IOT Y SU RELACIÓN CON LAS REDES DE CÓMPUTO, SERVICIOS DE RED Y CIBERSEGURIDAD

IOT AND ITS RELATIONSHIP WITH COMPUTER NETWORKS, NETWORK SERVICES AND CYBERSECURITY

Juan Pablo Ramírez López
Universidad Veracruzana, México
zS17014949@estudiantes.uv.mx

Fabián Higinio Dionisio
Universidad Veracruzana, México
zS17014924@estudiantes.uv.mx

Martha Elizabet Domínguez Bárcenas
Universidad Veracruzana, México
eldominguez@uv.mx

Willian Zárate Navarro
Universidad Veracruzana, México
wzarate@uv.mx

Héctor Xavier Limón Riaño
Universidad Veracruzana, México
hlimon@uv.mx

Recepción: 23/noviembre/2023 **Aceptación:** 26/diciembre/2023

Resumen

El Internet de las Cosas (IoT) está teniendo cada vez mayor presencia en múltiples ámbitos. Este documento tiene la finalidad de conocer IoT bajo la perspectiva de networking, servicios de red y ciberseguridad, ya que se observa una estrecha relación entre estas áreas y la arquitectura de IoT, además de que se ha detectado poca presencia de estos temas en carreras de tecnologías de la información. A través de una revisión sistemática de literatura se recuperó información sobre las áreas de aplicación que tiene IoT, protocolos y tecnologías utilizados, servicios de red que utiliza IoT en sus implementaciones, se aborda la seguridad en IoT explicando vulnerabilidades y ataques a la tecnología, así como algunas medidas de seguridad al respecto. De acuerdo con los resultados, este

trabajo puede servir como referente para incluir temas relacionados con IoT en los programas educativos interesados en abordar las áreas mencionadas.
Palabras Clave: Ciberseguridad, Internet de las Cosas, Redes.

Abstract

The Internet of Things (IoT) is having an increasing presence in multiple fields. This document has the purpose of knowing IoT from the perspective of networking, network services and cybersecurity, since a close relationship is observed between these areas and the IoT architecture, in addition to the fact that little presence of these topics has been detected in bachelor's degrees on information technology. Through a systematic literature review, information was recovered on the application areas of IoT, protocols and technologies used, network services that IoT uses, IoT security is addressed, explaining vulnerabilities and attacks on technology, as well as some security measures in this regard. According to the results, this work can serve as a reference to include topics related to IoT in educational programs interested in addressing the mentioned areas.
Keywords**:** *Cybersecurity, Internet of Things, Networking.*

1. Introducción

El término IoT tiene su origen a finales del siglo pasado (1999) cuando Kevin Ashton, directivo de Procter & Gamble, tuvo la iniciativa de crear un grupo de investigadores llamada Auto-ID Center en el Instituto Tecnológico de Massachussets (MIT), que se dedicaba a averiguar información sobre la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores [Adrián, 2018]. Sin embargo, el uso de los dispositivos inteligentes o dispositivos del Internet de las Cosas (dispositivos IoT) comenzó a ganar mucho terreno durante los últimos años, sobre todo a partir de la llamada “cuarta revolución industrial” o “Industria 4.0” [FOSTEC & Company GmbH, 2018]. Con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet, el Internet de las cosas (IoT) es una red de objetos físicos (“cosas”) que llevan incorporados sensores, software y otras tecnologías [Oracle Corporation, 2021.].

En México 7 de cada 10 empresas que han incursionado en temas de IoT tienen proyectos activos o en desarrollo y uno de los principales enfoques está en las operaciones manufactureras y logísticas. Sin embargo, los directivos se muestran preocupados por la disponibilidad de habilidades necesarias en su personal para utilizar esta tecnología, por lo que hay una brecha entre oferta y demanda de personal capacitado en tecnologías emergentes [PriceWaterhouseCoopers, 2019].
Sin duda, la academia puede contribuir a cerrar la brecha de profesionales capacitados para atender las necesidades de la sociedad. Además, se han identificado tres capas principales de la arquitectura de IoT que son: la capa de percepción, que contempla temas de infraestructura; la capa de red que aborda la conectividad entre dispositivos; y la capa de aplicación que hace uso de servicios de red [Mohamad, 2019]. Por ello se considera que la identificación de las tecnologías de Networking y Servicios de red presentes en las implementaciones de IoT, así como de los aspectos de ciberseguridad asociados a estas, podría contribuir para que la academia analice la pertienencia de incluir los temas correspondientes en la formación de profesionales de las Tecnologías de la Información.
En las siguientes secciones se describe la metodología aplicada para la investigación, se presentan los resultados y la discusión de los mismos, para finalizar con las conclusiones correspondientes.

2. Métodos

Para obtener la información necesaria en este trabajo se realizó una Revisión Sistemática de Literatura (RSL) basada en la metodología de Bárbara Kitchenham [Kitchenham, 2009].
Primero, se definieron las siguientes preguntas de investigación:

- P1: ¿Qué características debe tener una infraestructura de red para implementar la tecnología IoT?
- P2: ¿Qué protocolos de conectividad se utilizan al implementar IoT y cuáles son sus características?
- P3: ¿Qué aplicaciones tiene IoT y cuáles son los servicios de red asociados?

- P4: ¿Cuáles son las vulnerabilidades más frecuentes en entornos IoT y cuáles son sus causas?
- P5: ¿Qué recomendaciones de seguridad se deben tomar en cuenta en la implementación de IoT?

Después se realizó una búsqueda automatizada para encontrar información que respondiera a las preguntas de investigación. Para ello, se definieron conceptos clave de cada una de las preguntas de investigación y posteriormente se identificaron términos relacionados con cada concepto clave, tabla 1.

Tabla 1 Conceptos clave y términos relacionados.

Concepto clave	Términos
Network infrastructure	Network design, Network features
IoT	IoT, Internet of things, IIoT, Industrial internet of things
Protocols	Network protocols, Security protocols, IoT applications, IoT services
Solutions	
Vulnerabilities	Vulnerabilities, Risks
Security recommendations	Security recommendations, Cybersecurity, Security measures

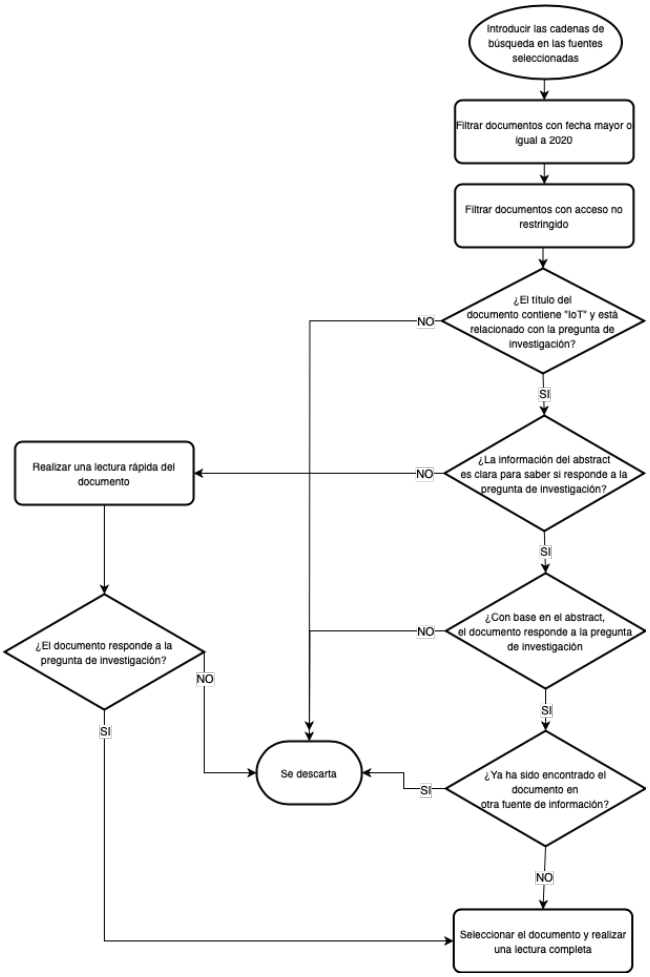
Fuente: elaboración propia.

Se realizaron cadenas de búsqueda utilizando los términos relacionados y se asoció cada pregunta de investigación (P) a una cadena (C) de búsqueda:

- P1-C1: (“IoT” OR “Internet of Things” OR “Industrial Internet of Things” OR “IIoT”) AND (“Network infrastructure” OR “Network design” OR “Network features”).
- P2-C2: (“IoT” OR “Internet of Things” OR “Industrial Internet of Things” OR “IIoT”) AND (“Network protocols”).
- P3-C3: (“IoT” OR “Internet of Things” OR “Industrial Internet of Things” OR “IIoT”) AND (“IoT applications” OR “IoT services”).
- P4-C4: (“IoT” OR “Internet of Things” OR “Industrial Internet of Things” OR “IIoT”) AND (“Vulnerabilities” OR “Risks”).
- P5-C5: (“IoT” OR “Internet of Things” OR “Industrial Internet of Things” OR “IIoT”) AND (“Security protocols” OR “Security recommendations” OR “Cybersecurity” OR “Security measures”).

Una vez definidas las cadenas de búsqueda, se introdujeron en fuentes de información para iniciar la búsqueda de estudios asociados. Dichas fuentes fueron ACM Digital Library, ScienceDirect e IEEE Xplore, pues son fuentes recomendadas en las áreas de computación por Kitchenham.

Se definieron criterios de inclusión y exclusión para filtrar los estudios que aporten la información más relevante y reciente para las preguntas de investigación: fecha de publicación mayor o igual a 2020, análisis del abstract para saber si el contenido está directamente relacionado con la investigación, lectura rápida del documento, descarte de artículos previamente identificados en otras fuentes de información, descarte de documentos de acceso restringido. Dichos criterios se ordenaron siguiendo el procedimiento de selección de estudios que se muestra en la figura 1.



Fuente: elaboración propia.

Figura 1 Diagrama del procedimiento de selección de estudios.

Por último, debido a la gran cantidad de resultados obtenidos por las cadenas de búsqueda, se decidió aplicar los siguientes criterios de detención [Garousi, 2019] durante la filtración del título del documento, ya que la metodología de Kitchenham no los contempla, los cuales fueron:

- Esfuerzo limitado: Se evaluaron los primeros 150 documentos encontrados.
- Agotamiento de evidencia: la interrupción de la búsqueda se vio influenciada por la calidad y la disponibilidad de los resultados.

Una vez concluida la selección de estudios se obtuvieron 59 resultados mediante la búsqueda automatizada, de los cuales, 12 artículos fueron hallados en ACM Digital Library, 27 documentos en IEEE Xplore y 20 resultados se encontraron en ScienceDirect. Posteriormente, de estos estudios se extrajo la información que respondiera a las preguntas de investigación definidas anteriormente.

Concluida la extracción de datos, fue necesario sintetizar dicha información para poder organizarla. Para la síntesis de datos se utilizó el método de Síntesis Temática [Cruzes, 2011], que consiste en:

- Identificar segmentos específicos de texto: de cada respuesta a las preguntas de investigación se crean partes o segmentos del texto que representan ideas distintas.
- Etiquetar segmentos de texto (codificación): es el proceso de organizar los datos contenidos de cada estudio de la revisión sistemática, identificando uno o más pasajes del texto que ejemplifiquen una misma idea teórica o descriptiva.
- Reducir la superposición (códigos repetidos) y traducir códigos a temas: primero se reducen los códigos repetidos (superposición) agrupando los códigos que hagan referencia al mismo concepto y después se realiza la traducción de códigos en temas, es decir, se analiza cómo se pueden combinar diferentes códigos para formar un tema general.
- Crear un modelo de temas de orden superior: los temas que surgieron en el paso anterior ahora pueden interpretarse de manera más detallada para crear un modelo de temas de orden superior.

3. Resultados

El modelo de temas de orden superior, resultado de la síntesis temática, permitió organizar los hallazgos que se presentan a continuación; estos surgieron a partir de la extracción de información del total de estudios seleccionados, cuya lista completa se puede consultar en el siguiente enlace:

https://uvmx-my.sharepoint.com/:x:/g/personal/zs17014949_estudiantes_uv_mx/EfGsf9JQrpIGtxLge1G6SvEBY8SlLt6S1Vy5Ac3ELxdaGA?rtime=BqMN4pj320g

Aplicaciones de IoT

IoT se puede clasificar en 3 casos de uso diferentes: Internet Industrial de las Cosas (IIoT), IoT del consumidor e IoT empresarial [Muteba, 2022].

El IoT del consumidor tiene como objetivo mejorar la calidad de vida y el bienestar de los usuarios individuales al automatizar y simplificar las tareas diarias [Muteba, 2022]. En esta categoría se encuentran aplicaciones como Smart Home y Smart Health. En Smart Home, IoT puede controlar todo lo que contiene una casa para hacerlo compatible con el entorno, siendo Internet el enlace que conecta los objetos entre sí, permite enviar y recibir información utilizando plataformas o aplicaciones para controlar los dispositivos remotamente. Estos dispositivos pueden ser refrigerador, aire acondicionado, sistema de alarma, luces, apagadores, enchufes, cerraduras y muchos otros [Najmi, 2021], [Khanam, 2020]. “Smart Health gestiona la salud del consumidor de manera eficiente” [Shafique, 2020], su función es ayudar a los médicos a diagnosticar el estado y necesidades de los pacientes, así como ayudar a mejorar las condiciones de los hospitales [Najmi, 2021]. Algunas aplicaciones de salud en IoT son: seguimiento de la información del paciente (presión arterial, nivel de glucosa y saturación de oxígeno), gestión de medicamentos, gestión de alimentos, sistema de rehabilitación, entre otros [Bhuiyan, 2021].

La mayoría de las inversiones que se han realizado, siendo el factor principal de lanzamiento de Internet Industrial de las Cosas (IIoT) son el negocio de fabricación, producción, generación de energía y agricultura [Javaid, 2021]. Existe un gran potencial para la eficiencia, el control de la calidad, la sostenibilidad, la seguridad y

el seguimiento de la producción con el uso de IIoT. Por ejemplo, la agricultura y el medio ambiente se pueden gestionar utilizando redes y dispositivos inteligentes, así como la ganadería y piscicultura convencionales debido a la integración de sensores y tecnologías RFID. Los sensores son capaces de monitorear diversos parámetros como la temperatura, humedad, y los contaminantes microbianos en la agricultura inteligente [Tariq, 2021], [Khanam, 2020].

IoT empresarial permite que los objetos con dispositivos informáticos integrados participen en las operaciones comerciales, sustituyendo el trabajo humano y mejorando la eficiencia corporativa [Muteba, 2022]. Algunos ejemplos son Smart City y Smart Grid.

Las ciudades inteligentes surgen de la integración de diferentes aplicaciones IoT en varios sectores [Khanam, 2020]. Este concepto se refiere al control inteligente de las ciudades utilizando métodos electrónicos, sensores, técnicas de comunicación avanzadas, etc., utilizando IoT para establecer una conexión entre sensores, dispositivos y redes. Smart Grid es la combinación de red eléctrica y red de comunicación para distribuir electricidad entre hogares y negocios desde la planta de energía de la manera más eficiente. Con ella, todos los sistemas como la iluminación, tráfico o ambiental pueden controlarse en una sola red [Janani, 2021], [Khanam, 2020]. Se logra utilizando redes de transmisión, software, transformadores, estaciones, subestaciones, sensores y sistemas embebidos.

Diseño e infraestructura de red en IoT

Los dispositivos más comunes en IoT son los sensores, actuadores y puertas de enlace [Aires, 2021]. Sin embargo, en ambientes industriales es posible encontrar más elementos que componen una infraestructura de red para IoT. Los dispositivos IoT tienen la característica de ser limitados en procesador, memoria y energía, sin embargo, generalmente se implementan en entornos hostiles, dinámicos y heterogéneos, por ello se conectan bajo las limitaciones de las redes de baja potencia y con pérdidas (LLN) [Khanam, 2020]. Las puertas de enlace o gateways actúan como un mediador, concentrando la comunicación entre los objetos y sistemas IoT incluso si estos se implementan utilizando protocolos y estándares

distintos. Soportan la gestión de las cosas, incluyendo aspectos como la heterogeneidad y la seguridad [Aires, 2021].

IoT se puede establecer con base en 2 tipos de infraestructura de red: redes dependientes de la infraestructura y redes independientes de la infraestructura. En las primeras hay dispositivos como routers, switches y estaciones base que se conectan con los dispositivos finales. Por otro lado, en las redes independientes de la infraestructura o redes ad-hoc no hay nodos fijos o centrales, son los dispositivos finales quienes trabajan en conjunto para establecer la comunicación [Shahraki, 2021].

En las redes IoT se utilizan comunicaciones inalámbricas y estas funcionan remotamente, suelen tener restricciones de recursos en los dispositivos, altas tasas de error, bajas tasas de datos e inestabilidad en los enlaces de comunicación [Tariq, 2021]. La arquitectura de IIoT exige una infraestructura de bajo costo y bajo consumo, por lo que se tienen requisitos más estrictos para lograr confiabilidad inalámbrica y baja latencia [Khanam, 2020]. Los protocolos utilizados para compartir datos del Internet convencional no son opciones compatibles con la restricción de baja potencia en IoT, además, no existe una única tecnología de comunicación que sea capaz de admitir entornos heterogéneos debido a la diversidad de dispositivos IoT [Al-Masri, 2020]. De acuerdo con el software integrado en dispositivos IoT con un sistema operativo ligero de uso general o un sistema operativo en tiempo real, los módulos de seguridad livianos, robustos y tolerantes a fallas deben diseñarse para pilas de protocolos y software livianos [Khanam, 2020]. Otra de las características que tiene una red IoT, es que es casi imposible configurar manualmente dispositivos remotos, por lo que se requiere que los proveedores de red puedan configurar dispositivos a través de la red desde un punto de administración centralizado [Alam, 2020].

Tecnologías y protocolos de comunicación en IoT

Actualmente no existe una arquitectura IoT adoptada de manera universal dado que varios autores han propuesto distintas arquitecturas [Khanam, 2020]. Khanam presenta una arquitectura basada en 3 capas: aplicación, red y percepción. La capa

de aplicación proporciona una interfaz entre los objetos y las redes, su objetivo principal es proporcionar diferentes servicios de aplicación a los usuarios finales. La capa de red se compone de software, protocolos y tecnologías que permiten la conectividad de objeto a objeto y de objeto a Internet, su función principal es transmitir los datos recopilados de la capa física en forma de una señal digital. La capa de percepción incluye objetos del mundo físico y entidades virtuales, su tarea principal es recopilar datos del entorno a través de varios sensores. Los sensores convierten los datos sin procesar, recopilados de los objetos físicos, en señales digitales legibles.

Entre los estándares, tecnologías y protocolos de comunicación utilizados en la capa de percepción IoT se encuentran: Ethernet 802.3, Wi-Fi 802.11, IEEE 802.15.4 (LR-WPAN), Zigbee, Z-Wave, NFC, RFID, Bluetooth, red de área amplia de baja potencia (LPWAN), red de sensores inalámbricos (WSN), WirelessHART, radios de largo alcance como LoRa, Sigfox y NB-IoT, GPS y tecnologías celulares como 2G (GSM), 2.5G (GPRS), 3G (UMTS/WCDMA/HSPA), 4G, LTE y 5G, entre muchos otros [Al-Masri, 2020], [Khanam, 2020], [Najmi, 2021], [Zaman, 2021].

Los protocolos de capa de red utilizan diferentes técnicas de identificación para ubicar a los dispositivos en las redes, ya sean pequeñas o grandes [Al-Masri, 2020]. Esta identificación se puede lograr mediante direcciones de red con protocolos como IPv4, IPv6 o 6LoWPAN. Sin embargo, existen otros protocolos en esta capa como: RPL, RoLL, EIGRP, ICMP, IGMP, OSPF, LOADng entre otros [Khanam, 2020], [Zaman, 2021]. RPL tiene propuestas de protocolos que intentan mejorarlo. Por ejemplo, para mejorar la escalabilidad, consumo de energía y memoria se encuentran MERPL y D-RPL. Para optimizar el reenvío con la ruta más corta están DT-RPL y DualMOPRPL. Para mejorar la movilidad se encuentran CoRPL y RDARPL [Rojas, 2021].

Entre los protocolos utilizados en la capa de aplicación se encuentran CoAP, HTTP, MQTT, MQTT-SN, XMPP, AMQP, DDS y REST [Sidna, 2020], [Khanam, 2020], [Zaman, 2021].

La red de área amplia de baja potencia (LPWAN) es un término para identificar las tecnologías inalámbricas que permiten la comunicación de área amplia a bajo costo

y consumo de energía [Ballerini, 2020], adecuada para comunicaciones IoT de largo alcance y redes celulares Machine-to-Machine (M2M) [Muteba, 2022].

En el mercado están surgiendo muchas tecnologías LPWAN con licencia y sin licencia, como Long Range (LoRa), LoRaWAN, LTE-M, Sigfox, Narrowband IoT (NB-IoT), IEEE 802.15.4w y Weightless [Ballerini, 2020], [Gomez, 2020], [Song, 2021].

Servicios de red en IoT

Las implementaciones de IoT requieren que sus dispositivos y sistemas se puedan administrar, y para ello hay 2 conceptos de gestión: remota y centralizada. Por un lado, las redes móviles e inalámbricas deben incluir mecanismos de administración remota para sus dispositivos y aplicaciones, permitiendo una programación inteligente, y así utilizar mejor las capacidades de los servicios IoT [Muteba, 2022]. Por otro lado, IoT requiere que los dispositivos se puedan configurar y reconfigurar a través de la red desde un punto de administración centralizado [Alam, 2020]. La infraestructura de red debe monitorearse periódicamente para detectar comportamientos anormales y abruptos en el tráfico, aumentando con ello la calidad de servicio (QoS) en la red [Shahraki, 2021]. De hecho, son los dispositivos como routers y switches quienes se encargan de estas tareas en las redes IoT dependientes de la infraestructura.

Entre los servicios de red que se utilizan para las implementaciones de IoT está el servidor web incorporado, que a menudo se integra en los dispositivos de red inteligentes para la configuración y operaciones remotas [Jiang, 2020]. Los dispositivos IoT proporcionan un mini servidor web o un servidor personalizado con un puerto de escucha que permite a los usuarios acceder y controlar el dispositivo [Zhou, 2021].

En IoT se tienen protocolos de descubrimiento de servicios: el de descubrimiento de servicios DNS (DNS-SD) y el sistema de nombres de dominio de multidifusión (mDNS). Estos ayudan a la gran escalabilidad de los mecanismos de gestión de recursos que pueden obtener registros autoconfigurados y descubrir recursos y servicios de manera efectiva [Bhuiyan, 2021].

Seguridad en IoT

El Internet de las Cosas no está exento de presentar vulnerabilidades y desafíos de seguridad. En primer lugar, los problemas de seguridad en IoT surgen debido a la naturaleza misma de los objetos inteligentes, pues los protocolos que utilizan están diseñados para dispositivos y redes con recursos limitados, donde se necesita minimizar la cantidad de datos intercambiados entre nodos, por lo que son susceptibles a ataques de seguridad [Khanam, 2020], [Litoussi, 2020]. Por ejemplo, en **Man in the Middle (MiTM)** un atacante interfiere en la transmisión de 2 dispositivos IoT para espiar, controlar la comunicación, u obtener acceso a información privada. Por otro lado, el **nodo falso** es una variación de MiTM, y ocurre cuando el atacante agrega un nodo de comunicación física adicional entre 2 o más nodos IoT legítimos de la red. El nodo inyectado participa en la comunicación y puede insertar información maliciosa o tomar el control del flujo de datos [Khanam, 2020], [Zaman, 2021]. En los **ataques de colisión** un atacante transmite en el mismo canal que un nodo legítimo, resultando un choque de transmisiones para que el receptor no pueda interceptar los datos recibidos, lo que lleva a la retransmisión del mismo paquete. En caso de que el ataque de colisión continúe hasta agotar la energía de un dispositivo, se denomina **ataque de agotamiento**. En **Denial of sleep** se ejecutan ataques de colisión repetidos para evitar que el nodo entre en suspensión [Butun, 2020], el atacante modifica la rutina habitual de reposo o fuerza a los sensores a estar activos [Zaman, 2021]. El **Eavesdropping** es una incursión en la que alguien intenta robar información que transmiten los dispositivos “escuchando a escondidas”, utilizando las líneas de comunicación inseguras para acceder a la información que se envía y recibe. De esta manera un atacante puede obtener acceso a una conversación privada y capturar datos como contraseñas [Butun, 2020], [Litoussi, 2020], [Zaman, 2021]. El **Jamming** es un problema donde el atacante selecciona canales o paquetes para transmitir una señal de alto rango y potencia. De esta manera se interrumpen, eliminan o mantienen ocupados los canales de transmisión IoT, creando problemas de disponibilidad de nodos al bloquear la comunicación [Zaman, 2021], [Chen, 2020]. El **Flooding** es un tipo de ataque DoS que está diseñado para transmitir tráfico masivo a través de un canal o

servicios de comunicación. Su objetivo es agotar los recursos de un nodo mediante el broadcasting de mensajes, haciendo que la víctima pierda disponibilidad [Khanam, 2020], [Zaman, 2021]. La **clonación de nodos** ocurre cuando un atacante coloca réplicas de los nodos IoT comprometidos en muchos lugares de la topología para generar inconsistencias. Esto afecta el comportamiento de la red y se pueden usar las credenciales de los nodos víctima para tener acceso a la red [Anand, 2020], [Butun, 2020]. Una variante de la clonación tiene por nombre **Sybil**, en este ataque un solo nodo no autorizado presenta sus propias y múltiples identidades a otros nodos en la red. Estas identidades se consideran una asignación desigual de recursos por parte del dispositivo y provocan confusión en la red, ya que los nodos reciben rutas contradictorias que pasan a través del atacante [Butun, 2020], [Khanam, 2020], [Zaman, 2021].

El hecho de que IoT tenga desafíos y ataques de seguridad ha abierto áreas de oportunidad para que se trabaje en la definición de distintas recomendaciones, herramientas o medidas de seguridad para intentar cubrir estas deficiencias. Por ejemplo, una forma de defenderse contra los ataques de nodos es simplemente ocultarlos o tener un despliegue masivo de estos, de modo que, si algunos nodos se destruyen o dejan de funcionar, otros cubrirían sus roles para volver a reanudar el funcionamiento de la red. Para defenderse contra la colisión y agotamiento se debe limitar el número solicitudes de cada nodo a un valor determinado, de modo que la red detecte solicitudes adicionales del mismo nodo y los descarte [Butun, 2020]. Para los ataques de Denial of sleep, se propone un sistema de detección de intrusos (IDS) basado en anomalías como forma de defensa, la propuesta funciona para redes ad-hoc y, por lo tanto, se adapta bien a IoT y WSN [Butun, 2020]. Algunas soluciones de seguridad para los ataques de Flooding puede ser a través de un IDS basado en la detección de anomalías o por medio de un protocolo de verificación de identidad, obligando a cada nodo a autenticar a cada uno de sus vecinos. Entre las medidas de seguridad contra la clonación existen soluciones centralizadas donde hay a un protocolo basado en “esquemas de distribución previa de claves aleatorias por pares”. También hay soluciones distribuidas donde cada nodo conoce su ubicación y la envía a un conjunto de sensores de vigilancia. Como medidas de

seguridad contra Sybil es necesario verificar las identidades de cada nodo. En la verificación directa un nodo verifica si la identidad de un vecino es válida. En la forma indirecta se proporciona la verificación de la identidad de un nodo a través de otro nodo de confianza [Butun, 2020].

El uso de los dispositivos inteligentes también se debe proteger, ya que son un objetivo para los atacantes. Para utilizar dispositivos IoT de forma segura en un hogar inteligente, las entidades involucradas en una plataforma IoT (dispositivo, aplicación móvil y nube) deben pasar por varios pasos de configuración [Zhou, 2021]. Además, los fabricantes deben asegurarse de que los dispositivos solamente se conecten con servicios aprobados y no se puedan reemplazar por instrucciones dañinas que afecten el funcionamiento del dispositivo [Najmi, 2021]. Algunos autores recomiendan que después de comprar un dispositivo inteligente se cambie la contraseña predeterminada, ya que esta suele ser demasiado simple y todos los dispositivos deben estar protegidos con contraseña [Hind, 2020], [Khanam, 2020]. Existen muchos métodos de autenticación para los dispositivos IoT, como el certificado digital, autenticación de 2 factores, identificación biométrica, verificación del dispositivo o la integración con otras tecnologías como Blockchain. El objetivo es tener un inicio de sesión de usuario confidencial [Baocheng, 2020], [Hind, 2020]. Una buena práctica es realizar las actualizaciones de software/firmware de los dispositivos tan pronto como estén disponibles para mantener la seguridad y la estabilidad. Así mismo, un dispositivo debe poder verificar que cualquier actualización provenga de fuentes legítimas para evitar la introducción de algún malware [Hind, 2020], [Jiang, 2020].

4. Discusión

De los 59 artículos seleccionados, todos responden a la pregunta de investigación correspondiente a la cadena de búsqueda con la que fueron encontrados, sin embargo, la mayoría respondieron a más de una pregunta. 23 respondieron a la pregunta 1, mientras que 34 aportaron información a la pregunta 2; en la pregunta 3, fueron 35 que contribuyeron a su respuesta; 31 fuentes presentaron información para la pregunta 4 y la pregunta 5 fue respondida por 31.

Con respecto a las preguntas de investigación, se encontró información de componentes físicos y lógicos de la infraestructura IoT y características de la tecnología, sin embargo, no se encontró suficiente información acerca de requisitos o recomendaciones que se deben tomar en cuenta para el diseño de una red, como el ancho de banda, área de cobertura y distancia entre nodos. De los protocolos y tecnologías de comunicación recopilados, varios son específicos para IoT, mientras que otros son más generales en las redes de comunicaciones como: Bluetooth, Wi-Fi, IPv4/IPv6 y HTTP. En cuanto a aplicaciones o casos de uso de la tecnología IoT se recopiló suficiente información, sin embargo, no fue así para los servicios de red, ya que solo algunos documentos mencionan en aplicaciones puntuales los servicios de red utilizados, los hallazgos se resumen en servidores web, de bases de datos y de monitoreo. Por otro lado, se pensaba encontrar ataques y desafíos de seguridad que vulneraran específicamente a la tecnología IoT como Denial of Sleep o Sybil, pero también se hallaron ataques que son más generales en la ciberseguridad como Man in The Middle y Flooding. Finalmente, en cuanto a las medidas de seguridad, se hallaron varias recomendaciones para la mitigación de distintos ataques, sin embargo, no se encontró una implementación específica.

5. Conclusiones

El Internet de las Cosas se ha utilizado cada vez más a lo largo de los años, sobre todo en la última década, a partir de la cuarta revolución industrial (Industria 4.0). Esta tecnología tiene el objetivo de facilitar los procesos en distintos ámbitos de uso, creando nuevas capacidades y aumentando la eficiencia para mejorar los resultados. El impacto que ha tenido ha sido positivo, pues la calidad de vida de los usuarios se ha beneficiado debido a la gran cantidad y versatilidad de dispositivos inteligentes que cumplen con funciones específicas para brindar distintos servicios. Esta investigación se realizó siguiendo los pasos de 2 metodologías, la primera fue una revisión sistemática de literatura que se utilizó para obtener la información requerida de acuerdo con los objetivos iniciales, y la segunda fue una síntesis temática para poder organizar y redactar los hallazgos. De acuerdo con los resultados obtenidos, se puede concluir que se logró cumplir con el objetivo de este

trabajo de investigación, el cual es dentificar tecnologías de redes de cómputo, servicios de red y aspectos de ciberseguridad que deben considerarse en IoT. Primero, al reconocer las tecnologías y protocolos utilizados para la comunicación de datos entre dispositivos y sistemas IoT. Después, al identificar las áreas o casos de uso de IoT categorizados en distintos ambientes, así como los servicios de red que se usan en distintas apliaciones. También al distinguir las vulnerabilidades o ataques presentes en la red y dispositivos de la tecnología IoT. Por último, al conocer las recomendaciones o medidas de seguridad que se pueden utilizar al implementar esta tecnología.

Como trabajo futuro se considera la identificación de metodologías para la implementación de IoT, profundizar en algunos temas que requieran más conocimiento técnico. Además, se podría realizar una guía paso a paso para implementar IoT en un entorno específico de manera segura.

6. Bibliografía y Referencias

[1] Adrián, C. (20 de agosto de 2018). IoT: origen, importancia en el presente y perspectiva de futuro. Itop. https://www.itop.es/blog/item/iot-origen-importancia-en-el-presente-y-perspectiva-de-futuro.html.

[2] Aires, F. y Vieira, M. (2021). Security Requirements and Solutions for IoT Gateways: A Comprehensive Study. IEEE Internet of Things Journal, 8(11), 8667-8679. https://doi.org/10.1109/JIOT.2020.3041049.

[3] Alam, I., Sharif, K., Li, F., Latif, Z., Karim, M. Biswas, S., Nour, B. y Wang, Y. (2020). A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV. ACM Computing Surveys, 53(2), 1-40. https://doi.org/10.1145/3379444.

[4] Al-Masri, E., Kalyanam, K., Batts, J., Kim, J., Singh, S., Vo, T. y Yan, C. (2020). Investigating Messaging Protocols for the Internet of Things (IoT). IEEE, 94880-94911. https://doi.org/10.1109/ACCESS.2020.2993363.

[5] Baocheng, W. y Shan, L. (2020). The Research of Security in NB-IoT. Association for Computing Machinery, 275- 279. https://doi.org/10.1145/3443467.3443767.

[6] Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S. Y Kumar, N. (2020). IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. IEEE Access. 8, 168825-168853. https://doi.org/10.1109/ACCESS.2020.3022842.

[7] Ballerini, M., Polonelli, T., Brunelli, D., Magno, M. y Benini, L. (2020). NB-IoT Versus LoRaWAN: An Experimental Evaluation for Industrial Applications. IEEE Transactions on Industrial Informatics, 16(12), 7802-7811. https://doi.org/10.1109/TII.2020.2987423.

[8] Bhuiyan, M. N., Rahman, M. M., Billah, M. M. y Saha, D. (2021). Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities. IEEE Internet of Things Journal, 8(13), 10474-10498. https://doi.org/10.1109/JIOT.2021.3062630.

[9] Butun, I., Österberg, P. y Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644. https://doi.org/10.1109/ COMST.2019.2953364.

[10] Chen, N., Qiu, T., Daneshmand, M. y Oliver Wu, D. (2021). Robust Networking: Dynamic Topology Evolution Learning for Internet of Things. ACM Transactions on Sensor Networks, 17(3), 1–23. https://doi.org/10.1145/3446937.

[11] Cruzes, D. y Dyba, T. (2011). Recommended Steps for Thematic Synthesis in Software Engineering. 2011 International Symposium on Empirical Software Engineering and Measurement, 275-284. https://doi.org/ 10.1109/ESEM.2011.36.

[12] FOSTEC & Company GmbH. (2018). Industria 4.0. https://www.fostec.com /es/competencias/estrategia-de-digitalizacion/industria-4-0/.

[13] Garousi, V., Felderer, M. y Mäntylä, M. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology, 106, 101-121. https://doi.org/10.1016 /j.infsof.2018.09.006.

[14] Gomez, C., Minaburo, A., Toutain, L., Barthel, D. y Zuniga, J. C. (2020) IPv6 over LPWANs: Connecting Low Power Wide Area Networks to the Internet (of Things). IEEE Wireless Communications, 27(1), 206-213. https://doi.org/10.1109/MWC.001.1900215.

[15] Hind, M., Noura, O., Mohammed, K. y Sanae, M. (2020). Internet of Things: Classification of attacks using CTM method. Association for Computing Machinery, 57, 1-5. https://doi.org/10.1145/3386723.3387876.

[16] Janani, RP., Renuka, K., Aruna, A. y Narayanan, L. (2021). IoT in smart cities: A contemporary survey. Global Transitions Proceedings, 2(2), 187-193. https://doi.org/10.1016/j.gltp.2021.08.069.

[17] Javaid, M., Haleem, A., Pratap Singh, R., Rab S. y Suman, R. (2021). Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT). Sensors International, 2. https://doi.org/10.1016/ j.sintl.2021.100129.

[18] Jiang, X., Lora, M., Y Chattopadhyay, S. (2020). An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices. ACM Transactions on Internet Technology, 20(16), 1–24. https://doi.org/10.1145/3379542.

[19] Khanam, S., Ahmedy, I., Idna, M., Hisham, M. y Bin, A. (2020). A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things. IEEE Access, 8, 219709-219743. https://doi.org/10.1109/ACCESS.2020.3037359.

[20] Kitchenham, B., Brereton, P., Budgen, D., Turner, M., Bailey, J. y Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. Information and Software Technology, 51(1), 7-15. https://doi.org/10.1016/j.infsof.2008.09.009.

[21] Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A. y Fartitchou, M. (2020). IoT security: challenges and countermeasures. Procedia Computer Science, 177, 503-508. https://doi.org/10.1016/j.procs.2020.10.069.

[22] Mohamad, M. y Haslina, W. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283-294. https://doi.org/10.1016/j.comnet.2018.11.025.

[23] Muteba, K.F., Djouani, K. y Owal, T. (2022). 5G NB-IoT: Design, Considerations, Solutions and Challenges. Procedia Computer Science, 198, 86-93. https://doi.org/10.1016/j.procs.2021.12.214.

[24] Najmi, K., AlZain, M., Masud, M., Jhanjhi, N.Z., Al-Amir, J. y Baz, M. (2021). A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability. Materials Today: Proceedings, 1-6. https://doi.org/10.1016/j.matpr.2021.03.417.

[25] Oracle Corporation. (10 de octubre de 2021). ¿Qué es IoT?. https://www.oracle.com/mx/internet-of-things/what-is-iot/.

[26] PriceWaterhouseCoopers. (2019). IoT Survey México. https://www.pwc.com/mx/es/prensa/archivo/2019/20191114vf-7-10-empresas-mexicanas-han-implementado-iot.pdf.

[27] Rojas, E., Hosseini, H., Gomez, C., Carrascal, D. y Rodrigues Cotrim, J. (2021). Outperforming RPL with scalable routing based on meaningful MAC addressing. Ad Hoc Networks, 114. https://doi.org/10.1016/j.adhoc.2021.102433.

[28] Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S. y Mustaqim, M. (2020). Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. IEEE Access, 8, 23022-23040. https://doi.org/10.1109/ACCESS.2020.2970118.

[29] Shahraki, A., Taherkordi, A. y Haugen, Ø. (2021). TONTA: Trend-based Online Network Traffic Analysis in ad-hoc IoT networks. Computer Networks, 194, 1-13. https://doi.org/10.1016/j.comnet.2021.108125.

[30] Sidna, J., Amine, B., Abdallah, N. y El Alami, H. (2020). Analysis and evaluation of communication Protocols for IoT Applications. Association for Computing Machinery, 42, 1-6. https://doi.org/10.1145/3419604.3419754.

[31] Song, Y., Yu, F., Zhou, L., Yang, X. y He, Z. (2021). Applications of the Internet of Things (IoT) in Smart Logistics: A Comprehensive Survey. IEEE Internet of Things Journal, 8(6), 4250-4274. https://doi.org/10.1109/JIOT.2020.3034385.

[32] Tariq, N., Aslam, F. y Asim, M. (2021). Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis. Procedia Computer Science, 191, 425-430. https://doi.org/10.1016/j.procs.2021.07.053.

[33] Zaman, S., Alhazmi, K., Aseeri, M., Admed, M., Khan, R., Kaiser, M. y Mahmud, M. (2021). Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. IEEE, 94668-94690. https://doi.org/10.1109/ACCESS.2021.3089681.

[34] Zhou, W., Cao, C., Huo, D., Cheng, K., Zhang, L., Guan, L., Liu, T., Jia, Y., Zheng, Y., Zhang, Y., Sun, L., Wang, Y. y Liu, P. (2021). Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems. IEEE Internet of Things Journal, 8(14), 11621-11639. https://doi.org/10.1109/JIOT.2021.3059457.