sociedad ofrece un refugio de confianza en la seguridad y la privacidad de los dispositivos IoT.

### 8.3.12. NEMA (ASOCIACIÓN NACIONAL DE FABRICANTES ELÉCTRICOS)

La Asociación nacional propone las mejores prácticas de ciberseguridad.

### 8.3.13. OCF (FUNDACIÓN DE CONECTIVIDAD ABIERTA)

Proporciona especificaciones de seguridad en lo que respecta a la conectividad.

### 8.3.14. PSA

Plataforma de arquitectura en seguridad.

**Tabla 1. Referencia básica sobre el aspecto de ciberseguridad para los dispositivos IoT**

| Capacidad de seguridad de dispositivo | Elementos comunes | Explicación | Ejemplo de referencias sobre dispositivos de internet de las cosas IoT |
|---|---|---|---|
| Se brinda la oportunidad de identificar e identificar un dispositivo IoT, así como sus componentes físicos y lógicos. | 1. Un único identificador lógico.<br><br>2. El identificador físico único, que se encuentre ubicado de manera externa o interna, y que solo se permita el acceso a entidades autorizadas.<br><br>Los identificadores tanto lógicos como físicos se representan un valor. | Es esencial contar con la habilidad de colaborar en la gestión de los recursos, lo que posibilita la administración de conocimientos específicos como accesos que protegen los datos y detectar incidentes.<br><br>El identificador lógico único puede ser utilizado para identificar el dispositivo, especialmente los demás, y para gestionar y vigilar de manera automatizada todos los dispositivos.<br><br>Se dispone de la habilidad de detectar un dispositivo IoT mediante sus atributos, | • **CSA:** 1<br>• **CSDE:** 5.1.1<br>• **CTIA:** 4.13<br>• **ENISA:** GP-PS-10<br>• **GSMA:** CLP13_6.6.2, 6.8.1, 6.20.1<br>• **IEC:** CR 1.2<br>• **IIC:** 7.3, 8.5, 11.7, 11.8<br>• **IoTSF:** 2.4.8.1, 2.4.14.3, 2.4.14.4<br>• **OCF:** 7.1.1<br>• **PSA:** C1.4, R2.1 |

| | | | |
|---|---|---|---|
| | | y determinar posibles riesgos.<br><br>Se debe garantizar la protección del uso y la gestión de los mismos. | |
| La configuración del dispositivo en cuestión en el ámbito software del dispositivo IoT puede ser modificada únicamente por entidades autorizadas. | 1. Disponer de la capacidad de modificar y configurar el software en el dispositivo.<br><br>2. Es imperativo que solo entidades autorizadas hagan cambios en la configuración.<br><br>3. Tener la capacidad de que solo entidades autorizadas puedan restaurar la configuración del dispositivo. | La capacidad de que solo el personal autorizado efectúe modificaciones posibilita la optimización de la gestión de accesos, la administración de vulnerabilidades, así como la protección de datos y la detección de intrusos.<br><br>Es factible que la entidad autorizada efectúe modificaciones y configuraciones en el dispositivo debido a diversas razones, entre las cuales se encuentran la privacidad y la facilidad de uso. Esto debe ser autorizado y documentado para posteriormente llevar a cabo una bitácora de cambios.<br>La capacidad para realizar actividades de ciberseguridad depende de ciertas medidas de protección y una persona responsable o un área que permita garantizar qué esta actividad se realiza.<br><br>Al establecer un control de acceso, es | • **BITAG:** 7.1<br>• **CSA:** 22<br>• **ENISA:** GP-TM-06<br>• **IEC:** CR 7.4, CR 7.6<br>• **IIC:** 7.3, 7.6, 8.10, 11.5<br>• **IoTSF:** 2.4.8.17, 2.4.15<br>• **ISOC/OTA:** 26<br>• **OCF:** 5.3.3, 8.2, 12, 13.3.1<br>• **PSA:** C2.3, R6.1, R7.1 |

| | | | |
|---|---|---|---|
| | | posible que otras personas intenten acceder y, por consiguiente, se debe llevar a cabo un procedimiento o manera de vigilar y monitorear los docks de acceso e intentos fallidos.<br><br>El dispositivo debe poseer la habilidad de restaurar de manera segura, proporcionando una copia para prevenir errores o perjuicios. | |
| La protección de datos en dispositivos de IoT posibilita la preservación de la información que se almacena y transmite, además de la seguridad en el acceso a modificaciones no autorizadas. | 1. Es imperativo que se utilicen módulos criptográficos seguros y algoritmos criptográficos estándares que permitan validar las firmas digitales, con el fin de prevenir la confiabilidad, la integridad de los datos almacenados en el dispositivo y la transmisión de los mismos.<br><br>2. Es esencial que las entidades autorizadas lleven a cabo un control del número de solicitudes o accesos no autorizados mediante la eliminación de claves criptográficas para los datos cifrados, entre otros procedimientos. | Contribuir en la gestión del acceso con el fin de garantizar la protección de datos y la identificación de posibles irregularidades.<br><br>Al llevar a cabo la implementación del acceso a entidades autorizadas, se requiere la vigilancia y registro de la eliminación de entidades no autorizadas o que han sido retiradas.<br><br>Las entidades autorizadas para preservar la integridad de los datos y prevenir la alteración o pérdida de ellos. | • **AGELIGHT:** 5, 7, 18, 24, 25, 34<br>• **BITAG:** 7.2, 7.10<br>• **CSDE:** 5.1.3, 5.1.4, 5.1.5, 5.1.8, 5.1.10<br>• **CTIA:** 4.8, 5.14, 5.15<br>• **ENISA:** GP-OP-04, GP-TM-02, GP-TM-04, GP-TM-14, GP-TM-24, GP-TM-32, GP-TM-34, GP-TM-35, GP-TM-39, GP-TM-40<br>• **ETSI:** 4.4-1, 4.5-1, 4.5-2, 4.11-1, 4.11-2, 4.11-3<br>• **GSMA:** CLP13_6.4.1.1, 6.11, 6.12.1.1, 6.19, 7.6.1, 8.10.1.1, 8.11.1<br>• **IEC:** CR 3.1, CR 3.4, CR 4.1, CR 4.2, CR 4.3 |

| | | | |
|---|---|---|---|
| | 3. En las opciones de configuración, es factible que las personas autorizadas proporcionen una gráfica y una longitud de clave robusta, además de ser renovadas cada cierto tiempo. | | • **IIC:** 7.3, 7.4, 7.6, 7.7, 8.8, 8.11, 8.13, 9.1, 10.4, 11.9<br>• **IoTSF:** 2.4.6.5, 2.4.7, 2.4.8.8, 2.4.8.16, 2.4.9, 2.4.12.2, 2.4.16.1, 2.4.16.2<br>• **ISOC/OTA:** 2, 17, 33<br>• **OCF:** 8.2, 11.2.1, 11.3, 14.2.2<br>• **PSA: C1.1, C1.4, C2.4, D5.2, R2.2, R2.3, R6.1, R7.1** |
| El acceso lógico al interfaz del dispositivo IoT debe limitarse tanto a las interfaces locales como a nivel de red, así como a los protocolos y servicios que son utilizados por usuarios autorizados. | 1. La habilidad de evitar de manera lógica o física cualquier acceso que no sea necesario o limitado por defecto para el dispositivo.<br><br>2. Es imperativo que se pueda limitar lógicamente el acceso a cada uno de los puertos y servicios, así como también implementar la autenticación a los usuarios y dispositivos mediante un cifrado.<br><br>3. Mediante la alternativa de configuración, se procederá a asegurar el acceso no autorizado a los servicios y a evitar la entrada no autorizada. | Para gestionar y administrar las vulnerabilidades, el acceso y la protección de datos son importantes para implementar y asegurar los dispositivos de IoT.<br><br>Al eliminar el acceso a las interfaces de red, se reduce la superficie de ataque sobre el dispositivo, además de limitar a los atacantes debido a que pueden identificar el dispositivo. Sin embargo, no pueden acceder debido a que se tiene un control de acceso que permite identificar el número de atacantes y reducir la posibilidad de comprometer el mismo. | • **AGELIGHT:** 10, 13, 14, 15, 16, 19<br>• **BITAG:** 7.1, 7.2, 7.3, 7.6<br>• **CSA:** 2, 4, 20<br>• **CSDE:** 5.1.2<br>• **CTIA:** 3.2, 3.3, 3.4, 4.2, 4.3, 4.9, 5.2<br>• **ENISA:** GP-TM-08, GP-TM-09, GP-TM-21, GP-TM-22, GP-TM-25, GP-TM-27, GP-TM-29, GP-TM-33, GP-TM-42, GP-TM-44, GP-TM-45<br>• **ETSI:** 4.1-1, 4.4-1, 4.6-1, 4.6-2<br>• **GSMA:** CLP13_6.9.1, 6.12.1, 6.20.1, 7.6.1, 8.2.1, 8.4.1<br>• **IEC:** CR 1.1, CR 1.2, CR 1.5, |

| | | | |
|---|---|---|---|
| | | La implementación de restricciones parciales con relación a los dispositivos posibilita la gestión de los usuarios que utilizan o consumen este recurso, lo que posibilita la identificación de cualquier tráfico inadecuado o anormal. | CR 1.7, CR 1.11, CR 2.1,<br>CR 2.2, CR 2.13, CR 7.7,<br>EDR 2.1**3**<br>• **IIC:** 7.3, 7.4, 8.3, 8.6, 11.7<br>• **IoTSF:** 2.4.4.5, 2.4.4.9,<br>2.4.5.5, 2.4.6.3, 2.4.6.4,<br>2.4.7, 2.4.8<br>• **ISOC/OTA:** 3, 12, 13, 14, 15,<br>16<br>• **NEMA:** Segmentación de redes, gestión de usuarios,<br>dispositivos de endurecimiento<br>• **OCF:** 5.1, 5.2, 10, 12<br>• **PSA:** C2.3, D2.1, D2.2, D2.3,<br>D2.4, D3.1 D3.3, R3.1, R3.2,<br>R3.3, R4.2, R4.5 R6.1 |
| El proceso de actualización de software solo puede ser llevado a cabo por el administrador, además de disponer de una política de actualización. | 1. Establecer políticas de seguridad que permitan realizar la actualización de los dispositivos de manera segura y que garanticen la disponibilidad del mismo.<br><br>2. Se requiere llevar a cabo una evaluación del dispositivo antes de efectuar cualquier modificación o actualización.<br><br>3. Se debe establecer una política | Las actualizaciones permiten eliminar las vulnerabilidades que se presentan en un dispositivo y disminuir la probabilidad de riesgo.<br><br>Las actualizaciones permiten corregir los bugs que se presentan al implementar nuevos sistemas o actualizar servicios mejorando la disponibilidad y el rendimiento del dispositivo | • **AGELIGHT:** 1, 2, 4<br>• **BITAG:** 7.1<br>• **CSDE:** 5.1.9<br>• **CTIA:** 3.5, 3.6, 4.5, 4.6, 5.5,<br>5.6<br>• **ENISA:** GP-TM-05, GP-TM-<br>06, GP-TM-18, GP-TM-19<br>• **ETSI:** 4.3-1, 4.3-2, 4.3-7<br>• **GSMA:** 7.5.1<br>• **IEC:** CR 3.4, EDR 3.10<br>• **IIC: 7.3,** 11.5.1<br>• **IoTSF: 2**.4.5.1, 2.4.5.2, |

| | | | |
|---|---|---|---|
| | en la cual se lleva a cabo un control y un método para reparar los cambios en la versión de software del dispositivo.<br><br>4. Se requiere limitar la aplicación de actualizaciones y la utilización de servicios por parte de individuos no autorizados.<br><br>5. Disponer de la opción de habilitar o deshabilitar las autorizaciones que se puedan realizar sobre el dispositivo.<br><br>6. Implementar o mejorar la capacidad de llevar a cabo actualizaciones de manera remota, activar las notificaciones cuando se presenten las actualizaciones disponibles. | Implementar medidas de seguridad que permitan satisfacer la necesidad de ciberseguridad en la organización y puntualmente sobre las actualizaciones en los dispositivos<br><br>Implementar o manejar medidas de seguridad para los dispositivos que se encuentran sin soporte o que serán administrados por terceros. | 2.4.5.3, 2.4.5.4, 2.4.5.8, 2.4.6.1<br>• **ISOC/OTA:** 1, 6, 8<br>• **NEMA:** Actualización de dispositivos<br>• **OCF:** 14.5<br>• **PSA:** C2.1, C2.2, R1.1, R1.2, R6.1 |
| Es esencial que se adopten medidas que permitan ocultar la información acerca de los dispositivos, ya que existe menos información. | 1. Implementar técnicas que limiten el acceso al dispositivo.<br><br>2. Se sugiere que el acceso a estos dispositivos sea exclusivamente destinado a individuos debidamente autorizados.<br><br>3. Se requiere la existencia de dispositivos de | Identificar los servicios y versión de los dispositivos que permitan asegurar la disponibilidad de los mismos y, a nivel de ciberseguridad, controlar los riesgos.<br><br>Se requiere activar los registros y acontecimientos que se encuentran registrados en el dispositivo, lo que | • **CSDE:** 5.1.7<br>• **CTIA:** 4.7, 4.12, 5.7, 5.16<br>• **ENISA:** GP-TM-55, GP-TM-56<br>• **ETSI:** 4.7-2, 4.10-1<br>• **GSMA:** CLP13_6.13.1, 7.2.1, 9.1.1.2<br>• **IEC:** CR 2.8, CR 3.9, CR 6.1, CR 6.2<br>• **IIC:** 7.3, 7.5, 7.7, 8.9, 10.3, |

| | | | |
|---|---|---|---|
| | monitoreo que permitan la vigilancia del desempeño y el estado actual de los servicios. | facilita la toma de decisiones y la identificación de atacantes que se encuentren en la red. | 10.4<br>• **IoTSF:** 2.4.7.5<br>• **NEMA:** Dispositivos y sistemas de vigilancia<br>• **OCF:** 5.1, 5.7, 8.6, 12, 13.8, 13.16<br>• **PSA:** C1.3, D1.1, D3.2, D3.4, D3.5, D5.1, R4.1, R4.3, R4.4 |

Fuente propia

# 9. LEGISLACIÓN ACTUAL AMERICA Y COLOMBIA SOBRE TECNOLOGIA IOT

La evolución tecnológica enfrenta desafíos para los diversos continentes y naciones, y ha diseñado estrategias para incorporar esta tecnología en sus procesos, así como regularla y articularla en todos los sectores.

Sin embargo, en California, en 2017 se presentó un proyecto para proteger la información y privada en los dispositivos IoT. Al realizar un tratamiento legislativo y después de 3 lecturas obligatorias. La presente ley fue promulgada por el gobierno de Jerry Brown, y se convirtió en una ley sobre el título de Security of Connected Devices.

Se ha establecido que los dispositivos como computadoras y portátiles, microondas, refrigeradores, juguetes, relojes inteligentes, cámaras, sensores que están conectados a internet.

Al realizar una compra de dispositivos debido a sus grandes ventajas, muchos de ellos no han sido informados sobre las consecuencias de la adquisición de estos. La mayoría de los individuos carecen de capacidades de seguridad fundamentales, lo que les convierte en vulnerables para ataques cibernéticos dirigidos. Por consiguiente, la legislación establece un requisito de seguridad que obliga al fabricante a optimizar el producto.

Esta ley obliga a los fabricantes a diseñar el dispositivo con conexión e indicaciones visuales, auditivas sobre la información recopilada y la aprobación o consentimiento del usuario, así como también notificar cualquier actualización o parche de seguridad.

El código civil de califórnica, puntualmente Sección 1708.8, establece que el individuo es responsable de la invasión de la privacidad al intentar capturar de manera ofensiva cualquier tipo de imagen o grabación de una persona sin su autorización previa.

Con relación a la sección 1798.81.5 b, es imperativo que cualquier organización adquiera una autorización que permita mantener la información personal acerca de los residentes de califórnica, con el fin de implementar, mantener e implementar los procedimientos y prácticas de seguridad adecuadas. Para proteger la información personal, el acceso no autorizado a la destrucción o modificación de la información.

De acuerdo con el código de negocios y profesionales en califórnica, la Sección 22948.20 establece que una persona y/o entidad no debe proporcionar una función de reconocimiento de voz sin ser informada. En consecuencia, cualquier grabación que se recopile mediante una función de reconocimiento de voz realizada por el fabricante con el propósito de mejorar esta función, no será vendido ni utilizada con fines publicitarios. [56]

En el Código penal en relación con la sección 637.5(a)(1) se establece que ninguna persona que opera y/o administra una compañía de televisión satelital y ofrece este servicio, utilice cualquier tipo de dispositivo electrónico para grabar, transmitir o registre y supervisar alguna conversación dentro de una residencia o lugar de trabajo del suscriptor sin previo aviso alguno.

La investigación llevada a cabo en califórnica sobre el internet de las cosas se ha destacado que en la actualidad existen diversos dispositivos para el hogar, juguetes y automóviles que se encuentran conectados a internet y recopilan una gran cantidad de información personal sensible. La falta de garantía adecuada de esta gran cantidad de información privada tiende a ser vulnerable por los ciberdelincuentes.

La ley, previamente mencionada, se integró al código civil de califórnica en la división de tres partes cuatro, las cuales son obligaciones derivadas de transición de particulares, bajo el título de seguridad de los dispositivos conectados.

[56] scielo.br. [Sitio web]. Bogotá: scielo.br. [consultado el 9 de abril de 2023]. Disponible en: https://www.scielo.br/j/rdgv/a/NBksbsTGzh38X5NDLsWNntq/?format=html .

Se descarta que en el ámbito de la aplicación se puedan presentar efectos extraterritoriales, ya que todos los fabricantes de estos artículos que realicen las ventas en califórnica, aunque su fabricación sea fuera del estado, deben cumplir con estándares de ciberseguridad para los dispositivos conectados hacia internet, tales como automóviles, cámaras web, drones, robots, sensores, termostatos, entre otros, bajo el título 1798.91.04 (a).[57]

Se solicita a los fabricantes de tecnología IoT que efectúan la comercialización de productos en califórnica, que añadan características de seguridad diseñadas para prevenir la intrusión o el acceso arbitrario al dispositivo, y que cumplan con las siguientes características:

- Es necesario cumplir con las características previamente expuestas y las funcionalidades necesarias.
- Es necesario efectuar una adaptación de la información al ser recopilada, contenida y transmitida, así como al realizar la transmisión de dicha información.
- Debe contar con sistemas de protección sobre la información que se encuentra en el mismo y un uso o tratamiento para la destrucción uso modificación y/o divulgación sin ser autorizada.

A continuación, se presenta el apartado b, el cual establece una exigencia que todo dispositivo conectado mediante una red local se convierte en un medio de comunicación o una característica de seguridad, y que debe cumplir con los siguientes requisitos:

- Se debe utilizar una contraseña única y programada por cada dispositivo que sea fabricado.
- El dispositivo deberá contar con una función de seguridad en la que se requiere un usuario y la creación de un nuevo método de autenticación al ingresar por primera vez.
- La autenticación es un método de verificación de la autoridad de un usuario, así como el proceso y el dispositivo que permiten acceder a los recursos de un sistema.

[57] scielo.br. [Sitio web]. Bogotá: scielo.br. [consultado el 9 de abril de 2023]. Disponible en: https://www.scielo.br/j/rdgv/a/NBksbsTGzh38X5NDLsWNntq/?format=html

- Se trata de un dispositivo conectado que permite conectarse directa o indirectamente a internet y que tenga una dirección establecida.
- La función de seguridad se refiere a una característica que debe proporcionar seguridad a un dispositivo.
- Se establecen medidas para la eliminación, desactivación, aplicación, modificación y difusión no autorizada por el consumidor.

El artículo 1798.91.06 (a) establece exclusiones o excepciones que se aplican sobre los artículos anteriores:

- Los fabricantes están eximidos de cualquier obligación para proteger el software que se ha instalado por el usuario.
- Es importante señalar que el dispositivo es controlado por un usuario y posee la habilidad de modificar el software o el firmware.
- Los deberes y obligaciones de impuestos son compuestos con cualquier otro deber y obligación impuesta en virtud de la legislación, y no deben ser eximidos a ninguna obligación impuesta.
- La ley establecida limitada a una agencia federal para obtener información sobre el dispositivo conectado de un fabricante en particular, de acuerdo con la ley o conformidad por orden de un tribunal de jurisdicción competente.
- Los proveedores de atención médica, plan de servicios, contratista empleador o cualquier otro actor que se encuentre o indirectamente basado en la ley federal de portabilidad y responsabilidad de seguros de la salud de 1996 o la ley de confidencialidad de información médica, no están sujetos a cualquier actividad regulada para estos actos.

El Estado de Califórnica se posiciona en la promulgación de leyes de privacidad y seguridad mediante la promulgación de la Ley de Privacidad del consumidor, la cual se ha estrenado en vigor desde el 01 de enero del año 2020 y tiene efectos extraterritoriales.[58]

[58] knowledgebase. [Sitio web]. Bogotá: knowledgebase.constantcontact.com. [consultado el 23 de septiembre del 2023] . Disponible en: https://knowledgebase.constantcontact.com/email-digital-marketing/articles/KnowledgeBase/36557-ley-de-privacidad-del-consumidor-de-California-CCPA?lang=es

## 8.1. CCPA (LEY DE PRIVACIDAD DEL CONSUMIDOR DE CALIFORNIA)

Se trata de un proyecto en el cual se establece que las empresas que se encuentran allí deben proteger la información personal de los consumidores.

La presente legislación contempla diversos aspectos políticos, tales como la protección de seguridad, los derechos del consumidor y establece que los consumidores poseen los siguientes derechos:

- El derecho a conocer exhaustivamente los datos que se han recopilado y la razón por la cual dichos datos son recopilados.
- El derecho de rechazar la transmisión de información a través de la comercialización de dicha información.
- Todos los derechos de que sus datos sean eliminados.
- El derecho a confirmar y solicitar previamente la autorización previa antes de la comercialización de información sobre menores de 16 años.
- El derecho a adquirir conocimiento acerca del intercambio de información a terceros.

Las solicitudes de los consumidores deben ser atendidas con quejas y reclamos que sean considerados razonables. El requisito establecido en la Ley es que las empresas deben responder a solicitudes antes de 45 días, cuando hayan obtenido un ingreso anual de 25000 dólares y 50000 dólares por año, y cuando tengan el 50% de ingresos a partir de la venta de información.

Se indica que los consumidores deben ajustarse a los lineamientos de la CCPA, y que cualquier daño o perjuicio puede causar una infracción de hasta 7500 USD.

De acuerdo con la normativa CCPA, los datos sensibles que se publican pueden ser asociados directa o indirectamente con un consumidor o familia en particular. Según dicha normativa, la información personal debe ser tratada de la siguiente manera:

- Los datos personales, tales como la identificación, el nombre real, la dirección de residencia, la identificación única, la dirección IP, la dirección de correo electrónico, el nombre de usuario, el número de seguridad social, el número de permisos de conducción y el número de pasaporte.
- Información comercial acerca del registro de bienes y productos o servicios comprados durante un período específico.
- La información biométrica es importante.
- Información acerca de las actividades llevadas a cabo en el sitio web, tales como el historial de navegación, el tipo de búsqueda y los datos relacionados con la interacción web.
- Los datos de geolocalización.
- Información de carácter multimedia.
- Información profesional sobre el empleo y la formación educativa.

En el año 2020, todas las compañías que laboran en califórnica deben responder a las consultas de los consumidores acerca del tratamiento de datos. Este género, que todas las compañías han revisado las políticas de tratamiento de datos personales, garantiza la información de los dispositivos que han lanzado al mercado.

## 8.2. SITUACIÓN ACTUAL EN COLOMBIA

A causa de la constante transformación económica, política y tecnológica del país en la actualidad, se encuentra en diversos cambios económicos, políticos y tecnológicos. El gobierno ha establecido la meta de alcanzar el 85% de la conectividad en el territorio nacional. En la actualidad, se encuentra en el 56.5% de los hogares que cuentan con acceso a internet, mientras que solo los sectores rurales cuentan con un 23.8%, según las cifras del DANE.[59]

La tecnología IoT se ha convertido en una gran oportunidad para empresas privadas y públicas que buscan innovación y mejora de los procesos. No obstante,

[59] sumamovil. [Sitio web]. Bogotá: sumamovil.com.co. [consultado el 23 de septiembre del 2023] . Disponible en: https://sumamovil.com.co/el-negocio-m2m-iot-en-colombia-cuenta-con-un-nuevo-aliado/

esto implica la anulación de puestos de trabajo en comparación con los costos de instalaciones de sensores, uso de máquinas, recopilación y almacenamiento de dicha información.

El plan de transición a nuevas tecnologías, elaborado por el Ministerio de Tecnologías de Información y Comunicación, se centra en la modernización de las tecnologías asociadas a los servicios móviles y de telecomunicaciones en todo el país. La presente estrategia persigue la consecución de una comunicación de excelencia a nivel internacional que permita contribuir a la economía colombiana.

Se destaca la importancia de que Colombia se encuentre trabajando en la construcción de ciudades inteligentes, ya que es fundamental, generando conciencia del unificar conceptos y comenzando a estandarizarlos. Actualmente, se encuentra en proceso de modernización hacia la fibra óptica bajo el reglamento técnico de redes internas de comunicaciones considerado fundamental. Asimismo, se requiere la gestión de la gestión de la cifra de datos de gran tamaño con el fin de centralizar y unificar la totalidad de la información generada en la urbe.

En el año 2022, el Ministerio de Tecnologías de la Información y Comunicación (Mintic) presentó el plan TIC 2022-2026, el cual propone una propuesta de transformación para los territorios históricamente olvidados mediante la democratización de la tecnología, el desarrollo y el conocimiento del sector.[60]

En la actualidad, la aceleración o apropiación digital se debe al aumento del uso de tecnologías de inteligencia artificial, internet de las cosas y la comunicación entre máquinas que conectarán ágil y rápidamente entre los dispositivos.[61]

---

[60] Mintic. [Sitio web]. Bogotá: mintic.gov.co. [consultado el 23 de septiembre del 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/275347:MINTIC-publica-para-comentarios-la-Agenda-Colombia-Digital-2022-2026

[61] Mintic. [Sitio web]. Bogotá: [consultado el 05 de octubre del 2023] . Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/280837:MinTIC-hace-un-llamado-a-seguir-el-camino-de-la-reindustrializacion-a-traves-de-la-tecnologia

Se considerarán esenciales en los ámbitos de la salud, la seguridad privada, la seguridad del estado y los servicios de emergencia. Se prevé que, en el presente año, el 47% de las empresas latinoamericanas han implementado una solución mediante el tráfico de datos digitales.

## 8.3. PROPUESTA DE NORMATIVIDAD PARA COLOMBIA

La investigación llevada a cabo tiene como propósito sensibilizar acerca de la adquisición de estos dispositivos, ya que Colombia se encuentra en un proceso de cambio tecnológico. En la actualidad, el sector industrial está adquiriendo la tecnología de la tecnología de la IoT, lo que resultaría más sencillo la elaboración de regulaciones o regulaciones que permitan regular a los diversos fabricantes.

Se recomienda que se adopte la legislación de la privacidad sobre el consumidor, la cual garantiza el derecho a los datos al usuario en relación con la información recopilada y compartida en el dispositivo. Además de notificar a los usuarios sobre las actualizaciones de seguridad para el producto.

En consecuencia, mi recomendación es que el ente público encargado de evaluar los productos que lleguen al mercado o deseen ofertar en Colombia con toda la información disponible. Se han examinado utilizando la metodología OWASP-FSTM para llevar a cabo un análisis de seguridad en todos los dispositivos que posibilitan asegurar las medidas de seguridad que se encuentren aplicadas en el lugar.

Asimismo, la implicación del laboratorio de internet de las cosas, denominado IoT LAB, en sus diversas actividades, fomenta la creación de un ente certificador, el cual, mediante las diversas metodologías actuales o la creación de una propia, permita evaluar y garantizar que los dispositivos IoT o sus aplicaciones cumplan con los estándares de seguridad y protege la privacidad del consumidor.

Desde mi perspectiva, es imperativo actualizar ciertos decretos e incluir puntualmente un decreto que permita ejercer los derechos sobre la protección de

datos digitales confidenciales de un consumidor u organización, a fin de que sean almacenados o compartidos sin previo aviso previo.

En la actualidad, Colombia tiene una ley de protección del consumidor que se fundamenta en la ley 1480 del 2011, en la que se indica explícitamente que tiene como objetivo proteger, promover y garantizar a los consumidores. La garantía de sus derechos a los bienes y servicios adquiridos.

Asimismo, es esencial involucrar a todos los proveedores que, en la actualidad o en el futuro, piensen realizar la distribución de este tipo de dispositivos en Colombia, lo cual garantice que la información privada de cualquier organización o persona natural sea tratada de manera correcta, evitando la fuga de información.

En la actualidad, se está intentando incorporar los diversos procedimientos y áreas de la economía para establecer una conexión entre objetos que incluyen sensores, software y tecnologías sin intercambiar información a través de la red.

El objetivo principal de la comunicación en tiempo real, la intercomunicación, es mejorar los procesos productivos y la prestación del servicio. Se aplican tres principios fundamentales para el desarrollo, la comunicación, la identificación e interacción en la tecnología IoT.

Por consiguiente, el Mintic busca asistir a los emprendimientos mediante la promoción, colaboración, divulgación y apropiación del conocimiento, generando innovación en las soluciones digitales que apuntan al futuro. No obstante, el aspecto de seguridad requiere de una serie de regulaciones o leyes por parte del Estado, las cuales protegen a los consumidores acerca de la privacidad sobre los datos recopilados por estos dispositivos y los diversos mecanismos que deben implementarse.

Asimismo, se realizará una concientización a través del ministerio de tecnologías de la información sobre el motivo por el cual se utilizan estos dispositivos en los diferentes procesos para las organizaciones industriales.

Se llevaron a cabo pruebas piloto en Ecopetrol, juntamente con la colaboración de Accenture, Claro y Microsoft, con el fin de llevar a cabo un análisis exhaustivo del funcionamiento operativo y de las labores de mantenimiento en la refinería de Barrancabermeja. En esta actividad se emplearon dispositivos IoT, asistencia remota, lo que resultó en la ejecución de actividades en tiempo récord y el empleo de recursos humanos que requerían llevar a cabo el traslado entre tres y 8 días.[62]

El proveedor Starlink ha concedido el permiso de utilizar el espectro para proporcionar internet de manera satelital. Con ello, el Ministerio de Tecnologías de la Información y Comunicaciones Mintic se esfuerza por fortalecer la implementación de tecnologías innovadoras, tales como la red 5G y el internet de las cosas para Colombia.

Starlink es un proyecto ambicioso liderado por Elon Musk, quien persigue la creación de una red de patentes que permita la aplicación de internet de banda ancha en la cobertura global. En Colombia se pretende eliminar la brecha digital, estableciendo la interconexión entre las regiones del país, asegurando el acceso a internet y convirtiéndolo en un servicio fundamental, apostando cada día a la creación de ciudades inteligentes.

En mi opinión, todas estas acciones requieren de responsabilidades y desafíos, los cuales aún existen en la actualidad, tales como los equipos de respuesta e incidentes de seguridad, estructurados en el ámbito gubernamental, quienes tienen la responsabilidad de gestionar y reaccionar sobre los diversos clientes que se encuentren en el país.

[62] Mintic. [Sitio web]. Bogotá: mintic.gov.co. [consultado el 23 de septiembre del 2023] . Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/238355:Gobierno-nacional-otorga-permiso-de-uso-de-espectro-para-servicios-de-radiocomunicaciones-a-la-compania-de-Internet-satelital-Starlink

# 9. CONCLUSIONES

- Este documento tiene como propósito sensibilizar a los proveedores, organizaciones y usuarios de que las nuevas tecnologías permiten hacer más sencillo tareas cotidianas. Actualmente, se están llevando a cabo grandes investigaciones científicas que utilizan dispositivos IoT, pero como tiene sus ventajas, también es importante estar al tanto de las amenazas actuales y futuras .

- Existen entidades sin ánimo de lucro y privadas que se han preocupado por la tecnología del Internet en las cosas, identificando amenazas, proporcionando documentos y lineamientos acerca de la seguridad en dispositivos IoT. Se promueve la mejora de las prácticas desde el diseño, desarrollo e implementación de servicios seguros, así como los mecanismos para evaluar las medidas de seguridad adoptadas, así como servicios confiables que posibilitan la adquisición de una escala mayor.

- Se ha establecido una normativa emitida por el gobierno de califórnica en los Estados Unidos, quienes se preocupan por la seguridad informática y los dispositivos tecnológicos que se encuentran implementados en el territorio, asegurando la privacidad de los consumidores. Al requerir que los diferentes proveedores implementen mecanismos de seguridad en sus dispositivos y brinden toda la información acerca del dispositivo a los usuarios.

- Colombia está trabajando para mejorar la conectividad a internet para todos los ciudadanos, lo que significará una gran infraestructura tecnológica que permite la intercomunicación entre regiones. La finalidad del Ministerio de Tecnologías de la Información y las Comunicaciones consiste en la creación de ciudades inteligentes mediante la utilización de dispositivos IoT. Este objetivo implica una ardua tarea en la que diversas autoridades a nivel ciberseguridad realicen un monitoreo, concientización, implementación de normativas en la implementación de leyes que obligué a proveedores de tecnología a cumplir e implementar mecanismos de seguridad.

# 10. RECOMENDACIONES

- La tecnología y los dispositivos IoT se convierten en un elemento vital para cualquier entidad. Por consiguiente, como futuros expertos en seguridad informática, se debe informar, investigar, diseñar políticas y estrategias para la implementación de dichos dispositivos. Elegir la metodología para evaluar las posibles amenazas con esto, construir medidas que permitan asegurar todos los activos que se encuentren en la infraestructura.

- Identificar las amenazas que se generan al usar e implementar dispositivos IoT en una infraestructura al intercomunicarse hacia internet. Diversas entidades, desarrolladores, Pentesters, Fabricantes e investigadores se encuentran trabajando en proyectos sin ánimo de lucro, documentación, uso de metodologías y herramientas públicas para evitar amenazas cibernéticas al utilizar estos productos.

- La información es un activo digital intangible, el cual se ha convertido en un objetivo para los ciberdelincuentes para ser adquirido ilegalmente. Este activo es el más relevante para cualquier organización; en la actualidad, diversas organizaciones se han preocupado por la privacidad de los datos almacenados en diferentes tecnologías y han publicado procedimientos y políticas que pueden ser utilizadas e implementadas para asegurar los dispositivos y servicios de la tecnología IoT.

## 11. BIBLIOGRAFÍA


ORTIZ GALEANO, DIANA, "Análisis General del enfoque IoT en redes". {En línea}. {09 de abril del 2023}.Disponible en: (http://caoba.sanmateo.edu.co/jspui/bitstream/123456789/124/1/PROYECTO%20DE%20GRADO%20FINAL-pdf.pdf).

ROJAS, SERGIO "Arquitectura empresarial con capas para el Internet de las Cosas". {En línea}. {09 de abril del 2023}. Disponible en: (https://www.vs-sistemas.com/Blog/Actualidad/arquitectura-empresarial-con-capas-para-iot).

TORRES, GUSTAVO "Conectividad IoT, el camino para el desarrollo de la agricultura inteligente". {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/conectividad-iot-el-camino-para-el-desarrollo-de- la-agricultura-inteligente/).

GONZÁLEZ LARÍN, YEISSON "El Internet de las cosas y sus riesgos para la privacidad".
{En línea}. {09 de abril del 2023}. Disponible en: (http://polux.unipiloto.edu.co:8080/00003525.pdf).

GONZÁLEZ VALENZUELA, CAROLINA "Esta es la historia de los teléfonos móviles: desde su origen hasta la actualidad". {En línea}. {10 de mayo del 2023}. Disponible en: (https://computerhoy.com/moviles/historia-telefonos-moviles-origen-actualidad- 1181484).

PEIRÓ, ROSARIO "Internet de las cosas (IoT)". {En línea}. {01 de julio del 2021}. Disponible en: (https://economipedia.com/definiciones/internet-de-las-cosas-iot.html).

PORROSÁEZ, IGNACIO "IoT: protocolos de comunicación, ataques y recomendaciones". {En línea}. {09 de abril de 2023}. Disponible en: (https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones).

SANDOVAL, DAVID "*IoT Security assessment*". {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/iot-security-assessment/).*

LA ROSA, ALEXANDER "LPWAN como base de comunicaciones para IoT". {En línea}.
{25 de mayo del 2023}. Disponible en: (https://pandorafms.com/blog/es/que-es-lpwan/).

TORRES, GUSTAVO "La seguridad del IoT en riesgo: qué son y cómo protegerse de los ataques DDoS". {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/la-seguridad-del-iot-en-riesgo-que-son-y-como- protegerse-de-los-ataques-ddos/).

TORRES, GUSTAVO "La tecnología IoT en el punto de mira de los ciberdelincuentes". {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/la-tecnologia-iot-en-el-punto-de-mira-de-los-ciberdelincuentes/).

TORRES, GUSTAVO "Los dispositivos IoT son una puerta abierta al hackeo de las Pymes". {En línea}.{30 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/los-dispositivos-iot-son-una-puerta-abierta-al- hackeo-de-las-pymes%ef%bf%bc/).

PINZÓN NIÑO, DAVID "Panorama de aplicación de internet de las cosas (IoT)". {En línea}. {05 de mayo del 2023}. Disponible en: (https://repository.usta.edu.co/bitstream/handle/11634/672/Panorama%20de%20aplicacion%20de%20internet%20de%20las%20cosas.pdf?sequence=1&isAllowed=y).

TORRES, GUSTAVO "Proteger los dispositivos conectados a IoT hace que Internet sea más seguro".{En línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/proteger-los-dispositivos-conectados-a-iot-hace- que-internet-sea-mas-seguro/).

LLAMAS, LUIS “Protocolos de comunicación para IoT“. {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.luisllamas.es/protocolos-de-comunicacion-para-iot/).

JOHNSTON, NICK “Proyecto abierto de seguridad de aplicaciones web OWASP“. {En línea}. {05 de mayo del 2023}. Disponible en: (*https://owasp.org/www-chapter- toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root- Causes.pdf*).

SANDOVAL, DAVID “OWASP FSTM, *stage 1: Information gathering and reconnaissance*“. {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-information-gathering/).*

SANDOVAL, DAVID “OWASP FSTM, *stage 2: Obtaining IOT device firmware*“. {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-obtaining-iot-device-firmware/).*

SANDOVAL, DAVID “OWASP FSTM, *stage 3: Analyzing firmware“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-stage- 3-analyzing-firmware/).*

SANDOVAL, DAVID “OWASP FSTM, stage 4: *Extracting the filesystem“.* {En línea}. {10 de mayo del 2023}. Disponible en: (https://www.tarlogic.com/blog/owasp-fstm-stage-4-extracting-the-filesystem/).

SANDOVAL, DAVID “OWASP FSTM, *stage 5: Analyzing filesystem contents*“. {En línea}. {10 de mayo del 2023}. Disponible en: (https://www.tarlogic.com/blog/owasp-fstm-analyzing-filesystem-contents/).

SANDOVAL, DAVID “OWASP FSTM *step 6: firmware emulation“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-step-6- firmware-emulation/*).

SANDOVAL, DAVID “OWASP FSTM *step 7: Dynamic analysis“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-dynamic-analysis/).*

SANDOVAL, DAVID “OWASP FSTM, *step 8: Runtime analysis“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-runtime-analysis/*).

SANDOVAL, DAVID “OWASP FSTM, *Stage 9: Exploitation of executables*“. {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-exploitation-of-executables/*).

LLAMAS, LUIS “¿Qué es MQTT? Su importancia como protocolo IoT“. {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/).

GRACIA, LUISMI “STOMP (*Streaming Text Oriented Messaging Protocol*)“. {En línea}. {25 de mayo del 2023}. Disponible en: (*https://unpocodejava.com/2010/12/07/stomp-streaming-text-oriented-messaging-protocol/).*

TORRES, GUSTAVO “Wayra presenta el primer laboratorio de 5G e IoT en Colombia“.
{En línea}. {10 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/wayra-presenta-el-primer-laboratorio-de-5g-e-iot-en-colombia/).

# ANEXOS

## *Anexo A Resumen RAE*

| 1. Información General | |
|---|---|
| **Tipo de documento** | Monografía |
| **Acceso al documento** | Trabajo monográfico para optar al título Especialización en seguridad informática |
| **Título del documento** | Seguridad en dispositivos IoT en organizaciones industriales en Colombia. |
| **Autor** | Oscar Giovanny Gonzalez Cruz |
| **Publicación** | Año 2023 |
| **Palabras Claves** | Activo, actualizaciones, amenaza, atacante, auditoria, backup, ciberdelincuente, cifrado, clave privada, clave pública, contraseña, impacto, incidente de seguridad, plan, política, protocolo, riesgo, seguridad, vulnerabilidad. |

| 2. Descripción |
|---|
| Durante los últimos años, se ha incrementado la adquisición de los dispositivos IoT, uno de los motivos radica en su asequible precio, además de la posibilidad de llevar a cabo tareas diarias de manera automatizada, lo que ha evidenciado un gran empleo en hogares. Según un experto que participó en el evento SaferNet Day 2023 existen actualmente 7000 millones de estos a nivel mundial y que se prevé para el 2025 alcanzarían a 22.000 millones de productos conectados. En Colombia se encuentra en diversas transformaciones en la economía política y tecnología. El gobierno colombiano persigue alcanzar un 85% de la conectividad en todo el país, lo cual ha permitido la utilización del dispositivo de IoT y la inteligencia artificial en las tareas de monitoreo, control y análisis de dispositivos remotos. Estos dispositivos tienen la capacidad de interconectar entre los sistemas microelectrónicos de manera inalámbrica y conectarlos a internet para ser monitoreados y operados remotamente. Generando nuevos desafíos ante la denominada cuarta revolución industrial. Debido a la gran cantidad de información y sus respectivos usuarios que están en peligro de ser interceptados por cibercriminales, la tecnología IoT se encuentra en su fase de desarrollo. Uno de los principales motivos radica en la falta de atención de los fabricantes para considerar el aspecto de la seguridad presente en sus productos, lo que desde su creación son inseguros. |

| 3. Fuentes |
|---|
| Ortiz Galeano, Diana "Análisis General del enfoque IoT en redes". {En línea}. {09 de abril del 2023}. Disponible en: (http://caoba.sanmateo.edu.co/jspui/bitstream/123456789/124/1/PROYECTO%20DE%20GRADO%20FINAL-pdf.pdf).<br><br>Rojas, Sergio “Arquitectura empresarial con capas para el Internet de las Cosas“. {En línea}. {09 de abril del 2023}. Disponible en: (https://www.vs-sistemas.com/Blog/Actualidad/arquitectura-empresarial-con-capas-para-iot).<br><br>Torres, Gustavo “Conectividad IoT, el camino para el desarrollo de la agricultura inteligente“. {En |

línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/conectividad-iot-el-camino-para-el-desarrollo-de-la-agricultura-inteligente/).

González Larín, Yeisson "El Internet de las cosas y sus riesgos para la privacidad". {En línea}. {09 de abril del 2023}. Disponible en: (http://polux.unipiloto.edu.co:8080/00003525.pdf).

González Valenzuela, Carolina "Esta es la historia de los teléfonos móviles: desde su origen hasta la actualidad". {En línea}. {10 de mayo del 2023}. Disponible en: (https://computerhoy.com/moviles/historia-telefonos-moviles-origen-actualidad-1181484).

Peiró, Rosario "Internet de las cosas (IoT)". {En línea}. {01 de julio del 2021}. Disponible en: (https://economipedia.com/definiciones/internet-de-las-cosas-iot.html).

Porro Sáez, Ignacio "IoT: protocolos de comunicación, ataques y recomendaciones". {En línea}. {09 de abril de 2023}. Disponible en: (https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones).

Sandoval, David "*IoT Security assessment*". {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/iot-security-assessment/).*

La rosa, Alexander "LPWAN como base de comunicaciones para IoT". {En línea}. {25 de mayo del 2023}. Disponible en: (https://pandorafms.com/blog/es/que-es-lpwan/).

Torres, Gustavo "La seguridad del IoT en riesgo: qué son y cómo protegerse de los ataques DDoS". {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/la-seguridad-del-iot-en-riesgo-que-son-y-como-protegerse-de-los-ataques-ddos/).

Torres, Gustavo "La tecnología IoT en el punto de mira de los ciberdelincuentes". {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/la-tecnologia-iot-en-el-punto-de-mira-de-los-ciberdelincuentes/).

Torres, Gustavo "Los dispositivos IoT son una puerta abierta al hackeo de las Pymes". {En línea}. {30 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/los-dispositivos-iot-son-una-puerta-abierta-al-hackeo-de-las-pymes%ef%bf%bc/).

Pinzón Niño, David "Panorama de aplicación de internet de las cosas (IoT)". {En línea}. {05 de mayo del 2023}. Disponible en: (https://repository.usta.edu.co/bitstream/handle/11634/672/Panorama%20de%20aplicacion%20de%20internet%20de%20las%20cosas.pdf?sequence=1&isAllowed=y).

Torres, Gustavo "Proteger los dispositivos conectados a IoT hace que Internet sea más seguro". {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.tecnogus.com.co/proteger-los-dispositivos-conectados-a-iot-hace-que-internet-sea-mas-seguro/).

Llamas, Luis "Protocolos de comunicación para IoT". {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.luisllamas.es/protocolos-de-comunicacion-para-iot/).

*Johnston, Nick* "Proyecto abierto de seguridad de aplicaciones web OWASP". {En línea}. {05 de mayo del 2023}. Disponible en: (*https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf*).

Sandoval, David "OWASP FSTM, *stage 1: Information gathering and reconnaissance*". {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-information-gathering/).*

Sandoval, David “OWASP FSTM, *stage 2: Obtaining IOT device firmware*“. {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-obtaining-iot-device-firmware/).*

Sandoval, David “OWASP FSTM, *stage 3: Analyzing firmware“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-stage-3-analyzing-firmware/).*

Sandoval, David “OWASP FSTM, stage 4: *Extracting the filesystem“.* {En línea}. {10 de mayo del 2023}. Disponible en: (https://www.tarlogic.com/blog/owasp-fstm-stage-4-extracting-the-filesystem/).

Sandoval, David “OWASP FSTM, *stage 5: Analyzing filesystem contents*“. {En línea}. {10 de mayo del 2023}. Disponible en: (https://www.tarlogic.com/blog/owasp-fstm-analyzing-filesystem-contents/).

Sandoval, David “OWASP FSTM *step 6: firmware emulation“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-step-6-firmware-emulation/*).

Sandoval, David “OWASP FSTM *step 7: Dynamic analysis“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-dynamic-analysis/).*

Sandoval, David “OWASP FSTM, *step 8: Runtime analysis“.* {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-runtime-analysis/*).

Sandoval, David “OWASP FSTM, *Stage 9: Exploitation of executables*“. {En línea}. {10 de mayo del 2023}. Disponible en: (*https://www.tarlogic.com/blog/owasp-fstm-exploitation-of-executables/*).

Llamas, Luis “¿Qué es MQTT? Su importancia como protocolo IoT“. {En línea}. {25 de mayo del 2023}. Disponible en: (https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/).

## 4. Contenidos

El documento está compuesto por seis etapas, en las que la primera se presenta una introducción al uso de los dispositivos de internet de las cosas, se realiza una descripción del problema, sus antecedentes y se formula un problema. A continuación, se plantean el objetivo general y los objetivos específicos. En la segunda está centrada en el marco teórico, concepto de los dispositivos IoT, concepto de los diferentes modelos que se encuentran utilizando tecnología del internet de las cosas. En el tercer apartado se identifican los principales ataques contra estos dispositivos, vectores de ataque y servicios ofrecidos. En la cuarta fase se presentan las metodologías más efectivas para llevar a cabo un análisis de auditoría. La quinta se refiere a todo lo concerniente a las buenas prácticas y a las diferentes entidades que están trabajando para mejorar la seguridad en esta tecnología. La fase sexta y última permite la identificación de las diversas normas que se encuentren implementadas en América Latina, a fin de elaborar propuestas o normativas para Colombia, además de generar conclusiones, recomendaciones y bibliografías investigadas.

| 5. Metodología |
|---|
| El proceso se lleva a cabo siguiendo un esquema estructurado; en la primera fase se identificó el problema a explorar debido a que estos dispositivos se encuentran utilizando en diferentes actividades y en la vida cotidiana. En la segunda fase, a partir del paso previo, se requiere realizar una investigación e identificación de las tecnologías y protocolos implementados en la tecnología IoT. Asimismo, se debe identificar entidades sin ánimo que han desarrollado metodologías para evaluar los dispositivos implementados, así como también entidades y organizaciones gubernamentales que han elaborado guías de buenas prácticas para implementar en cualquier organización, asegurando la infraestructura de una compañía u hogar. Finalmente, identificar qué leyes gubernamentales se encuentran en América Latina que posibilitan asegurar a los usuarios que utilizan las tecnologías del internet de las actividades con el propósito de proponer y/o mejorar las normas gubernamentales en Colombia, ya que estos dispositivos actualmente se encuentran implementados tanto en sectores públicos como privados y son los principales objetivos para los ciber atacantes. |

| 5. Conclusiones |
|---|
| Este documento tiene como propósito sensibilizar a los proveedores, organizaciones y usuarios de que las nuevas tecnologías permiten hacer más sencillo tareas cotidianas. Actualmente, se están llevando a cabo grandes investigaciones científicas que utilizan dispositivos IoT, pero como tiene sus ventajas, también es importante estar al tanto de las amenazas actuales y futuras.<br><br>Existen entidades sin ánimo de lucro y privadas que se han preocupado por la tecnología del Internet en las cosas, identificando amenazas, proporcionando documentos y lineamientos acerca de la seguridad en dispositivos IoT. Se promueve la mejora de las prácticas desde el diseño, desarrollo e implementación de servicios seguros, así como los mecanismos para evaluar las medidas de seguridad adoptadas, así como servicios confiables que posibilitan la adquisición de una escala mayor.<br><br>Se ha establecido una normativa emitida por el gobierno de califórnica en los Estados Unidos, quienes se preocupan por la seguridad informática y los dispositivos tecnológicos que se encuentran implementados en el territorio, asegurando la privacidad de los consumidores. Al requerir que los diferentes proveedores implementen mecanismos de seguridad en sus dispositivos y brinden toda la información acerca del dispositivo a los usuarios.<br><br>Colombia está trabajando para mejorar la conectividad a internet para todos los ciudadanos, lo que significará una gran infraestructura tecnológica que permite la intercomunicación entre regiones. La finalidad del Ministerio de Tecnologías de la Información y las Comunicaciones consiste en la creación de ciudades inteligentes mediante la utilización de dispositivos IoT. Este objetivo implica una ardua tarea en la que diversas autoridades a nivel ciberseguridad realicen un monitoreo, concientización, implementación de normativas en la implementación de leyes que obligué a proveedores de tecnología a cumplir e implementar mecanismos de seguridad. |

| | |
|---|---|
| **Elaborado por:** | Oscar Giovanny Gonzalez Cruz |

| | | | |
|---|---|---|---|
| **Fecha de elaboración del Resumen:** | 20 | 12 | 2023 |