OFICINA DE POSGRADOS

Tema:

ANÁLISIS DE AMENAZAS IOT EN UN SISTEMA DOMÓTICO

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Protección de datos y comunicaciones

Autor:

Miguel Alejandro López Naranjo

Director:

Ing. Mg. Galo Mauricio López Sevilla

Ambato – Ecuador

Septiembre 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

ANÁLISIS DE AMENAZAS IOT EN UN SISTEMA DOMÓTICO

Línea de Investigación:

Protección de datos y comunicaciones

Autor:

Miguel Alejandro López Naranjo

Galo Mauricio López Sevilla, Mg. f._____
CALIFICADOR

Santiago Alejandro Acurio Maldonado, Mg. f._____
CALIFICADOR

Darío Javier Robayo Jácome, Mg. f._____
CALIFICADOR

Juan Carlos Acosta Teneda, P. Ph.D. f._____
COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villaroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
DIRECCIÓN CENTRO DE POSGRADOS Sede Ambato

Pontificia Universidad Católica del Ecuador
SECRETARIA GENERAL PROCURADURÍA

Ambato – Ecuador

Julio 2022

DECLARACIÓN Y AUTORIZACIÓN

Yo: **MIGUEL ALEJANDRO LÓPEZ NARANJO,** con **CC. 180399185-8**, autor del trabajo de graduación intitulado: "ANÁLISIS DE AMENAZAS IOT EN UN SISTEMA DOMÓTICO", previa obtención del título profesional de **Magister en Ciberseguridad**, en la escuela de **Sistemas**.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, julio 2022

MIGUEL ALEJANDRO LÓPEZ NARANJO

CC. 180399185-8

DEDICATORIA

A Dios quien ha sido mi guía, fortaleza y su mano de fidelidad y amor han estado conmigo hasta el día de hoy.

A mi familia y amigos quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

Mi profundo agradecimiento a todas las autoridades y personal que hacen la Pontificia Universidad Católica del Ecuador Sede Ambato, por confiar en mí, abrirme las puertas, a mis profesores quienes con la enseñanza de sus valiosos conocimientos hicieron que crezca día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

RESUMEN

La creciente demanda en el uso de dispositivos electrónicos IoT en hogares y organizaciones, así como la facilidad con, la cual, se integran a los sistemas y redes de internet, ponen en riesgo la seguridad de la información de los usuarios. En este sentido resulta importante analizar las amenazas más frecuentas y evaluar los niveles de seguridad que presentan los dispositivos IoT en un sistema domótico, para desarrollar un manual técnico de buenas prácticas que permita mitigar el riesgo de sufrir ciberataques. El objetivo del presente trabajo es analizar las amenazas IoT que existen en un sistema domótico, mediante un enfoque cualitativo y diseño preexperimental. Para lo cual, se procedió a realizar una revisión bibliográfica, necesaria para comprender los conceptos, generar ideas y comprobar el estado actual de los conocimientos la tecnología IoT. La investigación, se basó en el análisis de documentos, revistas, paginas académicas de internet con la finalidad de aportar y recopilar con información necesaria sobre la estructura y características de la arquitectura IoT, además, de las amenazas presentes frecuentemente en los dispositivos IoT y seguridad de los sistemas domóticos. Toda esta información recopilada sirvió como base para realizar el diseño de un entorno domótico simulado usado posteriormente para verificar los niveles de seguridad de los dispositivos IoT y plasmar todos estos resultados obtenidos en un manual técnico con los pasos y buenas prácticas de ciberseguridad, el cual, permite solventar los problemas de seguridad estudiados.

Palabras claves: internet de las cosas, seguridad, domótica.

ABSTRACT

The growing demand in the use of IoT electronic devices in homes and organizations, as well as the ease with which they are integrated into systems and internet networks, put the security of user information at risk. In this sense, it is important to analyze the most frequent threats and evaluate the security levels of IoT devices in a home automation system, in order to develop a technical manual of good practices to mitigate the risk of cyber-attacks. The objective of this work is to analyze the IoT threats that exist in a home automation system, through a qualitative approach and pre-experimental design. To this end, a literature review was carried out, which was necessary to understand the concepts, generate ideas and check the current state of knowledge of IoT technology. The research was based on the analysis of documents, magazines, academic web pages in order to provide and collect the necessary information about the structure and characteristics of the IoT architecture, as well as the threats frequently present in IoT devices and security of home automation systems. All this information collected served as a basis for the design of a simulated home automation environment used later to verify the security levels of IoT devices and to translate all these results obtained in a technical manual with the steps and good practices of cybersecurity, which allows to solve the security problems studied.

Keywords: internet of things, security, domotics.

ÍNDICE

ÍNDICE DE TABLAS

INDICE DE CUADROS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

El internet revoluciono las comunicaciones tradicionales en todo el mundo de una manera radical, a tal punto de convertirse en el medio global de comunicación cotidiano, se lo usa para casi todo, ya sea para adquirir algún producto o servicio, buscar información sobre un tema en específico hasta enviar mensajes y compartir fotografías o archivos multimedia con amigos. La conectividad a internet permite que las personas estén informadas de lo que sucede en otros lugares del mundo de manera inmediata y sin necesidad de esperar a que medios locales distribuyan la información a través de medios impresos.

En este contexto el internet es, también, una plataforma para que los dispositivos electrónicos se conecten y compartan la información y datos que obtiene del ambiente que los rodea entre ellos, tanto así que las personas conectadas a nivel mundial en los inicios del internet eran mínimas y solo existía un dispositivo conectado por persona, mientras que en la actualidad, se estima total de 20 billones de dispositivos IoT en todo el mundo, lo cual, sugiere un aumento de un 82 % a comparación del año 2018 y más de un dispositivo conectado por persona (Gartner, 2017).

El Ecuador ya es común hablar de Ciudad Inteligente (Smart City) , dispositivos que se conectan a los teléfonos para recopilar todo tipo de información cada vez son más comunes en los hogares, industrias, en el área de la salud y entidades gubernamentales, así como también, el acceso a internet se ha convertido en un servicio básico en los hogares ecuatorianos al establecer comunicación con todas las áreas urbanas y rurales de la región, en este sentido el gobierno, se ha visto comprometido en alcanzar un alto nivel de desarrollo digital que permita mejorar las condiciones de vida de los ciudadanos a través del uso de las tecnologías.

En la actualidad el internet de las cosas (IoT), ha tomado gran fuerza en el mundo de la tecnología, ofrece la posibilidad de que la gran mayoría de dispositivos electrónicos tengan la capacidad de conectarse al internet, establece un medio de comunicación entre todos los dispositivos y permite al usuario acceder a ellos

desde cualquier lugar del mundo.- Esta tendencia ha cambiado la forma de comunicación tradicional y ha transformado el uso de internet, aumentó la integración entre la persona y los dispositivos tecnológicos y facilitó las tareas cotidianas de los usuarios (Rose, Eldridge, & Chapin, 2015).

A pesar de los beneficios que trae el internet de las cosas en la actualidad, su tecnología emergente; que está en constante evolución, ha dejado rezagado el tema de la seguridad por la rapidez con la que los grandes fabricantes crean dispositivos inteligentes, esto expone al usuario a amenazas relacionadas con la ciberseguridad como: ataques denegación de servicios distribuidos *DDoS*, espionaje y vigilancia, movimientos laterales, *Ransomware, Spoofing* (Andrea, Chrysostomou, & Hadjichristofi, 2015).

Los ecosistemas domóticos IoT se componen de un centro de operaciones donde se integra e interconecta una gran cantidad de dispositivos electrónicos, de los cuales, recopila toda la información, la procesa y emite ordenes que automatiza las tareas previamente programadas por los usuarios a través de cualquier red de datos que permitan el acceso a internet; habitualmente no usan estructuras y protocolos homogéneos entre fabricantes y gran parte no cuenta con estándares de seguridad adecuados en los dispositivos que distribuyen para el consumo; esto incrementa el umbral de riesgo de seguridad digital y proporciona una puerta de acceso a personas no autorizadas. En este contexto el problema es: ¿Como minimizar los riesgos de seguridad que existen en los dispositivos electrónicos Iot de un sistema Domótico?

Lo expuesto anteriormente conduce al investigador a formular las siguientes preguntas científicas como parte de la investigación:

- ¿Cuál es el fundamento teórico que soporta el funcionamiento de los dispositivos IoT dentro de un sistema domótico?
- ¿Cuál es la metodología adecuada para la detección de riesgos de seguridad en dispositivos IoT?

- ¿Cuál es la metodología adecuada para el control de vulnerabilidad de un sistema domótico frente a ataques informáticos a los dispositivos IoT?
- ¿Se mitigaría el riesgo de sufrir ciberataques a los dispositivos IoT en un sistema domótico mediante una guía de buenas prácticas?

En este sentido este trabajo tiene como objetivo principal Analizar las amenazas de ciberseguridad que presentan los dispositivos IoT en un sistema domótico.
Subsecuente a ello de detallaran las tareas para resolver el problema mencionado:

1. Fundamentación teórica para conocer el funcionamiento de los dispositivos IoT dentro de un sistema domótico.
2. Investigación de metodologías para la detección de riesgos más frecuentes que presentan los dispositivos IoT.
3. Verificación de los niveles de seguridad de dispositivos IoT en un sistema domótico simulado.
4. Redacción de un manual técnico de buenas prácticas de seguridad para dispositivos IoT en sistemas domóticos.

Metodología de la Investigación:

Para realizar la investigación se realiza una revisión bibliográfica, necesaria para comprender los conceptos, generar ideas y comprobar el estado actual de los conocimientos del tema que se investigó. La investigación bibliografía se basó en el análisis de documentos, revistas, paginas académicas de internet con la finalidad de aportar y recopilar con información necesaria para el desarrollo del presente proyecto.

Metodología de Desarrollo:

La metodología de desarrollo utilizada en la investigación está orientada a la simulación, la cual, es una técnica que permite simular el comportamiento de un sistema como si fuese la vida real, esto a su vez permite someterlo a diferentes

pruebas para analizar su respuesta ante estos estímulos. La simulación permite estudiar y analizar los procesos de un sistema, así como también, evaluar su funcionamiento sin preocuparnos de los riesgos que existen si fuesen realizados en sistemas reales de gran escala.

A continuación, se muestra las fases de la metodología para una simulación:

- Formulación del problema: Tener claros los objetivos del proyecto
- Diseño de modelo conceptual: Se elabora un diseño conceptual para entender de una mejor manera como son los procesos que interactúan en un sistema
- Recolección de datos: Se verifica que los datos obtenidos sean confiables y suficientes para el modelo planteado
- Construcción del modelo: En esta etapa se construye el modelo mediante entornos o un software especializado para la simulación
- Verificación y validación: Se verificar que la simulación esté acorde al modelo conceptual y se procede a comprobar cumpla con los objetivos propuestos.
- Análisis: Se experimenta con el modelo realizado sometiéndole a diferentes pruebas de seguridad para identificar las vulnerabilidades investigadas.
- Preparación del manual técnico con pasos y buenas prácticas para mitigar algunos de los problemas de seguridad analizados.

Justificación

Garantizar la seguridad en los dispositivos Iot es una prioridad fundamental, cada vez son más las personas que acceden a esta tecnología y confían ciegamente en la supuesta seguridad implementada y a medida que estos entornos son implantados en hogares o industrias es imprescindible asegurar que las funciones programadas y la información que se transmite no se vean comprometidos por agentes maliciosos externos. Es por tanto primordial asegurar los puntos débiles de los sistemas domóticos, aplicar configuraciones y protocolos de seguridad

adecuados para salvaguardar la integridad de todos los sistemas a, los cuales, estén conectados.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Internet de las cosas (IoT)

El internet de las Cosas (IoT) es uno de los temas primordiales en la industria, política y la ingeniería, esta se ha considerado como una verdadera revolución tecnológica en las diferentes áreas en las que se desenvuelven los seres humanos.

El termino internet de las Cosas (IoT) fue empleado por primera vez en el año 1999 por el británico Kevin Ashton usado para describir un sistema por, el cual, objetos físicos usados en el mundo cotidiano se conectan al internet por medio de diferentes sensores.

Este término se usó para ilustrar el poder de conectar a la red de internet las etiquetas de identificación por radiofrecuencia (RFID) utilizadas en cadenas de suministro corporativos, las cuales, eran usadas para contar y realizar seguimiento de las mercaderías de forma automática excluye de las mismas la intervención Humana (Singh, Tripathi, & Jara, 2014).

Es así como el concepto de combinar las computadoras y las redes para controlar y monitorear diferentes dispositivos ha existido desde épocas pasadas, a finales de la década de 1970 ya se encontraban en el mercado sistemas disponibles que permitían monitorear medidores conectados a redes eléctricas de forma remota a través de líneas telefónicas. En la década de 1990, los avances de las tecnologías inalámbricas brindaron una solución en la difusión corporativa e industrial “maquina a máquina” (M2M) con el fin de monitorear y operar diferentes equipos.
La comunicación M2M es el paso siguiente de la conexión de uno a uno o conexión de una maquina a otra, en la actualidad el termino M2M se refiere a la comunicación entre maquinas remotas para el intercambio de información. El objetivo principal es recopilar los datos que son transmitidos por la red, además, usa secuencias de eventos para ejecutar acciones de forma automática entre las

maquinas que están conectadas, sirve como base para la inteligencia artificial y el Internet de las Cosas. (Rose et al., 2015)

El lenguaje M2M se considera el nivel base para la comunicación entre maquinas dentro de una misma red, el internet de las cosas utiliza esta comunicación para que los dispositivos inteligentes se conecten entre ellos para transferir información y controlarla a través de dispositivos móviles, entendiéndose que esta correlación directa es la que permite las capacidades y soluciones IoT.

Sin embargo, muchas de las soluciones M2M se basaban en redes especialmente dedicadas y construida para este propósito y con estándares de propietarios específicos de la industria a, la cual, pertenecía más no en redes b asadas en protocolo IP y estándares de Internet.

A partir de este inconveniente, se concretó la idea de conectar a internet dispositivos que no son computadoras por medio de IP, es así que en los años siguientes se presentó las primeras “cosas” conectadas vía IP entre ellas la primera tostadora conectada a internet se controlar su encendido y apagado a través de la red, luego de este significativo salto en el área de investigación y desarrollo de redes de objetos inteligentes ayudo a sentar los cimientos del Internet de las Cosas como se conoce hoy en día (Ghirardello, Maple, Ng, & Kearney, 2018).

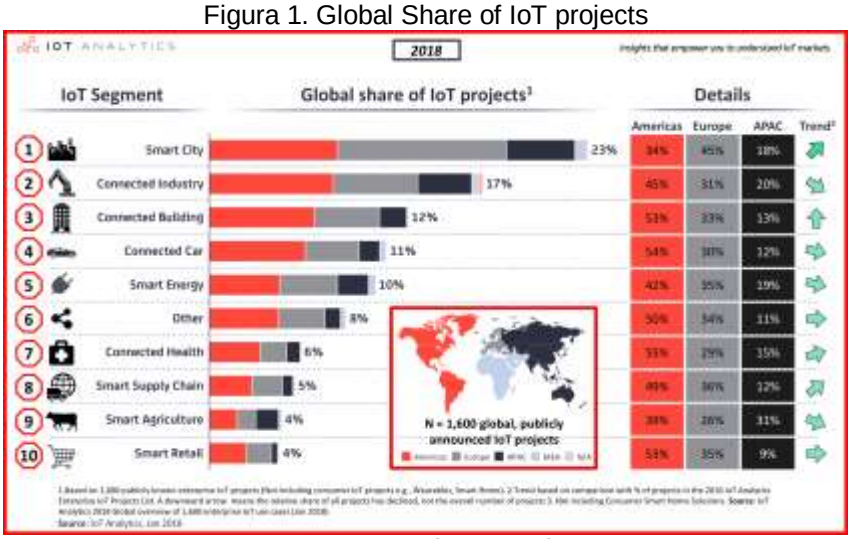
El internet de las cosas en la actualidad es considerado como una verdadera revolución tecnológica, en especial en el área de las comunicaciones, se trata de una red inteligente entre dispositivos que permiten el intercambio de información y comunicación entre ellos capaces de procesar y gestionar ordenes que son programadas y monitoreadas por las personas (Espina Suárez & Gómez Hormaza, 2021).

El Internet de las Cosas se aplica en todas las áreas en las que interactúan las personas, ya sea el área de salud, construcciones, transporte, agricultura, educación, visión artificial, ambiente, industrias. La interacción de estos

dispositivos en varias áreas de desarrollo de IoT busca fortalecer la formación de ciudades inteligentes (*Smart Cities*) automatiza un sin número de servicios públicos y privados y aprovecha los recursos de forma eficiente. (Alvear Puertas, Rosero Montalvo, Peluffo Ordóñez, & Pijal Rojas, 2017)

En la figura 1 identifica en que porcentaje se ve involucrado la tecnología IoT en proyectos de diferente índole alrededor del mundo.

Figura 1. Global Share of IoT projects

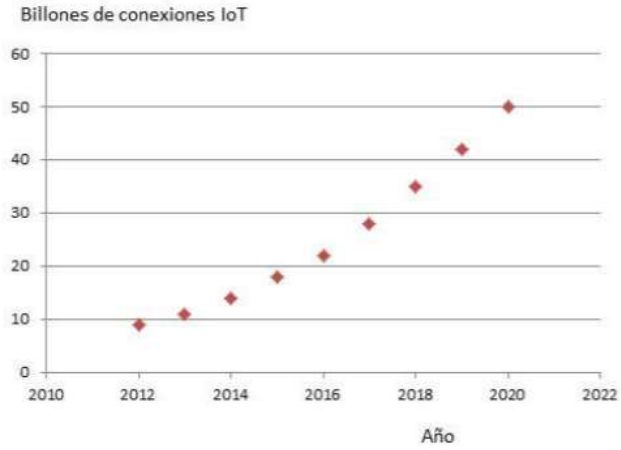


Fuente: IoT Analytics (Sánchez Sánchez, 2018)

Al tomar en cuenta estos avances que ha tenido los dispositivos inteligentes, muchas organizaciones han desarrollado sus propias clasificaciones de IoT según sus aplicaciones y casos de uso. Por ejemplo, IoT industrial, es un término ampliamente utilizado por las empresas para describir aplicaciones de dispositivos IoT que están relacionados con la producción de bienes o servicios, en la industria de la manufactura y en los servicios públicos. Otras empresas discuten la IoT según el tipo de dispositivo, por ejemplo, dispositivos para vestir y electrodomésticos, mientras otros, también, abordan la IoT en el contexto de implementaciones integradas basado en ubicación como, por ejemplo, hogares y ciudades inteligentes, lo que demuestra que la IoT está involucrado a casi todos los aspectos de nuestras vidas y permite cada vez más interconectar dispositivos más pequeños de una forma económica y sencilla (Anabalon, 2016).

En la figura 2 muestra el número de conexiones IoT desde el año 2010 hasta la actualidad, en el cual, se evidencia que existe un incremento notable cada año.

Figura 2. Conexiones IoT



Fuente: Tech-pedía Internet de las cosas

Las aplicaciones y servicios que proporcionan las IoT es prácticamente ilimitado y se adapta a todos los campos de la actividad humada, facilita las tareas y mejora la calidad de vida de la persona, las nuevas aplicaciones y servicios que ofrece esta tecnología la vuelve adaptable y escalable para permitir al ser humano aprovechar todas estas características en los diferentes campos en los que se desempeña como:

Edificios inteligentes conectados: Las mejoras en la eficiencia (gestión de la energía y el ahorro) y de seguridad (sensores y alarmas). Aplicaciones domóticas que incluyen sensores y actuadores inteligentes para controlar electrodomésticos. Los servicios de salud y educación en el hogar. Control remoto de los tratamientos para los pacientes. Servicios de cable / satélite. Sistemas de almacenamiento / generación de energía. Apagado automático de la electrónica cuando no esté en uso. Termostatos inteligentes. Los detectores de humo y alarmas. Aplicaciones de control de acceso. Cerraduras inteligentes. Los sensores incorporados en la construcción de infraestructura para guiar a los primeros auxilios y asistencias. Seguridad para todos los miembros de la familia.

Ciudades inteligentes y transporte: Integración de los servicios de seguridad. Optimización del transporte público y privado. Sensores de aparcamiento. Gestión inteligente de los servicios de estacionamiento y el tráfico en tiempo real. Gestión inteligente de semáforos en función de las colas de tráfico. Localización de los coches que han sobrepasado el tiempo de estacionamiento. Las redes energéticas inteligentes. Seguridad (cámaras, sensores inteligentes, información a los ciudadanos). Administración del Agua. Riego de parques y jardines. Contenedores de basura inteligentes. Controles de contaminación y movilidad. Obtener una respuesta inmediata y conocer las opiniones de los ciudadanos. Gobernanza inteligente. Sistemas de Votación. Monitoreo de accidentes, la coordinación acciones de emergencia.

Educación: Vinculación de aulas virtuales y físicas para el aprendizaje, *elearning* más eficiente y accesible. Servicios de acceso a bibliotecas virtuales y portales educativos. Intercambio de informes y resultados en tiempo real. El aprendizaje permanente. Aprendizaje de idiomas extranjeros. Gestión de la asistencia.

Electrónica de consumo: Teléfonos inteligentes. Televisión inteligente. Laptops, computadoras y tabletas. Refrigeradores, lavadoras y secadoras inteligentes. Sistemas de cine en casa inteligentes. Aparatos inteligentes. Sensores para el collar del animal doméstico. Personalización de la experiencia del usuario. El funcionamiento del producto autónomo. Localizadores personales. Gafas inteligentes.

Salud: Monitoreo de las enfermedades crónicas. Mejora de la calidad de la atención y la calidad de vida de los pacientes. Trackers de Actividad. Diagnóstico remoto. Pulseras conectadas. Cinturones interactivos. Deporte y monitoreo de actividades de fitness. Etiquetas inteligentes para fármacos. Seguimiento del uso de drogas. Los biochips. Interfaces cerebro-ordenador. Monitoreo de los hábitos alimenticios. • Automoción: Smart Cars. Control de tráfico. Avanzar en la información sobre lo que está roto. Monitoreo inalámbrico de presión de los neumáticos de coche. La gestión inteligente de la energía y el control. Auto diagnóstico. Los acelerómetros. Sensores de posición, de presencia y de

proximidad. Análisis de la mejor manera de ir en tiempo real a un sitio. Localización por GPS. Control de la velocidad del vehículo. Vehículos autónomos que utilizan los servicios de la IoT

Agricultura y medio ambiente: Medición y control de la contaminación del medio ambiente (CO2, el ruido, los elementos contaminantes presentes en el 21 ambiente). Pronosticar cambios climáticos basados en el monitoreo de sensores inteligentes. Las etiquetas RFID pasivas asociadas a los productos agrícolas. Sensores en *palets* de productos. Gestión de residuos. Cálculos de Nutrición.

Los servicios de energía: Datos precisos sobre el consumo de energía. La medición inteligente. Redes inteligentes. Análisis y predicción de comportamientos de consumo de energía y patrones. Pronosticar las tendencias y necesidades futuras de energía. Redes de sensores inalámbricos. La producción de energía y el reciclaje.

Conectividad inteligente: Gestión de datos y prestación de servicios. El uso de medios de comunicación y las redes sociales. El acceso a los servicios de correo electrónico, voz y video. La comunicación de grupo interactiva. En *streaming* en tiempo real. Juegos interactivos. Realidad aumentada. Supervisión de la seguridad de la red. Interfaces de usuario disponibles. La computación afectiva. Métodos de autenticación biométrica. Telemática de consumo. Servicios de comunicación M2M. Análisis de grandes datos. Realidad virtual. Servicios de computación en nube. Computación ubicua. Visión por computador. Antenas inteligentes.

Fabricación: Gas y sensores de flujo. Sensores inteligentes de humedad, temperatura, movimiento, fuerza, carga, fugas y niveles. Visión de máquinas. Detección acústica y de vibraciones. Aplicaciones compuestas. Control inteligente de robots. Control y optimización de los procesos de fabricación. Reconocimiento de patrones. Aprendizaje automático. El análisis predictivo. Logística móvil. Gestión de almacenes. Prevenir la sobreproducción. Logística eficiente.

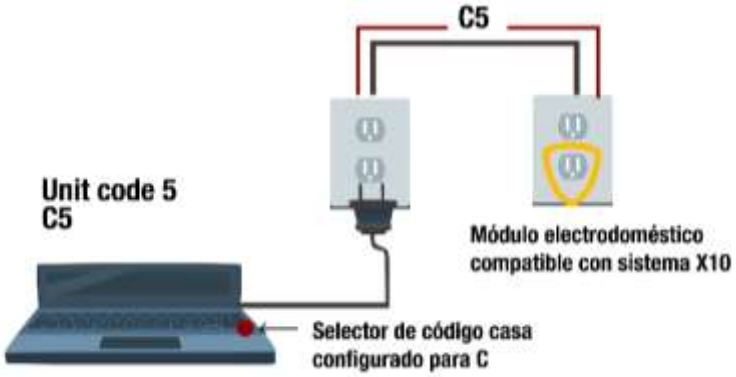
Compras: Compras inteligentes. RFID y otras etiquetas electrónicas y lectores. Los códigos de barras en el comercio minorista. Inventarios. Control de la procedencia geográfica de los alimentos y productos. Control de calidad de los alimentos y de la seguridad.(Salazar Soler & Silvestre Bergés, 2016)

1.2. Domótica

La domótica es una de las áreas con mayor alcance del internet de las cosas, involucra al usuario con la tecnología a tal punto de convivir con ella desde la comodidad de su hogar, al hacer uso de aplicaciones que le permitan controlar los dispositivos IoT que se encuentran en la vivienda.

La domótica tuvo sus inicios desde la década de los años 70, en los cuales, aparecieron los primeros dispositivos domóticos que requerían el uso de circuitos integrados como se los conoce a los primeros microprocesadores. A partir de ello empresas Electrónicas de esa época desarrollaron sistemas domóticos que usan el protocolo de comunicaciones X10, el cual, usa como medio de comunicación la red de potencia como se visualiza en la figura 3.

Figura 3. Conexiones IoT



Fuente: ina-pidte.ac.cr domótica

Esta tecnología en el campo de la domótica se la conoce como *Power Line Carrier Conmmunication* (PLC) y en la actualidad todavía se utiliza y comercializa este tipo de tecnología. La compañía INSTEON especializada en tecnologías de automatización hizo mejoras a este protocolo, se integra protocolos inalámbricos,

dio robustez a los dispositivos y con la ventaja de poseer tecnología hibrida que evita perder la comunicación con los demás elementos de la red.

Aunque este avance tecnológico aporto a gran medida al desarrollo de la domótica el verdadero impulso se impuso a finales de la década de los 80 e inicio de los 90, momento en, el cual, las computadoras personales salieron al mercado y su popularidad se incrementó, convirtiéndose en un artículo de primera necesidad en las oficinas. L a presencia de estos nuevos dispositivos origino a que los edificios comenzaran a instalar sistemas de cableado estructurado (SCE), el cual, permitía trasportar internamente datos y voz. Es en ese momento en, el cual, a todos los edificios que contaban con SCE los comenzaron a llamar edificios inteligentes (Rojas García, 2015).

A comienzos de los años noventa esta tecnología que en su inicio solo era utilizado con fines comerciales, comenzó a expandirse a los hogares y gracias a los avances de las comunicación y redes informáticas, el WIFI y la evolución de los protocolos de comunicación han permitido que hoy en día se ofrezca un sinfín de posibilidades para crear verdaderas casas inteligentes.

En la actualidad los servicios domóticos han ganado popularidad, los protocolos actuales permiten que las personas gocen de un desarrollo tecnológico que se consideró impensables años atrás, los nuevos sistemas inalámbricos proveen una nueva tecnología que permite una baja tasa de envío de datos y rapidez de respuesta, además, de un sinnúmero de funciones que permiten a los usuarios mantener los dispositivos de sus hogares conectados y monitoreados. (INAVIRTUAL, s. f.)

El desarrollo de la domótica como un sistema automatizado ha sido de gran provecho tanto en las oficinas, edificios y hogares. La evolución de ella ha sido drástica y novedosa tanto así que hoy en día a pesar de su costo elevado en algunos países es un sistema sumamente beneficioso para los usuarios que lo utilicen.

Al hablar de domótica, se esboza inmediatamente el termino de control remoto, que es muy utilizado para cualquier proceso, logra como resultado el manejo de los dispositivos que se requieren contralar. En el caso de una vivienda inteligente basada en protocolo de comunicación en su ámbito doméstico se controla desde una computadora, un celular, un PDA, elementos como los sistemas de iluminación, climatización, así como cualquier dispositivo electrónico; utilizar para compras por internet o incluso vigilar las actividades en distintas habitaciones a través de una cámara web. La flexibilidad de este tipo de control permite a las personas un mejor desempeño en las actividades cotidianas a nivel familiar como tecnológico, al promover el bienestar social y tecnológico si se habla de automatización.

La implantación de domótica en una vivienda proporciona un sin número de beneficios y ventajas con respecto a una tradicional desde diversos puntos de vista como la seguridad, el ahorro de recursos, la comodidad, la protección del medio ambiente y el confort; todo esto se resumen en una mejor calidad de vida y una de las mejores inversiones que se realizan (Herrera Quintero, 2005).

1.3. Seguridad IoT

Si bien es cierto el concepto de seguridad de la información en la actualidad no es nuevo, la implementación de la tecnología IoT presenta nuevos y únicos desafíos de seguridad. Así pues, garantizar la seguridad en un sistema IoT es el objetivo principal, a medida que esta tecnología es más difundida y se integra en todos los aspectos de nuestra vida hay que generar en los usuarios confianza en los dispositivos, en sus servicios y funciones que ofrecen, así como también, mantener sus datos seguros y libre de vulnerabilidades.

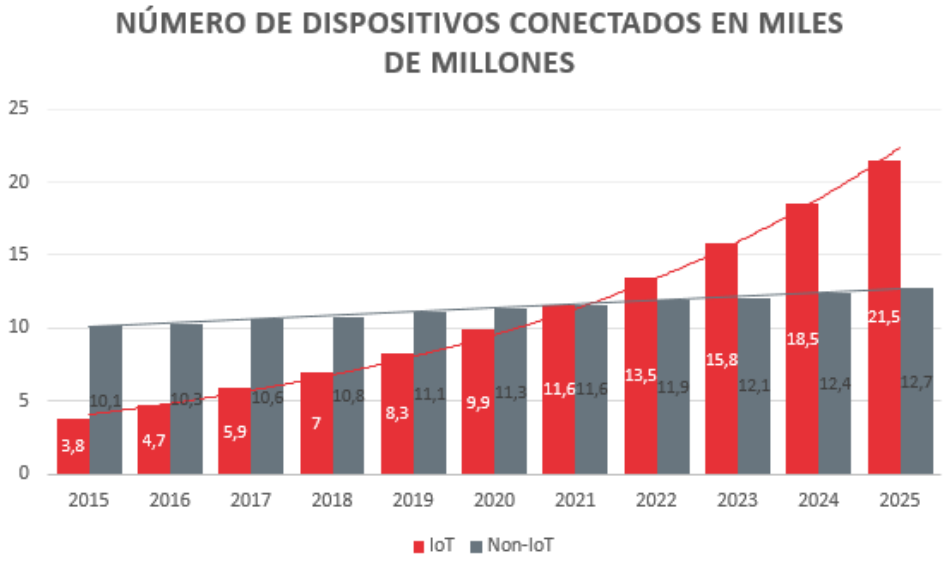
Debido a la gran cantidad de dispositivos IoT conectados a la red, los ciberdelincuentes tienen una brecha de ataque cada vez más extensa, basta con encontrar alguna vulnerabilidad en un dispositivo para cometer algún tipo de delito informático al poner en evidencia información delicada y confidencial de los usuarios (Arias Silva, 2019).

Desde la perspectiva de la industria el Internet de las cosas aún no ha alcanzado la madurez en términos de seguridad y privacidad de datos razón, por la cual, se menciona a IoT como “Internet de las Amenazas, Inseguridad de las Cosas” son varios de los significados que se ha dado a IoT debido al crecimiento exponencial de dispositivos IoT a lo largo del tiempo, así como la utilización de dispositivos inteligentes que no incluyen funciones de seguridad por los fabricantes.

Los dispositivos IoT han dejado de ser un mercado minorista, la tendencia de tener todos los dispositivos interconectados en conjunto con el bajo costo en la fabricación de las tecnologías impulsa a gran medida su popularidad. Además, se visualiza que en los próximos años este hecho vaya en incremento de la mano con la implementación del espacio de direcciones IPV6 y el despliegue de la nueva tecnología 5G en todas las redes móviles (Meneghello, Calore, Zucchetto, Polese, & Zanella, 2019).

Como se visualiza en la figura 4 la tasa de crecimiento de los dispositivos IoT es exponencial y se estima que en 2025 estos sean más de 21.000 millones, en comparación con los dispositivos que no son IoT (non-IoT), los cuales, presentan un bajo crecimiento anual.

Figura 4. Estadística de dispositivos IoT en el tiempo



Fuente: IoT Analytics, 2018

Existen varias razones, por la cual, los riesgos de seguridad del Internet de las cosas en la actualidad suponen el reto más importante para los usuarios y fabricantes:

- El número de dispositivos IoT crece a toda velocidad y los fabricantes de dispositivos instalan sensores IoT en todos los aparatos electrónicos, coches, combillas, toma corrientes, refrigeradores, entre otros electrodomésticos. Estos sensores permiten a los dispositivos conectarse a internet para comunicarse con los sistemas informáticos para su control y programación.
- Los dispositivos Iot, además, de proporcionarnos numerosas y novedosas funciones y capacidades, introducen posibles vulnerabilidades de seguridad. Por esta razón la tecnología IoT tiene que ser sometida periódicamente a mantenimiento y protección a medida que se detectan nuevas vulnerabilidades.
- Muchos dispositivos no incluyen funciones de seguridad, la velocidad con la que los fabricantes sacan nuevos dispositivos al mercado provoca que dejen de lado el desarrollo de una interfaz de seguridad y aunque los propios dispositivos son cada vez más sofisticados a menudo no existen sistemas de seguridad IoT subyacentes para protegerlos.
- Inclusive si los dispositivos IoT incluyen funciones de seguridad, los usuarios generalmente no dedican el tiempo suficiente para configurarlos y mantenerlos adecuadamente. Su fácil configuración y puesta en marcha hace que la gente se preocupe más por el ver que su dispositivo funcione sin novedad que configurar las funciones de seguridad o tal vez no saben cuánto afecta la seguridad a la privacidad de sus datos.

Como se pude apreciar la aplicabilidad en este campo es ilimitada lo que provoca que exista una feroz competencia entre las empresas de tecnología por quien lanza más rápido al mercado un dispositivo IoT, este desarrollo prematuro de productos hace que se cometa errores en la implementación de la seguridad, en los casos en los que se implementa (Molina García, 2006).

La empresa de seguridad Kaspersky Lab, en 2015 comprobó que la seguridad de la mitad de los dispositivos analizados no eran seguros. A principios del 2018 se publicó un estudio en el que se constataban los mismos resultados. En este estudio la principal característica que llama la atención es que las vulnerabilidades más comunes encontradas ha sido una contraseña débil por defecto y más aún que no es posible cambiarla (Miñano Carmona, 2019)

Como consumidores nos parece útil y divertido contar con un hogar digital que nos facilite las tareas del hogar y que ajuste la comodidad del hogar según nuestras peticiones, pero no se toma en cuenta los riesgos de seguridad que conlleva esto: toda la información, la inteligencia y la intercomunicación necesaria para alcanzar ese nivel de automatización lo aprovechan personas maliciosas que desean esa misma información para sus propios fines, a continuación, se detalla algunas de las principales amenazas para la seguridad IoT de consumo:

Protección de datos: En los últimos años los dispositivos inteligentes han llevado la recopilación de datos a niveles que nunca se pensaba, lo que se ha convertido como la principal preocupación la privacidad del IoT. Por ejemplo, algunos altavoces, televisores graban conversaciones mientras ejecutan y escuchan ordenes inclusive han intentado obtener datos de estos por medio de vías judiciales durante alguna investigación al pensar que un pequeño altavoz habría grabado una conversación incriminadora. Por otra parte, algunos distribuidores han tenido que retirar juguetes al descubrir que un osito o un artefacto graba voces de los niños y los envía al fabricante.

Los dispositivos IoT recopilan toda clase de datos del usuario, como distribución de horarios, hábitos de las personas, entre otras. Un estudio comprobó que, de 81 dispositivos de consumo IoT comunes 72 enviaban datos a terceros distintos del fabricante original. Eso no significa que se deba apagar cualquier tipo de conexión, los dispositivos necesitan por lo menos un punto de acceso a datos para realizar las funciones por las que lo compraron, sin embargo, cabe la posibilidad que el usuario tenga un mínimo control sobre el acceso del dispositivo.

Amenazas de *malware*: Como los dispositivos IoT no cuentan en su mayoría con medidas de seguridad, los ciberdelincuentes no les resulta difícil acceder dentro, así como sucede con los dispositivos comunes como PCS, teléfonos móviles, los dispositivos IoT son vías para una infección de malware.

Algunos ciberdelincuentes han utilizado malware para transformar dispositivos IoT como medios para propagación de más malware o para contribuir en ataques distribuidos de negación de servicio o simplemente un malware que permita el bloqueo del dispositivo.

Dispositivos secuestrados: Las cámaras de seguridad que cuentan con escasa seguridad son foco principal de los ciberdelincuentes que buscan secuestrar dispositivos IoT. En varias ocasiones se reciben advertencias falsas cobre misiles balísticos y amenazas sobre secuestros de menores de edad. Otros incidentes populares son voces que surgen de la cámara o desde otro dispositivo IoT conectado a la red, así como también, el control de dispositivos sensores que permiten regular la temperatura o controlar ciertos aspectos del hogar.

Algunas de las situaciones son resultados de un mal comportamiento del usuario al momento de la configuración de la seguridad, al no usar contraseñas robustas o la utilización de las mismas contraseñas en todos los sitios. Los ciberdelincuentes tras robar estas contraseñas obtienen acceso a las aplicaciones que administran los dispositivos inteligentes, si sucede algo como esto son muy pocas las aplicaciones que avisan si un tercero comienza a utilizar los dispositivos de la red.

Intrusión en el Hogar: Una vez que el ciberdelincuente ha logrado estar dentro de un dispositivo de internet de las cosas, o ya está dentro de la red a través de uno de estos dispositivos, los intrusos recopilan datos privados sobre su hogar y venderlos.

Las personas muchas de las ocasiones no ponen atención a esto o no saben el valor que tiene el historial del comportamiento de mi casa o de mis hábitos. Pues

es que las posibles vulnerabilidades son muchas, algunos dispositivos inteligentes almacenan contraseñas, números de tarjetas de crédito, claves de cifrado u otra información. Un delincuente, también, hace uso de los datos de su hogar para saber si la casa está vacía o sin monitorear (Fisher, 2019)

Los dispositivos IoT al tener una naturaleza interconectada conlleva a que un dispositivo mal asegurado que esté conectado al internet pone en riesgo la seguridad y la integridad a nivel global de los sistemas.

Los vectores de ataques más comunes utilizados por los ciberdelincuentes en los dispositivos IoT son:

- **Ataque de fuerza Bruta:** Para obtener contraseñas, descubrir puertos abiertos (por ejemplo, al usar la aplicación telnet), o incluso el *login* y *password* de uno de los nodos para acceder a la red.

- **Ataque de negación de servicio (DDoS):** Ataques que inhabilitan el sistema y le impiden realizar su función. Si un atacante conoce o adivina una secuencia de acciones (por ejemplo, una secuencia de voltajes en su módulo de alimentación) en un sensor que provoca que deje de tomar muestras; esto va a impedir que el sistema al que pertenece ese sensor realice su función. Por ejemplo, en un sistema de ayuda a la conducción en un vehículo en el que se toman muestras a través de una cámara que captura las imágenes de señales del tráfico. Si se inhabilita dicha cámara o se provoca un malfuncionamiento, el sistema de ayuda a la conducción no opera correctamente, incluso informar mal de señales con la velocidad máxima incorrecta, esto ocasiona que el conductor incremente la velocidad del vehículo en una zona que está limitada a menor velocidad, lo cual, llega a provocar que el conductor cometa una infracción y se vea obligado a pagar una multa por exceso de velocidad.

- **Acceso a uno de los nodos de la red:** El atacante, consciente de que la seguridad desde el exterior es probablemente más robusta que desde el

interior, logra encontrar un punto o un nodo más débil con menos protección, acceder a dicho nodo para entrar en la red y una vez dentro realizar el ataque al nodo o al subsistema que desee. En este tipo de ataques, también, emplea uno de estos nodos, como una etapa más (trampolín) para cubrir el rastro del atacante, que perpetra un ciberataque a otro sistema y necesita ocultar su identidad y evitar que su IP sea rastreada al usar conexiones sucesivas a varios nodos de distintas redes.

Normalmente en estos casos el atacante, también, combina técnicas de fuerza bruta, para conectarse a los diferentes nodos de la red.

- **Obtención de datos:** El atacante accede al sistema o al dispositivo IoT para obtener información y revelarla o entregársela a un tercero, bien sea de los datos personales de los usuarios del sistema (*logins, passwords*, números de tarjetas de crédito, números de cuenta bancaria, etcétera), de la organización a la que pertenece la IoT o del propio sistema.

Es muy probable que para efectuar uno de estos ataques, el cibercriminal tenga que combinar técnicas, o aprovecharse de varias debilidades a la vez. Es por tanto primordial proteger el sistema, aunque simplemente se fortalezca uno de dichos puntos débiles, se evita varias tipologías de ataques con relativamente poco esfuerzo.(Domínguez Margareto, 2020)

Los consumidores y empresas cada vez cuentan con más dispositivos IoT que son capaces de comunicarse entre ellos, estos dispositivos se extienden más allá de los hogares y oficinas, hasta llegar inclusive a los autos u otros vehículos de motor hasta lograr formar una ciudad inteligente *Smart City*.

Resulta aún complejo que un software proteja cada dispositivo de manera individual, al combinar todos los dispositivos en un solo sistema la vulnerabilidad de un dispositivo se vuelve la vulnerabilidad de todo el sistema. Por ello antes de introducir un dispositivo nuevo a un sistema de hogar u empresa hay que asegurar de tener una estrategia de seguridad integral en la red.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología de Investigación:

Tipo y enfoque de investigación

La modalidad utilizada en el proyecto está orientada bajo un enfoque cualitativo, el cual, permite comprender la realidad y el contexto del objeto que se investigó, al usar la recolección de datos de tipo cualitativo permite indagar a profundidad sobre los diferentes temas que comprenden el internet de las cosas. Con el enfoque cualitativo se obtiene descriptivos al usar distintas fuentes de información para entender el tema que se investigó.

Búsqueda Bibliográfica

Para realizar la investigación es necesario realizar una revisión bibliográfica, necesaria para comprender los conceptos, generar ideas y comprobar el estado actual de los conocimientos del tema investigado. La investigación bibliografía se basó en el análisis de documentos, revistas, paginas académicas de internet con la finalidad de aportar y recopilar con información necesaria para el desarrollo del presente proyecto.

Analítico

Se empleo el método analítico, el cual, implica descomponer el objeto de estudio en diferentes partes para facilitar su análisis y ayudar a comprender los elementos que lo conforman, de esta manera se conoce la naturaleza del objeto que se estudia y a partir de eso se comprende su comportamiento y replicarlo bajo un ambiente controlado.

Este método se usó para conocer sobre el Internet de las Cosas, sus características, su utilización en el campo de la domótica, así como también, sus

diferentes topologías, protocolos de comunicación y las vulnerabilidades, a las cuales, son susceptibles estos sistemas, para establecer las bases e indicadores para la simulación de un sistema domótico en un entorno controlado.

Técnicas e instrumentos de recolección de datos

Para el desarrollo de la investigación es necesario la recolección de datos e información que sirvan de sustento y apoyo para solucionar el problema, de esta manera se usa la siguiente técnicas e instrumento para la obtención de datos:

- Análisis documental:

Instrumento:

Ficha de registro de datos

La ficha de registro de datos se usa como instrumento de la investigación documental mediante, el cual, se registra los datos significativos de las diferentes fuentes consultadas sobre los temas esenciales para el desarrollo de la simulación y es información base para la solución del problema planteado. Los elementos biográficos del presente proyecto fueron usados como fuentes de información para el desarrollo de la presente investigación, en el cuadro 1 se evidencia el formato de ficha de registro de datos que fue usada para toda la bibliografía.

Cuadro 1. Ficha de registro de datos

Ficha de Registro de datos:	
Autor	
Tema	
Dirección electrónica	
Fecha de consulta	

Fuente: Elaboración propia

Bitácora de búsqueda

La bitácora de búsqueda es un instrumento que permite registrar los detalles y dirección de los sitios web donde se encontró y recolecto información para el desarrollo del proyecto, descritas en el cuadro 2.

Cuadro 2. Bitácora de búsqueda

Bitácora de búsqueda			
Motor de búsqueda	Palabra clave	Dirección de la pagina	Información que se encontró
Google Web	Internet de las cosas	https://www.redhat.com/es/topics/internet-of-things/what-is-iot	Descripción general, funcionamiento del Internet de las Cosas
Google Web	Internet de las cosas	https://www.sap.com/latinamerica/insights/what-is-iot-internet-of-things.html	Definición de internet de las cosas, evolución IoT
Google Web	Internet de las cosas	https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html	Introducción y tecnologías IoT
Google Web	Internet de las cosas	https://www.sas.com/es_mx/insights/big-data/internet-of-things.html	Historia del Internet de las Cosas
Google Web	Internet de las cosas	https://www.avast.com/es-es/c-what-is-the-internet-of-things#gref	Fundamentos de IoT
Google Web	Arquitectura IoT	https://www.inforges.es/post/iot-o-internet-de-las-cosas-que-es	Capas que conforman IoT, resumen y ejemplos
Google Web	Arquitectura IoT	https://www.t-systemsblog.es/estas-son-las-capas-del-internet-de-las-cosas/	Capas del internet de las cosas
Google Web	Arquitectura IoT	https://www.ecotec.edu.ec/material/material_2015T_TPS420_11_43905.pdf	Definición y descripción de las tres capas básicas del IoT
Google Web	Arquitectura IoT	https://repositorio.unillanos.edu.co/bitstream/handle/001/1486/Monograf%EDa%20Internet%20de%20las%20cosas%20modelos%20de%20comunicaci%F3n,desaf%EDos%2	Modelos de comunicación, desafíos y aplicaciones

		0y%20aplicaciones..pdf;jsessionid=5338549B1C1A859FBBAD95629ACB421 1?sequence=3	
Google Web	Seguridad y privacidad IoT	https://www.avast.com/es-es/c-what-is-the-internet-of-things#gref	Ventajas IoT, seguridad y privacidad IoT
Google Web	Domótica	https://comparaiso.es/domotica	Definición de la domótica, funcionamiento y ejemplos
Google Web	Domótica	http://www.cedom.es/sobre-domotica/que-es-domotica	Aportes de la domótica en el mundo
Google Web	Domótica	https://www.enerxia.net/portal/index.php/i-domo/884-domotica-tipos-de-sistemas-domoticos-elementos-de-red-y-topologia-de-las-redes-domoticas	Tipos de sistemas domóticos
Google Web	Domótica	https://tucasainteligente.org/comunicaciones/	Funcionamiento de comunicación domótica
Google Web	Arquitectura Domótica	http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-56092005000200006	Viviendas Inteligentes, arquitectura y protocolos
Google Web	Topología domótica	https://micasainteligente.site/sistemas-domoticos/	Tipos y topologías de sistemas domóticos
Google Web	Protocolos de comunicación domótica	http://catarina.udlap.mx/u_dl_a/tales/documentos/mesp/galeana_m_ma/capitulo2.pdf	Sistemas y protocolos existentes en domótica
Google Web	Vulnerabilidades IoT	https://corredoresymediadores.senassur.es/destacados/iot-ventajas-y-vulnerabilidades/	Ventajas y vulnerabilidades del Internet de las Cosas
Google Web	Seguridad IoT	https://repository.unad.edu.co/bitstream/handle/10596/33326/naariass.pdf?sequence=1&isAllowed=y	Vulnerabilidades más frecuentes en dispositivos IoT

Fuente: Elaboración propia

2.2. Metodología Desarrollo:

La simulación digital es una técnica que permite simular en el comportamiento de un sistema como si fuese la vida real, permite someterlo a distintos cambios, estímulos y pruebas. La simulación permite comprender y analizar los procesos de un sistema, así como también, evaluarse sin correr el riesgo que existe si se las lleva a cabo en un sistema real, permite estudiar su estructura y su respuesta ante ciertas situaciones para comprender la causa y efecto entre ellos.

En la figura 5 se describe las etapas de la metodología de simulación que se lleva a cabo para la preparación del manual técnico.

Figura 5. Metodología de simulación

Fuente: Elaboración propia

Formulación del problema:

Tener claros los objetivos del proyecto que se va a desarrollar y expresarlos formalmente

Diseño de modelo conceptual:

Se elabora un diseño conceptual para entender de una mejor manera como son los procesos que interactúan en un sistema IoT, se usara herramienta de modelado para diagramas de fujo o de secuencia.

Recolección de datos:

Se verifica que los datos obtenidos para el desarrollo sean confiables y suficientes para el modelo planteado

Construcción del modelo:

Se construye el modelo sin olvidar que el propósito no es el modelo en sí, sino resolver el problema. En esta etapa se usa entorno o software especializado para la simulación.

Verificación y validación:

La verificación implica asegurarse de que el modelo de simulación sigue las especificaciones del modelo conceptual. La validación requiere comprobar que las hipótesis de trabajo sean correctas, es decir, el modelo se basa en el mundo real para que sus resultados sean válidos.

Análisis:

Se experimenta con el modelo realizado sometiéndole a diferentes pruebas de seguridad para identificar las vulnerabilidades que se investigó.

Preparación del manual técnico:

Preparación del documento final, en el cual, evidencia el cumplimiento del objetivo del proyecto.

Formulación del problema:

Las amenazas latentes en los dispositivos IoT en la actualidad ponen en riesgo los datos personales y la infraestructura de los sistemas domóticos que se implementan hoy en día en la gran mayoría de los hogares del mundo. Razón, por la cual, esta simulación tiene como objetivo simular un sistema domótico con una arquitectura y un modelo adecuado para someterlo a pruebas de vulnerabilidad para analizar sus resultados y así elaborar un manual de buenas prácticas para mitigar los riesgos que fueron evaluados.

Para establecer límites para el desarrollo y definir los plazos y el entregable del proyecto desarrollado se elaboró un formulario guía de alcance como se detalla en el cuadro 3, en el cual, permite visualizar el ciclo de vida del proyecto con el fin de garantizar que el objetivo planteado se cumpla en el tiempo establecido.

Cuadro 3. Formulario de alcance del proyecto

Nombre:	ANÁLISIS DE AMENAZAS IOT EN UN SISTEMA DOMÓTICO
Objetivos del Proyecto:	Analizar las amenazas de ciberseguridad que presentan los dispositivos IoT en un sistema domótico
Recursos:	Computadora
Entregable	Manual técnico de buenas prácticas
Hoja de ruta y cronograma	
20 al 26 de noviembre de 2021: Introducción del proyecto 26 de noviembre al 04 de diciembre de 2021: Definición de las bases teóricas del proyecto 04 al 09 de diciembre de 2021: Definición de la metodología de la investigación 09 al 13 de diciembre de 2021: Definición de la metodología de desarrollo 14 de diciembre de 2021: formulación del Problema 15 de diciembre de 2021: Diseño del modelo conceptual 15 al 16 de diciembre de 2021: Recolección de datos 16 al 19 de diciembre de 2021: construcción del modelo 20 al 31 de diciembre: Verificación y validación de del modelo 04 al 15 de enero 2022: Análisis del modelo 16 de enero al 03 de febrero 2022: Preparación del manual técnico de buenas prácticas	
Fuera del alcance:	

Fuente: Elaboración propia

Diseño de modelo conceptual:

El modelo conceptual es la descripción de la como se relacionan los diferentes conceptos de un problema, se usa para representar un problema mediante

gráficos, al modelar el problema se identifica el funcionamiento de todos los procesos que intervienen para lograr solucionar los problemas.

En esta fase se incluyen las entidades del sistema que se va a simular, las relaciones que existen entre los elementos, además, la estructura del sistema desde el punto de vista de datos. Tiene por objeto describir formalmente los datos que se usara en el sistema para lograr entender de una mejor manera el fujo de la información dentro de un sistema domótico

Arquitectura IoT

Los dispositivos IoT cuentan con tres capas: capa física, capa de red y de capa de aplicación. La capa física consta de sensores, Radio *Frequency Identification* (RFID), medidores inteligentes y otros dispositivos para detectar parámetros físicos externos como presión, temperatura, humedad, entre otras para transmitirlas a la capa de transporte.

En la capa de red, los datos se envían a la capa superior, la fragmentación de paquetes y la optimización de enrutamiento son realizados por la capa de red. Los datos se almacenan y analizan para buscar la información que es procesada mediante la capa de gestión de datos. Esta capa utiliza técnicas avanzadas como *Big Data* y *cloud computing*.

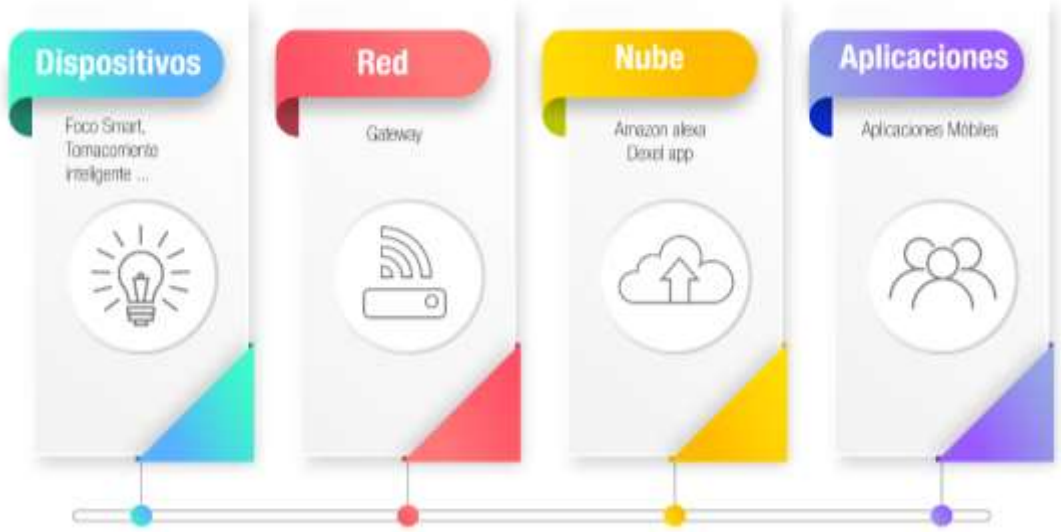
En la capa de aplicación se diseñan los protocolos de interacción con el usuario.
RPL es un protocolo de enrutamiento para redes inalámbricas de bajo consumo de energía y susceptibles a pérdidas de paquetes (Pérez, Bustos, Berón, & Rangel Henriques, 2018).

La arquitectura IoT basada en RPL de igual manera se explica en tres capas. La capa MAC encargada de administrar los datos enviados y recibidos, la capa física. La capa de red y transporte con protocolos RPL, ICMP y UDP gestionan los problemas de enrutamiento y transporte, la capa de aplicación se diseña los protocolos HTTP, CoAP y MQTT, en resumen, los protocolos de comunicación

están desarrollados para satisfacer las demandas de IoT de baja potencia, baja memoria y capacidad de procesamiento de datos (Sebastian & Sivagurunathan, 2018).

Para simular las vulnerabilidades y amenazas que presenta un sistema domótico, se simuló un hogar típico con tecnología IoT, en la cual, se integraran dispositivos inteligentes para comunicación entre si mediante su plataforma de internet a la nube para que, finalmente, sean controlados mediante aplicaciones con interacción grafica de los usuarios finales que hacen uso de estos sistemas como se observa en la figura 6.

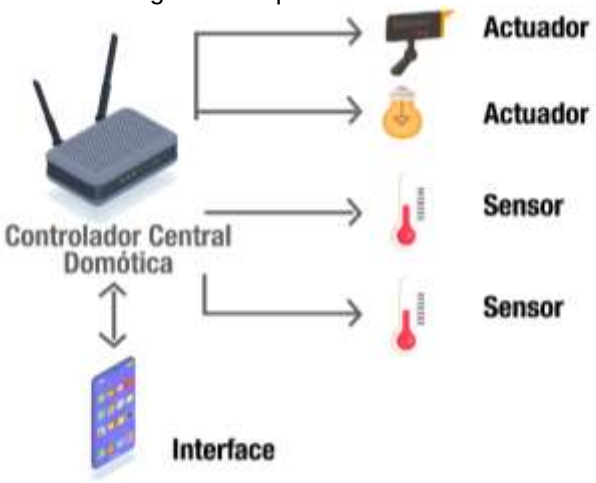
Figura 6. Diseño de la arquitectura IoT



Fuente: Elaboración propia

La arquitectura que se usó es centralizada, como se muestra en la figura 7 usa un controlador centralizado, el cual, envía la información a los dispositivos e interfaces a través del programa que se ha configurado y esta información es recibida por los sensores, los dispositivos y los usuarios. La conexión se realiza mediante una topología estrella, por medio, de la cual, todos los dispositivos inteligentes se interconectan a través de un controlador central, misma que aprovecha los recursos de la red y minimiza el uso de la energía eléctrica debido a que todos los sistemas están activos de forma continua todo el día durante todo el año.

Figura 7. Arquitectura Centralizada



Fuente: Elaboración propia

Una vez elegidas la arquitectura y la topología de conexión de los dispositivos IoT, en la figura 8 se muestra el modelo del sistema domótico a simular, este modelo es el más frecuente existente en la mayoría de los hogares.

Figura 8. Modelo del sistema domótico genérico

Fuente: Elaboración propia

Descripción del Modelo del Sistema domótico

El planteamiento de los diagramas de arquitectura y el modelo del sistema permite detallar los componentes del sistema y su interacción, así como también,

los protocolos de comunicación y su tecnología, el modelo del sistema domótico está basado en las tres capas básicas*, hardware, middleware* e interfaz de usuario.

La capa de hardware incluye los sensores y actuadores los mismos que incluyen una tecnología de comunicación con el Gateway. Los protocolos más utilizados para la comunicación en entornos domóticos son: Zigbee 802.15.4, WiFi 802.11, Z-Wave G.9959, Bluetooth de baja energía (BLE).

En la tabla 1 se observa las principales características que presentan los protocolos más usados por los dispositivos IoT para su comunicación.

Tabla 1. Comparación de protocolos de comunicación

	ZigBee	Z-Wave	Bluetooth	Wifi
Frecuencia de operación	2.4 Ghz, 915 Mhz, 868 Mhz	900 Mhz	2.4 Ghz	2.4Ghz, 5Ghz
Alcance	500 m	100 m	50 m	100 m
Tasa de datos	250 kbps	40 kbps	1 Mbps	600 Mbps
Número de nodos	65.536	232	8	N/A
Consumo medio	Tx: 25 – 30 mA Rx: 20 – 30 mA	Tx: 30 – 40 mA Rx: 20 – 30 mA	Tx: 15 – 20 mA Rx: 15 – 20 mA	Tx: > 220 mA Rx: > 215 mA

Fuente: Comparación de protocolos de comunicación (González García, 2017)

Para la comunicación con la red se incluye un dispositivo concentrador que cumple la función de *Gateway,* el cual, permite la comunicación entre dispositivos y la red para transmitir datos hacia la capa middleware. La capa *middleware* usa el concepto de la computación en la nube, dispone de recursos para el procesamiento de los datos que se han generado en la capa anterior, los almacena y convierte en información que es entregada a los usuarios.

Cloud Computing ofrece al usuario la posibilidad de almacenar y acceder a datos y programas por medio del internet desde cualquier lugar donde se encuentre y desde cualquier dispositivo. La computación en la nube tiene un papel primordial para la gestión de la gran cantidad de datos que se recolectan de los dispositivos IoT, es el complemento fundamental para el almacenamiento, análisis y acceso a toda la información recolectada.

La capa de interfaz de usuario permite la presentación de los diferentes servicios, así como la administración de los dispositivos conectados mediante el uso de distintas aplicaciones.

Recolección de datos:

Vectores de ataque IoT de OWASP

Open Web Application Security Project (OWASP) es una fundación sin fines de lucro, la cual, trabaja para ayudar a mejorar la seguridad de software por medio de proyectos de código abierto, para ayudar a comprender las vulnerabilidades que tiene los dispositivos IoT OWASP elaboró una lista de las 10 vulnerabilidades de seguridad principales que tienen los dispositivos IoT detallados, a continuación, en el cuadro 4.

Cuadro 4. Top 10 Vulnerabilidades

Vulnerabilidad	Descripción
Contraseñas débiles, adivinables o codificadas	La mala administración de contraseñas es un problema habitual de y crítico de seguridad, en especial porque muchos de los propietarios de dispositivos inteligentes dejan la configuración de contraseña predeterminada
Servicios de red inseguros	Conexiones de red inseguros y puertos innecesarios abiertos incrementan la superficie de ataque de los dispositivos IoT, lo cual, aumenta la posibilidad de sufrir perdida de información o ejecución remota de códigos.
Interfaces de ecosistemas inseguras	Las interfaces con las que interactúan los dispositivos IoT se ven afectadas por fallas de seguridad, interfaces móviles, web aplicaciones o la nube proveen acceso a delincuentes informáticos acceso no autorizado a través de una configuración insegura
Falta de un mecanismo de actualización seguro	Las actualizaciones aportan un arma valiosa al momento d abordar un fallo de seguridad en los sistemas y la falta de una configuración adecuada de actualizaciones da como resultado software con un alto índice de fallos de seguridad.
Uso de componentes inseguros u obsoletos	Componentes heredados y obsoletos al no contar con las actualizaciones necesarios ponen en riesgo el sistema IoT, estos componentes incorporan fallas por medio, de las cuales, personas no autorizadas tienen acceso a los sistemas.
Protección de la Privacidad insuficiente	El almacenamiento no autorizado de datos personales o almacenamiento de datos locales son una vulnerabilidad de seguridad debido a que la información queda expuesta a personas no autorizadas
Transferencia y almacenamiento de datos inseguros	Cifrado insuficiente o deficiente de los datos e inexistencia de mecanismos de autenticación proveen una puerta de entrada para que ciberdelincuentes roben nuestra información
Falta de gestión de dispositivos	La falta de una imagen de la infraestructura de todos los dispositivos IoT que nos permita saber qué es lo que sucede con el sistema, se vuelve imposible administrar la defensa y las respuestas ante las amenazas que se presenten
Configuración predeterminada insegura	La configuración predeterminada es aplicada al tomar en cuenta la seguridad del usuario final y a largo plazo, por lo general la configuración predeterminada representa un enfoque mínimo e incluso traer consigo vulnerabilidades, contraseñas y servicios expuestos que ejecutan permisos de root, los dispositivos tienen la posibilidad de que los administradores corrijan las falencias.
Falta de endurecimiento físico	No descuidar el endurecimiento físico de los dispositivos contra ataques que extraen información confidencial que es usada para ataques remotos o para obtener control del dispositivo

Fuente: OWASP

Amenazas IoT

Tradicionalmente las amenazas a la seguridad de los dispositivos IoT surgen en el entorno virtual y se dirigen al proceso de manipulación de datos, es así que conduce a la interpretación de seguridad de la tecnología de la Información (TI)

como el conjunto de sus principales aspectos como son confidencialidad, integridad, disponibilidad (CIA).

La Unión Internacional de Telecomunicaciones (ITU-T Y.4806) clasifica las amenazas principales de los dispositivos IoT según sus vectores de impacto, los cuales, provienen de un entorno virtual y del entorno físico, como se muestra en la figura 9 los problemas surgen de ambos tipos de entornos y afectar los aspectos físicos , aspectos virtuales y del dispositivo en si (UIT-T, 2017).

Figura 9. Clasificación amenazas IoT

Fuente: ITU-T Y.4806

Amenazas entorno virtual:

Las amenazas lógicas afectan al software de los dispositivos, comprenden una gran variedad de programas informáticos que dañan la integridad del sistema informático y aprovechar las vulnerabilidades de los dispositivos.

Amenazas entorno físico:

Las amenazas físicas afectan a la parte del hardware del sistema, se producen de forma voluntaria o involuntaria, como ejemplo se nombra los siguientes: robos, sabotajes, incendios, cortes eléctricos, catástrofes naturales o artificiales y demás peligros a los que están expuestos los dispositivos.

En este sentido el especto primordial a estudiar es el vector que proviene del entorno virtual, el cual, a través de las vulnerabilidades que presentan los dispositivos IoT conectados a la red afectan tanto su entorno virtual como físico.

Modelo de amenazas STRIDE

STRIDE es un acrónimo de seis categorías de amenazas: Suplantación de identidad *(Spoofing*), manipulación de datos (*Tampering*), amenazas de repudio (Repudio), divulgación de información (*Information disclosure*), denegación de servicio (*Denal of service*) y elevación de privilegios (*Elevation of privileges*).

STRIDE desarrollado por Microsoft, modela riesgos y evalúa las amenazas para los entornos de tecnologías de la información. El modelo STRIDE se amplió, también, para incorporar amenazas que están presentes en los sistemas IoT.

En términos de STRIDE un atacante es la entidad maliciosa que tiene por objetivo evitar que un activo trabaje como fue programado, compromete su integridad, disponibilidad y confidencialidad de un sistema de datos. Los adversarios aprovechan las vulnerabilidades de dichos activos para comprometer la información del sistema, razón, por la cual, el modelo de amenazas describe un conjunto de posibles ataques a un activo, estas amenazas se clasifican según la gravedad y las posibles contramedidas .(Schrecker, 2016)

En el cuadro 5 se observa con mayor detalle las amenazas del modelo STRIDE.

Cuadro 5. Amenazas STRIDE

Modelo de amenazas STRIDE	
Suplantación de identidad *(Spoofing*),	Una persona o dispositivo usa credenciales de otro usuario con el objetivo de acceder a los datos y acciones a las que no tiene autorización.
Manipulación de datos (*Tampering*)	Se trata de modificar y manipular la información para causar caos en el sistema. Manipulación de datos en rutas del sistema, manipular datos sensibles en puntos de transporte procesamiento o almacenamiento.
Amenazas de repudio (Repudio)	Negar a una persona o dispositivo involucrado en una transacción o evento específico del sistema o a su vez transmitir datos incorrectos que confunde procesos de análisis y operación
Divulgación de información (*Information disclosure*)	Intrusión de una persona no autorizada con el fin de interceptar la transmisión de datos y capturar información confidencial
Denegación de servicio (*Denal of service*)	Capacidad de hacer que un servicio en particular deje de estar disponible, generalmente a través del consumo de recurso o ejecuciones no confiables
Elevación de privilegios (*Elevation of privileges*).	Capacidad de que un usuario sin privilegios gane suficiente acceso para comprometer el sistema. El atacante penetra las defensas de un sistema y transformarse en un dispositivo más de la red.

Fuente: Industrial Internet of Things .(Schrecker, 2016)

Construcción del modelo:

La aplicación práctica de un modelo domótico permite profundizar el conocimiento sobre la seguridad de los sistemas, mostrar el funcionamiento, las ventajas y las diferentes experiencias que brinda a los usuarios, como también, las vulnerabilidades y amenazas a los que se expone estos sistemas.

Para la construcción del modelo domótico se implementó un hogar IoT común, se tomó como referencia la arquitectura y topología seleccionada para este estudio, el sistema domótico incluye dispositivos Iot, la red de comunicación, por la cual, se integran los dispositivos, la plataforma de internet y la nube, así como también, la aplicación con, las cuales, los usuarios interactúan y manipulan los dispositivos.

En la figura 10 se observan los dispositivos IoT que se usan con frecuencia en los hogares, mismo que se usó para realizar las diferentes pruebas ante las amenazas del modelo STRIDE.

Figura 10. Dispositivos IoT implementados

Fuente: Elaboración propia

En el cuadro 6 se detalla el modelo y la marca de los dispositivos que se usaron para realizar las pruebas.

Cuadro 6. Detalles dispositivos IoT implementados

#	Dispositivo	Modelo	Marca
1	Iluminación	Wifi RGB Smart A60 Ligth Bulb	Dexel
2	Iluminación	Smart LED Ligth Bulb	Sengled
3	Tomacorriente	Wifi Smart Power Plug	Dexel
4	Tomacorriente	Amazon Smart Plug	Amazon
5	Switch	Wifi Smart switch DIY mode	Sonoff
6	Camara de Video	Wifi Smart Camera Vigilance	CTVISON
7	Router	TP LINK 450M Wireless	TP LINK
8	Alexa	Echo Dot Alexa	Amazon

Fuente: Elaboración propia

Los dispositivos se distribuyeron por diferentes áreas estratégicas del hogar, los cuales, tienen la función de automatizar los ambientes y mejorar la calidad de vida de los usuarios, estos elementos son útiles para analizar las vulnerabilidades y amenazas que se presentan en los sistemas domóticos, para posteriormente evaluar los mecanismos de seguridad que se aplica para mitigar ese riesgo.

Configuración de dispositivos y comunicación con la Red

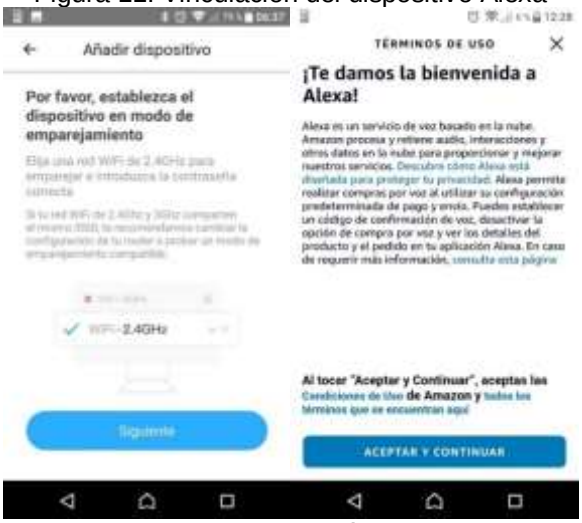
Una vez ubicados los dispositivos en los lugares estratégicos se procedió a la conexión de los dispositivos con la red para la comunicación con la nube, además, se enlaza los dispositivos a las diferentes aplicaciones que permiten la administración de entornos domótico.

Aplicación Amazon Alexa

Para la configuración del dispositivo Alexa se descargó la app desde los repositorios autorizados y se instaló en un dispositivo móvil de prueba modelo Sony Xperia X, la aplicación inicialmente solicito el registro mediante correo electrónico y un código de verificación, para la conexión del dispositivo la aplicación solicitó activar el bluetooth y ubicación del móvil.

Se realizó el escaneo de dispositivo y una vez localizado el elemento para emparejarlo con éxito se compartió la red Wifi para completar la vinculación a la red domestica para su comunicación con otros dispositivos y con la nube para su correcto funcionamiento como se visualiza en la figura 11.

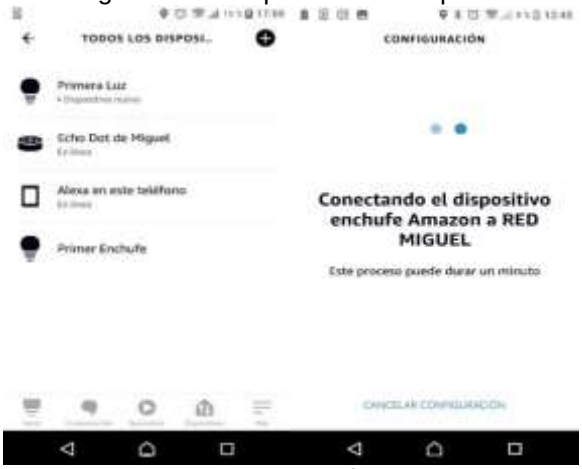
Figura 11. Vinculación del dispositivo Alexa



Fuente: Elaboración propia

Una vez completado la vinculación en la figura 12 se observa el proceso de agregar nuevos dispositivos de los distintos ambientes del hogar para controlarlos mediante la aplicación de Alexa.

Figura 12. Integración de dispositivos a la aplicación de Alexa

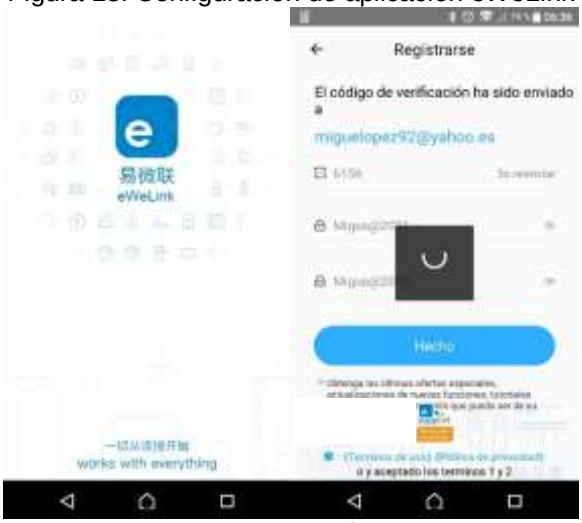


Fuente: Elaboración propia

Aplicación eWeLink

En la figura 13 se muestra la instalación de la aplicación eWeLink, la cual, se procedió de la misma manera que las aplicaciones anteriores, se descargó la aplicación de sitios oficiales al teléfono móvil de pruebas, se crea la cuenta y se la activa mediante el uso de un correo electrónico.

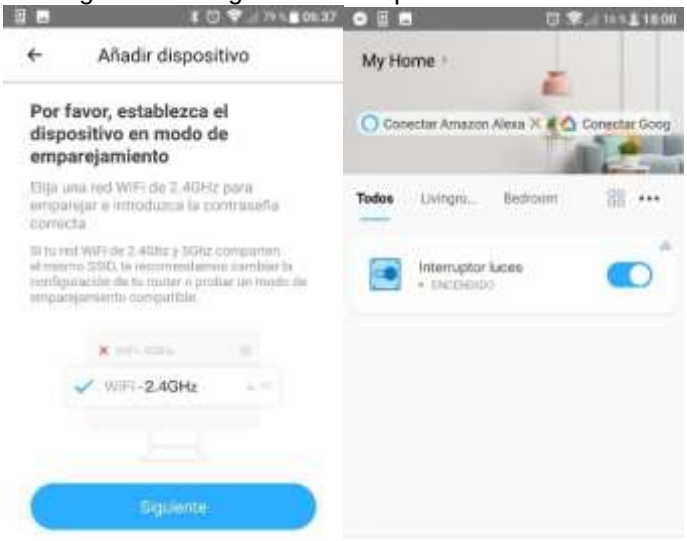
Figura 13. Configuración de aplicación eWeLink



Fuente: Elaboración propia

Una vez finalizado el registro de la cuenta en la aplicación, se agregó los dispositivos en la aplicación como se observa en la figura 14, los cuales, son administrarlos y conectarlos a la red para su comunicación, además, se observa que los dispositivos son compatibles con Alexa para lograr una mejor integración.

Figura 14. Integración de dispositivos a eWeLink



Fuente: Elaboración propia

Dexel Smart devices

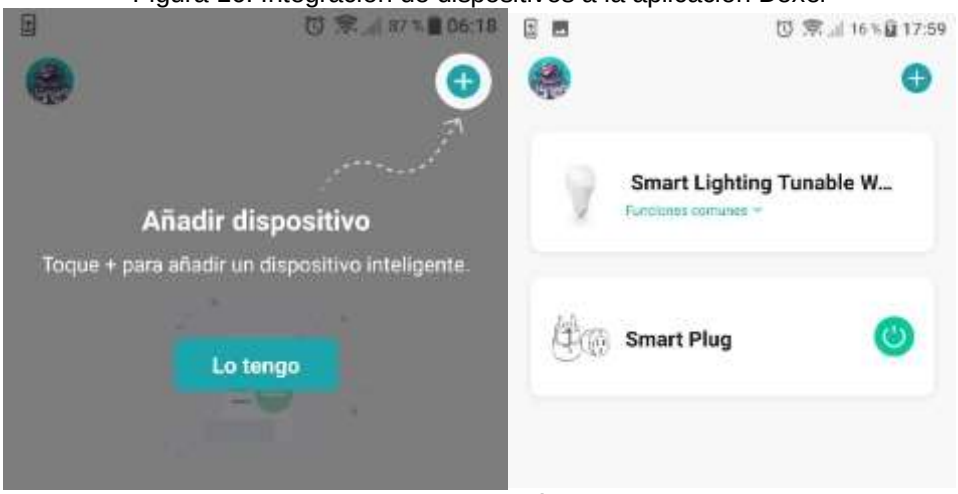
En la figura 15 se observa el proceso de descarga e instalación de la aplicación Dexel para la integración de los dispositivos de dicha marca.

Figura 15. Instalación y registros de la aplicación Dexel

Fuente: Elaboración propia

Finalmente, se agregó los dispositivos de marca Dexel a la aplicación para su comunicación con la red y otros dispositivos, en la figura 16 se observa la integración de los dispositivos a la aplicación que administrara su funcionamiento.

Figura 16. Integración de dispositivos a la aplicación Dexel



Fuente: Elaboración propia

Se procedió a integrar las cámaras a la aplicación descargada e instalada para que se integre de igual forma a la red como se observa en la figura 17.

Figura 17. Integración de cámaras inteligentes a la red.

Fuente: Elaboración propia

Al integrar los dispositivos al sistema domótico se evidencia las prestaciones y las ventajas que se tiene al automatizar los diferentes ambientes del hogar, permite controlar acciones cotidianas como encender las luces, vigilancia de las habitaciones, control de electrodomésticos, programación de eventos y control de información mediante comandos y demás funciones que posee los sistemas IoT. En secciones anteriores se identifica que la creciente demanda y popularidad de los dispositivos IoT provoca que las brechas de inseguridad aumenten y por ende son susceptibles a amenazar informáticas generadas por ciberdelincuentes, en el

siguiente apartado se revisaran las vulnerabilidades y amenazas, a los cuales, se exponen los dispositivos.

Verificación y validación:

La verificación permite asegurarse que el modelo de red de dispositivos IoT en un sistema domótico sigue las especificaciones de arquitectura del modelo conceptual. Una vez implementado el sistema domótico el usuario administra y controla los dispositivos conectados a la red por medio de las aplicaciones que fueron instaladas en el teléfono ovil de prueba, la información se almacena y se gestiona por medio de la nube para ser transmitida a la interfaz del usuario. En la figura 18 se detalla el funcionamiento de la red domótica configurada y la manera, en la cual, se transmite la información desde los dispositivos hasta el usuario final.

Figura 18. Modelo de sistema domótico implementado

Fuente: Elaboración propia

Se procedió a verificar el correcto funcionamiento de los dispositivos mediante las utilidades de las aplicaciones para enviar las órdenes y registrar los datos generados como se muestra en el cuadro 7.

Cuadro 7. Verificación del correcto funcionamiento del sistema Domótico

Aplicación Domótica	Dispositivo	Acceso a la Red	Ahorro de energía	Comunicación	Compatibilidad
Amazon Alexa	Alexa	X	X	X	X
	Enchufe Smart	X	X	X	X
	Foco Smart	X	X	X	X
Dexel Lite	Foco Smart Lighting	X	X	X	X
	Smart Plug	X	X	X	X
eWeLink	Interruptor Sonoff	X	X	X	X
360 eyes	Cámaras wifi Smart	X	X	X	X

Fuente: Elaboración propia

Análisis:

Los dispositivos desde el momento en que se integran a la red de internet empiezan a compartir información entre los elementos del sistema, todos los datos recolectados por los sensores y actuadores son enviados a la nube a través del *gateway*, en el cual, son almacenados, procesados y retransmitidos por internet hacia las aplicaciones instaladas en el móvil para, finalmente, retornar a los dispositivos. Todo este camino que recorre la información es susceptible a amenazas de seguridad y ponen en riesgo la privacidad de los usuarios del sistema domótico.

Identificación de vulnerabilidades

Para descubrir las diferentes vulnerabilidades del sistema IoT, existen varias herramientas de auditoria para identificar brechas de seguridad de los sistemas conectados a una red, a continuación, se lista el software utilizado para nuestro objetivo:

- Advance Ip scanner
- NetScan Tools
- MobaXTerm
- Nmap Kali Linux
- Wireshark

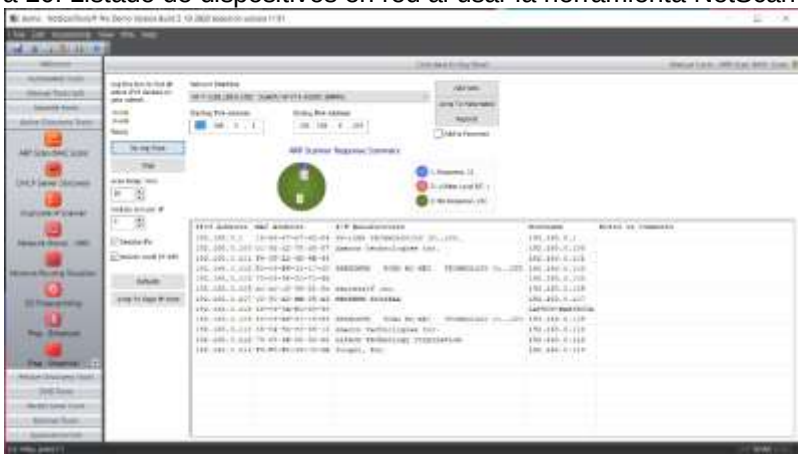
Advance IP Scanner: Es un scanner de red que se usó para escanear la red LAN para lograr detectar todos los dispositivos que se encuentran conectados a la red, al realizar el escaneo con la herramienta se observa todos los dispositivos que están conectados actualmente en la red del sistema domótico como se muestra en la figura 19.

Figura 19. Listado de dispositivos conectados a la red

Fuente: Elaboración propia

NetScan Tools: Es una Herramienta gratuita para escaneo de redes, posee un kit de herramientas diseñadas para usuarios que trabajan con ingeniería, seguridad y administración de redes. En la figura 20 se observa el resultado obtenido al ejecutar el análisis con NetScan, en el cual, se identifica los dispositivos que se encuentran conectados actualmente posee utilidades que nos permiten verificar el estado de los puertos de los dispositivos como se muestra, a continuación.

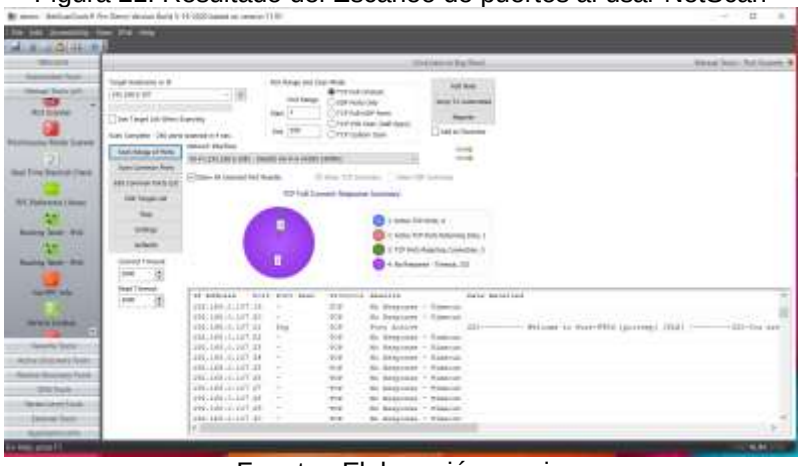
Figura 20. Listado de dispositivos en red al usar la herramienta NetScanTools



Fuente: Elaboración propia

Además, se verifica los puertos que se encuentran habilitados en un dispositivo en específico de una manera gráfica y amigable para el usuario, además, se cuenta con diferentes funcionalidades que nos ayudan a localizar más información acerca del dispositivo como se evidencia en la figura 21.

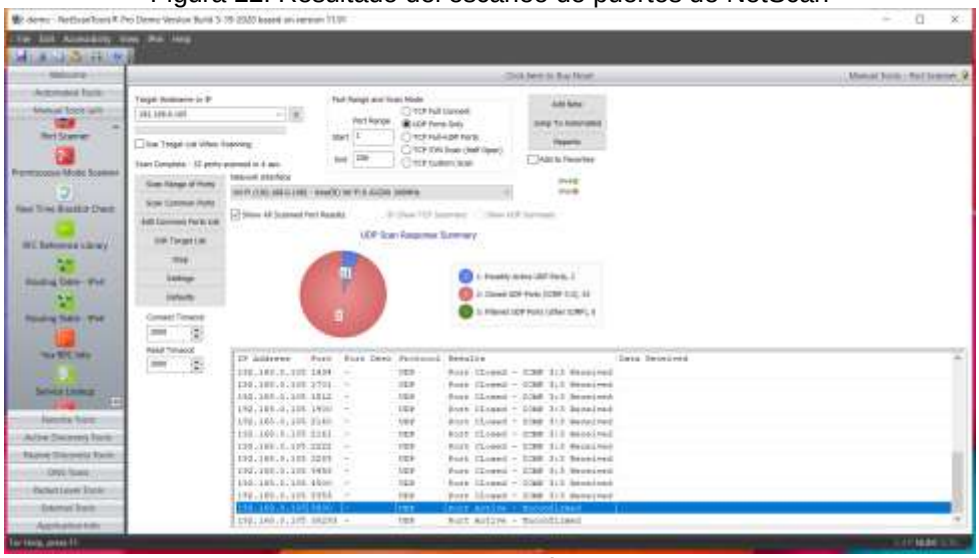
Figura 21. Resultado del Escaneo de puertos al usar NetScan



Fuente: Elaboración propia

En la figura 22 se visualiza el detalle de los puertos analizados al host 192.168.0.105, en el cual, se evidencia que existe mayor cantidad de puertos están cerrados.

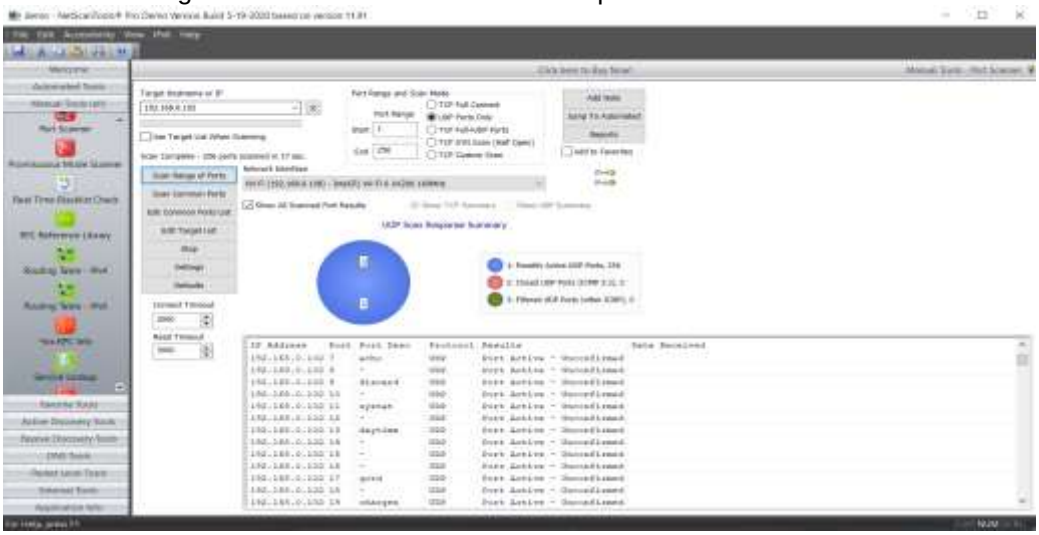
Figura 22. Resultado del escaneo de puertos de NetScan



Fuente: Elaboración propia

En la figura 23 se evidencia el resultado del escaneo del host 192.168.0.102, en el cual, se evidencia que la mayor cantidad de puertos se encuentran abiertos.

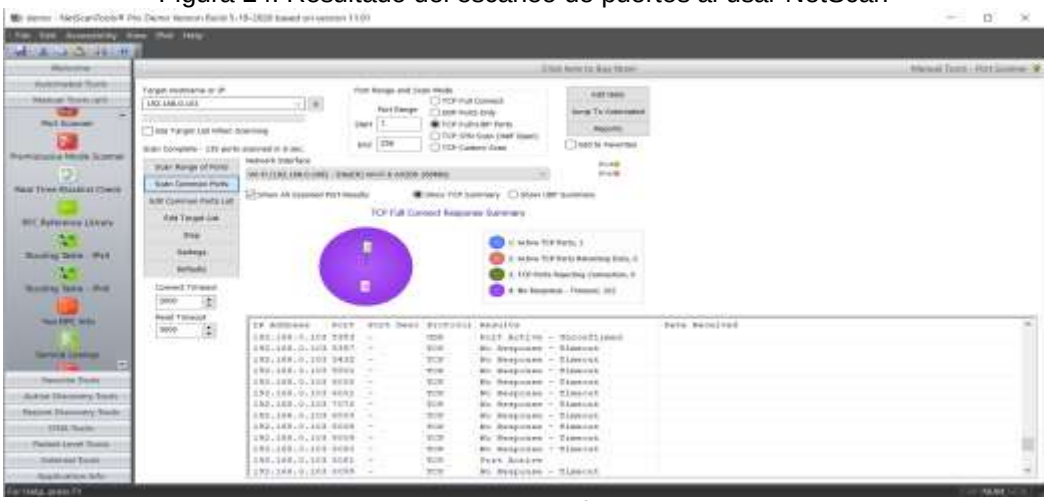
Figura 23. Resultado del escaneo de puertos al usar NetScan



Fuente: Elaboración propia

En la figura 24 se evidencia el resultado del escaneo del host 192.168.0.103, en el cual, se evidencia que existe un mínimo de puertos abiertos y en la mayoría de los puertos no existe respuesta.

Figura 24. Resultado del escaneo de puertos al usar NetScan



Fuente: Elaboración propia

MobaXTerm: es una herramienta informática que proporciona herramientas remotas de red y, además, se usa comandos Linux desde la interfaz de la aplicación en Windows, se usó una de las funciones de la herramienta que sirve para detectar los puertos abiertos en los dispositivos como se visualiza en la figura 25.

Figura 25. Detalle de puertos al usar la herramienta MobaXTerm

Fuente: Elaboración propia

Nmap Kali Linux: es una herramienta potente de escaneo de redes, es gratuita y utilizada en distintas plataformas, a continuación, se realizó la enumeración de los dispositivos de la Red como se muestra en la figura 26.

Figura 26. Enumeración de dispositivos con la herramienta Nmap

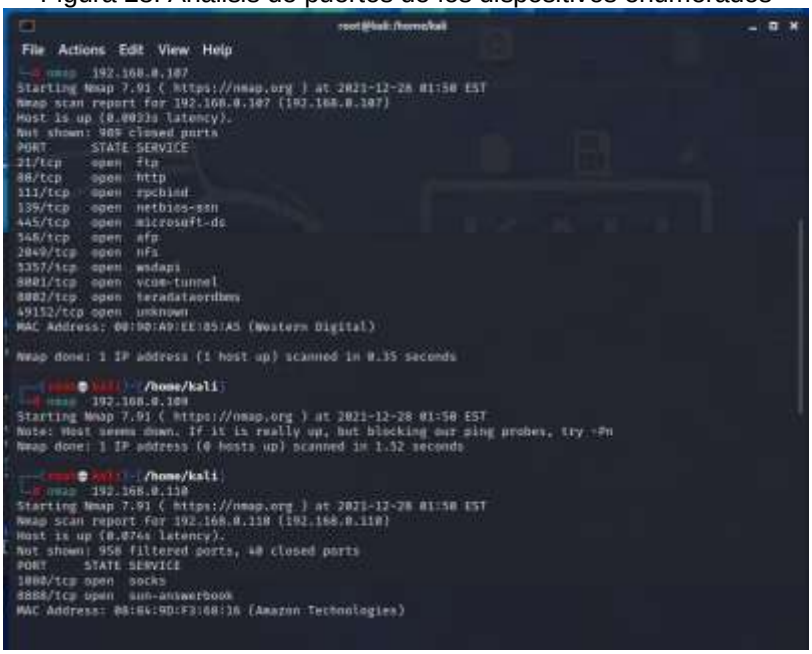
Fuente: Elaboración propia

Una vez realizada la enumeración de los dispositivos se los interrogó de manera individual como se muestra en la figura 27, 28 y 29 para obtener los puertos abiertos en el equipo.

Figura 27. Análisis de puertos de los dispositivos enumerados

Fuente: Elaboración propia

Figura 28. Análisis de puertos de los dispositivos enumerados



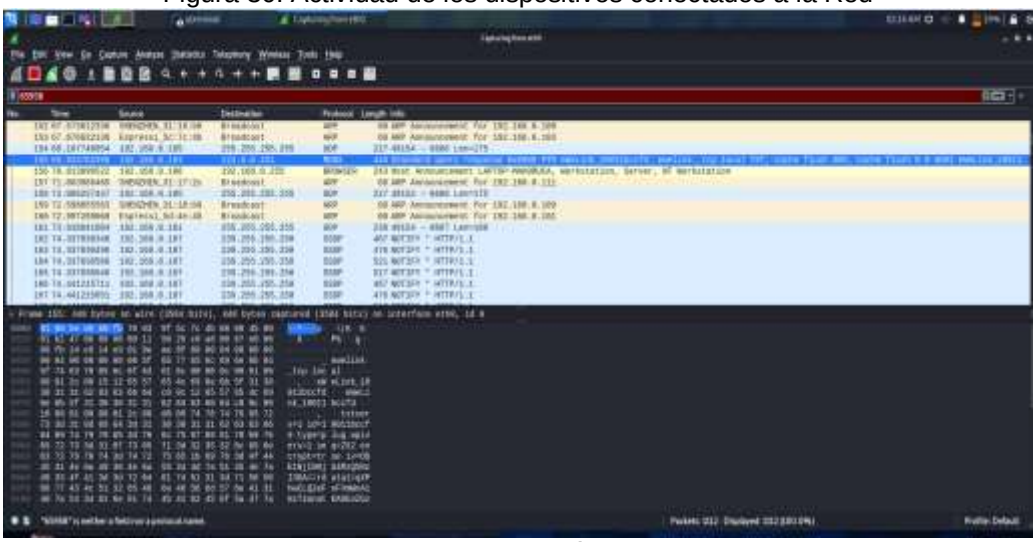
Fuente: Elaboración propia

Figura 29. Análisis de puertos de los dispositivos enumerados

Fuente: Elaboración propia

Wireshark: Es una herramienta que permite ver todo el tráfico que recorre por la red de manera gráfica, además, se logra ver toda la información capturada, lo cual, nos permite visualizar las peticiones y respuestas de los dispositivos dentro del sistema domótico, en la figura 30 se visualiza el tráfico existente en la red domótica.

Figura 30. Actividad de los dispositivos conectados a la Red



Fuente: Elaboración propia

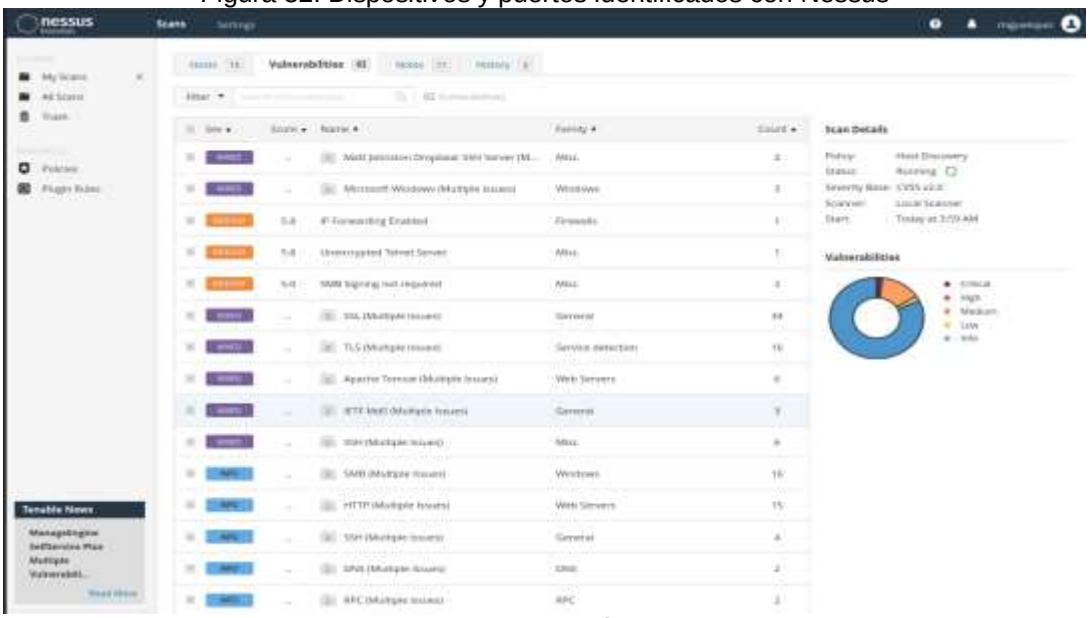
Nessus: Es una herramienta que permite es escaneo de vulnerabilidades de los dispositivos, con la cual, se pudo identificar de una manera más específica los puertos vulnerables de una manera gráfica y, además, con los detalles de cómo explotar la vulnerabilidad como se visualiza en la figura 31.

Figura 31. Dispositivos y puertos identificados con Nessus

Fuente: Elaboración propia

En la figura 32 se visualiza de manera detallada las vulnerabilidades existentes en el dispositivo analizado de forma gráfica, además, del tipo de riesgo existente y la categoría, en la cual, se enmarca.

Figura 32. Dispositivos y puertos identificados con Nessus



Fuente: Elaboración propia

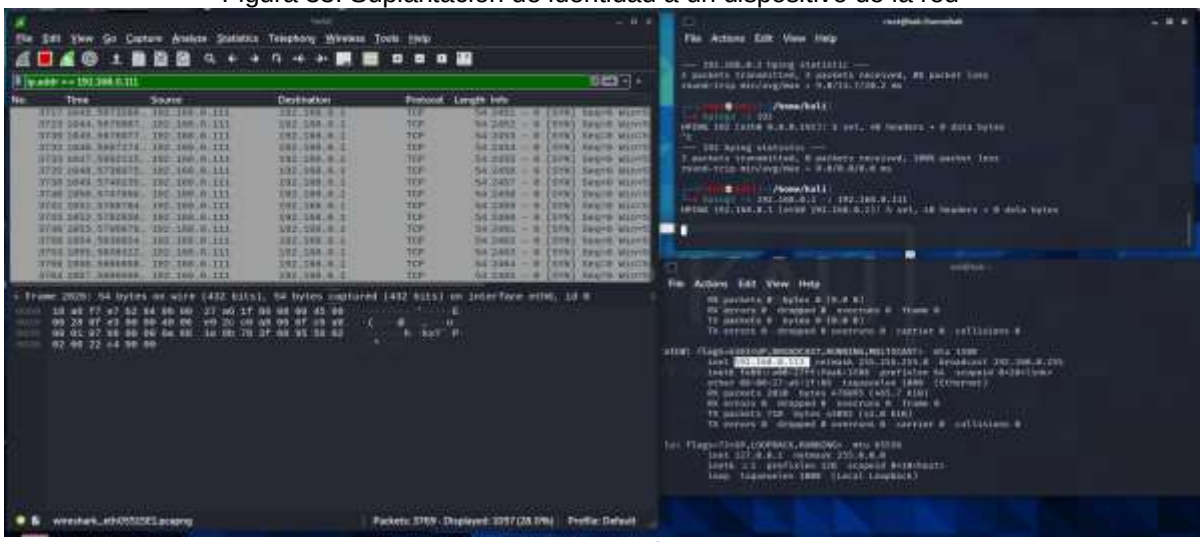
Suplantación de Identidad

Una vez descubierto que los dispositivos poseen vulnerabilidades, se procede a realizar pruebas de las diferentes amenazas a las que están susceptibles en la vida real, en este caso la suplantación de identidad donde un dispositivo se hace pasar por otro, para enviar paquetes de información hacia un servidor y obtener una respuesta hacia la víctima.

Para esta prueba se usa el sistema operativo Kali Linux y el comando hping3, con la cual, se envía solicitudes de ping a una dirección objetivo, para engañarlo y que la respuesta sea a la dirección ip suplantada.

Hping3 es una poderosa herramienta que permite probar firewalls y enrutadores, como paso inicial se identifica la ip del equipo atacante, en este caso es la 192.168.0.113, la cual, se hace pasar por un dispositivo conectado a la red, identificado para la práctica con la ip 192.168.0.111, la con el comando hping3 -S 192.168.0.1 -a 192.168.0.111 ejecutado desde el terminal que realiza la suplantación de identidad, se envía una petición al servidor 192.168.0.1 haciéndose pasar por el dispositivo 192.168.0.111 como se muestra en la figura 33.

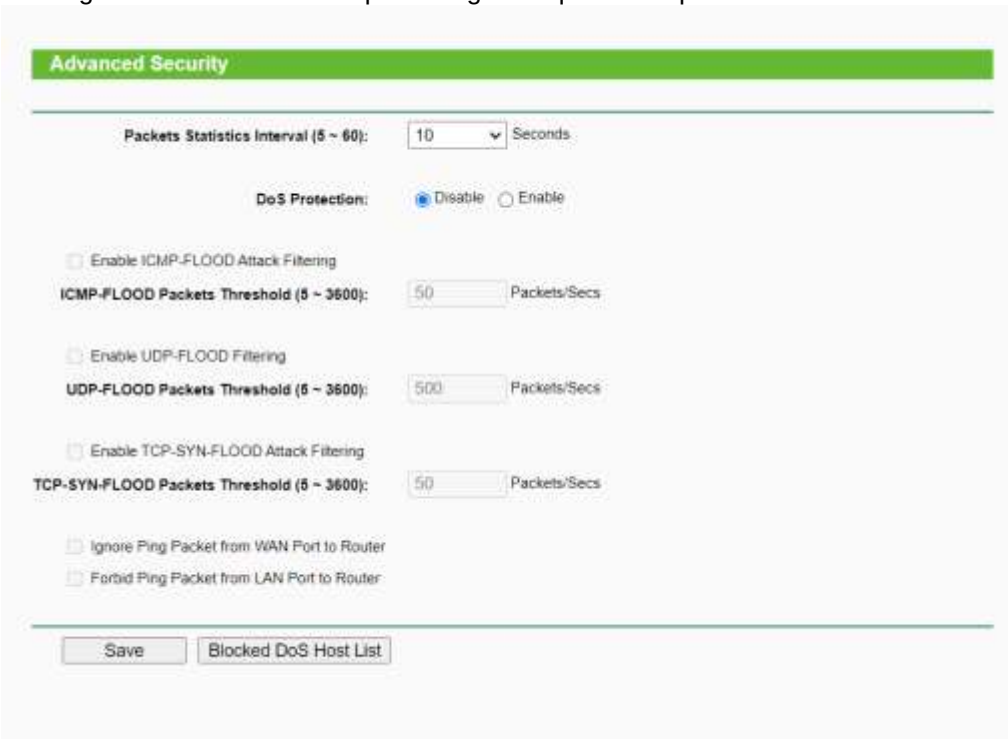
Figura 33. Suplantación de identidad a un dispositivo de la red



Fuente: Elaboración propia

Para mitigar el riesgo de sufrir suplantación se adoptan medidas de seguridad para evitar vulnerabilidad del protocolo TCP/IP, una técnica recomendable es configurar filtros en el router central de comunicación del sistema domótico para controlar el tráfico que transita por la red y controlar el acceso como se observa en la figura 34.

Figura 34. Filtro en router para mitigar ataques de suplantación de identidad



Fuente: Elaboración propia

Manipulación de datos

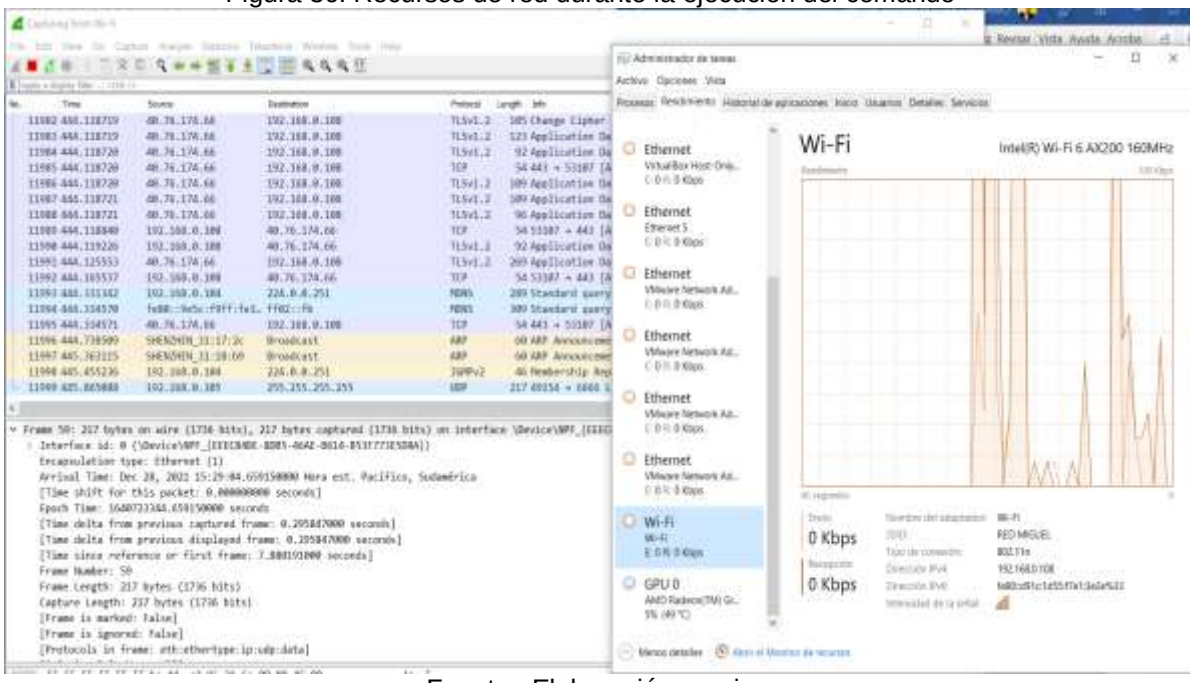
Esta amenaza permite manipular la información del tráfico de la red, lo que causa caos en los dispositivos y en el sistema domótico, para esta prueba se usa la herramienta *hexinject que* es un inyector y rastreador de paquetes, el cual, usa la línea de comandos para el acceso a la red. En la figura 35 se observa el funcionamiento de esta utilidad, con la cual, se pudo interceptar y modificar el tráfico de la red de una manera transparente al enviar tráfico aleatorio hexadecimal, lo cual, provocó un uso excesivo del tráfico de la red.

Figura 35. Modificación del tráfico de la red con la utilidad hexinject

Fuente: Elaboración propia

En la figura 36 se observa que los recursos de la red exceden los valores inusuales y llegan al máximo de su rendimiento durante la ejecución del comando.

Figura 36. Recursos de red durante la ejecución del comando



Fuente: Elaboración propia

Este tráfico inusual se controla mediante la aplicación de reglas de cortafuego para lograr definir el tipo de trafico de la red que se permite o se bloquea y permiten controlar las conexiones que se generan en la red

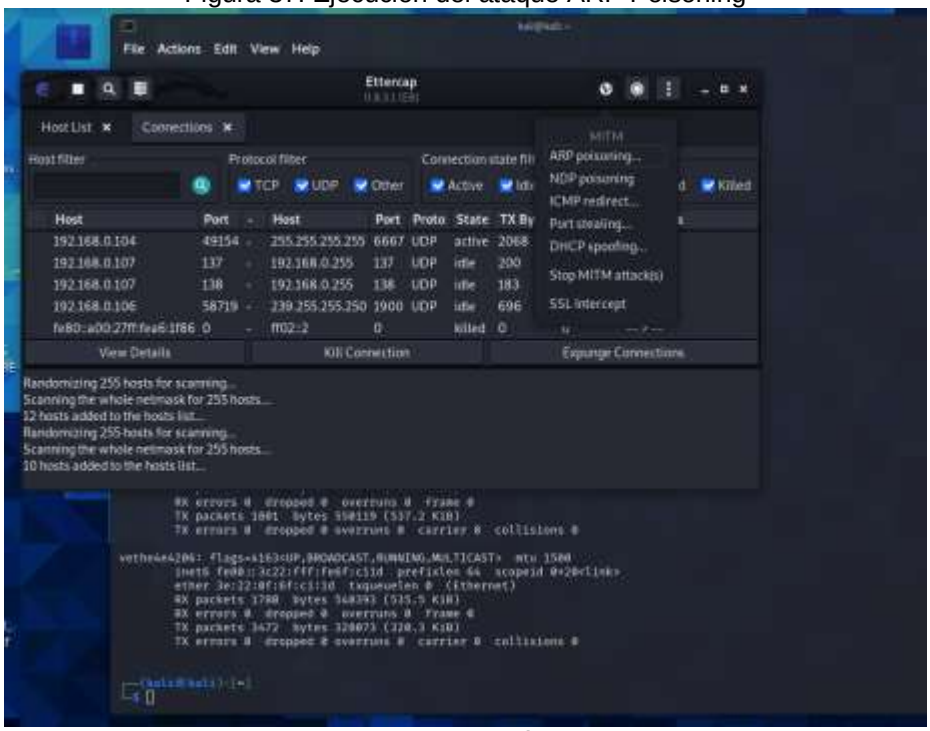
Amenazas de repudio

Esta amenaza niega a un dispositivo del sistema domótico una transacción especifica, esta amenaza niega el envío de mensajes desde el origen, así como también, bloquear su recepción.

El ataque *Arp poisoning* de Kali permitió envenenar la tabla ARP de las víctimas, haciéndole creer que el router es el atacante, con el fin de reenviar todo su tráfico al atacante, de esta manera el dispositivo victima envía sin saber todo su tráfico al atacante.

En la figura 37 muestra la ejecución del ataque *ARP Poisoning* al usar las herramientas que ofrece Kali Linux.

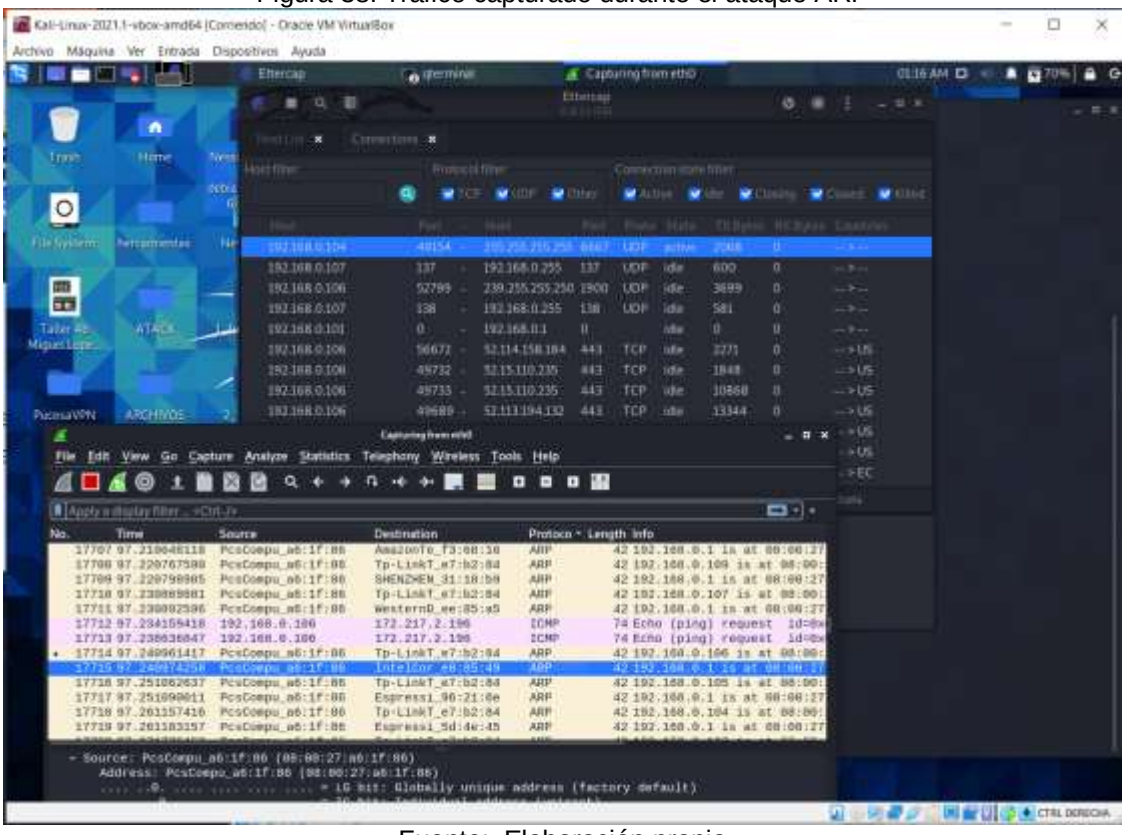
Figura 37. Ejecución del ataque ARP Poisoning



Fuente: Elaboración propia

En la figura 38 se visualiza el tráfico generado en la comunicación de los dispositivos usados para la prueba durante el ataque ARP.

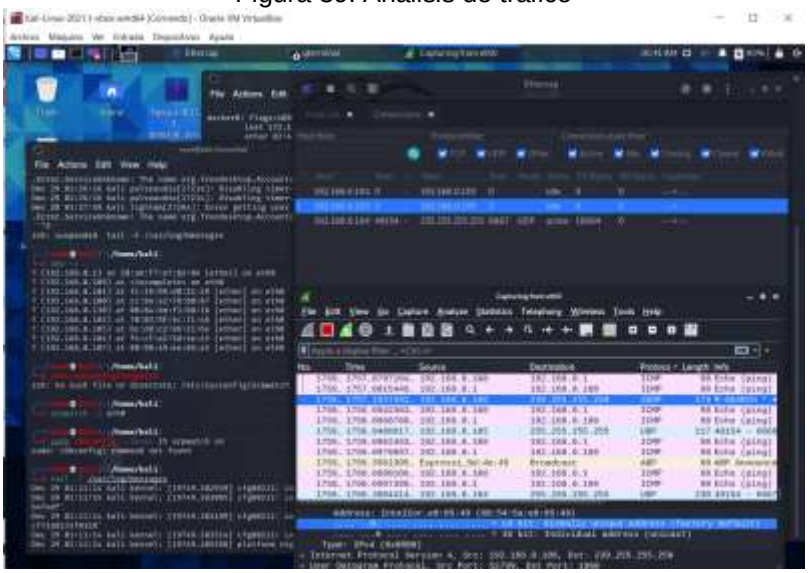
Figura 38. Trafico capturado durante el ataque ARP



Fuente: Elaboración propia

Para mitigar el riesgo de sufrir el ataque se usa programas de código abierto que ayuden a monitorear la actividad del tráfico en la red, y los cambios que se dan en las direcciones ip y mac de los dispositivos, para esta prueba se usó Arpwatch, el mismo que permite observar con atención si aparece una actividad de emparejamiento en la red y, también, reportar las actividades maliciosas como se muestra en la figura 39.

Figura 39. Análisis de tráfico

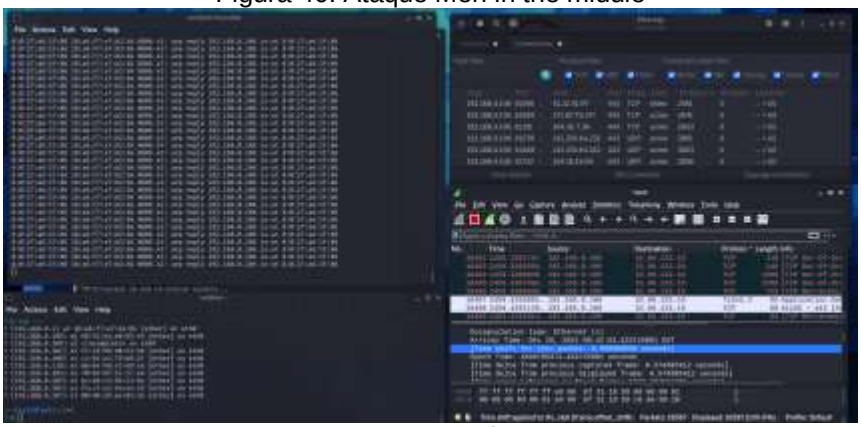


Fuente: Elaboración propia

Divulgación de información

Esta amenaza consiste en la intrusión de una Persona no autorizada con el fin de interceptar el tráfico y la información que es transmitida por la red domótica. Para esta prueba se usó el ataque llamado *Men in the middle,* con el cual, se logró interceptar las comunicaciones entre dos dispositivos. A continuación, en la figura 40 se muestra la ejecución del ataque mediante, el cual, nuestra máquina de Kali se hace pasar por el dispositivo víctima.

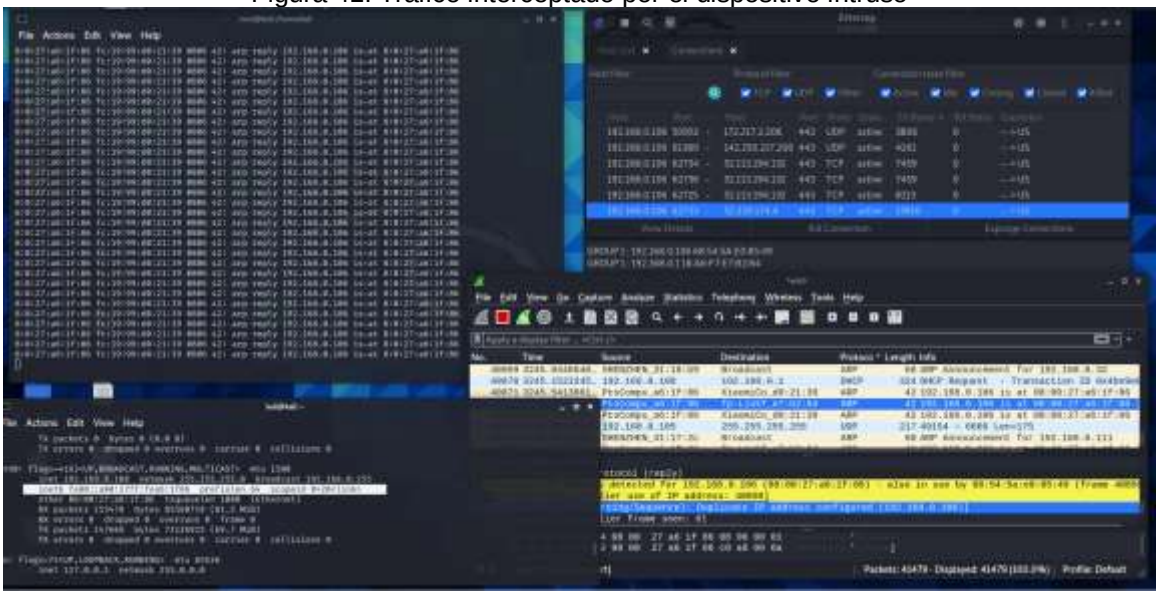
Figura 40. Ataque Men in the middle



Fuente: Elaboración propia

En la figura 41 se observa el tráfico que es interceptado por el dispositivo duplicado durante la ejecución del ataque.

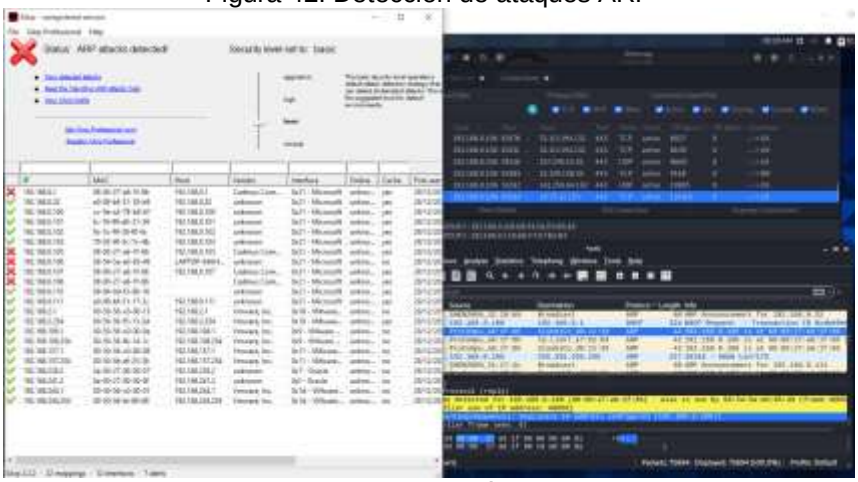
Figura 41. Trafico interceptado por el dispositivo intruso



Fuente: Elaboración propia

Se usó el software XARP para monitorear la actividad del sistema domótico e identificar los ataques Arp y verificar que dispositivo fue interceptado, como se muestra en la figura 42 el software detecta el ataque y nos muestra en un entorno grafico los dispositivos que fueron vulnerados.

Figura 42. Detección de ataques ARP



Fuente: Elaboración propia

Denegación de servicio

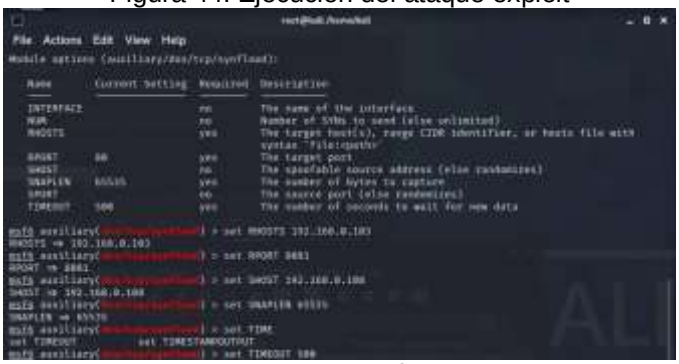
Un ataque DDoS permite colapsar el tráfico de una red para negar el servicio del puerto, por el cual, se realiza el ataque, para esta prueba se usa un exploit, el cual, funciona al explotar el proceso de reconocimiento de una conexión TCP. Como punto inicial se realiza la enumeración de los puertos para verificar los puertos abiertos de los dispositivos como se muestra en la figura 43.

Figura 43. Enumeración de puertos

Fuente: Elaboración propia

Una vez identificado el puerto abierto y la dirección IP del dispositivo se procedió a registrar las opciones del *exploit*, dirección ip de destino, numero de paquetes que se envía, tiempo estimado. En la figura 44 se visualiza la ejecución del exploit y para verificar el ataque se usó *wireshark,* en el cual, se observa el tráfico generado por el ataque.

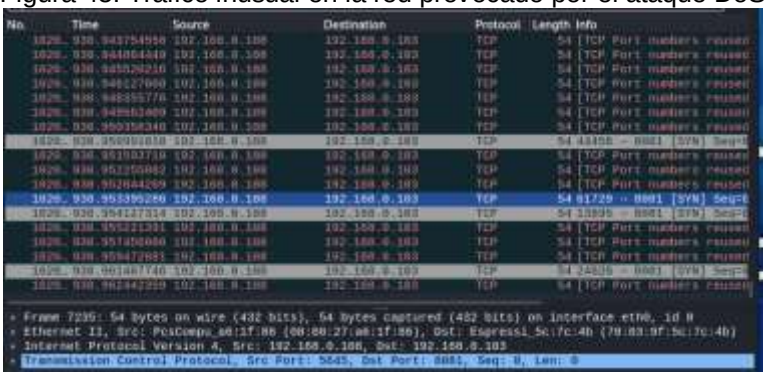
Figura 44. Ejecución del ataque exploit



Fuente: Elaboración propia

En la figura 45 se observa la actividad de la red al usar una herramienta de monitoreo, se identifica el tráfico inusual provocado por el ataque al dispositivo, con esta información los usuarios bloquean la IP del atacante y así mitigar el ataque.

Figura 45. Trafico inusual en la red provocado por el ataque DoS



Fuente: Elaboración propia

Elevación de privilegios

Es la capacidad de un usuario sin privilegios gane acceso suficiente al sistema para comprometerlo, para esta prueba se analizó los dispositivos conectados a la red y con la herramienta NMAP se realizó el escaneo para detectar el puerto y el número de vulnerabilidad como se observa en la figura 46.

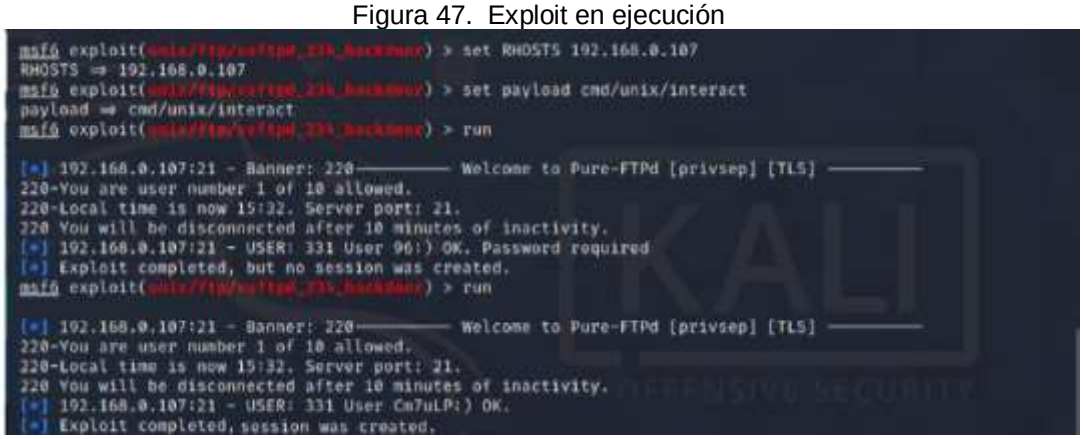
Figura 46. Escaneo de puertos vulnerables

Fuente: Elaboración propia

Como se observa en la figura 46 existe el puerto 22 que se encuentra abierto y con estado vulnerable, al usar el exploit correspondiente para esa función se pudo tener acceso al dispositivo.

En la figura 47 se observa la configuración con el *host* que se desea atacar, así como también, el exploit que se ejecuta y la sesión establecida con el dispositivo.

Figura 47. Exploit en ejecución



Fuente: Elaboración propia

Para prevenir que los dispositivos IoT sean víctimas de este tipo de ataques es necesario que tengan habilitados solamente los puertos necesarios o a su vez tengan protección con una contraseña robusta, como se visualiza en la figura 48 se encuentra habilitado el puesto ftp, por el cual, tienen acceso personas no autorizadas.

Figura 48. Configuración de dispositivo para evitar conexiones por el puerto ftp

Fuente: Elaboración propia

Preparación del manual técnico con pasos y buenas prácticas para mitigar algunos de los problemas de seguridad analizados.

Después de analizar las vulnerabilidades y amenazas de los dispositivos IoT en sistemas domóticos se elaboró un manual de buenas prácticas, el cual, ayudara a mitigar los riesgos que existen en una red de un sistema domótico. Este manual se observa en el anexo 2.

Para la elaboración del manual se utilizó las fuentes bibliográficas utilizadas en el presente documento, así como también, el análisis y los resultados obtenidos en la simulación.

El manual de buenas prácticas consta de las siguientes partes:

- Introducción
    - Internet de las Cosas
    - Elementos IoT
    - Protocolos de comunicación
    - Domótica

- Seguridad
    - Vulnerabilidades IoT
    - Amenazas IoT en un Sistema Domótico

- Buenas prácticas de seguridad
    - Amenazas STRIDE
    - Recomendaciones de seguridad

- Bibliografía

En la figura 49 se observa la plantilla que tiene el manual de buenas prácticas que se desarrolló una vez finalizado el proceso de análisis.

Figura 49. Plantilla y desarrollo del manual de buenas prácticas

Fuente: Elaboración propia

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Una vez aplicados los diferentes métodos de identificación, detección de vulnerabilidades a los diferentes dispositivos que integran el sistema domótico se obtuvieron los siguientes resultados

3.1. Resultados del proceso de enumeración de dispositivos de la red

Uno de los primeros pasos que se realizan para descubrir vulnerabilidades en dispositivos conectados a la RED es el proceso de enumeración mediante, el cual, se logró descubrir todos los dispositivos inteligentes que se encuentran conectados a nuestro sistema domótico y se obtiene los siguientes resultados:

Tabla 2. Resultado de la enumeración del sistema Domótico

Estado	Nombre	IP	Fabricante	Dirección MAC
Activado	192.168.0.1	192.168.0.1	TP-LINK TECHNOLOGIES CO.,LTD.	18:A6:F7:E7:B2:84
Activado	192.168.0.101	192.168.0.101		F4:CF:A2:5D:4E:45
Activado	192.168.0.102	192.168.0.102	Liteon Technology Corporation	70:C9:4E:08:80:D6
Activado	192.168.0.105	192.168.0.105	Espressif Inc.	BC:DD:C2:96:21:6E
Activado	192.168.0.106	192.168.0.106		FC:19:99:D0:21:39
Activado	192.168.0.107	192.168.0.107	WESTERN DIGITAL	00:90:A9:EE:85:A5
Activado	192.168.0.109	192.168.0.109	SHENZHEN TONG BO WEI TECHNOLOGY Co.,LTD	E0:09:BF:31:18:B9
Activado	192.168.0.110	192.168.0.110		08:84:9D:F3:68:16
Activado	192.168.0.111	192.168.0.111	SHENZHEN TONG BO WEI TECHNOLOGY Co.,LTD	E0:09:BF:31:17:2C
Activado	192.168.0.112	192.168.0.112	Google, Inc.	F4:F5:E8:19:72:9A
Activado	192.168.0.113	192.168.0.113	PCS Systemtechnik GmbH	08:00:27:A6:1F:86
Activado	LAPTOP-MAH9RUCA	192.168.0.108		68:54:5A:E0:85:49
Activado	192.168.0.100	192.168.0.100	Amazon Technologies Inc.	CC:9E:A2:78:B8:67
Inactivo	192.168.0.103	192.168.0.103		70:03:9F:5C:7C:4B

Fuente: Elaboración propia

Con el proceso de enumeración se logra conocer la dirección IP y la MAC de los dispositivos, información con, la cual, se obtiene acceso a datos y lograr descubrir las vulnerabilidades detalladas de cada elemento del sistema Domótico.

3.2. Resultados del proceso de análisis de puertos

Con la ayuda de las herramientas usadas en el desarrollo del proyecto se logró identificar los puertos habilitados que en muchas de las ocasiones estos no se encuentran en uso, convirtiéndose en una vulnerabilidad para los dispositivos y el sistema domótico, a continuación, se presenta el detalle de los resultados obtenidos en el análisis de los puertos de la red.

Tabla 3. Resultado del proceso de escaneo de puertos del Sistema Domótico

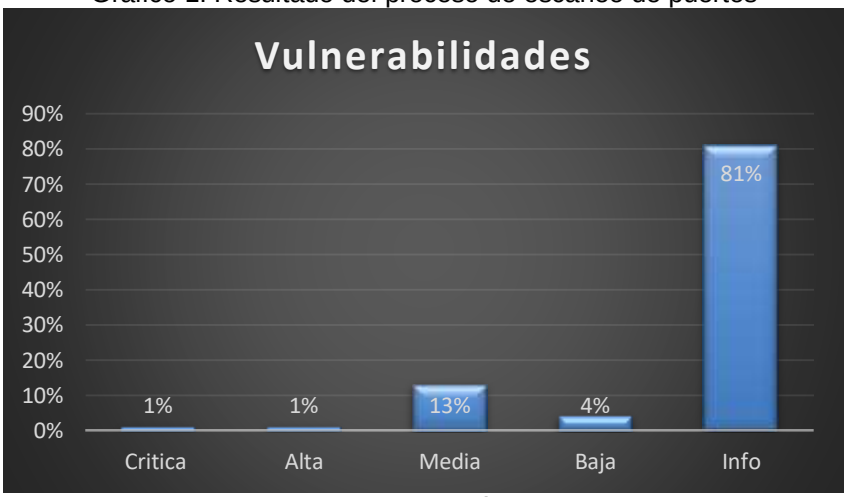
Host	Sistema Operativo	Puertos
192.168.0.1	TP-Link TL-WR940N/TL – WR941ND 6.0	22, 53, 80, 1900, 49152
192.168.0.101	Ethernet Board OkiLan 8100	6668
192.168.0.102	Linux Kernel 2.6	1900, 2870, 9080
192.168.0.105		6668
192.168.0.106		5353
192.168.0.107	Wester Digital Corporation	21, 80 ,111, 137, 139, 445, 548, 1900, 2049, 5353, 8001, 8002, 8003, 33210, 34490, 34737, 35635, 37445, 43465, 50386, 53107, 54087, 56001
192.168.0.109		
192.168.0.110	Linux Kernel	1080, 5353, 8888
192.168.0.111		
192.168.0.112	Linux Kernel 3.2 Linux Kernel 3.3	1900, 5353, 8008, 8009, 8443, 9000, 10001, 10101
192.168.0.113	Linux Kernel 5.10.0-kali3-amd64	23, 8081, 8834
192.168.0.108	Microsoft Windows 10	135, 137, 139, 445, 5355, 49664, 49665, 49666, 49667, 49668, 49674
192.168.0.100		
192.168.0.103	EthernetBoard OkiLAN 8100e	8081

Fuente: Elaboración propia

3.3. Resultados del proceso de análisis de vulnerabilidades

El análisis e identificación de vulnerabilidades generado nos ayuda a comprender e identificar los fallos de seguridad que posee un dispositivo en la red domótica. Mediante la detección de las vulnerabilidades se logró identificar las falencias que poseen los dispositivos de la red como se visualiza en el siguiente gráfico, además, de localizar los posibles vectores de ataque que los ciberdelincuentes aprovechan, en el anexo 1 se observa de forma más detallada cada uno de los fallos de seguridad que se muestra, a continuación.

Gráfico 1. Resultado del proceso de escaneo de puertos



Fuente: Elaboración propia

3.4. Resultados de análisis de amenazas STRIDE

Las pruebas realizadas en el desarrollo del proyecto permitieron evidenciar las vulnerabilidades y amenazas a las que están expuestos los sistemas domóticos, con los resultados analizados se logra aplicar mecanismos y recomendación para mitigar el riesgo que ocasiona a la seguridad de la información dentro de un sistema domótico, los cuales, están incluidos en el manual de buenas prácticas.

3.5 Resultados de los ataques realizados

En el cuadro 8 se visualiza la descripción de la prueba de vulnerabilidad usada y, además, el resultado obtenido al utilizar una forma de mitigación para la amenaza del modelo STRIDE investigada, la cual, se detalla en la guía de buenas prácticas elaborado en el presente proyecto.

Cuadro 8. Resultado mitigación de amenazas STRIDE

Resultado mitigación de amenazas STRIDE			
	Descripción	Prueba de ejemplo de amenaza	Forma de mitigación para la amenaza
Suplantación de identidad (Spoofing),	Una persona o dispositivo usa credenciales de otro usuario con el objetivo de acceder a los datos y acciones a las que no tiene autorización.	Se logro suplantar un dispositivo al clonar su IP con Hping3 de Kali Linux	Aplicación de filtros y firewall en el router central del Sistema domótico para evitar Ataques de spoofing
Manipulación de datos (Tampering)	Se trata de modificar y manipular la información para causar caos en el sistema. Manipulación de datos en rutas del sistema, manipular datos sensibles en puntos de transporte procesamiento o almacenamiento.	Con la herramienta hexinject, se envió información hexadecimal, lo cual, provocó un tráfico excedente en la red domótica	Aplicación de reglas de cortafuego y Firewall para establecer que el tráfico solo es transmitido por los dispositivos asignados.
Amenazas de repudio (Repudio)	Negar a una persona o dispositivo involucrado en una transacción o evento específico del sistema o a su vez transmitir datos incorrectos que confunden los procesos de análisis y operación	Se uso el ataque ARP poisonning para negar la transmisión de los datos a través de la red y son direccionados a la maquina atacante.	Uso de programas para monitoreo el tráfico de la red domótico para controlar y avisar sobre los cambios en la red domótica
Divulgación de información (Information disclosure)	Intrusión de una persona no autorizada con el fin de interceptar la transmisión de datos y capturar información confidencial	El ataque Men in the middle permitió interceptar el tráfico de uno de los dispositivos victima	El software XARP detecta ataques ARP y nos muestra el listado de dispositivos vulnerados
Denegación de servicio (Denal of service)	Capacidad de hacer que un servicio en particular deje de estar disponible, generalmente a través del consumo de recurso o ejecuciones no confiables	Se utilizo un exploit para ejecutar el ataque en, el cual, una vez identificado con nmap el puerto habilitado de un dispositivo se inundó de peticiones, lo cual, provocó un aumento en el tráfico del sistema	Se utilizó la herramienta wireshark para detectar el tráfico inusual de la red e identificar la ip de origen del ataque y bloquear al equipo
Elevación de privilegios (Elevation of privileges).	Capacidad de que un usuario sin privilegios gane suficiente acceso para comprometer el sistema. El atacante penetra las defensas de un sistema y transformarse en un dispositivo más de la red.	Se utilizo un análisis de puerto y vulnerabilidades para usar esos datos con un exploit especifico que nos permita el acceso al dispositivo y archivos	Bloquear todo tipo de comunicaciones que no sean necesarias o caso contrario protegerlas con contraseñas robustas

Fuente: Elaboración propia

3.6. Validación de expertos

El juicio de expertos es un método de validación útil para verificar la fiabilidad de la investigación, el cual, se define como una opinión informada de personas con una trayectoria sobre el tema y que dan evidencia, juicio o valoración a la utilidad de la guía de Buenas prácticas de ciberseguridad en dispositivos IoT y así conocer si realmente la propuesta aporta un valor para la resolución a la problemática actual.

Para realizar la validación del contenido se usa el método de Hernández Nieto, el cual, permite valorar el grado de acuerdo con expertos (el autor recomienda la participación de tres a cinco expertos) respecto a cada uno de los ítems y al instrumento en general. Para lo cual, tras la aplicación de una escala de tipo *Likeert*, la misma que es una escala de calificación que se utiliza para cuestionar a una persona sobre su nivel de acuerdo o desacuerdo con un contenido o investigación (Pedrosa, Suárez, & García, 2013).

Hernández Nieto recomienda varios aspectos del *test* a evaluar entre, los cuales, se ha definido los siguientes:

Coherencia: El ítem guarda relación lógica y adecuada que se identifica entre las distintas partes que conforman el manual.

Claridad: El ítem es claro (no genera confusión o contradicciones).

Relevancia: El ítem es relevante para cumplir con las preguntas y objetivos de la investigación.

Pertinencia: El ítem responde a la necesidad e importancia del proyecto dentro del campo o disciplina en que se desarrolla, así como su adecuación e idoneidad para la realidad en que es aplicado.

Formato: La forma en cómo se presentan los ítems y sus posibles respuestas están claros.

Cada uno de estos aspectos se evaluaron por cada experto, se utilizó una escala de Likert en, el cual, los calores posibles se representan mediante números. Se propuso la siguiente escala, para validar cada ítem del *test:*

1. Inaceptable
2. Deficiencia
3. Regular
4. Bueno
5. Excelente

La interpretación del Coeficiente de Validez del Contenido (CVC) se realizó con la siguiente escala de valores:

a) Menor a 0.6 validez y concordancia inaceptable
b) Igual o mayor a 0.6 y menor a 0.7, validez y concordancia deficientes
c) Mayor que 0.71 y menos o igual a 0.8, validez y concordancia aceptables
d) Mayor que 0.8 y menor o igual a 0.9, validez y concordancia buenas
e) Mayor que 0.9, validez y concordancia excelentes.

Los ítems a los que se evaluó y realizó el cálculo están detallados, a continuación:

- Elementos esenciales: Portada, nombre de la institución, logotipo, nombre del manual e índice
- Introducción
- Contenido: seguridad IoT
- Contenido: buenas prácticas de seguridad
- Ortografía y gramática del manual técnico
- Diseño: Organización de la información
- Contenido visual (ilustraciones e imágenes)
- Contenido (Desarrollo del manual de buenas prácticas) y presentación

- Objetivo del manual de buenas practicas
- Soluciones para los problemas de seguridad investigados

Una vez identificados los aspectos que se va a evaluar se procedió a realizar la validación con un *test* aplicado al siguiente grupo de expertos como se muestra en el siguiente cuadro:

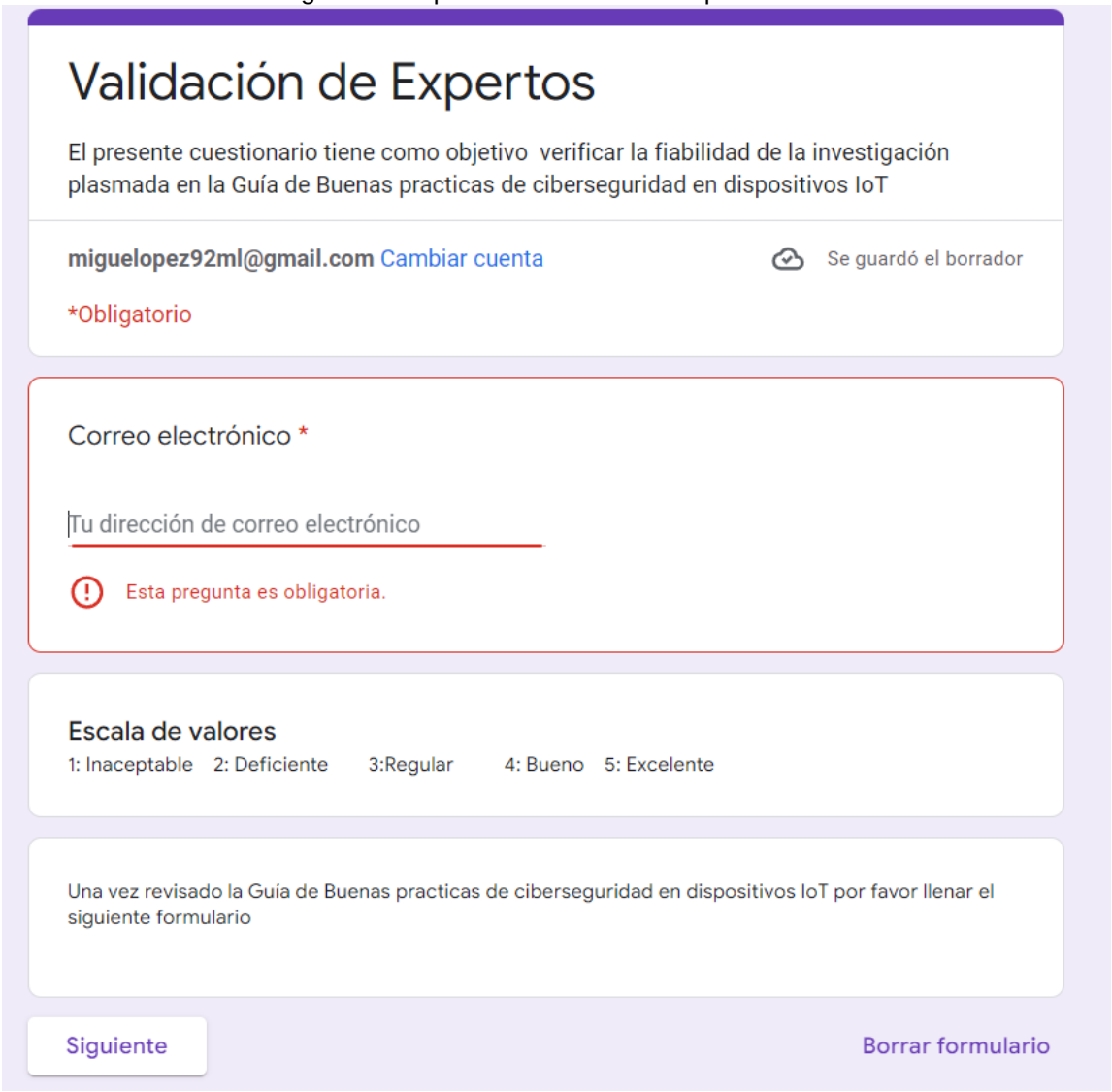
Cuadro 9. Expertos a los cuales se aplicó el test

NOMBRE	TITULO	CARGO
Santiago David Jara Moya	Máster Universitario en Investigación e Innovación en tecnologías de la información y las comunicaciones	Programador y asistente de la Dirección de educación a Distancia y Virtual Docente Universitario Universidad Técnica de Ambato • Desarrollo asistido por software • Manejo y configuración de software • Ingeniería económica para software • Algoritmos y lógica de programación • Gestión de calidad y seguridad de software • Seguridad y aplicación de dispositivos inteligentes al desarrollo de software
Leonardo David Torres Valverde	Máster Universitario en Investigación e Innovación en tecnologías de la información y las comunicaciones	Desarrollador de software orientado a aplicaciones con dispositivos móviles e IoT Docente Universitario Universidad Técnica de Ambato • Fundamentos de Programación • Programación orientada a objetos • Modelamiento y Diseño de Software
Wilson Iván Sánchez Paredes	Ingeniero en Sistemas Computacionales e Informáticos	Gerente de empresa de Seguridad y desarrollo de software • Instalación de cámaras y dispositivos de seguridad • Instalación de dispositivos IoT

Fuente: Elaboración propia

El *test* se lo realizó de forma interactiva mediante el uso de las utilidades de *Google Forms* como se visualiza en la figura 51.

Figura 50. Expertos a los cuales se aplicó el test



Fuente: Elaboración propia

Una vez concluido el test por parte de los expertos se recopiló los resultados y organizo la información por cada experto en hojas de cálculo como se aprecia en la tabla 9,10,11.

Tabla 4. Respuestas del test aplicado a los expertos

Evaluador:	Miguel Alejandro López Naranjo							
Fecha:	5/5/2022	Instrumento:						
			Indicadores					
Coherencia:	El ítem guarda relación lógica y adecuada que se identifica entre las distintas partes que conforman el manual.							
Claridad:	El ítem es claro (no genera confusión o contradicciones)							
Relevancia:	El ítem es relevante para cumplir con las preguntas y objetivos de la investigación							

Pertinencia:	El ítem responde a la necesidad e importancia del proyecto dentro del campo o disciplina en que se desarrolla, así como su adecuación e idoneidad para la realidad en que es aplicado.							
Formato:	La forma en cómo se presentan los ítems y sus posibles respuestas están claros.							
Escala de valores								
1: Inaceptable 2: Deficiente 3: Regular 4: Bueno 5: Excelente								
Contenido			Evaluación					
Ítem	Indicadores Generales	Observaciones	1	2	3	4	5	TOTAL
1	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
2	Coherencia					x		22
	Claridad						x	
	Redacción					x		
	Escala						x	
	Relevancia					x		
3	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
4	Coherencia						x	23
	Claridad					x		
	Redacción						x	
	Escala						x	
	Relevancia					x		
5	Coherencia						x	23
	Claridad					x		
	Redacción						x	
	Escala					x		
	Relevancia						x	
6	Coherencia					x		22
	Claridad					x		
	Redacción						x	
	Escala					x		
	Relevancia						x	
7	Coherencia						x	23
	Claridad					x		
	Redacción						x	
	Escala					x		
	Relevancia						x	
8	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
9	Coherencia						x	25

	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
10	Coherencia						x	23
	Claridad					x		
	Redacción						x	
	Escala						x	
	Relevancia					x		
Experto:	Santiago David Jara Moya							

Fuente: Elaboración propia

Tabla 5. Respuestas del test aplicado a los expertos

Evaluador:	Miguel Alejandro López Naranjo								
Fecha:	5/5/2022	Instrumento:							
			Indicadores						
Coherencia:	El ítem guarda relación lógica y adecuada que se identifica entre las distintas partes que conforman el manual.								
Claridad:	El ítem es claro (no genera confusión o contradicciones)								
Relevancia:	El ítem es relevante para cumplir con las preguntas y objetivos de la investigación								
Pertinencia:	El ítem responde a la necesidad e importancia del proyecto dentro del campo o disciplina en que se desarrolla, así como su adecuación e idoneidad para la realidad en que es aplicado.								
Formato:	La forma en cómo se presentan los ítems y sus posibles respuestas están claros.								
Escala de valores									
1: Inaceptable 2: Deficiente 3: Regular 4: Bueno 5: Excelente									
Contenido			Evaluación						
Ítem	Indicadores Generales	Observaciones	1	2	3	4	5	TOTAL	
1	Coherencia					x		22	
	Claridad					x			
	Redacción						x		
	Escala					x			
	Relevancia						x		
2	Coherencia						x	23	
	Claridad						x		
	Redacción					x			
	Escala					x			
	Relevancia						x		
3	Coherencia						x	25	
	Claridad						x		
	Redacción						x		
	Escala						x		
	Relevancia						x		
4	Coherencia						x	25	
	Claridad						x		
	Redacción						x		

	Escala						x	
	Relevancia						x	
5	Coherencia					x		22
	Claridad						x	
	Redacción						x	
	Escala					x		
	Relevancia					x		
6	Coherencia					x		22
	Claridad						x	
	Redacción					x		
	Escala						x	
	Relevancia					x		
7	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
8	Coherencia						x	24
	Claridad						x	
	Redacción					x		
	Escala						x	
	Relevancia						x	
9	Coherencia						x	24
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia					x		
10	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
Experto:	Leonardo David Torres Valverde							

Fuente: Elaboración propia

Tabla 6. Respuestas del test aplicado a los expertos

Evaluador:	Miguel Alejandro López Naranjo							
Fecha:	5/5/2022	Instrumento:						
			Indicadores					
Coherencia:	El ítem guarda relación lógica y adecuada que se identifica entre las distintas partes que conforman el manual.							
Claridad:	El ítem es claro (no genera confusión o contradicciones)							
Relevancia:	El ítem es relevante para cumplir con las preguntas y objetivos de la investigación							
Pertinencia:	El ítem responde a la necesidad e importancia del proyecto dentro del campo o disciplina en que se desarrolla, así como su adecuación e idoneidad para la realidad en que es aplicado.							
Formato:	La forma en cómo se presentan los ítems y sus posibles respuestas están claros.							

Escala de valores								
1: Inaceptable 2: Deficiente 3: Regular 4: Bueno 5: Excelente								
Contenido			Evaluación					
Ítem	Indicadores Generales	Observaciones	1	2	3	4	5	TOTAL
1	Coherencia					x		24
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
2	Coherencia					x		23
	Claridad					x		
	Redacción						x	
	Escala						x	
	Relevancia						x	
3	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
4	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
5	Coherencia					x		21
	Claridad					x		
	Redacción						x	
	Escala					x		
	Relevancia					x		
6	Coherencia						x	24
	Claridad						x	
	Redacción					x		
	Escala						x	
	Relevancia						x	
7	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
8	Coherencia						x	24
	Claridad					x		
	Redacción						x	
	Escala						x	
	Relevancia						x	
9	Coherencia						x	24
	Claridad						x	
	Redacción						x	
	Escala						x	

	Relevancia					x		
10	Coherencia						x	25
	Claridad						x	
	Redacción						x	
	Escala						x	
	Relevancia						x	
Experto:	Wilson Iván Sánchez Paredes							

Fuente: Elaboración propia

En la tabla 12 se observa los resultados de los test aplicados por cada ítem y se efectúa el cálculo del Coeficiente de Validez de Contenido de cada uno de los Ítems del test, para luego efectuar un promedio para validar todo el test.

Tabla 7. Respuestas del test aplicado a los expertos

ITEM	Experto 01	Experto 02	Experto 03	S	M	Sx	CVC	P	CVCt
Ítem 01	25	22	24	71	25	2,84	0,95	0,04	0,91
Ítem 02	22	23	23	68	25	2,72	0,91	0,04	0,87
Ítem 03	25	25	25	75	25	3	1,00	0,04	0,96
Ítem 04	23	25	25	73	25	2,92	0,97	0,04	0,94
Ítem 05	23	22	21	66	25	2,64	0,88	0,04	0,84
Ítem 06	22	22	24	68	25	2,72	0,91	0,04	0,87
Ítem 07	23	25	25	73	25	2,92	0,97	0,04	0,94
Ítem 08	25	24	24	73	25	2,92	0,97	0,04	0,94
Ítem 09	25	24	24	73	25	2,92	0,97	0,04	0,94
Ítem 10	23	25	25	73	25	2,92	0,97	0,04	0,94
								Promedio:	0,91

Fuente: Elaboración propia

La columna titulada S se obtiene al sumar las calificaciones obtenidas de cada juez por cada criterio evaluado.

La columna M mantiene un valor constante, el cual, representa la puntuación máxima por cada ítem, como se usó una escala de *Likert* de cinco puntos y se evalúa cinco criterios el valor es 5 x 5= 25.

La columna titulada Sx, se obtiene al dividir la sumatoria de las calificaciones obtenidas según cada uno de los tres jueces sobre la puntuación máxima de cada ítem.

La columna denominada CVC es la primera estimación del coeficiente de validez de contenido para el ítem, se obtiene al dividir la columna anterior para el numero de jueces.

La columna P es la probabilidad de error, la cual, se obtiene al dividir uno para el numero de jueces y se lo eleva a la potencia con el valor del número de jueces.

Finalmente, la última columna CVCt se obtiene de la resta de la columna CVC con la probabilidad de error P, el cual, representa el coeficiente de validez de contenido de la pregunta o ítem del *test.*

Finalmente, se promedian todos los resultados y se obtiene el coeficiente de validez de contenido de todo el test, según Hernández – Nieto. Para esta investigación el coeficiente de *test* seria: CVC=0.91, lo cual, representa un coeficiente de validez y concordancia que caen dentro de lo aceptable. Por lo que se cuenta con una guía con validación aceptable.

CONCLUSIONES

- La fundamentación teórica para conocer el funcionamiento de los dispositivos IoT dentro de un sistema domótico, deja en claro que en la actualidad esta tecnología brinda una gran cantidad de herramientas y funcionalidades capaces de ejecutar tareas cotidianas y acciones que antes se creían impensables de ser controladas, son los dispositivos IoT una de las tecnologías más usadas en todo el planeta al optimizar el tiempo, recursos y mejor la calidad de vida de las personas.

- La investigación de las metodologías para la detección de riesgos más frecuentes que presentan los dispositivos IoT, permite tener una visión de la cantidad de aplicaciones utilizadas para administrar y controlar los dispositivos IoT de un sistema domótico y la potencial brecha de seguridad para la gran cantidad de información que es recolectada y transmitida a través de la red de internet. El modelo STRIDE nos ofrece una interesante división de amenazas que se emplean para identificar y categorizar las amenazas de seguridad informática dentro de un sistema domótico.

- La verificación de los niveles de seguridad de dispositivos IoT en un sistema domótico simulado permitió estudiar su estructura y la respuesta ante diferentes pruebas de seguridad informática, logrando comprender la causa y efecto que tiene en el sistema y toda esa información recolectada sirvió como la base de conocimientos para la construcción de un manual de buenas prácticas para el control de las vulnerabilidades mencionadas en el modelo STRIDE.

- La redacción de un manual técnico de buenas prácticas de seguridad para dispositivos IoT en sistemas domóticos ofrece a los usuarios métodos de configuración e información necesaria para mitigar el riesgo de sufrir algún tipo de ataque. La información es prioridad en los todos los hogares, por lo que las personas necesitan tomar conciencia sobre el manejo seguro de la información, no basta solamente con tener un sistema de información

actualizado, si los usuarios no configuran de una formada adecuada todos los dispositivos conectados en la red, es propenso a dejar brechas de seguridad con, las cuales, son víctimas de infiltraciones y acceso no autorizados a datos confidenciales de las viviendas.

RECOMENDACIONES

- Verificar que los dispositivos IoT que se vaya a utilizar tengan un firmware actualizado y sea compatible con otras plataformas para evitar el uso de varias aplicaciones para controlar el sistema domótico.

- Una vez finalizada la instalación de los dispositivos IoT en del sistema domótico comprobar su funcionamiento con el fin de verificar la correcta comunicación entre los dispositivos.

- Se recomienda utilizar la Guía de buenas prácticas elaborada en la presente investigación, misma que se usó como pauta el modelo de amenazas STRIDE, la cual, ayuda y orienta a los usuarios sobre las amenazas existentes en los dispositivos IoT y la forma de mitigar dichas amenazas en los sistemas domóticos implementados en el hogar.

BIBLIOGRAFÍA

Alvear Puertas, V., Rosero Montalvo, P., Peluffo Ordóñez, D., & Pijal Rojas, J. (2017). I*nternet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones*. Enfoque UTE, 8, 244-256.https://doi org/10.29 019/enfoq ueut e.v8n 1.121

Anabalon, J. (2016). Internet of Threats (IoT): *Una visión de la arquitectura, aplicaciones, riesgos y desafíos futuros*. Universidad de Santiago de Chile. Recuperado de https://www.researchgate.net/profile/Juan-Ana balo n/pu blication/324900392_Internet_of_Threats_IoT_Una_vision_de_la_arquitect ura_aplicaciones_riesgos_y_desafios_futuros/links/5aea32a345851588dd8 28383/Internet-of-Threats-IoT-Una-vision-de-la-arquitectura-aplicaciones-riesgos-y-desafios-futuros.pdf

Andrea, L., Chrysostomou, C., & Hadjichristofi, G. (2015). *Internet of Things: Security vulnerabilities and challenges*. 2015 IEEE Symposium on Computers and Communication (ISCC). https:// doi.org/ 10.1109 /ISCC.20 15.7405513

Arias Silva, N. A. (2019). *Análisis de seguridad de vulnerabilidades y ataques presentados en 4 dispositivos de Internet de las cosas*,. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD.Recuperado de http ://re posi tory.unad.edu.co/handle/10596/33326

Domínguez Margareto, D. (2020). *Ciberseguridad en Internet of Things: Análisis de amenazas, riesgos y vulnerabilidades*. (1), 90.

Espina Suárez, E. A., & Gómez Hormaza, G. E. (2021). *Mitigación de riesgos a través del uso de una arquitectura de ciberseguridad mediante modelamiento de amenazas en la implementación de sistemas de información basados en internet de las cosas*. Universidad Peruana de Ciencias Aplicadas (UPC). Recuperado de https://repositorioacademico upc.edu.pe/handle/10757/655934

Fisher, S. (2019, diciembre 9). *Riesgos de seguridad en el Internet de las cosas.* Riesgos de seguridad en el Internet de las cosas, *1*(1). Recuperado de https://www.avast.com/es-es/c-iot-security-risks

Gartner. (2017). 8.4 *Billion Connected Things Will be in Use 2017* [Gartner dice que 8.4 mil millones de «cosas» conectadas estarán en uso en 2017, un 31 por ciento más que en 2016]. Recuperado 26 de noviembre de 2021, de Gartner website: https://www.gartner.com/en/newsroom/pressreleases/

2017- 02-07-gartner-says-8 -billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). *Cyber security of smart homes: Development of a reference architecture for attack surface analysis.* Living in the Internet of Things: Cybersecurity of the IoT - 2018, 1-10. https://doi.org/10.1049/cp.2018.0045

González García, A. J. (2017). *IoT: Dispositivos, tecnologías de transporte y aplicaciones.* Recuperado de http://openaccess.uoc.edu/webapps/o2/handle/10609/64286

Herrera Quintero, L. F. (2005). *Viviendas Inteligente Domótica*. *25*(2), 8.

Inavirtual. (s. f.). *Domótica* [CURSO]. Recuperado 1 de mayo de 2022, de Desarrollo y evolución de la domótica website: https://www.ina-pidte.ac.cr/course/view.php?id=912

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: *Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices.* IEEE Internet of Things Journal, 6(5), 8182-8201. https://doi.org/10.1109/JIOT.2019.2935189

Miñano Carmona, P. A. (2019). *Seguridad en los ecosistemas IoT.* Universitat Oberta de Catalunya (UOC), 69.

Molina García, J. A. (2006). *La importancia de la gestión de riesgos y seguridad en el internet de las cosas (IOT)*. Universidad Piloto de Colombia, 12.

Pedrosa, I., Suárez, J., & García, E. (2013, junio 12). *Evidencias sobre la validez de contenido: avances teóricos y métodos para su estimación content validity evidences: theoretical advances and estimation methods.* Universidad de Oviedo, 1(1), 16.

Pérez, N. B., Bustos, M. A., Berón, M., & Rangel Henriques, P. (2018). *Análisis sistemático de la seguridad en internet of things*. Presentado en XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste)., Universidad Nacional del Nordeste. Recuperado de http://sedici.unlp.edu.ar/handle/10915/68387

Rojas García, C. R. (2015). *Creación de un sistema domótico de seguridad y consumo energético para hogares:homenode.* Recuperado 10 de diciembre de 2021, de https://1library.co/document/7q046g9z-creacion-sistema-domotico segurida d -consumo-energetico-hogares-homeno de. html

Rose, K., Eldridge, S., & Chapin, L. (2015). *La internet de las cosas— una breve reseña*. Internet Society, (1), 83.

Salazar Soler, J., & Silvestre Bergés, S. (2016). *Internet de las cosas—CORE.* Recuperado 3 de diciembre de 2021, de Internet de las cosas website: https://core.ac.uk/display/81581111?recSetID=

Sánchez Sánchez, J. D. (2018, abril 23). I*oT o internet de las cosas: Qué es y cómo puede transformar mi negocio [Artículo]*. Recuperado 8 de diciembre de 2021, de Inforges website: https://www.inforges.es/post/iot-o-internet-de-las-cosas-que-es

Schrecker, S. (2016). *Industrial Internet of Things.* IIC:PUB:G4:V1.0:PB:20160926, G4: Security Framework, 173.

Sebastian, A., & Sivagurunathan, S. (2018). Multi DODAGs in RPL for Reliable *Smart City IoT. Journal of Cyber Security and Mobility, 7*(1), 69-86. https: //doi.org/10.13052/jcsm2245-1439.716

Singh, D., Tripathi, G., & Jara, A. J. (2014). *A survey of Internet-of-Things: Future vision, architecture, challenges and services.* 2014 IEEE World Forum on Internet of Things (WF-IoT), 287-292. https://doi.org/10.1109/WF-IoT.2 014 .6803174

Uit-t. (2017). Y.4806: *Security capabilities supporting safety of the Internet of things.* E 42087. Recuperado de https://www.itu.int/rec/T-REC-Y.4806-2017 11-I/en

ANEXOS

Anexo 1: Informe escaneo de vulnerabilidades

Vulnerabilities by Host

192.168.0.1

1	0	2	3	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 33

SEVERITY	CVSS V2.0	PLUGIN	NAME
CRITICAL	10.0	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.8	50686	IP Forwarding Enabled
MEDIUM	5.0	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	153953	SSH Weak Key Exchange Algorithms Enabled

LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification

INFO	N/A	117886	OS Security Patch Assessment Not Available

INFO	N/A	66334	Patch Report

INFO	N/A	10180	Ping the remote host
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection

INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	11026	Wireless Access Point Detection

Vulnerabilities Total: 5

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10180	Ping the remote host
INFO	N/A	10287	Traceroute Information

Vulnerabilities

Total: 8

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	10180	Ping the remote host

INFO	N/A	10287	Traceroute Information

Vulnerabilities — Total: 18

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	19689	Embedded Web Server Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP)

			Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	10180	Ping the remote host
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	35712	Web Server UPnP Detection

Vulnerabilities

Total: 8

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	10180	Ping the remote host

INFO	N/A	10287	Traceroute Information

Vulnerabilities Total: 7

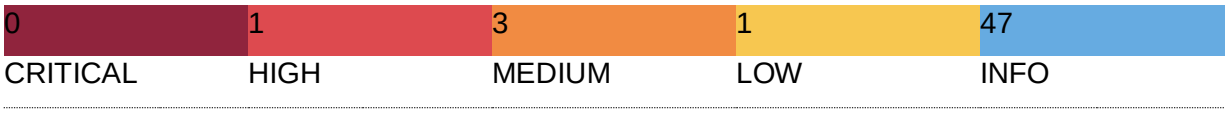
SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10180	Ping the remote host
INFO	N/A	10287	Traceroute Information
INFO	N/A	66717	mDNS Detection (Local Network)

Vulnerabilities — Total: 7

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	50350	OS Identification Failed
INFO	N/A	10180	Ping the remote host
INFO	N/A	10287	Traceroute Information

Vulnerabilities Total: 7

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10180	Ping the remote host
INFO	N/A	10287	Traceroute Information
INFO	N/A	66717	mDNS Detection (Local Network)



Vulnerabilities

Total: 52

SEVERITY	CVSS V2.0	PLUGIN	NAME
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	42255	NFS Server Superfluous
INFO	N/A	10223	RPC portmapper Service Detection

INFO	N/A	45380	AFP Server Share Enumeration (guest)
INFO	N/A	10666	Apple Filing Protocol Server Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	42149	FTP Service AUTH TLS Command Support
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	106658	JQuery Detection
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy

	INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
	INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
	INFO	N/A	11011	Microsoft Windows SMB Service Detection
	INFO	N/A	23974	Microsoft Windows SMB Share Hosting Office Files
	INFO	N/A	60119	Microsoft Windows SMB Share Permissions Enumeration
	INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
	INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
	INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
	INFO	N/A	11219	Nessus SYN scanner
	INFO	N/A	19506	Nessus Scan Information
	INFO	N/A	11936	OS Identification

O				
		N/A	10919	Open Port Re-check
	INF			
O				
		N/A	10180	Ping the remote host
	INF			
O				
		N/A	11111	RPC Services Enumeration
	INF			
O				
		N/A	53335	RPC portmapper (TCP)
	INF			
O				
		N/A	10860	SMB Use Host SID to Enumerate Local Users
	INF			
O				
		N/A	56984	SSL / TLS Versions Supported
	INF			
O				
		N/A	10863	SSL Certificate Information
	INF			
O				
		N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
	INF			
O				
		N/A	21643	SSL Cipher Suites Supported
	INF			
O				
		N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
	INF			
O				
		N/A	94761	SSL Root Certification Authority Certificate Information

	INF			
O				
		N/A	22964	Service Detection
	INF			
O				
		N/A	11153	Service Detection (HELP Request)
	INF			
O				

INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	135860	WMI Not Available
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	66717	mDNS Detection (Local Network)

192.168.0.108

CRITICAL	HIGH	MEDIUM	LOW	INFO

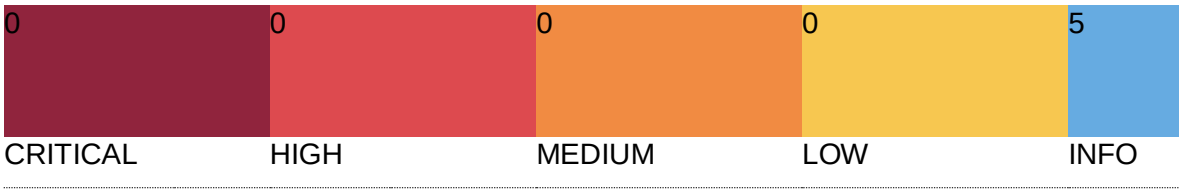
Vulnerabilities Total: 21

SEVERITY	CVSS V2.0	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses

INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	11936	OS Identification

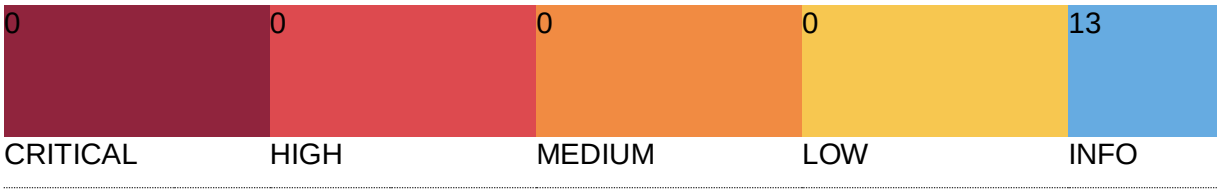
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	10180	Ping the remote host
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided

INFO	N/A	10287	Traceroute Information
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure



Vulnerabilities Total: 5

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10180	Ping the remote host
INFO	N/A	10287	Traceroute Information



Vulnerabilities Total: 13

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification

INFO	N/A	10180	Ping the remote host
INFO	N/A	11865	SOCKS Server Detection
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	66717	mDNS Detection (Local Network)

Vulnerabilities Total: 6

SEVERITY	CVSS V2.0	PLUGIN	NAME
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10180	Ping the remote host
INFO	N/A	10287	Traceroute Information

Vulnerabilities

Total: 33

SEVERITY	CVSS V2.0	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)

INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	10180	Ping the remote host
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	83298	SSL Certificate Chain Contains Certificates Expiring Soon

INFO	N/A	42981	SSL Certificate Expiry - Future Expiry

INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection

INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	35712	Web Server UPnP Detection
INFO	N/A	66717	mDNS Detection (Local Network)

192.168.0.113

Vulnerabilities Total: 41

SEVERITY	CVSS V2.0	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	147164	Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple Vulnerabilities
MEDIUM	5.0	152182	Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability
MEDIUM	5.0	144050	Apache Tomcat 9.x < 9.0.40 Information Disclosure
MEDIUM	5.0	12085	Apache Tomcat Default Files
MEDIUM	4.0	141446	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up

INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	55472	Device Hostname
INFO	N/A	54615	Device Type
INFO	N/A	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	33276	Enumerate MAC Addresses via SSH
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	43111	HTTP Methods Allowed (per directory)

INFO	N/A	10107	HTTP Server Type and Version

INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10147	Nessus Server Detection
INFO	N/A	64582	Netstat Connection Information
INFO	N/A	14272	Netstat Portscanner (SSH)
INFO	N/A	11936	OS Identification
INFO	N/A	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	110695	OS Security Patch Assessment Checks Not Supported
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	66334	Patch Report
INFO	N/A	10180	Ping the remote host

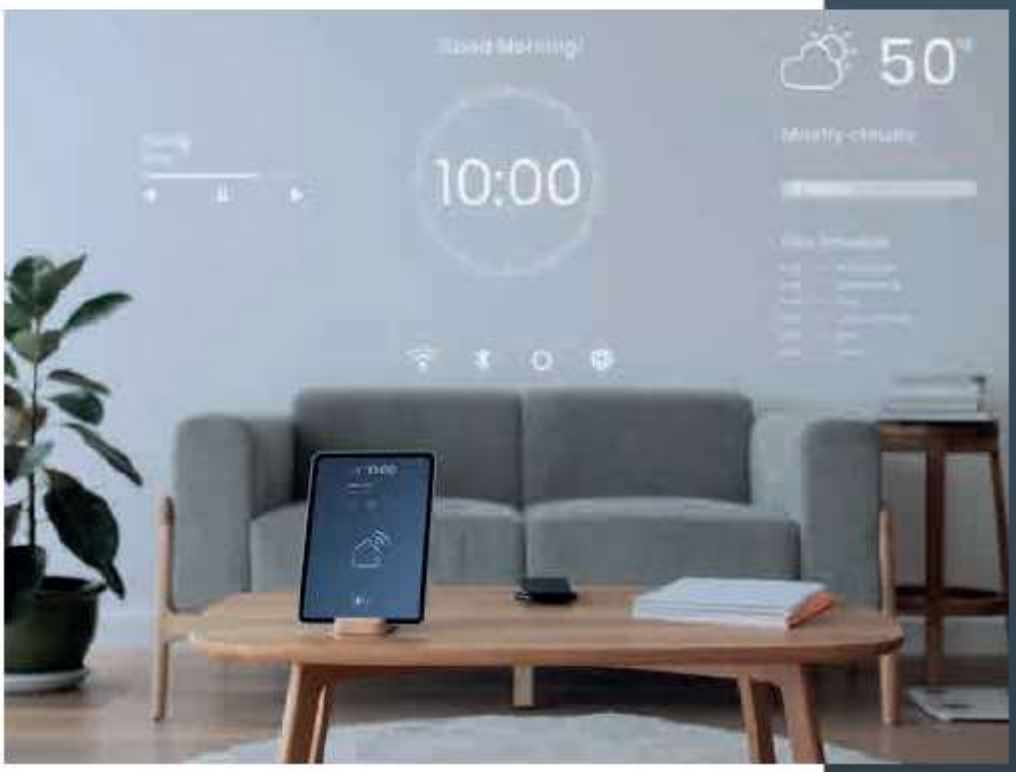
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	22964	Service Detection
INFO	N/A	42822	Strict Transport Security (STS) Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	56468	Time of Last System Startup

Anexo 2: GUÍA DE BUENAS PRÁCTICAS

GUÍA DE BUENAS PRÁCTICAS
de Ciberseguridad en dispositivos IoT

Ing. Miguel Alejandro López Naranjo
Ing. Mg. Galo Mauricio López Sevilla

PUCE | Sede Ambato



ÍNDICE

PUCE | Sede Ambato

PUCE Sede Ambato

IoT

Internet de las Cosas

El internet de las cosas es considerado como una verdadera revolución tecnológica, en especial en el área de las comunicaciones, se trata de una red inteligente entre dispositivos que permiten el intercambio de información y comunicación entre ellos capaces de procesar y gestionar ordenes que son programadas y monitoreadas por las personas.

En la actualidad el Internet de las Cosas se aplica en todas las áreas en las que interactúan las personas, ya sea el área de salud, construcciones, transporte, agricultura, educación, visión artificial, ambiente, industrias. La interacción de estos dispositivos en varias áreas de desarrollo de IoT busca fortalecer la formación de ciudades inteligentes (Smart Cities) automatizando un sin número de servicios públicos y privados y aprovechando los recursos de forma eficiente.

Elementos IoT

1

Elementos de campo o hardware

Componen todos los sensores, actuadores (dispositivos que controlen los sistemas) y otros dispositivos integrados en los objetos y los cuales con los responsables de la interacción y la comunicación con el exterior

2

Plataforma Middleware

Software que permite el intercambio de información entre las aplicaciones, como también las herramientas informáticas que permiten procesar y analizar la información, además provee interfaces de programación para consumir dicha información

3

Aplicaciones e interfaz de interacción con el Usuario

Herramientas que permiten una visualización de la información que sea fácil de interpretar por el usuario y pueden ser accedidas desde cualquier dispositivo vinculado

Machine to Machine
M2M

La comunicación M2M es el paso siguiente de la conexión de uno a uno o conexión de una maquina a otra, en la actualidad el termino M2M se refiere a la comunicación entre maquinas remotas para el intercambio de información. El objetivo principal es recopilar los datos que son transmitidos por la red, además usando secuencias de eventos puede ejecutar acciones de forma automática entre las maquinas que están conectadas, sirviendo como base para la inteligencia artificial y el Internet de las Cosas.

El lenguaje M2M se considera el nivel base para la comunicación entre maquinas dentro de una misma red, el internet de las cosas utiliza esta comunicación para que los dispositivos inteligentes se conecten entre ellos para transferir información y poder ser controlada a través de dispositivos móviles, entendiéndose que esta correlación directa es la que permite las capacidades y soluciones IoT.

Protocolos de Comunicación IoT

Protocolos usados por M2M e IoT

- **AMQP** (Advanced Message Queuing Protocol)
- **WAMP** (Web Application Messaging Protocol)
- **CoAP** (Constrained Application Protocol)
- **XMPP** (Extensible Messaging and Presence Protocol)
- **IRC** (Protocolo Internet Relay Chat)

6

Protocolos usados por M2M e IoT

AMQP
(Advanced Message Queuing Protocol)

Es un protocolo M2M ligero, que fue desarrollado por John O'Hara en JPMorgan Chase en Londres, Reino Unido en 2003. Es un protocolo de mensajería corporativa diseñado para fiabilidad, seguridad, aprovisionamiento e interoperabilidad.
AMQP admite tanto solicitud / respuesta como publicación / suscripción arquitectura. Ofrece una amplia gama de funciones relacionadas a la mensajería, como una cola confiable, mensajería de suscripción y publicación basada en temas, enrutamiento y transacciones flexibles.

WAMP
(Web Application Messaging Protocol)

Es un modelo arquetípico de pilas de soluciones de servicios web, denominado como un acrónimo de los nombres de sus cuatro componentes originales: el sistema operativo Windows, el servidor HTTP Apache, el sistema de gestión de bases de datos relacionales MySQL y el lenguaje de programación PHP.

CoAP
(Constrained Application Protocol)

Es un protocolo M2M ligero del IETF Grupo de trabajo CoRE (entornos RESTful restringidos). Es principalmente desarrollado para interoperar con HTTP y RESTful Web a través de proxy simples. A diferencia de MQTT, CoAP usa Universal Identificador de recurso (URI) en lugar de temas. El editor publica datos en el URI y el suscriptor se suscribe a un recurso particular indicado por el URI. Cuando un editor publica nuevos datos en el URI, entonces todos los suscriptores son notificados sobre el nuevo valor según lo indicado por el URI.

XMPP
(Extensible Messaging and Presence Protocol)

Implementa el paradigma de publicación-suscripción, un ancho de banda altamente escalable y sistema de distribución de eventos energéticamente eficiente [19] donde solo cambios en los datos detectados se transmiten a los receptores registrados desacoplando el involucraron dispositivos de comunicación entre sí. XMPP no se basa únicamente en su mecanismo impulsado por eventos, sino que también admite un esquema de solicitud-respuesta para solicitar explícitamente servicios o datos remotos.

IRC
(Protocolo Internet Relay Chat)

Protocolo que se basa en la comunicación por medio de texto en tiempo real con los dispositivos, donde utiliza el puerto 6667 o 6668 para transmitir datos. Es uno de los protocolos más antiguos pero que se usa aún en la actualidad para la implementación de dispositivos inteligentes por lo que ha tenido un gran alcance, al ser un protocolo sencillo también presenta riesgos de seguridad ya que tiene puertos abiertos y libres para el acceso de atacantes cibernéticos.

Domótica

La domótica es una de las áreas con mayor alcance del internet de las cosas, involucrando al usuario con la tecnología a tal punto de convivir con ella desde la comodidad de su hogar usando aplicaciones que le permitan controlar los dispositivos IoT que se encuentran en la vivienda.

Controlar o manipular dispositivos electrónicos de forma manual quedó rezagado ya que gracias a las tecnologías existentes del IoT permiten que la domótica facilite la vida de las personas además de brindarle confort en su hogar y optimizar los recursos disponibles.

Cuando se habla de domótica se esboza inmediatamente el termino de control remoto, que es muy utilizado para cualquier proceso, logrando como resultado el manejo de los dispositivos que se requieren contralar. En el caso de una vivienda inteligente basada en protocolo de comunicación en su ámbito doméstico se puede controlar desde una computadora, un celular, un PDA, elementos como los sistemas de iluminación, climatización, así como cualquier dispositivo electrónico; utilizar para compras por internet o incluso vigilar las actividades en distintas habitaciones a través de una cámara web. La flexibilidad de este tipo de control permite a las personas un mejor desempeño en las actividades cotidianas a nivel familiar como tecnológico, promoviendo el bienestar social y tecnológico cuando se habla de automatización.

La implantación de domótica en una vivienda proporciona un sin número de beneficios y ventajas c con respecto a una tradicional desde diversos puntos de vista como la seguridad, el ahorro de recursos, la comodidad, la protección del medio ambiente y el confort; todo esto se resumen en una mejor calidad de vida

Redes Domóticas

Las redes domóticas deben cumplir con unas especificaciones técnicas mínimas, los requerimientos más importantes que se debe considerar al momento de implementar una red domótica son:

- Arquitectura
- Topología
- Medios de Transmisión
- Protocolos y Tecnologías

Arquitectura de Redes Domóticas

La arquitectura de red son las acciones que definen el diseño y las funciones de los componentes de hardware y software, esto quiere decir que se puede llegar a conocer los protocolos, dispositivos y tecnología que se necesita en el sistema domótico.

Arquitectura Centralizada: Este tipo de arquitectura consta de un dispositivo central cuya función es recibir los datos de los dispositivos que son parte de la red, así como también procesarlos y enviarlos a la interfaz de usuario, para que programe las ordenes que considere necesarias.

Arquitectura Distribuida: Este tipo de arquitectura descentraliza el sistema de control en cada uno de los dispositivos instalados, mismos que tienen la capacidad de procesar datos y enviarlos al usuario de forma independiente.

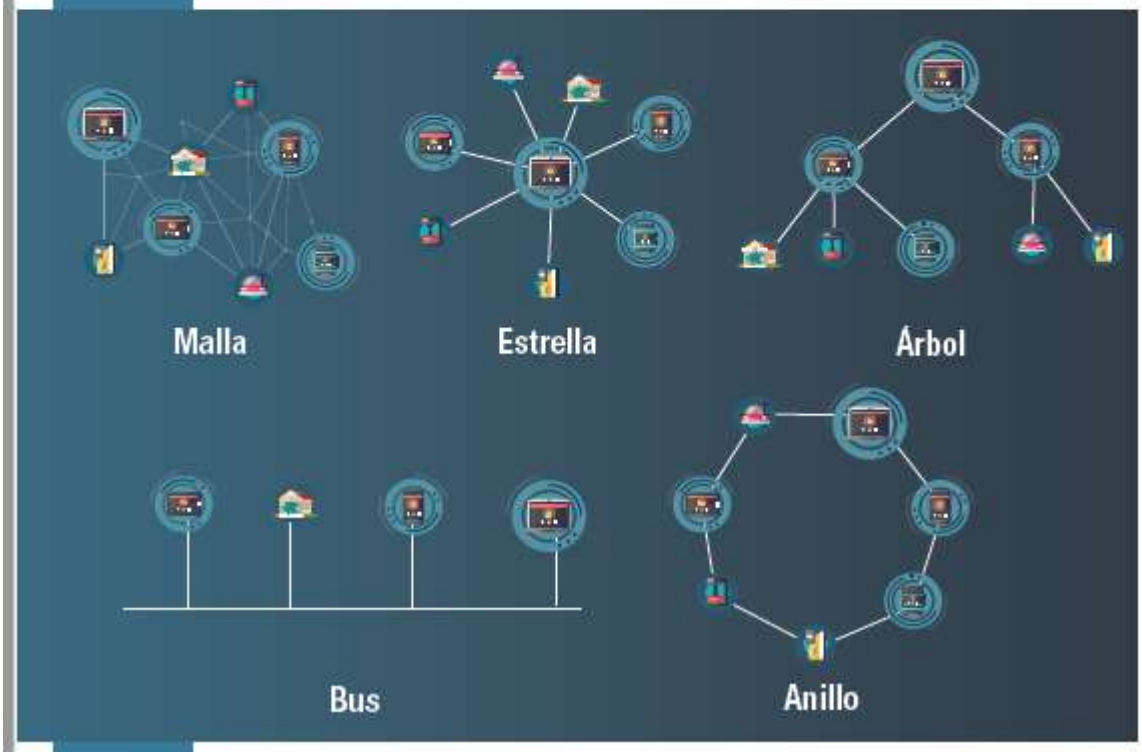
Arquitectura Mixta: Esta arquitectura combina las características de la arquitectura centralizada y distribuida en un mismo sistema con la finalidad de crear distintos controladores capaces de captar y procesar la información recopilada de los dispositivos que se encuentran en la red y transmitirlos al usuario

Topologías usadas en las Redes

Las topologías de red domesticas al igual que las redes de comunicación definen el tipo de configuración con la cual se conectarán los dispositivos y equipos en la red para su comunicación y transmisión de datos.

Topología de Red Lógica: Se entiende como la forma en la cual se comunican los equipos o dispositivos asociados a la red basado en su configuración de software independiente de sus conexiones físicas.

Topología de Red Física: Se entiende como la forma en la cual están conectados los equipos o dispositivos asociados a la red desde el punto de vista de enlaces o medios físicos de transmisión



Medios de transmisión usadas por redes domóticas

Los medios de transmisión que usan las redes domóticas tienen como finalidad ser un puente para la comunicación y transferencia de datos entre los dispositivos de la red. Los medios de comunicación que se usan se distinguen entre sí por su velocidad de transmisión de datos, accesibilidad, costo y distancia de conexión entre puntos.

Medios de Transmisión Cableados.- Los medios de transmisión cableados transmiten señales de datos eléctricas por medio de cables que están conectados a los dispositivos o equipos de la red. En la actualidad los medios de transmisión cableados son usados para la implementación de redes domóticas en hogares por su corta distancia de conexión.

La principal desventaja de los medios cableados es su sensibilidad e interferencia ante el ruido eléctrico además de su difícil instalación en hogares que no cuentan con la infraestructura adecuada para ese tipo de conexiones.

Medios de Transmisión Inalámbricos.- Los medios de transmisión inalámbricos utilizan antenas como su medio de envío y recepción de información mediante señales electromagnéticas entre todos los dispositivos de la red. Este medio de transmisión se adapta con facilidad a su entorno, su instalación es sencilla y fácil de implementar ya que su medio de transmisión es el aire. Los medios inalámbricos en ciertas condiciones proporcionan un extenso rango de cobertura y una alta velocidad de transmisión de datos.

A diferencia de las redes cableadas su costo es elevado, además este medio es susceptible a interferencia en sus señales electromagnéticas por condiciones atmosféricas. Algunas de las tecnologías que se usan como medio de transmisión inalámbricas en la actualidad son: ZigBee, Bluetooth y WiFi.

Medios de Transmisión Ópticos.- Los medios de transmisión ópticos son aquellos que utilizan rayos de luz modulados para la comunicación de los dispositivos, donde la señal de datos puede ser transmitida a través del aire con línea de vista directa entre los equipos o dispositivos, o por medio de su confinación en delgadas hebras de cristal o plástico interconectadas entre los equipos o dispositivos de la red.

Este medio es capaz de transmitir grandes cantidades de datos a tasas de velocidad bastante altas. Además, puede abarcar grandes distancias de comunicación ya que la señal de datos presenta muy bajas atenuaciones ya que carece de interferencias. Al tener un costo elevado para su adquisición e instalación a diferencia de otros medios es muy complicado que los hogares accedan a esta tecnología.

En el presente existen dos tipos de medios ópticos que han sido utilizados en el mercado para la implementación de redes domóticas: el infrarrojo y la fibra óptica

Protocolos de comunicaciones

Partiendo de las arquitecturas de las redes domóticos a continuación se detallan algunos protocolos de comunicación, que no son otra cosa que el idioma por el cual se comunican los dispositivos IoT para la transmisión de datos.

X-10

Protocolo orientado a la utilización de la red eléctrica de las viviendas. Allí se usa corrientes portadoras para controlar los dispositivos conectados a la red a través de las líneas de corriente domestica mediante la modulación de impulsos de 120 khz.

EIB (European Installation Bus)

Sistema domótico desarrollado por la unión europea para evitar las importaciones de productos de características similares desde japo y Norteamérica. Estándar que define una relación extrema a extremo entre los dispositivos distribuyendo la inteligencias entre todos los sensores y actuadores de toda la vivienda.

Konnexx

Es la iniciativa de las asociaciones EIBA, EHSA y BCI con el objetivo de unir esfuerzos de varios fabricantes de sistemas domóticos. El modelo konnexx es la evolución lógica que concentra toda la experiencia y conocimientos de los principales estándares.

LonWorks

Sistema de control domótico propietario presentado por la firma Echelon en 1992. Debido a su costo los dispositivos no han tenido una implantación masiva en los hogares.

Jini

Tecnología de Sun Microsystems que permite descubrir nuevos dispositivos que se van incorporando en la red domestica mediante cualquier medio.

Tcp/IP

Está siendo usado en infinidad de computadores y aplicaciones, de forma que ha conseguido un volumen de negocio tal que ha hecho de esta herramienta ideal para asegurar la interconectividad total entre maquinas en todo el mundo.

Vectores de ataque IoT de OWASP

Open Web Application Security Project (OWASP) es una fundación sin fines de lucro, la cual trabaja para ayudar a mejorar la seguridad de software por medio de proyectos de código abierto, para ayudar a comprender las vulnerabilidades que pueden tener los dispositivos IoT OWASP elaboró una lista de las 10 vulnerabilidades de seguridad principales que pueden tener los dispositivos IoT.

Vectores de ataque IoT de OWASP

Contraseñas débiles, adivinables o codificadas

La mala administración de contraseñas es un problema habitual de y crítico de seguridad, en especial porque muchos de los propietarios de dispositivos inteligentes dejan la configuración de contraseña predeterminada

Servicios de red inseguros

Conexiones de red inseguros y puertos innecesarios abiertos incrementan la superficie de ataque de los dispositivos IoT, generando la posibilidad de sufrir perdida de información o ejecución remota de códigos.

Interfaces de ecosistemas inseguras

Las interfaces con las que interactúan los dispositivos IoT pueden verse afectadas por fallas de seguridad, interfaces móviles, web aplicaciones o la nube proveen acceso a delincuentes informáticos acceso no autorizado a través de una configuración insegura

Falta de un mecanismo de actualización seguro

Las actualizaciones aportan un arma valiosa al momento d abordar un fallo de seguridad en los sistemas y la falta de una configuración adecuada de actualizaciones da como resultado software con un alto índice de fallos de seguridad.

Uso de componentes inseguros u obsoletos

Componentes heredados y obsoletos al no contar con las actualizaciones necesarios pueden poner en riesgo el sistema IoT, estos componentes pueden incorporar fallas por medio de las cuales personas no autorizadas pueden tener acceso a nuestros sistemas.

Vectores de ataque IoT de OWASP

Protección de la Privacidad insuficiente

El almacenamiento no autorizado de datos personales o almacenamiento de datos locales pueden ser una vulnerabilidad de seguridad debido a que la información puede quedar expuesta a personas no autorizadas

Transferencia y almacenamiento de datos inseguros

Cifrado insuficiente o deficiente de los datos e inexistencia de mecanismos de autenticación proveen una puerta de entrada para que ciberdelincuentes puedan robar nuestra

Falta de gestión de dispositivos

La falta de una imagen de la infraestructura de todos los dispositivos IoT que nos permita saber qué es lo que está pasando con el sistema se vuelve imposible administrar la defensa y las respuestas ante las amenazas que se presenten

Configuración predeterminada insegura

La configuración predeterminada debe aplicarse tomando en cuenta la seguridad del usuario final y a largo plazo, por lo general la configuración predeterminada representa un enfoque mínimo e incluso puede traer consigo vulnerabilidades, contraseñas y servicios expuestos que ejecutan permisos de root, los dispositivos deben tener la posibilidad de que los administradores puedan corregir las falencias.

Falta de endurecimiento físico

No descuidar el endurecimiento físico de los dispositivos contra ataques que extraen información confidencial que puede ser usada para ataques remotos o para obtener control del dispositivo

Amenazas IoT

Tradicionalmente las amenazas a la seguridad de los dispositivos IoT surgen en el entorno virtual y se dirigen al proceso de manipulación de datos, es así que conduce a la interpretación de seguridad de la tecnología de la Información (TI) como el conjunto de sus principales aspectos como son confidencialidad, integridad, disponibilidad (CIA).

La Unión Internacional de Telecomunicaciones (ITU-T Y.4806) clasifica las amenazas principales de los dispositivos IoT según sus vectores de impacto, los cuales pueden provenir de un entorno virtual y del entorno físico, como se muestra en la figura 11 los problemas pueden surgir de ambos tipos de entornos y afectar los aspectos físicos , aspectos virtuales y del dispositivo en si

Amenazas entorno virtual:
Las amenazas lógicas afectan al software de los dispositivos, comprenden una gran variedad de programas informáticos que pueden dañar la integridad del sistema informático aprovechando las vulnerabilidades de los dispositivos.

Amenazas entorno físico:
Las amenazas físicas afectan al parte del hardware del sistema, se pueden producir de forma voluntaria o involuntaria, como ejemplo podemos nombrar los siguientes: robos, sabotajes, incendios, cortes eléctricos, catástrofes naturales o artificiales y demás peligros a los que están expuestos nuestros dispositivos.


CYBER SECURITY
CYBER SECURITY
Buenas
Prácticas de
SEGURIDAD
17

Amenazas STRIDE

STRIDE es un acrónimo de seis categorías de amenazas: Suplantación de identidad (Spoofing), manipulación de datos (Tampering), amenazas de repudio (Repudio), divulgación de información (Information disclosure), denegación de servicio (Denal of service) y elevación de privilegios (Elevation of privileges).

STRIDE desarrollado por Microsoft, modela riesgos y evalúa las amenazas para los entornos de tecnologías de la información. El modelo STRIDE se amplió también para incorporar amenazas que pueden estar presentes en los sistemas IoT.

S — **Suplantación de identidad (Spoofing)**
Una persona o dispositivo usa credenciales de otro usuario con el objetivo de acceder a los datos y acciones a las que no tiene autorización.

T — **Manipulación de datos (Tampering)**
Se trata de modificar y manipular la información para causar caos en el sistema.

R — **Amenazas de repudio (Repudio)**
Negar a una persona o dispositivo involucrado en una transacción o evento específico del sistema o a su vez transmitir datos incorrectos que pueden confundir procesos de análisis y operación

I — **Divulgación de información (Information disclosure)**
Intrusión de una persona no autorizada con el fin de interceptar la transmisión de datos y capturar información confidencial

D — **Denegación de servicio (Denal of service)**
Capacidad de hacer que un servicio en particular deje de estar disponible, generalmente a través del consumo de recurso o ejecuciones no confiables

E — **Elevación de privilegios (Elevation of privileges)**
Capacidad de que un usuario sin privilegios gane suficiente acceso para poder comprometer el sistema.

18

IS

Suplantación de identidad (Spoofing)

Recomendación

Para evitar estas amenazas es fundamental que los sistemas de Autenticación entre plataformas y dispositivos sean robustos.

Aplicación de filtros y firewall en el router central del Sistema domótico para evitar Ataques de spoofing

19

IT

Manipulación de datos (Tampering)

Recomendación

Dispositivos con firmware seguro y certificados, elevan el nivel de seguridad y reducen dramáticamente la posibilidad de que un agente no deseado modifique su hardware o software para alterar su funcionamiento.

Aplicación de reglas de cortafuego y Firewall para establecer que el tráfico solo puede ser transmitido por los dispositivos asignados.

IR

Amenazas de repudio (Repudio)

Recomendación

Para minimizar estos riesgos es fundamental la NO compartición de usuarios y contraseñas de acceso, así como la trazabilidad y almacenado histórico de cualquier acceso y operación realizada en los sistemas.

Usar de programas para monitoreo el tráfico de la red domótica para controlar y avisar sobre los cambios en la red domótica

21

II

Divulgación de información (Information disclosure)

Recomendación

Asegurar que la información digital en los dispositivos y en el tráfico por la red, está encriptada siempre.

Usar software especializado en detectar ataques ARP para identificar los dispositivos que han sido vulnerados.

ID

Denegación de servicio (Denal of service)

Recomendación

La segmentación de red impedirá que el número de dispositivos involucrados en DoS solo se propagara a un segmento de red. Los sistemas de Backup y recovery permitirían que, cualquier dispositivo o sistema parado, pueda ser restaurado rápidamente a su estado anterior.

Utilizar software de detección de tráfico en la red para detectar algún evento inusual en el tránsito de la información, identificar la ip de origen del ataque y bloquear el equipo para evitar el bloqueo de servicios.

23

IE

Elevación de privilegios (Elevation of privileges)

Recomendación

La escalación de privilegios viene normalmente causada por fallos de diseño, que en muchos casos se hacen públicos o semi públicos en forma de vulnerabilidades.

Bloquear todo tipo de comunicaciones que no sean necesarias o caso contrario protegerlas con contraseñas robustas

Bibliografía

- Alvear Puertas, V., Rosero Montalvo, P., Peluffo Ordóñez, D., & Pijal Rojas, J. (2017). Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones. Enfoque UTE, 8, 244-256. https://doi.org/10.29019/enfoqueute.v8n1.121

- Atmoko, R. A., Riantini, R., & Hasin, M. K. (2017). IoT real time data acquisition using MQTT protocol. Journal of Physics: Conference Series, 853, 012003. https://doi.org/10.1088/1742-6596/853/1/012003

- Domínguez Margareto, D. (2020). Ciberseguridad en Internet of Things: Análisis de amenazas, riesgos y vulnerabilidades. 1, 90.

- Gartner. (2017). 8.4 Billion Connected Things Will be in Use 2017 (Gartner dice que 8.4 mil millones de «cosas» conectadas estarán en uso en 2017, un 31 por ciento más que en 2016). Gartner. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

- Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). Cyber security of smart homes: Development of a reference architecture for attack surface analysis. Living in the Internet of Things: Cybersecurity of the IoT - 2018, 1-10. https://doi.org/10.1049/cp.2018.0045

- González García, A. J. (2017). IoT: Dispositivos, tecnologías de transporte y aplicaciones. http://openaccess.uoc.edu/webapps/o2/handle/10609/64286

- Herrera Quintero, L. F. (2005). Viviendas Inteligente Domótica. 25(2), 8.

- Kirsche, M., & Klauck, R. (2012). Unify to bridge gaps: Bringing XMPP into the Internet of Things. 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, 455-458. https://doi.org/10.1109/PerComW.2012.6197534

- Mora González, S. (2015). Entendiendo el Internet de las cosas | Investiga.TEC. https://revistas.tec.ac.cr/index.php/investiga_tec/article/view/2381

- Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. 2017 IEEE International Systems Engineering Symposium (ISSE), 1-7. https://doi.org/10.1109/SysEng.2017.8088251

- Rojas García, C. R. (2015). CREACIÓN DE UN SISTEMA DOMÓTICO DE SEGURIDAD Y CONSUMO ENERGÉTICO PARA HOGARES. HOMENODE. https://1library.co/document/7q046g9z-creacion-sistema-domotico-seguridad-consumo-energetico-hogares-homenode.html

- Salazar Soler, J., & Silvestre Bergés, S. (2016). Internet de las cosas—CORE. Internet de las cosas. https://core.ac.uk/display/81581111?recSetID=

- Sánchez Sánchez, J. D. (2018, abril 23). IoT o internet de las cosas: Qué es y cómo puede transformar mi negocio [Artículo]. Inforges. https://www.inforges.es/post/iot-o-internet-de-las-cosas-que-es

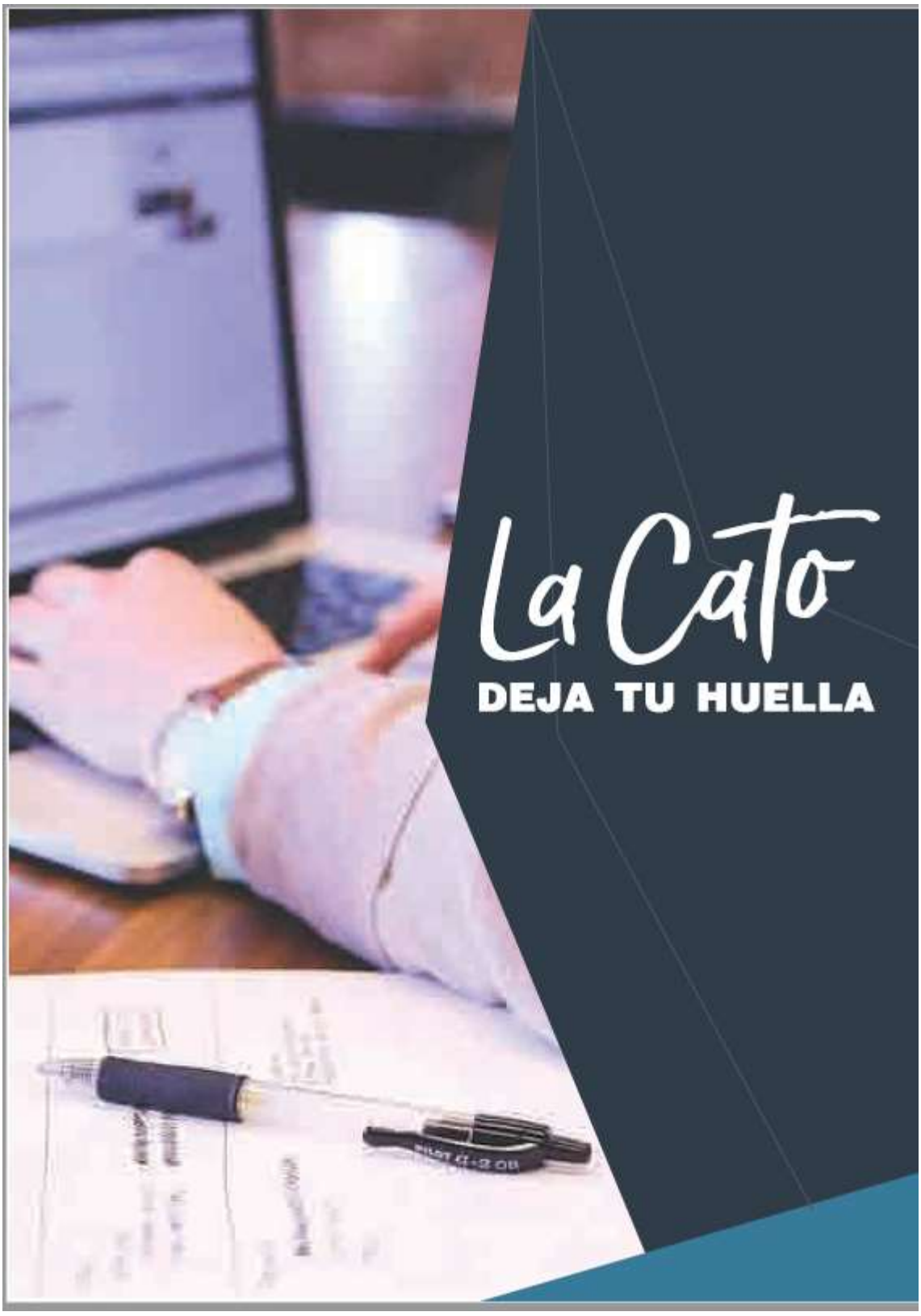
- Schrecker, S. (2016). Industrial Internet of Things. IIC:PUB:G4:V1.0:PB:20160926, G4: Security Framework, 173.

- Sebastian, A., & Sivagurunathan, S. (2018). Multi DODAGs in RPL for Reliable Smart City IoT. Journal of Cyber Security and Mobility, 7(1), 69-86. https://doi.org/10.13052/jcsm2245-1439.716

- UIT-T. (2017). Y.4806: Security capabilities supporting safety of the Internet of things. E 42087. https://www.itu.int/rec/T-REC-Y.4806-201711-I/en

- Xue Jun, L., Maode, M., & Yi Lin, Y. (2019). Detecting IRC-based Botnets by Network Traffic Analysis Through Machine Learning | IEEE Conference Publication | IEEE Xplore. 1(1). https://ieeexplore.ieee.org/abstract/document/9077964

- Yantao, K. (2015). A High Security Data Sharing Platform for Internet of Things based on WAMP Structure using Secure-RESTful Strategy. https://repository.hanyang.ac.kr/handle/20.500.11754/127722


La Cato
DEJA TU HUELLA

PUCE | Sede Ambato

GUÍA DE BUENAS PRACTICAS

de Ciberseguridad en dispositivos IoT