Universidad Nacional de Loja

Carrera de Ingeniería en Sistemas / Computación

Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

Carrera de Ingeniería en Sistemas

Exploración de los problemas de seguridad que presenta el IoT en el contexto del Edge Computing

Trabajo de Titulación previo a la obtención del título de Ingeniera en Sistemas.

AUTOR:

Nora Cecivel Solano Chamba

DIRECTOR:

Ing. Hernán Leonardo Torres Carrión, Mg. Sc.

Loja-Ecuador

2022

Certificación

Certificado Nro. 001-CIS-C-FEIRNNR-UNL-HT

Ing. Hernán Leonardo Torres Carrión, Mg. Sc.
DIRECTOR DEL TRABAJO DE TITULACIÓN

Certifico:

Que he dirigido, revisado y corregido en todas sus partes el desarrollo del trabajo de titulación denominado **"EXPLORACIÓN DE LOS PROBLEMAS DE SEGURIDAD QUE PRESENTA EL IoT EN EL CONTEXTO DEL EDGE COMPUTING"** desarrollado por la egresada **Nora Cecivel Solano Chamba** con número de cédula **1105652372**, una vez terminada la misma y luego de que reúne satisfactoriamente los requisitos exigidos, certifico que ha cumplido con el **100% del trabajo de titulación**, considerando pertinente la presentación, sustentación y defensa del trabajo ante el tribunal que se designe para el efecto.

Loja, 24 de septiembre de 2021

Firmado electrónicamente por:
HERNAN LEONARDO
TORRES CARRION

Ing. Hernán Leonardo Torres Carrión, Mg. Sc.
Docente de la Carrera de Ingeniería en Sistemas/Computación

Autoría

Yo, **Nora Cecivel Solano Chamba**, declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido de la misma. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma: Firmado electrónicamente por: NORA CECIVEL SOLANO CHAMBA

Cédula de Identidad: 1105652372

Correo personal: cecitasolano@gmail.com

Correo institucional: ncsolanoc@unl.edu.ec

Celular:0990919156

Carta de autorización del Trabajo de Titulación por parte del autor, para la consulta, reproducción parcial o total, y publicación electrónica del texto completo

Yo, **Nora Cecivel Solano Chamba,** declaro ser autor del Trabajo de Titulación que versa: **Exploración de los problemas de seguridad que presenta el IoT en el contexto del Edge Computing**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional: Los usuarios pueden consultar el contenido de este trabajo en el (RDI), en las redes de información del país y del exterior, con los cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veintisiete días del mes de mayo del dos mil veintidós.

Firma: Firmado electrónicamente por: **NORA CECIVEL SOLANO CHAMBA**

Autor: Nora Cecivel Solano Chamba

Cédula: 1105652372

Dirección: Macará (Calle Av. El ejército)

Correo Electrónico: cecitasolano@gmail.com

Celular: 0990919156

DATOS COMPLEMENTARIOS:

Director del Trabajo de Titulación: Ing. Hernán Leonardo Torres Carrion, Mg. Sc.

Tribunal de Grado: Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

Ing. Cristian Ramiro Narváez Guillen, Mg. Sc.

Ing. Roberth Gustavo Figueroa Diaz, Mg. Sc.

Dedicatoria

Este triunfo se lo dedico a mi madre Lida Chamba quien es mi fuente de inspiración para salir adelante pese a cualquier dificultad, por siempre brindarme su apoyo incondicional y haber confiado en mis capacidades dándome la fortaleza día a día para no darme por vencida, a mi padre José Solano (+) por los valores que me enseño en vida; a mi hermana Adriana por todo su sacrificio y apoyo incondicional para que yo pudiera seguir estudiando, a mis hermanas Verónica y Mariuxi por sus palabras de aliento para que no me rindiera; a mi sobrino Leonardo por su cariño incondicional y compañía. Finalmente, a mis amigos y compañeros por brindarme su ayuda y compartir conmigo sus conocimientos a lo largo de la carrera.

Nora Cecivel Solano Chamba

Agradecimiento

Todos los días doy gracias a Dios en mis oraciones por haberme dado una segunda oportunidad para poder cumplir mis metas, por la sabiduría y fortaleza para poder seguir adelante cuando quería darme por vencida; sin el nada hubiera sido posible.

A toda mi familia, en especial a mi madre, hermanas y hermanos, por su infinito amor, por todos sus consejos y su apoyo incondicional en todos los aspectos de mi vida, especialmente en mi formación académica.

A mi sobrino Leonardo, por pasar sus vacaciones conmigo para que no me sintiera sola, gracias a todos sus consejos que me ayudaron a no darme por vencida y seguir luchando por mi sueño.

A mis amigos, quienes de una u otra manera aportaron a que yo pudiera cumplir mi meta, gracias por sus consejos y apoyo incondicional.

Mi profundo agradecimiento a mi director de tesis, el Ing. Hernán Leonardo Torres Carrión M. Sc, quien con su sabiduría, paciencia, experiencia y conocimiento me ha sabido orientar de la mejor manera para poder culminar con éxito mi trabajo.

Finalmente, mi gratitud a cada uno de los docentes que formaron parte de mi carrera universitaria, gracias por impartirme sus conocimientos durante toda mi formación académica.

Nora Cecivel Solano Chamba

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Índice de Anexos

1. Título

Exploración de los problemas de seguridad que presenta el IoT en el contexto del Edge Computing.

2. Resumen

El rápido crecimiento de los dispositivos del Internet de las cosas y la gran cantidad de datos generados en el perímetro de la red han ocasionado que el modelo tradicional de computación en la nube (Cloud Computing) se convierta en un cuello de botella, debido a las limitaciones de ancho de banda y la alta latencia que se produce entre la interacción de los dispositivos inteligentes y los servidores centralizados. Este problema ha motivado en los últimos años el avance de la computación perimetral (Edge Computing) o computación en la niebla (Fog Computing), la cual brinda capacidades de análisis y procesamiento más cerca de donde se generan los datos; de este modo, ofrece grandes servicios a entornos IoT que requieren de respuesta inmediata o aquellos que tienen una conectividad muy limitada con la nube. Tomando en consideración la cantidad de información que estará expuesta, surge la necesidad de estudiar a profundidad la seguridad en los escenarios que plantean estos nuevos paradigmas, tomando como base la hipótesis de que el Internet en sí, no es seguro; por lo tanto, el Cloud y Edge Computing que hacen uso del mismo, no serán la excepción; por tal motivo, nace la necesidad de realizar una investigación donde se analice si el nuevo paradigma denominado Edge Computing brindara la seguridad suficiente en el tratamiento, almacenamiento y respuesta de los datos.

En consecuencia, el presente trabajo de titulación tuvo propósito, realizar una Revisión Sistemática de Literatura (SLR) que permitió establecer cuáles son los problemas de seguridad que actualmente afectan al IoT en el contexto del Edge Computing, mismo que se lo realizó en base a las tres fases de la metodología de SLR propuesta por Torres-Carrión, la misma que está basada en el protocolo de Kitchenham y Bacca. De los estudios analizados se identificaron 24 problemas de seguridad, los cuales se los identifican como ataques que afectan en su gran mayoría al IoT y también son los más frecuentes en Edge y Fog Computing. Además, como un aporte adicional se identificaron algunas soluciones planteadas por los autores para prevenir ciertos ataques de seguridad; de igual manera, se determinó qué: el conocimiento de la ubicación, la distribución geográfica, la arquitectura descentralizada, el soporte de movilidad, la escalabilidad y el consumo energético reducido, son características que sirven de punto de entrada para que se produzcan ataques de seguridad.

Finalmente, se concluyó que los problemas de seguridad más frecuentes en el IoT como son: ataque DoS, DDoS, hombre en el medio, suplantación de identidad, repetición, colisión, manipulación física, inyección de nodo falso y clonación de dispositivos, también afectan al Edge Computing por su naturaleza mismo, ya que este paradigma nace gracias a la existencia de IoT y se implementa sobre la base del mismo, el cual en sí tiene muchas fallas de seguridad, y la mayoría de estos problemas son a causa de que los fabricantes y desarrolladores se enfocan más en la utilidad que los dispositivos pueden darle al usuario que en la seguridad; También, es importante enfatizar que los mecanismos de seguridad

ampliamente estudiados y utilizados en la computación tradicional no pueden ser implementados directamente en Edge Computing, debido que en su mayoría requieren bastante capacidad computacional, así mismo, debido a la heterogeneidad de los dispositivos que conforman los nodos Edge en los diferentes entornos de aplicación, no es posible diseñar mecanismos de seguridad genéricos para todos los entornos de Edge Computing.

2.1. Abstract

The rapid growth of Internet of Things devices and the large amount of data generated at the network perimeter have caused the traditional Cloud Computing model to become a bottleneck, due to bandwidth limitations and high latency between the interaction of smart devices and centralised servers. This problem has led in recent years to the advancement of Edge Computing or Fog Computing, which provides analysis and processing capabilities closer to where data is generated, thus offering great services to IoT environments that require immediate response or those that have very limited connectivity to the cloud. Taking into consideration the amount of information that will be exposed, the need arises to study in depth the security in the scenarios posed by these new paradigms, based on the hypothesis that the Internet itself is not secure; therefore, the Cloud and Edge Computing that make use of it, will not be the exception; for this reason, the need to conduct a research where the new paradigm called Edge Computing will provide sufficient security in the processing, storage and response of data arises.

Consequently, the purpose of this degree project was to carry out a Systematic Literature Review (SLR) that allowed us to establish the security problems that currently affect the IoT in the context of Edge Computing, based on the three phases of the SLR methodology proposed by Torres-Carrión, which is based on the Kitchenham and Bacca protocol. From the studies analysed, 24 security problems were identified, which are identified as attacks that mostly affect the IoT and are also the most frequent in Edge and Fog Computing. Furthermore, as an additional contribution, some solutions proposed by the authors to prevent certain security attacks were identified; likewise, it was determined that: location awareness, geographic distribution, decentralised architecture, mobility support, scalability and reduced energy consumption are characteristics that serve as entry points for security attacks to occur.

Finally, it was concluded that the most frequent security problems in IoT such as: DoS attack, DDoS, man-in-the-middle, spoofing, replay, collision, physical tampering, fake node injection and device cloning, also affect Edge Computing by its very nature, since this paradigm is born thanks to the existence of IoT and is implemented on the basis of it, which itself has many security flaws, and most of these problems are because manufacturers and developers focus more on the utility that the devices can give to the user than on security; Also, it is important to emphasise that the security mechanisms widely studied and used in traditional computing cannot be directly implemented in Edge Computing, because most of them require a lot of computational capacity, and also, due to the heterogeneity of the devices that make up the Edge nodes in the different application environments, it is not possible to design generic security mechanisms for all Edge Computing environments.

3. Introducción

El Internet de las cosas (IoT) conecta miles de millones de dispositivos heterogéneos para realizar tareas inteligentes, lo que reduce los esfuerzos humanos. Esta tecnología ha alcanzado una multitud de entornos de aplicación, que incluyen: atención médica personal, monitoreo ambiental, automatización del hogar, movilidad inteligente, industria 4.0, entre otros. Por lo tanto, cada vez se implementan más dispositivos IoT en diferentes entornos, convirtiéndolos en objetos comunes en la vida cotidiana[1]. Según Statista [2] indica que, a fines de 2018, había aproximadamente 22 mil millones de dispositivos conectados a IoT en uso y se prevé que para 2030 existan alrededor de 50 mil millones de estos dispositivos IoT en uso en todo el mundo, creando una red masiva de dispositivos interconectados que abarca, desde teléfonos inteligentes hasta electrodomésticos de cocina. De igual manera, según el informe de [3] se espera que la cantidad de datos generados por estos dispositivos IoT interconectados alcance los 73,1 ZB (zettabytes) para el 2025.

La gran cantidad de objetos conectados genera un volumen significativo de datos, lo que hace de la computación en la nube un concepto que juega un papel importante en el acceso ubicuo, disponibilidad, capacidad de almacenamiento, escalabilidad y la gestión de datos; sin embargo, el envío de todos los datos a la nube genera cuellos de botella [4]. Esto afecta de forma directa al tiempo de respuesta de los sistemas de IoT, lo que, en entornos como vehículos inteligentes, monitoreo de salud e industria 4.0 puede provocar problemas críticos [5].

La computación tradicional en la nube, que se utiliza para soportar sistemas informáticos generales, difícilmente puede satisfacer las necesidades de IoT y servicios móviles, debido a razones tales como: desconocimiento de ubicación, escasez de ancho de banda, imposición de costos operativos, falta de servicios en tiempo real y falta de garantía de privacidad de datos. Estas limitaciones han provocado el surgimiento del paradigma de Edge/Fog Computing. La idea básica de este paradigma según [6] es: “utilizar una infraestructura descentralizada y semidistribuida en la que los servidores virtualizados, o nodos perimetrales, se implementan en el perímetro de la red. Estos nodos perimetrales coexisten y cooperan entre sí y con sistemas de nube centralizados”. Permite utilizar los recursos informáticos y de almacenamiento de los equipos de red, como enrutadores y conmutadores ubicados entre objetos conectados y centros de datos en la nube. Tiene el potencial de proporcionar servicios de bajo costo, con suficiente ancho de banda y en tiempo real para respaldar las aplicaciones emergentes de ciudades inteligentes. Sin embargo, las propiedades de la computación perimetral plantean nuevos desafíos de seguridad y privacidad. Por lo tanto, las soluciones existentes para la Cloud Computing no se pueden aplicar directamente a Edge Computing debido a sus propiedades específicas, como movilidad, heterogeneidad, gran escala y distribución geográfica [6] [7][8]. De modo, que a pesar de que los dominios de servicio y

distribución de mercado de IoT están creciendo rápidamente, sus condiciones de seguridad siguen siendo preocupantes.

La seguridad es un desafío importante en la computación de borde, debido a que todo el ecosistema no estará controlado por un solo propietario, aún más, los centros de datos Edge son capaces de proporcionar servicios sin depender continuamente de una infraestructura central. Por lo tanto, todos los niveles, incluida la infraestructura de red, centros de datos perimetrales, infraestructura central, la infraestructura de virtualización y los dispositivos de usuario, no estarán controlados por una sola entidad sino por varios actores (incluidos en algunos casos, usuarios finales) que necesitan cooperar entre sí. Por un lado, el Edge Computing proporciona campos de aplicación muy importantes; y por otro, su surgimiento crea más amenazas de seguridad, ya que aumenta la superficie de ataque; en este sentido, se deben tener en cuenta varios aspectos a la hora de analizar las amenazas a la seguridad como son: poder de cálculo débil, desconocimiento del ataque, sistema operativo, heterogeneidades de protocolo y el control de acceso [6]. Por lo tanto, la seguridad y la privacidad deben abordarse en todas las capas del diseño de los sistemas de computación de borde, infraestructura central, servidores Edge, red Edge y dispositivos Edge [1].

Los dispositivos IoT y de borde generalmente se implementan lejos de una infraestructura de datos centralizada, lo que hace que sea básicamente más difícil de monitorear desde el punto de vista de la seguridad física y digital. Además, los mecanismos de seguridad existentes en la nube tradicional para mitigar ataques IoT como: DoS, Hombre en el medio, Ransonware, inyección de código malicioso, suplantación de identidad, entre otros; no pueden ser implementados en Edge, debido a los recursos limitados que estos poseen [6].

La seguridad en este nuevo paradigma sigue sin estar clara, debido a que existen muy pocas investigaciones dedicadas a su análisis, esto se pudo evidenciar en los estudios analizados para llevar a cabo este trabajo de titulación, en los cuales la mayoría de las investigaciones se enfocan en estudiar el tema de manera general y en resaltar las ventajas que tendría el IoT al ser implementado en el Edge; sin embargo, la seguridad es un tema que no se le ha dado la importancia que requiere; por tal motivo, es necesario analizar si el nuevo paradigma de Edge Computing brindara la seguridad suficiente en el tratamiento, almacenamiento y respuesta de los datos. Para lo cual se han planteado dos preguntas de investigación: ¿Cómo los problemas de seguridad que presenta actualmente el IoT afectan al Edge Computing? y ¿Cuáles son las características del Edge Computing que generan problemas de seguridad en dispositivos IoT? Para dar respuesta a estas preguntas, se consideró importante desarrollar el presente trabajo de titulación, que tiene como objetivo principal realizar una revisión sistemática de literatura que permita establecer cuáles son los problemas de seguridad que actualmente engloba al IoT en el contexto del Edge Computing. Para alcanzar este objetivo principal se definieron tres objetivos específicos.

En el primero objetivo (Planificar la Revisión Sistemática de Literatura) definiendo la pregunta de investigación y el protocolo de revisión): se identificó la necesidad de la revisión, se analizó el estado actual del problema de la investigación se plantearon las preguntas de investigación antes mencionadas, se desarrolló el protocolo de revisión donde se estructuró las cadenas de búsqueda y la definición de los criterios de inclusión y exclusión. Así mismo, en el segundo objetivo (Identificar y analizar los estudios que abordan los problemas de seguridad en IoT en el contexto del Edge Computing): se realizó el proceso de selección, evaluación de calidad y extracción de los estudios primarios, se sintetizó los datos y se dio respuesta a las preguntas de investigación planteadas en el primer objetivo. Finalmente, en el tercer objetivo se presentaron los resultados obtenidos durante todo el TT en formato de un artículo científico.

De acuerdo con los lineamientos establecidos por la Universidad Nacional de Loja el Trabajo de Titulación se encuentra estructurado de la siguiente manera:

La sección Revisión de Literatura, abarca los fundamentos teóricos para el desarrollo y ejecución de los objetivos del TT. En la sección de Materiales y Métodos, se especifica el tipo y método de investigación utilizados para el desarrollo del TT. En la sección Resultados, se presenta los hallazgos obtenidos en la ejecución del TT. En la sección Discusión, se interpreta el significado de los resultados obtenidos por cada objetivo específico y qué mejoras o qué aporte ha dado el presente TT frente a los trabajos relacionados. En la sección de Conclusiones se describe los resultados destacados o sobresalientes obtenidos. Finalmente, en la sección de Recomendaciones se establecen los aportes más importantes, que se consideran para trabajos futuros procedentes del presente TT.

4. Marco Teórico

Esta sección presenta las bases teóricas que sustentan el presente Trabajo de Titulación, dicha información se obtuvo a través de un proceso de revisión bibliográfica.

4.1. Revisión sistemática de literatura.

Una revisión sistemática de literatura o también conocida como SLR (Systematic Literature Review, por sus siglas en inglés),es la identificación, evaluación e interpretación de manera crítica de trabajos de investigación de distintos autores, con el fin de poder dar respuesta a una o más preguntas de investigación definidas de manera clara [9].

Los documentos que se analizan son denominados estudios primarios, mientras que la SLR resultante del análisis es considerado un estudio secundario.

Existen varios motivos por los que se puede realizar una SLR según lo establece [10] las más comunes son:

- Para resumir la evidencia existente sobre un tratamiento o tecnología.
- Identificar las lagunas en la investigación actual para sugerir áreas para una mayor investigación.
- Proporcionar un marco / antecedentes para posicionar adecuadamente las nuevas actividades de investigación.

Este tipo de revisión, resulta de gran importancia para encontrar nuevos hallazgos en un campo específico, y de esta manera poder justificar nuevas investigaciones que pueden plantearse a futuro [9].

4.1.1. Proceso de la SLR

Según[11] el proceso de un SLR está dividido en tres fases principales que son:

4.1.1.1. Planificación de la revisión

En la etapa de planificación se justifica la necesidad de la revisión a través del planteamiento de las preguntas de investigación y el diseño de la cadena de búsqueda para obtener la documentación referente al tema de estudio, mediante la cual se verifica si existen trabajos donde las preguntas formuladas ya hayan sido respondidas, caso contrario se continuará con la investigación.

4.1.1.2. Realización de la revisión

Etapa donde se lleva a cabo el proceso de búsqueda, selección, y evaluación de la calidad de los documentos de estudio referentes al tema en cuestión, además se lleva a cabo la extracción y síntesis de los datos.

4.1.1.3. Informarme de la revisión

Documentación de los resultados obtenidos mediante del proceso de búsqueda, selección y evaluación de los documentos referentes al tema en cuestión, así mismo, la redacción de los resultados obtenidos para dar respuesta a cada una de las preguntas de investigación.

4.2. Parsifal

Herramienta online diseñada para brindar ayuda a investigadores en el desarrollo de revisiones sistemáticas de literatura en el contexto de la Ingeniería de Software, aunque también se puede utilizar en otros contextos. Una de las principales ventajas que brinda esta herramienta es que permite que varios investigadores puedan trabajar juntos dentro de un espacio de trabajo compartido, diseñando el protocolo y realizando la revisión [12].

La herramienta permite realizar tareas de manera fácil dentro de cada una de las fases que se desarrollan en la metodología para la SLR, es decir, en tres fases: Planificación, realización e informe.

4.3. Internet de las cosas (IoT)

4.3.1. Descripción general

El Internet de las Cosas se define como “el conjunto de tecnologías que permiten que objetos cotidianos pueden comunicarse a través de la red con el propósito de recopilar información que nos permita supervisar el estado y comportamiento de dichos objetos”[13].

Los Dispositivos que trabajan dentro de un sistema IoT se caracterizan por ser dispositivos pequeños con recursos limitados como son: sensores, teléfonos inteligentes, dispositivos portátiles, termostatos, refrigeradores y cualquier otro tipo de máquina conectada a una red de Internet [14].

Esta Tecnología está presente cada vez más en la vida cotidiana de más personas y en múltiples sectores realizando tareas inteligentes, reduciendo el esfuerzo humano, a pesar de esto debido a la evolución exponencial de IoT tienden a surgir problemas de seguridad que afectan de forma directa en la utilización de esta tecnología[15].

La integración de IoT con la Cloud Computing aporta muchas ventajas a las diferentes aplicaciones de IoT. Sin embargo, como hay un gran número de dispositivos IoT con plataformas heterogéneas, el desarrollo de nuevas aplicaciones de IoT es una tarea difícil. Esto se debe a que las aplicaciones de IoT generan enormes cantidades de datos procedentes de sensores y otros dispositivos. Estos big data se analizan posteriormente para determinar decisiones sobre diversas acciones. El envío de todos estos datos a la nube requiere un ancho de banda de red excesivamente elevado [16] . Mientras más crece el volumen de estos datos el Cloud ha llegado a saturar la red, presentando problemas como lo menciona [17] [14]: “alta latencia, baja disponibilidad de ancho de banda, interrupciones momentáneas de Internet, problemas de seguridad en el envío de los datos entre otros temas de seguridad”.

4.3.2. Arquitectura IoT

No existe un consenso único sobre una arquitectura universal para IoT. Diferentes estudios muestran diferentes arquitecturas que van desde la arquitectura básica que contiene tres capas hasta una más completa de cinco capas.

La arquitectura básica de tres capas se introdujo en las primeras etapas de la investigación

del IoT [18]. Compuesta por la capa de percepción, capa de red y capa de aplicación, pero no es suficiente, ya que el IoT va evolucionando constantemente y cada vez se necesita ir mejorando las arquitecturas. Por eso, los investigadores mencionan una variedad de arquitecturas en sus estudios, una de estas arquitecturas es la de cinco capas, esta arquitectura incluye dos capas más a la arquitectura básica como es la capa de procesamiento y negocio. Las cinco capas son capa de percepción, transporte, procesamiento, aplicación y capa de negocio. Ver Figura 1.

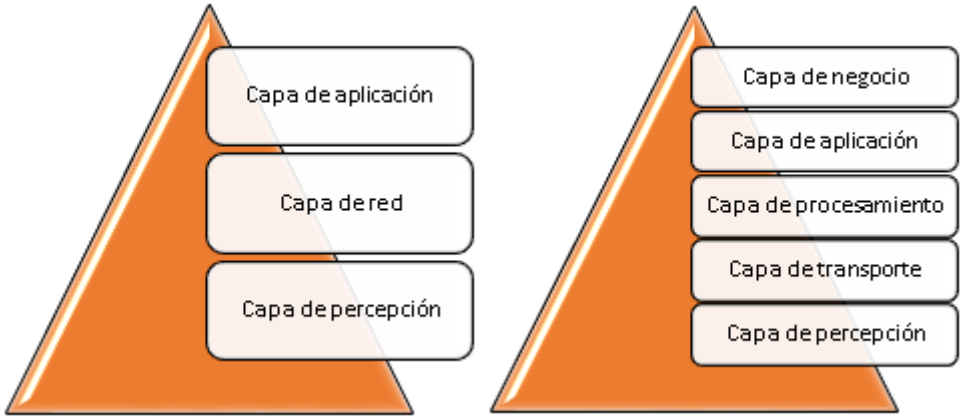

Figura 1. Arquitectura IoT en tres y cinco capas (fuente propia).

Capa de percepción: correspondiente a la capa física donde se encuentran los sensores para detectar y recopilar información sobre el medio ambiente y otros objetos inteligentes en su entorno.

Capa de red: Encargada de conectarse a otros objetos inteligentes, dispositivos de red y servidores, además, sus funciones también permiten transmitir y procesar datos de los sensores.

Capa de aplicación: Encargada de brindar servicios específicos de la aplicación al usuario. Define varias de las aplicaciones donde se puede implantar el IoT, por ejemplo, Ciudades inteligentes, salud inteligente, hogares inteligentes.

En la arquitectura de cinco capas, la capa de percepción y aplicación tienen la misma función que en la arquitectura básica; sin embargo, a continuación, se especifica la función de la capa de transporte, procesamiento y de negocio.

Capa de transporte: Encargado de trasferir los dados producidos por los sensores en la capa de percepción hasta la capa de procesamiento a través de redes inalámbricas wifi, bluetooth, 3g, 5g, Zigbee, etc.

Capa de procesamiento o middleware: Almacena, analiza y procesa grandes cantidades de datos provenientes de la capa de transporte. Puede administrar diversos servicios a las capas inferiores, además, utiliza tecnologías como como bases de datos, módulos de procesamiento de big data.

Capa de negocio: Encargada de gestionar todo el sistema IoT e incluidas las aplicaciones,

los modelos comerciales y de ganancia, así como la respectiva privacidad de los usuarios.

4.3.3. Entornos de aplicación IoT

Esta Tecnología está presente cada vez más en la vida cotidiana de más personas y en múltiples entornos. A pesar de esto debido a la evolución exponencial de IoT tienden a surgir problemas de seguridad que afectan de forma directa en la utilización de esta tecnología [19]. Los entornos de aplicación de IoT se pueden observar en la Figura 2.

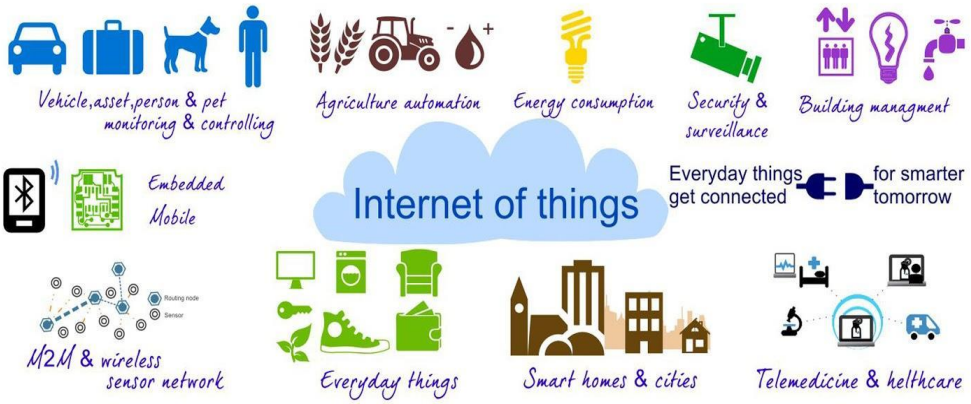

Figura 2. Escenarios de aplicación para IoT [19].

4.4. Edge Computing

4.4.1. Descripción general

La computación de borde o Edge Computing es un modelo de computación que acerca las capacidades de análisis y procesamiento al lugar en el que se generan los datos, este modo, ofrece grandes servicios a entornos IoT que requieren de respuesta inmediata o aquellos que tienen una conectividad muy limitada con la nube o Cloud [13]. Al no tener que enviar los datos a infraestructuras remotas para su evaluación y análisis se reduce la latencia, se mejora el tiempo de respuesta de las aplicaciones y disminuye el volumen de datos enviados a la red; por lo cual, resulta de gran ayuda al trabajar a la par con IoT ya que evita la saturación que se había generado en el Cloud. Al ofrecer servicios de inteligencia de vanguardia, el Edge Computing, cumple con los requisitos clave de la digitalización de la industria para una conectividad ágil, servicios en tiempo real, optimización de datos, inteligencia de aplicaciones, automatización de servicios, seguridad y protección de la privacidad [13][20][6].

4.4.2. Características Edge Computing

Las características representativas de Edge Computing son las siguientes.

- **Baja latencia:** Los nodos Edge facilitan el procesamiento de datos descargado de los servidores centralizados al borde de la red, que está más cerca de los dispositivos finales. La comunicación entre el dispositivo IoT y un nodo Edge puede tardar aproximadamente milisegundos, mientras que la comunicación con la Cloud puede llevar minutos [14].
- **Distribución Geográfica**: Los nodos de niebla se despliegan en ciertas posiciones,

como a lo largo de carreteras, en estaciones base celulares, en el suelo de un museo y en un punto de interés. La razón es garantizar que los nodos de niebla pueden recibir flujo de datos de alta calidad de dispositivos IoT, incluso cuando estos dispositivos pasan entre dos nodos de niebla [21].

- **Descentralización**: La computación de niebla es una arquitectura descentralizada en la que no existe un servidor centralizado para administrar recursos y servicios. Los nodos de niebla se auto organizan para proporcionar de forma cooperativa servicios en tiempo real y aplicaciones de IoT a los usuarios [22].

Además, la computación Edge tiene varias características generales como: soporte de movilidad, reducido consumo de banda ancha, escalabilidad, soporte de aplicaciones a gran escala.

4.4.3. Importancia de Edge Computing

El crecimiento constante de los datos generados por los dispositivos IoT conectados a la red, disminuye cada vez más la velocidad en que estos llegan a la Cloud para su posterior procesamiento, por tanto, este proceso resulta demasiado largo; por tal motivo, se considera que este procesamiento de datos se lo realice en el mismo lugar donde se genera, es decir, en el borde, más cerca del usuario lo que ocasiona tiempos de respuesta más cortos además de una mayor precisión para realizarlo y lo que es muy importante, mejora la seguridad, ya que los datos no tienen que pasar por ninguna red para su tratamiento, garantizando una menor probabilidad de ser vulnerados [23].

4.4.4. Edge Computing ofrece algunas ventajas

Según [20] los flujos de datos procedentes de diferentes fuentes de datos son procesados por los nodos para filtrar información sin valor, esto permite ahorrar ancho de banda y recursos de almacenamiento. Por otra parte, la proximidad y baja latencia, gracias a procesos de información cercanos a su fuente de origen. Además, ofrece almacenamiento y procesamiento descentralizado de los objetos lo que mejora la escalabilidad y por último los nodos de las arquitecturas Edge proporcionan a cada nodo de la red aislamiento y privacidad.

4.4.5. Aplicaciones Edge Computing

La computación Edge tiene muchas aplicaciones prometedoras en varios aspectos. A continuación, se presenta varios casos de aplicaciones emergentes [1].

- **Descarga en la nube**: Con el rápido aumento de los dispositivos terminales (por ejemplo, teléfonos inteligentes, dispositivos portátiles, computadoras portátiles y televisión por Internet), muchas aplicaciones requieren de una baja latencia para tomar decisiones en tiempo real (por ejemplo, automóviles autónomos, realidad virtual y operación remota). En la informática perimetral, las entidades perimetrales suelen tener ciertos recursos informáticos que podrían brindar la oportunidad de descargar algunas o todas las cargas de trabajo mediante el almacenamiento en caché de datos

y operaciones en el perímetro de la nube.

- **Análisis de video:** Con el rápido aumento de los dispositivos IoT, los sistemas de video vigilancia desplegados hoy en día todavía no son capaces de realizar un análisis autónomo de eventos complejos en cámaras masivas. Con la colaboración de la computación de borde, los resultados del análisis de vídeo pueden generarse desde la nube y distribuirse a los servidores de borde locales en un área determinada. Cada usuario puede realizar operaciones con sus solicitudes en estos servidores de borde locales, y sólo necesita informar de los resultados operativos a la nube.
- **Red inteligente:** Con el paradigma de la computación de borde, es posible almacenar y procesar los datos de consumo de energía en los servidores de borde, por ejemplo, las micro redes y los contadores inteligentes, y equilibrar la carga de los centros de datos en la nube.
- **Internet vehicular:** En este paradigma, la red vehicular puede lograr la comunicación bidireccional de manera eficiente mediante el despliegue de servidores de borde en las carreteras, y mientras tanto extender el servicio de la nube al borde de las carreteras mediante la integración de los mecanismos de comunicación y computación. Comparativa entre Edge Computing y Cloud Computing

4.4.6. Arquitectura general Edge Computing

La gestión de las redes de IoT supone un reto debido a la heterogeneidad de sus recursos, creando dificultades en los protocolos de comunicación, los procesos en tiempo real, la gestión de datos, el almacenamiento de big data, la seguridad o la privacidad. En este sentido, las arquitecturas de Edge Computing ofrecen una solución a las infraestructuras IoT porque son capaces de gestionar los datos heterogéneos generados por los dispositivos IoT [24]. La Figura 3 muestra un ejemplo de una arquitectura general de Edge Computing de cuatro capas, Infraestructura central, servidores Edge, red Edge y dispositivos Edge [1].

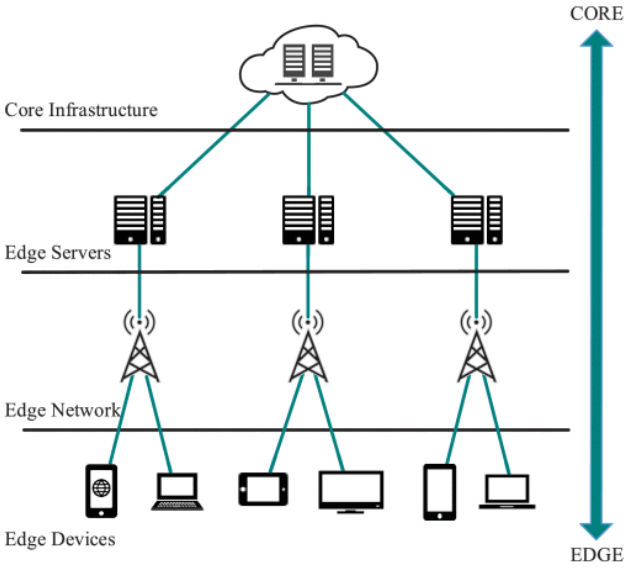

Figura 3. Arquitectura general Edge Computing de cuatro capas [1].

La infraestructura central proporciona acceso a la red central (por ejemplo, Internet, red central móvil), servicios de computación en la nube centralizados y funciones de administración para dispositivos de borde móvil. Los servidores perimetrales, que son propiedad del proveedor de la infraestructura y están implementados por este, están equipados con una infraestructura de virtualización multiusuario, estos son responsables de proporcionar servicios de gestión múltiples y virtualizados. Además, la infraestructura de computación perimetral realiza la conexión entre dispositivos de borde, servidores perimetrales y la infraestructura central con red inalámbrica, red de centro de datos e Internet. Finalmente, los dispositivos de borde incluyen todos los tipos de dispositivos conectados a la red de borde (por ejemplo, terminales móviles, dispositivos IoT).

4.4.7. Arquitectura de Referencia para Edge

4.4.7.1. Multi-access Edge Computing (MEC)

Según la definición de [25] "La informática de borde móvil proporciona un entorno de servicios de TI y capacidades de computación en la nube en el borde de la red móvil, dentro de la red de acceso por radio (RAN) y muy cerca de los suscriptores móviles". Al permitir el tráfico móvil directo entre la red central y el usuario final, MEC conecta al usuario directamente a la red de borde habilitada para servicios en la nube más cercana. La implementación de MEC en la estación base mejora el cálculo y evita cuellos de botella y fallas del sistema [26] [27].

En entornos MEC, la inteligencia, la capacidad de comunicación y la potencia de procesamiento se transfieren a la RAN, por lo que MEC se está volviendo más popular en 4G y en las futuras redes 5G [28]

Varias tecnologías se identifican como tecnologías habilitadoras para la realización de MEC, que incluyen redes definidas por software (SDN), virtualización de funciones de red (NFV), redes centradas en la información (ICN) y segmentación de redes [29].

4.4.7.2. Casos de Uso MEC

MEC es un desarrollo natural en la evolución de las estaciones base móviles y la convergencia de las redes de telecomunicaciones y TI. Edge Computing de múltiples accesos permitirá nuevos segmentos comerciales verticales y servicios para consumidores y clientes empresariales [25]. Los casos de uso incluyen: vehículos conectados, análisis de video, servicios de localización, Internet de las cosas (IoT), realidad aumentada/virtual, distribución de contenido local optimizado, almacenamiento en caché de datos, integración de redes móviles "privadas" en redes empresariales, internet industrial.

4.4.7.3. MEC para IoT

ETSI ha identificado a IoT como uno de los casos de uso clave de MEC [25]. MEC ha abierto muchas fronteras nuevas para que los operadores de red, proveedores de servicios y contenido implementen servicios versátiles e ininterrumpidos en aplicaciones de IoT. IoT expande los servicios MEC a todo tipo de objetos inteligentes que van desde sensores y actuadores hasta vehículos inteligentes. Como se muestra en la Figura 4, los servidores MEC pueden funcionar como nodos de puerta de enlace que pueden agregar y procesar los pequeños paquetes de datos generados por los servicios de IoT antes de que lleguen a la red central [30] [10].

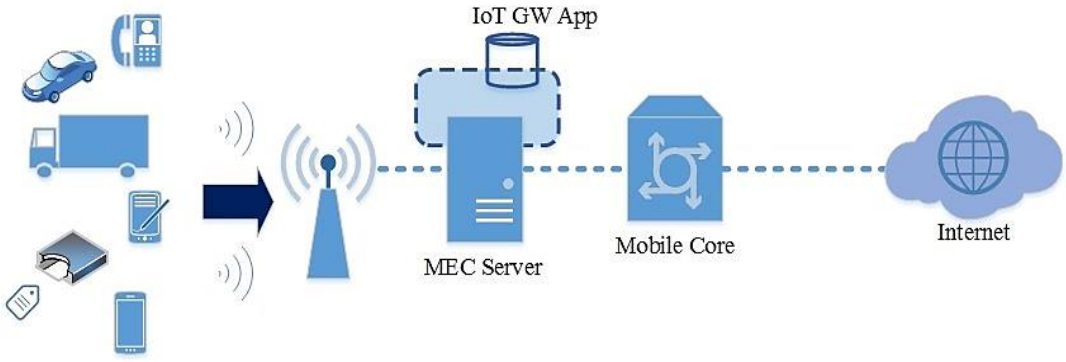

Figura 4. Escenario de servicio de puerta de enlace IoT [29].

4.4.7.4. Arquitecturas de MEC

La arquitectura general de MEC se muestra en la Figura 5. Como se muestra, diferentes tipos de dispositivos móviles y sensores, están conectados a la red central o Internet móvil a través del borde red, es decir, RAN y MEC, y la red central está conectada a la red de nube privada. Con la evolución de la RAN basada en LTE, se ha vuelto más factible implementar MEC, que acerca los servicios en la nube a los suscriptores móviles. Cada plataforma de borde representa una nube de borde con aplicaciones y servicios específicos para el entorno móvil objetivo. MEC constituye servidores geo distribuidos o servidores virtuales con servicios de TI integrados. Estos servidores se implementan localmente en las instalaciones de los usuarios móviles [31].

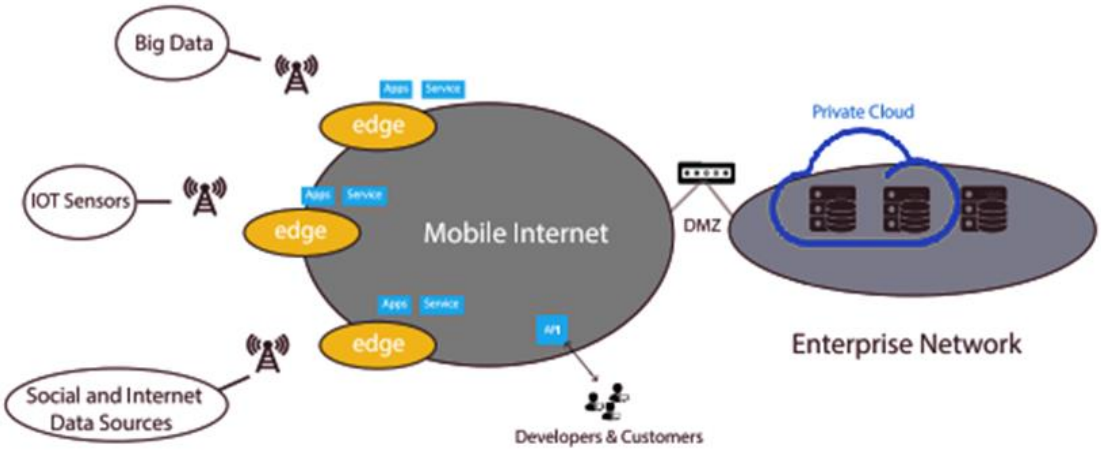

Figura 5. Arquitectura MEC [28].

4.5. Fog Computing

4.5.1. Descripción general

Fog Computing es una arquitectura descentralizada de computación donde los datos se procesan y almacenan entre la fuente de origen y una infraestructura en la Cloud.

Conduce a la minimización de los gastos generales de transmisión de datos y, posteriormente, mejora el rendimiento de la computación en plataformas Cloud típicas al reducir el requisito de procesamiento y almacenar una gran cantidad de datos superfluos.

El paradigma de Fog Computing está altamente motivado por un aumento rápido y continuo en los dispositivos de Internet de las cosas (IoT), donde se genera una cantidad cada vez mayor de datos (con respecto al volumen, la variedad y la velocidad). La computación de niebla también puede tratarse como una solución de impulso para la velocidad de la red, conservación del ancho de banda, direccionamiento de seguridad en cada capa, confiabilidad operativa, computación y análisis de datos de bajo costo [13]. Uno de los beneficios que ofrece la Fog Computing es un diseño más tolerante a fallas, que ayuda a reducir el volumen de información y la complejidad en la arquitectura de la aplicación.

Fog Computing es una extensión de la computación en la nube donde los beneficios de esta deben preservarse en estas extensiones de niebla, la contenerización, la virtualización, la orquestación, la capacidad de administración y la eficiencia [32].

El objetivo de la computación en la niebla IoT es mejorar la eficiencia y el rendimiento y reducir la cantidad de datos transferidos a la nube para su procesamiento, análisis y almacenamiento. Como resultado, los datos recopilados por los sensores se envían a los dispositivos finales para su procesamiento y almacenamiento en caché, en lugar de ir a la nube, lo que reduce el tráfico y la latencia de la red.

4.5.2. Características Fog Computing

Según [16] las características Fog se resumen de la siguiente manera:

- **Conocimiento de la ubicación y baja latencia:** Los nodos Fog pueden desplegarse en diferentes lugares, además, como los nodos se encuentran ubicados cerca de los dispositivos finales proporciona menor latencia al procesar los datos.
- **Distribución geográfica:** los servicios y aplicaciones proporcionados por la niebla están distribuidos y pueden desplegarse en cualquier lugar.
- **Heterogeneidad:** Los nodos de la niebla o los dispositivos finales son diseñados por diferentes fabricantes y, por tanto, vienen en diferentes formas y deben desplegarse en función de sus plataformas.
- **Soporte para la analítica en línea y la interacción con la nube:** La niebla se sitúa entre la nube y los dispositivos finales para desempeñar un papel importante en la absorción y el procesamiento de los datos cerca de dispositivos finales.
- **Escalabilidad:** Permite integrar nodos, dispositivos y servicios según sea la necesidad sin producir fallas en los servicios.

4.5.3. Aplicaciones Fog Computing

Fog Computing demuestra ser un paradigma prometedor para apoyar el IoT. A continuación de describen los 5 dominios más estudiados: Sistemas de Transporte Inteligente (ITS), Smart Healthcare, Sector de seguridad pública, Smart Grids, Industria 4.0 [32][33].

- **Sistemas de inteligencia y transporte:** La seguridad vial y los servicios de conducción autónoma requieren tiempos de respuesta inferiores a 50 ms, lo que generalmente no se puede lograr con CC. Además, ahorra ancho de banda, al evitar que todos los datos recopilados por los vehículos y por la infraestructura fija se envíen a la nube; proporciona servicios críticos de ITS también en presencia de conectividad de red intermitente hacia la nube; y permite que las FN brinden servicios contextuales a los vehículos en su proximidad (por ejemplo, alertándolos de malas condiciones del camino en esa área).
- **Smart Healthcare:** Fog Computing ofrece tiempos de respuesta bajos y predecibles, que a menudo pueden marcar la diferencia entre la vida y la muerte de los pacientes; asegura que al menos la parte más crítica del servicio general esté siempre disponible para el paciente, también en presencia de entornos hostiles con conectividad de red intermitente o nula a la nube; y protege los datos confidenciales relacionados con la salud manteniéndolos localmente.
- **Smart Grids:** En una red inteligente, la energía es generada por varias estaciones ampliamente distribuidas, y los medidores inteligentes y otros nodos sensores se emplean para monitorear y controlar el consumo de energía. muchos servicios de

Smart Grid requieren tiempos de respuesta rápidos y predecibles, generalmente entre tres y 20 ms. Smart Grid basada en Fog donde los medidores inteligentes se agrupan para formar grupos de cómputo y almacenamiento, y así se crea una capa Fog en el extremo de la red.

- **Industria 4.0:** Los dispositivos emiten datos que pasan por un operador, que a su vez los envía a través de Internet a un servidor en la nube y espera la respuesta. Con Fog Computing, el dispositivo contacta directamente con el servidor cloud para agilizar todo el proceso. Esto reduce la latencia, mejora de la ciberseguridad industrial, optimización de gestión de datos, interoperabilidad, reducción de costes de almacenamiento.
- **Hogar inteligente y edificio inteligente:** Los edificios inteligentes pueden contener miles de sensores para medir varios parámetros operativos del edificio, que incluyen temperatura, humedad, ocupación, apertura / cierre de puertas, lectores de tarjetas, ocupación del espacio de estacionamiento, seguridad, ascensores y calidad del aire.

4.5.4. Arquitectura de referencia OpenFog para Fog Computing

El Consorcio OpenFog fue fundado por ARM, Cisco, Dell, Intel, Microsoft y la Universidad de Princeton en noviembre de 2015. La arquitectura de referencia OpenFog ayuda a los líderes empresariales, desarrolladores de software, arquitectura de silicio y diseñadores de sistemas a crear y mantener el hardware y software y lo elementos del sistema que son indispensables para la computación de niebla.

El crecimiento exponencial de datos generados por dispositivos conectados crea problemas de rendimiento, seguridad, ancho de banda, confiabilidad entre otros, problemas que hacen que la computación en la Cloud no sea aplicable para muchos casos de uso, la misma que no puede actualmente mantener la velocidad de los datos proyectada y los requisitos de volumen de IoT, por esta razón el Consorcio OpenFog vio la necesidad de definir una arquitectura que permita abordar los desafíos de infraestructura y conectividad en el borde llamado computación en la niebla [32].

El OpenFog RA permite interfaces niebla-nube y niebla-niebla. Las arquitecturas OpenFog ofrecen varias ventajas únicas sobre otros enfoques, que se denomina SCALE:
Seguridad: Seguridad adicional para garantizar transacciones seguras y confiables
Cognición: Conciencia de los objetivos centrados en el cliente para permitir la autonomía
Agilidad: Innovación rápida y escalado asequible bajo una infraestructura común
Latencia: Procesamiento en tiempo real y control del sistema ciberfísico.
Eficiencia: Agrupación dinámica de recursos locales no utilizados de los dispositivos de usuario final participantes.

OpenFog RA define la infraestructura para la construcción de Fog a as Service (FaaS) que incluye infraestructura como servicio (IaaS), plataforma como servicio (PaaS) Software como servicio (SaaS). El OpenFog RA describe una plataforma genérica deseada para ser aplicada

en muchas áreas que van desde transporte, agricultura, ciudades inteligentes, atención médica, servicio financieros entre otras, generando valor comercial para aplicaciones IoT que requieren tomar decisiones en tiempo real, necesitan baja latencia y están restringidas por la red [32].

4.5.5. Pilares OpenFog RA

OpenFog RA se basa en un conjunto de principios básicos que representan los atributos clave en los que sustenta su propuesta de arquitectura [32].

- **Pilar de Seguridad:** Los atributos principales de este pilar son: la privacidad, anonimato, integridad, autenticación, verificación y la medición.
- **Pilar de Escalabilidad:** Los aspectos que se consideran deben ser escalables, estos son los siguientes: rendimiento, capacidad, usabilidad, seguridad, software y administración,
- **Pilar de apertura:** Los principales puntos de apoyo de este pilar son: modularidad, interoperabilidad, datos abiertos, ubicación de las insistencias.
- **Pilar de autonomía:** Las siguientes funciones deben ser autónomas y por lo tanto debe seguir estando presentes, aunque sus correspondientes en la Cloud ya no lo estén: Descubrimiento de servicios y recursos, orquestación y gestión de los servicios, seguridad, operación.
- **Pilar de programabilidad:** Programación del hardware y el software, virtualización y multicliente, fluidez de aplicaciones.
- **Pilar RAS (Reliability, Availability, Serviceability):** Fiabilidad, disponibilidad y utilidad, este pilar debe estar presente tanto en el hardware como en el software y la red, al cumplir con este pilar se asegura que el sistema seguirá dando servicio ante los eventos adversos que puedan ocurrir.
- **Pilar de Agilidad:** Permite tomar decisiones de negocio de una manera rápida y fiable.
- **Pilar de jerarquía:** Una infraestructura Openfog puede estar formada tan solo un edificio, un campus de varios edificios o una ciudad completa, todo depende de la aplicación en cuestión y del caso de negocio que se quiere resolver. Se espera que la mayor parte de los sistemas sean una mezcla de Fog y Cloud, y muy pocos sean puramente Fog o solo Cloud.

4.6. Proyectos de Edge Computing de código abierto plataformas

Al igual que se han desarrollado sistemas de computación de borde para propósitos específicos, asimismo se han lanzado algunos proyectos de computación de borde de código abierto. En el 2018 la Fundación Linux puso en marcha el proyecto, Akraino Edge Stack centrado en proporcionar servicios de nube de borde mientras que Microsoft público el

proyecto Azure IoT Edge en el 2017 y lo anunció como código abierto en 2018, proyecto enfocado en proporcionar análisis hibrido en el borde de la nube [34].

4.6.1. Akraino Edge Stack

Akraino Edge Stack, iniciado por AT&T e Intel y ahora alojado por Linux Fundation, es un proyecto enfocado en el desarrollo de una solución holística para infraestructura de borde integrada con el fin de admitir servicios de nube de borde de alta disponibilidad [35].

Proyecto de etapa 3 (o etapa de "impacto") bajo el paraguas de LF Edge, Akraino Edge Stack está creando una pila de software de código abierto que admite una pila de nube de alta disponibilidad optimizada para sistemas y aplicaciones de computación de borde.

Ofrece una infraestructura critica para satisfacer las necesidades de la informática de punta, baja latencia, alto rendimiento, alta disponibilidad, escalabilidad, etc.

Akraino “es un conjunto de infraestructuras abiertas y planos de aplicación para Edge, que abarca una amplia variedad de casos de uso, incluidos 5G, AI, Edge IaaS / PaaS, IoT, tanto para dominios de borde de proveedores como de empresas” [36].

Akraino Edge Stack [35] va desde la capa de infraestructura hasta la capa de aplicación dividiéndose en 3 capas como se muestran en la siguiente Figura 6.

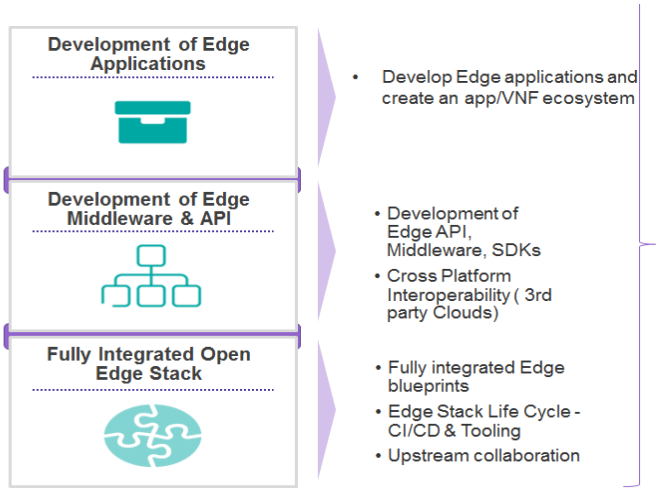

Figura 6. Akraino Edge Stack [35].

En la Figura 6, se detalla la primera capa de aplicación creando un ecosistema de función de red virtual (VNF), la segunda capa consta de un middlware que plantea desarrollar API’S para la intemporalidad de proyectos con terceros, en la capa inferior se desarrolla una pila de software de código abierto maximizado proyectos como Kubernets, Openstack, etc. Se espera que los dominios de aplicación se apliquen en más IoT empresarial e industrial. De los planos presentados por Akraino se muestran los procesamientos de medios de borde y micro-MEC que pretende desarrollar una nueva infraestructura de servicios con una alta capacidad de datos para los ciudadanos que se encuentren haciendo uso de las ciudades inteligentes, a diferencia del procesamiento de medios de borde que a su vez pretende desarrollar una nube

de red permitiendo el procesamiento de medios en tiempo real y con baja latencia en el análisis de IA de medios de borde.

Azure IoT Edge, CORD y Akraino Edge Stack son sistemas de computación perimetral que hacen uso de máquinas virtuales, para permitir a los usuarios gestionar sus aplicaciones agregando o eliminando imágenes de módulos.

Cuando se habla de servicios de borde móvil estos dos sistemas CORD y Akraino Edge Stack, son los idóneos para implementarlos en la infraestructura de telecomunicaciones a través de una red de acceso móvil como 4G y 5G satisfaciendo la necesidad de casos como automóviles no tripulados y drones.

4.6.2. Microsoft Azure IoT

Microsoft Azure IoT es una plataforma informática de borde abierto en la que las empresas pueden crear sus propios servicios en la nube y desarrollar aplicaciones de borde. Además, pueden mejorar la capacidad de procesamiento simultáneo y la capacidad de mantenimiento de datos de sus sistemas mediante el uso de la función de servicio de datos de Azure [37].

4.6.2.1. Azure IoT Edge

Azure IoT Edge, desarrollado por Microsoft Azure como proveedor de servicios en la nube, traslada el análisis de la nube y la lógica empresarial personalizada a los dispositivos periféricos. Los dispositivos de borde pueden ser enrutadores, puertas de enlace u otros dispositivos que cuenten con recursos informáticos. El modelo de programación de Azure IoT Edge, permite al usuario mover ciertas cargas de trabajo al borde de la red de modo que los dispositivos tardan un tiempo mínimo comunicándose con la nube, reaccionan más rápido a los cambios locales y operan de manera confiable incluso en periodos prolongados fuera de línea [38] [35] .

Los servicios de Azure, como las funciones de Azure, Azure ML y el análisis de flujo de Azure, se pueden usar para implementar tareas complejas en los dispositivos de borde como ML, reconocimiento facial y otras tareas sobre la IA. Azure es una plataforma en la nube de terceros con capacidad informática de alto rendimiento, que lleva el entrenamiento de la máquina en el sistema. El modelo de visión artificial para la formación basada en la nube se puede aplicar al reconocimiento facial, la inspección de calidad industrial, la gestión urbana y la seguridad pública, etc. Azure ofrece servicios para implementar estos modelos visuales en dispositivos locales, proporcionando una respuesta de reconocimiento rápida por un lado, y reduciendo el costo del ancho de banda de transmisión de video o imagen por otro lado [37].

Azure IoT Edge se compone de tres componentes: módulos de IoT Edge, tiempo de ejecución de IoT Edge y una interfaz en la nube, como se muestra en la Figura 7, Los dos primeros componentes se ejecutan en dispositivos de borde, el último es una interfaz en la nube [34].

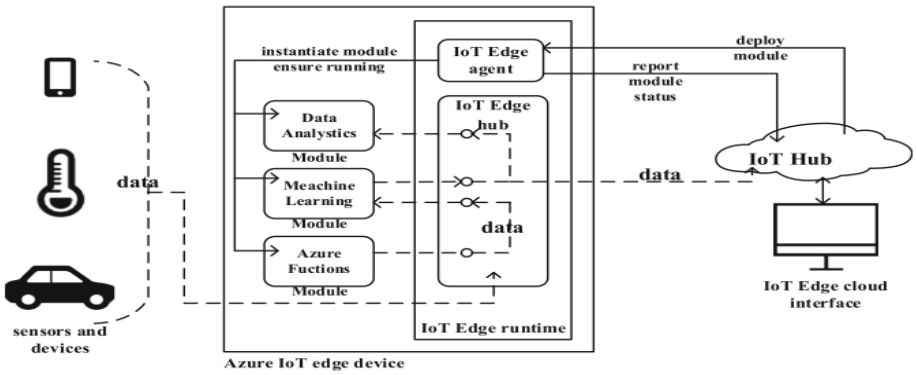

Figura 7. Diagrama Azure IoT Edge [34].

- **Los módulos de IoT Edge:** son contenedores que ejecutan servicios de Azure, servicios de terceros o su propio código. Los módulos se implementan en dispositivos IoT Edge y se ejecutan localmente en esos dispositivos [38] [35].
- **El tiempo de ejecución de IoT Edge:** actúa como un administrador en los dispositivos de borde, lo conforman dos módulos: “IoT Edge hub y IoT Edge agent. IoT Edge Hub actúa como un proxy local para IoT Hub, que es un servicio administrado, y un centro de mensajes central en la nube. Como agente de mensajes, IoT Edge Hub ayuda a los módulos a comunicarse entre sí y transportar datos a IoT Hub. El agente de IoT Edge se usa para implementar y monitorear los módulos de IoT Edge. Recibe la información de implementación sobre los módulos de IoT Hub, crea una instancia de estos módulos y garantiza que se estén ejecutando” [34].
- **Una interfaz basada en la nube:** Le permite al cliente crear aplicaciones de borde, enviar estas aplicaciones al dispositivo y monitorear y administrar de forma remota el estado de ejecución de los dispositivos IoT Edge [38].

Azure IoT Edge tiene amplias áreas de aplicación como son: Fabricación inteligente, sistema de riego, sistema de gestión de drones, etc. Vale la pena señalar que Azure IoT Edge es de código abierto, pero los servicios de Azure, como las funciones de Azure, Azure Machine Learning y el flujo de Azure, se cobran [35].

5. Metodología

5.1. Tipos de investigación

Durante la ejecución del presente TT se empleó el tipo de investigación exploratoria, con el propósito de conocer cuáles son los problemas que aquejan al IoT actualmente, como se están mitigando y como se está integrando esta tecnología al nuevo paradigma Edge Computing; fue necesario realizar esta investigación para obtener las bases necesarias para continuar con el desarrollo del TT. Según [39], este tipo de investigación busca incrementar el conocimiento sobre un tema muy poco explorado y sobre el cual, es difícil formular hipótesis precisas, como es el caso de Edge Computing.

Asimismo, se utilizó la investigación descriptiva y explicativa para describir el problema, las causas y los efectos del mismo, esto permitió responder las preguntas de investigación; ¿Cómo los problemas de seguridad que presenta actualmente el IoT afectan al Edge Computing?, ¿Cuáles son las características del Edge Computing que generan problemas de seguridad en dispositivos IoT?; la respuesta descriptiva y explicativa de cada una de las preguntas planteadas se encuentra en el apartado de resultados en el objetivo 2.

5.2. Métodos de investigación

5.2.1. Método de revisión sistemática de literatura

Se utilizó el método para la revisión sistemática de literatura aplicada a ingeniería y educación planteada por Torres-Carrión [11], basada en el protocolo de revisión sistemática de Kitchenham [40].

Este método permitió identificar, seleccionar y evaluar críticamente las investigaciones relevantes para luego analizar la información obtenida. Esta metodología consta de tres etapas principales, que se describen a continuación en la Tabla 1.

Tabla 1. Fases para la SLR

1. Panificación de la revisión.	**2. Realización de la revisión**	**3.Informe de la revisión**
1.1 Identificación de la necesidad de revisión. 1.1.1 Estado actual del problema de Investigación. 1.1.2 Preguntas de investigación. 1.1.3. "Mentefacto conceptual" 1.1.4. Revisiones sistemáticas relacionadas. 1.2. Desarrollo de un protocolo de revisión. 1.2.1. Definición de criterios de inclusión y exclusión. 1.2.2. Preparación de un formulario de extracción de datos. 1.2.3. Selección de revistas o bases de datos.	2.1. Identificación de la investigación. 2.2. Selección de estudios primarios. 2.3. Evaluación de la calidad del estudio. 2.4. Extracción y seguimiento de datos. 2.5. Síntesis y monitoreo de datos.	3.1. Redactar informe de la revisión.

.

6. Resultados

En la presente sección se describe el resultado de cada uno de los objetivos específicos desarrollados para dar cumplimiento al presente Trabajo de Titulación (TT).

6.1. Objetivo 1: Planificar la Revisión Sistemática de Literatura (SLR) definiendo la pregunta de investigación y el protocolo de revisión.

6.1.1. Planificación

La planificación, es uno de los procesos fundamentales de una SLR, esta se divide en dos fases, para el cumplimiento eficaz del mismo: Identificación de la necesidad de la revisión y el desarrollo de un protocolo de revisión.

Estas fases, contienen a su vez diferentes apartados, que buscan realizar un filtrado a fondo de la información, con respecto a las premisas para completar cada fase, en función del tema a buscar.

En la siguiente sección se detalla cada una de las etapas que conforma la planificación de la SLR, y cómo estas fueron cumplidas, en relación a la exploración de los problemas de seguridad que presenta el IoT en el contexto del Edge Computing.

6.1.1.1. Identificación de la necesidad de la SLR

El propósito de esta SLR surge de la necesidad de conocer el estado actual de la seguridad del IoT con respecto a su integración con el nuevo paradigma Edge Computing, específicamente interesa conocer cuáles son los problemas de seguridad que ambos comparten. Cabe recalcar que a pesar de que Edge Computing es un paradigma que fue introducido por Cisco Company en 2014, no cuenta con los estudios necesarios que aborden de forma precisa la seguridad respecto a su integración con el IoT. A causa de esto, es importante analizar el estado actual de los problemas de seguridad que afectan al IoT bajo el contexto del Edge Computing y también es necesario conocer ciertas características que posee el Edge Computing que causan problemas de seguridad en dispositivos IoT.

6.1.1.2. Estado actual del problema de Investigación

El uso de dispositivos IoT, está presente en cada elemento que nos rodea, 8.9 billones aproximadamente de dispositivos IoT están conectados a la red según la información emitida por [41]. Ambientes como la salud, seguridad, transporte e industria 4.0 son campos que están interesados en actualizar y automatizar sus procesos; esto también, ha traído preocupaciones debido a que el IoT está presentando algunos problemas de velocidad, seguridad, tiempo de respuesta y consumo de ancho de banda; ante estas premisas, este campo de investigación ha ido creciendo, principalmente con la intención de analizar la factibilidad y seguridad de implementar el IoT en el Edge Computing, como la posible solución a los problemas, principalmente de: tratamiento, almacenamiento y respuesta de dicha información.

6.1.1.2.1. Objetivos de la SLR

Para realizar una buena SLR, se plantean primeramente objetivos claros que permitirán iniciar con el proceso de investigación y plantear el problema de forma clara, precisa y accesible.
Los objetivos que se plantearon, se describen a continuación:

- Identificar qué problemas de seguridad afectan actualmente al IoT
- Identificar que problemas de seguridad afectan al Edge Computing.
- Determinar que problemas de seguridad engloban tanto al IoT como al Edge Computing.
- Establecer cuáles son las características del Edge Computing que ponen en riesgo la seguridad de los dispositivos IoT.

6.1.1.2.2. Justificación del estudio: ¿por qué? ¿y para qué? del estudio.

El Internet de las cosas (IoT) es una tecnología emergente de interés técnico, social y económico. Su uso abarca distintos escenarios de aplicación que van desde: hogares inteligentes, vehículos automatizados, monitoreo y control de salud hasta su creciente implementación en la industria 4.0, entre otros. Hoy en día, los datos son considerados como la nueva materia prima de la economía, por lo que también ha despertado el interés de los hackers maliciosos en buscar nuevas formas de robar información, identificando la mínima vulnerabilidad en la seguridad tanto de la red como de los dispositivos que se encuentran conectados en los diferentes ambientes, evidenciando de tal forma que el IoT tiene algunos problemas de seguridad ya identificados; por tal motivo, es una preocupación global mantener segura toda esta información.
Debido a todo lo antes mencionado, nace el nuevo paradigma Edge Computing, siendo considerado como una alternativa para complementar al Cloud Computing, proporcionando una solución flexible a la necesidad de recopilación y análisis de datos en tiempo real. Este nuevo paradigma ha logrado despuntar principalmente en: la industria 4.0, vehículos autónomos, automatización del hogar y atención médica personal, siendo el auge tecnológico más exitoso de hoy en día, que no va en contra de la Cloud; si no, que nació para complementarla y lograr que las operaciones sean más eficientes y ágiles, dos cualidades que busca toda organización. Además, los temas de seguridad en este ámbito son muy importantes, sobre todo cuando se trata de proteger la información generada por todos los dispositivos IoT. Es por esto, la importancia de realizar un estudio exhaustivo a través de la SLR, para analizar los problemas de seguridad presentes en la aplicación de IoT basado en Edge Computing; además, de conocer los avances que se han realizado hasta ahora y lo que aún falta por trabajar en este campo.
El resultado de este estudio, será una base de conocimiento que servirá de ayuda para investigadores, docentes y estudiantes, que deseen explorar más a fondo el tema e

implementar una plataforma segura basada en el Edge Computing, incluso servirá para proporcionar nuevas soluciones, que permitan mitigar los problemas de seguridad que sean identificados.

6.1.1.3. Viabilidad del estudio

6.1.1.3.1. Disponibilidad de recursos

La realización y desarrollo de la revisión sistemática de literatura, es totalmente viable ya que se cuenta con el acceso a bases de datos científicas, como: Web of Science (WoS), Scopus, IEEE Digital Library y Google Scholar, las cuales, permitirán obtener documentación de calidad para el respectivo análisis.

6.1.1.3.2. Alcance del estudio

En la presente SLR, se realizará el análisis de los problemas de seguridad que afectan hoy en día el IoT y Edge Computing; además, se identificará aquellos problemas que engloban a los dos campos. Así mismo, se determinará cuáles son las características de Edge Computing que generan problemas de seguridad en los dispositivos IoT.

6.1.1.3.3. Implicaciones y consecuencias del estudio

La información que se recopile de dicha investigación será una base fundamental para los investigadores interesados en proponer nuevos mecanismos de seguridad, que ayuden a solucionar los problemas que se identifiquen, además, el estudio será una base de conocimiento importante, que permitirá establecer si es conveniente o no implementar IoT en la Edge Computing, y tener una idea de cómo afectaría de forma positiva o negativa, tanto el IoT a Edge Computing y viceversa.

6.1.1.4. Deficiencias en el conocimiento del problema

6.1.1.4.1. Estado del conocimiento

A pesar de que Edge Computing, fue introducido por Cisco Company en el año 2014, es un tema emergente que aún no ha sido estudiado a fondo, especialmente, en cuestiones de seguridad, motivo por el cual, no existe mucha documentación al respecto, específicamente, trabajos primarios que analicen la seguridad del IoT basado en el Edge Computing y los desafíos de seguridad que trae consigo este nuevo paradigma.

6.1.1.4.2. Nuevas perspectivas para estudiar

El Internet de las cosas es un campo en constante crecimiento, que ha permitido aumentar los dispositivos conectados y de esa manera generar una gran cantidad de datos, los cuales hoy en día están almacenándose en la Cloud para de ahí, ser procesados y enviados a los lugares donde se generan dichos datos. Para poder alivianar la carga de procesamiento en la Cloud se crea este nuevo paradigma denominado Edge Computing el cual tiene como objetivo principal, reducir latencia y disminuir el consumo de ancho de banda; sin dejar de lado la seguridad de los datos que generan los usuarios. Estudiar la seguridad en este nuevo

paradigma, brinda muchas posibilidades de establecer soluciones a problemas, que permitan incrementar el grado de confianza en los usuarios que utilizaran plataformas basadas en Edge Computing.

6.1.2. Preguntas de investigación

Con la finalidad de examinar la seguridad en los escenarios de IoT y Edge/Fog Computing, se plantaron las siguientes preguntas de investigación, que son la base sobre la cual, se guía el desarrollo de dicho estudio, véase Tabla 2.

Tabla 2. Preguntas de Investigación

IDENTIFICADOR	PREGUNTA
RQ1	¿Cómo los problemas de seguridad que presenta actualmente el IoT afectan al Edge Computing?
RQ2	¿Cuáles son las características del Edge Computing que generan problemas de seguridad en dispositivos IoT?

6.1.3. Mentefacto conceptual

El mentefacto conceptual es un ideograma o boceto gráfico que asume una idea compleja y la conceptualiza, en él se plasman las ideas fundamentales y se desechan las secundarias. Esta acción requiere responder cuatro preguntas: ¿qué lo caracteriza, en esencia? ¿En qué grupo de cosas lo incluye? ¿Cuáles son tus diferencias con objetos similares? y, ¿hay subtipos tuyos? A partir de estas preguntas, se ensambla el andamiaje de los conceptos, resultando cuatro grupos de pensamientos: 1) isoordinado, 2) supraordinado, 3) excluido e 4) infraordinado. Los isoordinados muestran esencialidades; los supraordinados, el grupo que incluye el concepto; los excluidos, señalan las nociones más cercanas al concepto; y, los infraordinados, especifican las clases y subtipos del concepto, según lo indica [11].

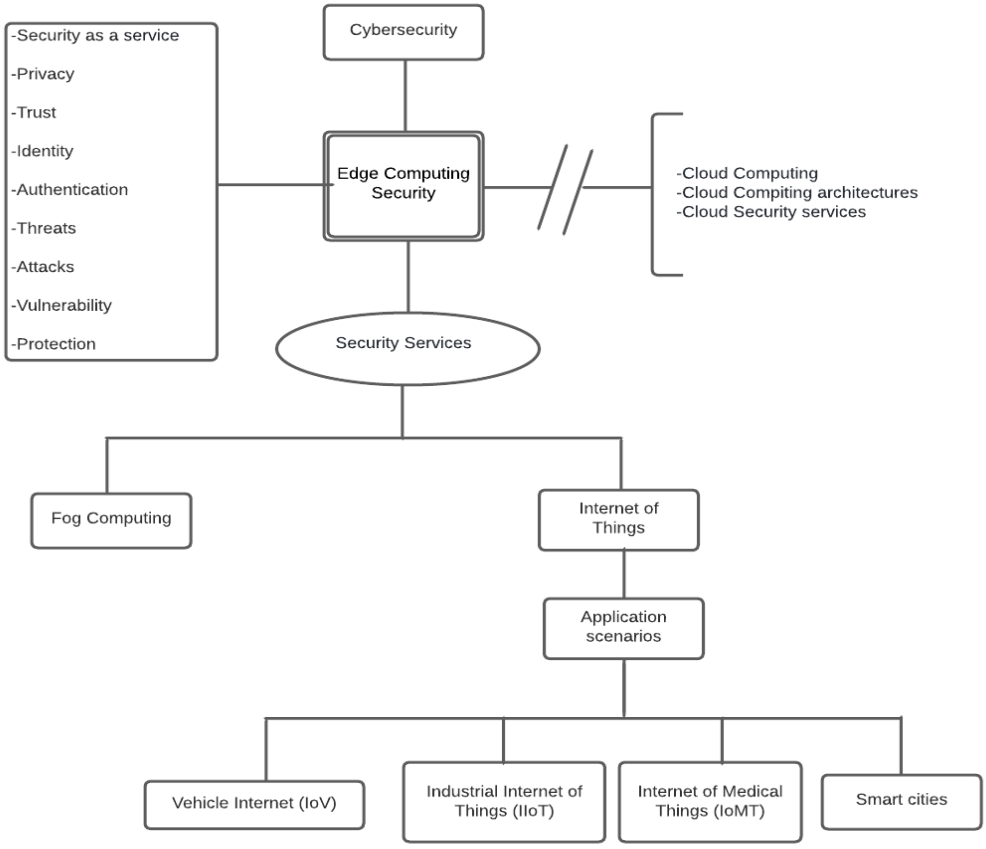

Figura 8. Mentefacto Conceptual “Security Edge Computing” (Fuente propia)

En la Figura 8, se muestra el mentefacto conceptual desarrollado para esta SLR.

A continuación, explica de manera detallada el mentefacto conceptual elaborado para la SLR. La “Edge Computing Security” es una subclase de la “Cybersecurity”. Además, es diferente de la tecnología de “Cloud Computing”, “Cloud Computing Architectures” y “Cloud Security Services”; sin embargo, puede en algún momento establecer una relación, pero no es constante. La “Edge Computing Security, se caracteriza o tiende a ofrecer la “Security as a Service”, “Privacy”, “Trust”,” Identity”, “Authentication” y “Protection” de los datos; además, analiza las “Threats”, “Attacks”, “Vilnerability” tanto en la arquitectura de la niebla como de los usuarios finales. Finalmente, a nivel de “Security Services” debemos pensar en proteger tanto “Fog Computing” como el “Internet of Things” y sus diferentes “Application Scenarios” como son: “Vehicle Internet (IoV)”, “Industrial Internet of Things (IIoT”), “Internet of Medical Things (IoMT)”, “Smart cities”. Cabe recalcar que la construcción del mentefacto conceptual proporcionó los elementos necesarios para aplicar en los criterios PICOC [42] que sirvió para estructurar de mejor manera las cadenas de búsqueda. Se tomó en cuenta el lado izquierdo correspondiente a la Isoordinación y la parte inferior Infraordinación para las palabras de búsqueda (Keywords) para la SLR, los datos que se encuentran en la parte superior

denominada Supraordinación y la parte derecha Exclusión sirvieron para detallar los criterios de inclusión y exclusión para la SLR.

6.1.4. Revisiones sistemáticas relacionadas

Como primer paso antes de iniciar el desarrollo del estudio, se constató que no existan trabajos realizados, donde den respuesta total a las preguntas de investigación planteadas, para asegurar que dicha investigación, sea original y brinde una contribución útil a la comunidad científica. En este caso, se realizó una búsqueda general de SLR relacionadas, tratando de aplicar una sintaxis de búsqueda lo más similar posible en las 4 bases de datos: WoS, Scopus, IeeeXplore, Google Scholar, además, el filtrado se ha orientado a "Review" o Survey". La cadena de búsqueda general utilizada para hacer la primera revisión se muestra a continuación:

(''Survey'' OR ''Review'') AND (''IoT'' OR ''Internet of Things'') AND (''Edge Computing'' OR ''Edge'' OR ''Fog Computing'' OR ''Fog'') AND (''security'') AND (''privacy'') AND (''security problems'' OR ''securityissues'' OR ''threats'' OR ''attacks'' OR ''vulnerability'')NOT (''cloud'')

De dicha búsqueda, se obtuvieron 5 estudios que tienen relación con la temática de interés, estos resultados arrojaron, que no existen investigaciones publicadas específicamente que den respuesta total a las preguntas de investigación, pero sí se encontró documentación con información relevante sobre la temática, la cual sirvió, de base para iniciar el desarrollo del estudio. A continuación, en la Tabla 3 se muestra una breve descripción.

Tabla 3. SLR Relacionadas

N°	Titulo	Descripción
1	**A survey on security and privacy issues in Edge Computing-assisted Internet of Things** **Estudio sobre los problemas de seguridad y privacidad en la Internet de las cosas asistida por Edge Computing**	El estudio [22] presenta una encuesta exhaustiva sobre algunas cuestiones de seguridad y privacidad en el contexto del IoT asistido por EC, describe algunos de los posibles ataques en las diferentes capas y niveles como son: dispositivos EC, comunicaciones y servidores/nodos EC y servidores en la nube de redes IoT asistidas por EC, en el cual determina que los ataques de inyección maliciosa de hardware/software, ataques de interferencia, ataques de denegación de servicio distribuidos (DDoS), ataques físicos o manipulación, ataque de repetición o ataques de frescura, son algunos de las amenazas más comunes a la seguridad en estos paradigmas, Además, proporciona un análisis de los mecanismos de seguridad y privacidad y las contramedidas correspondientes en las diferentes capas de la red de IoT, algunas de las principales contramedidas utilizadas para contrarrestar los ataques y

		amenazas son: Contramedidas para hardware/software malicioso, mecanismos basados en políticas de inyección, sistema de detección de intrusiones (IDS), esquemas criptográficos, autorización, combinación de tecnologías EC y Blockchain.
2	**A survey on the Edge Computing for the Internet of Things** **Un estudio sobre el Edge Computing para el Internet de los objetos**	En [43] se habla sobre la mejora que proporciona la Edge Computing en el rendimiento de las redes IoT, la latencia de la red, la ocupación del ancho de banda, consumo de energía y gastos generales, además, realizan el análisis de la seguridad y privacidad de la EC, determinando que son las dos cuestiones más críticas eh importantes que se deben tener en cuenta al momento de adoptar el IoT basado en EC. Consideran también que a pesar de los grandes beneficios que brindara el EC al IoT también plantar nuevos e imprevistos problemas de seguridad. Para finalizar consideran que los escenarios no estudiados como la interacción de nodos de borde heterogéneos y la migración de servicios a escalas globales y locales, crean el potencial para canales originales de comportamiento malicioso.
3	**A Survey: Integration of IoT and Fog Computing** **Un estudio: Integración de IoT y Fog Computing**	El siguiente estudio [44] presenta un análisis de IoT y FC, evidenciando el beneficio de la combinación de ambas tecnologías. Los autores en esta investigación mencionan 5 ataques a la seguridad que pueden ser provocados por un usuario malicioso: Manipulación, escucha, denegación de servicio, Colisión y Hombre en el medio. Para mitigar dichos ataques el IoT y FC tiene algunos desafíos de seguridad como: Autenticación, verificación de la ubicación y control de acceso, desafíos de seguridad que según los autores consideran son la solución para los problemas antes mencionados.
4	**Security challenges in Fog and IoT, Blockchain technology and cell tree solutions: a review.** **Retos de seguridad en Fog e IoT, tecnología Blockchain y soluciones de árboles celulares: una revisión**	En este trabajo de investigación[45], se analiza el panorama general de la seguridad de la Fog Computing. Se describen problemas de autenticación en IoT, se enfocan en Blockchain como una de las soluciones para la autenticación en IoT, por otro lado, está determinado que Blockchain es uno mecanismo de seguridad que se ha adoptado mucho en los sistemas médicos para la lucha contra el COVID-19. Los autores proponen Cell Tree una arquitectura para sistemas de almacenamiento como una solución a algunos de los problemas de seguridad presentes en IoT.
5	**A Systematic Survey on Fog steered IoT:**	En este documento [46] se presenta una revisión enfocada en las arquitecturas de FC y en las amenazas omnipresentes en

	Architecture, Prevalent Threats and Trust Models **Un estudio sistemático sobre el IoT dirigido por la niebla: Arquitectura, Amenazas Prevalentes y Modelos de Confianza**	Fog-IoT, la mayoría de los estudios revisados para llevar a cabo esta revisión son conceptuales debido a que la FC está en sus primeras etapas de infancia, lo cual deja claro que los problemas de seguridad son un tema importante que se debe abordar. La aparición de la capa de FC aumenta exponencialmente las posibilidades de ataques por ejemplo MITM; Sybil, etc. Son problemas de seguridad que inciden directamente en la red establecida por la niebla.

6.1.5. Desarrollo de un protocolo de revisión

6.1.5.1. Estrategias de búsqueda

El protocolo a implementar es el recomendado por Petticrew y Roberts [42], a través del uso de PICOC (Población, Intervención, Comparación, Resultado y Contexto), se estructuran los cinco componentes para construir la cadena de búsqueda, además, se utilizó la ayuda de la herramienta en línea Parsifal para organizar y seleccionar de mejor manera la documentación. A continuación, se describe los elementos PICOC que se identificaron para la SLR.

Población: Vehicle Internet (IoV), Industrial Internet of Things (IIoT), Internet of Medical Things (IoMT), Smart Cities.

Intervención: Internet of Things (IoT), Edge Computing, Fog Computing.

Comparación: No aplica.

Resultados: Threats, Attacks, Vulnerability, Issues

Contexto: Security information.

6.1.5.2. Selección de Base de datos

Para la búsqueda y obtención de la documentación se ha seleccionado las bases de datos científicas más relevantes. Se trabaja con la Web of Science (Wos) y Scopus por ser bases de datos que abarcan una gran cantidad de revistas de calidad en las diferentes áreas de la ciencia; además, tienen un criterio de selección riguroso para aprobar las publicaciones que van a formar parte de ello, esto según el estudio realizado por [47]. La IEEE Digital Library se utilizó por ser una base de datos de investigación académica, que proporciona el acceso a un gran número de artículos y trabajos sobre Ciencias de la computación e Ingeniería Eléctrica y Electrónica. Por último, se seleccionó Google Scholar el cual, según [48] es uno de los mejores indexadores de literatura científica y académica, pero se debe tener en cuenta que también permite sitios web que no realizan control riguroso de calidad en sus publicaciones, concluye que es válido su uso como fuente bibliográfica primaria; además, porque sirve para evitar el sesgo en la investigación. En la Tabla 4, se muestra las bases de datos académicas utilizadas en esta SLR, según el orden de relevancia y su dirección Web correspondiente.

Tabla 4. Bases de datos científicas

BASE DE DATOS	DIRECCIÓN WEB
Web of Science	https://www.recursoscientificos.fecyt.es/
Scopus	http://www.scopus.com
IEEE Digital Library	http://ieeexplore.ieee.org
Google Scholar	https://scholar.google.com/

6.1.5.3. Estructura semántica de búsqueda

Para formular las cadenas de búsqueda, primero se estableció de manera clara y precisa las palabras clave, aplicando algunos de los criterios semánticos del mentefacto conceptual y el PICOC, para luego establecer la relación entre ellos a través de los operadores booleanos AND, OR y NOT.

6.1.5.4. Definir palabras clave para el problema de estudio

Con la elaboración del mentefacto conceptual y la definición de los criterios PICOC se obtuvo un conjunto de palabras claves, las mismas que permitieron construir las cadenas de búsquedas, estas son: Internet de las cosas, computación de niebla, computación de borde, niebla, borde, seguridad, problemas, amenazas, ataques, vulnerabilidades. Además, su traducción al inglés: Internet of things, fog computing, edge computing, fog, edge, security, problems, issues, threats, attacks, vulnerabilities.

6.1.5.5. Cadenas de búsqueda

Para crear la cadena de búsqueda genérica se utilizó los términos definidos en las preguntas de investigación y las palabras utilizadas en el método PICOC. La cadena genérica se muestra a continuación.

"Edge Computing" OR "Fog computing" OR "Edge" OR "Fog" AND "Internet of Things" OR "IoT" AND "security" OR "security problems" OR "security issues" OR "threats" OR "attacks" OR "vulnerability"

Para evitar el sesgo en la búsqueda se trató de utilizar la sintaxis lo más similar posible en las cuatro bases de datos: WoS, Scopus, IEEE Digital Library y Google Scholar. En la Tabla 5 se muestra las cadenas de búsqueda con la estructura aplicadas a cada base de datos.

Tabla 5. Cadenas de búsqueda de acuerdo a cada base de datos

Base de datos	Cadena de búsqueda
WoS	(TI = ("Edge Computing" OR "Fog Computing" OR "Edge" OR "Fog") AND TI = ("Internet of Things" OR "IoT") AND TS = ("security" OR "security problems" OR "security issues" OR "threats" OR "attacks" OR "vulnerability"))
Scopus	TITLE ("Edge Computing" OR "Fog computing" OR "Edge" OR "Fog") AND TITLE ("Internet of Things" OR "IoT") AND TITLE-ABS-KEY ("security" OR "security problems" OR "security issues" OR "threats" OR "attacks" OR "vulnerability")
IEEE Digital Library	("Document Title":"Edge Computing" OR "Document Title":"Fog computing" OR "Document Title":"Edge" OR "Document Title":"Fog") AND ("Document Title":"Internet of things" OR "IoT") AND ("Abstract": "security" OR "Abstract":"security problems" OR "Abstract":"security issues" OR "Abstract":"threats" OR "Abstract":"attacks" OR "Abstract": "vulnerability*")
Google Scholar	allintitle: ("Edge Computing" OR "Fog computing" OR Edge OR Fog AND "Internet of things" OR "IoT" AND security) AND "security problems" OR "security issues" OR threats OR attacks OR vulnerability

6.1.5.6. Definición de criterios de inclusión y exclusión

6.1.5.6.1. Criterios de inclusión

La definición de los criterios de inclusión permitió seleccionar la documentación secundaria para dar respuesta a las preguntas de investigación planteadas. A continuación, en la Tabla 6, se menciona los ocho criterios de inclusión tomados en cuenta.

Tabla 6. Criterios de inclusión

ID	Criterios de inclusión
CI_1	Los artículos deben estar escritos en inglés.
CI_2	Los artículos deben estar publicados desde el 2016 al 2020.
CI_3	Los artículos deben contener problemas de seguridad en Edge Computing o Fog Computing.
CI_4	Los artículos deben contener problemas de seguridad en IoT.
CI_5	Los artículos deben estar enfocados en el área de las ciencias de la computación.

CI_6	Se tomará en cuenta artículos que propongan soluciones para resolver los problemas de seguridad en IoT o Edge Computing.
CI_7	Los artículos cuyo título y resumen contengan las palabras clave.
CI_8	Se tomarán en cuenta artículos científicos, conferencias, revistas.

6.1.5.6.2. Criterios de exclusión

Los criterios de exclusión permitieron excluir todos aquellos artículos que no cumplieran con las necesidades de la investigación, para esto se tomó en cuenta la clase excluyente del mentefacto conceptual que se muestra en la Figura 8. En la Tabla 7 se menciona los 6 criterios de exclusión especificados.

Tabla 7. Criterios de exclusión

ID	Criterios de exclusión
CE_1	Todos los artículos que no contengan información sobre seguridad IoT.
CE_2	Todos los artículos que no contengan información sobre seguridad Edge Computing o Fog Computing.
CE_3	Todos los artículos que no aporten a resolver las preguntas de investigación.
CE_4	Los artículos que solo conceptualicen el IoT y Edge Computing.
CE_5	Todos los artículos que contengan información de seguridad en Cloud Computing.
CE_6	Todos los artículos que no estén escritos en inglés.

6.1.5.7. Preparación de un formulario de extracción de datos

En esta sub-etapa de la SLR, se especificó y preparo las herramientas y espacios necesarios para la organización y almacenamiento de resultados. Para la administración de la bibliografía se utilizó la herramienta de gestión bibliográfica Mendeley[1]. Para la identificación y eliminación de documentos duplicados entre las diferentes bases de datos científicas se usó la herramienta Parsifal [12] que además facilito el desarrollo de algunas fases de la SLR. Así mismo, para organizar y facilitar el análisis de la documentación se crearon tablas con información de acuerdo a la pregunta de investigación, título y base de datos a la que pertenece cada artículo.

[1] https://www.mendeley.com/library/

6.2. Objetivo 2: Identificar y analizar los estudios que abordan los problemas de seguridad en IoT en el contexto del Edge Computing.

6.2.1. Realización de la revisión

6.2.1.1. Identificación de la investigación

Esta sub-fase complementa de alguna manea al protocolo de revisión expuesto en la fase de planificación, aquí se realiza una búsqueda exhaustiva en cada una de las bases de datos previamente establecidas.

6.2.1.2. Selección de estudios primarios

En la Figura 9, se elaboró un diagrama de flujo del proceso que se realizó para la selección de estudios primarios.

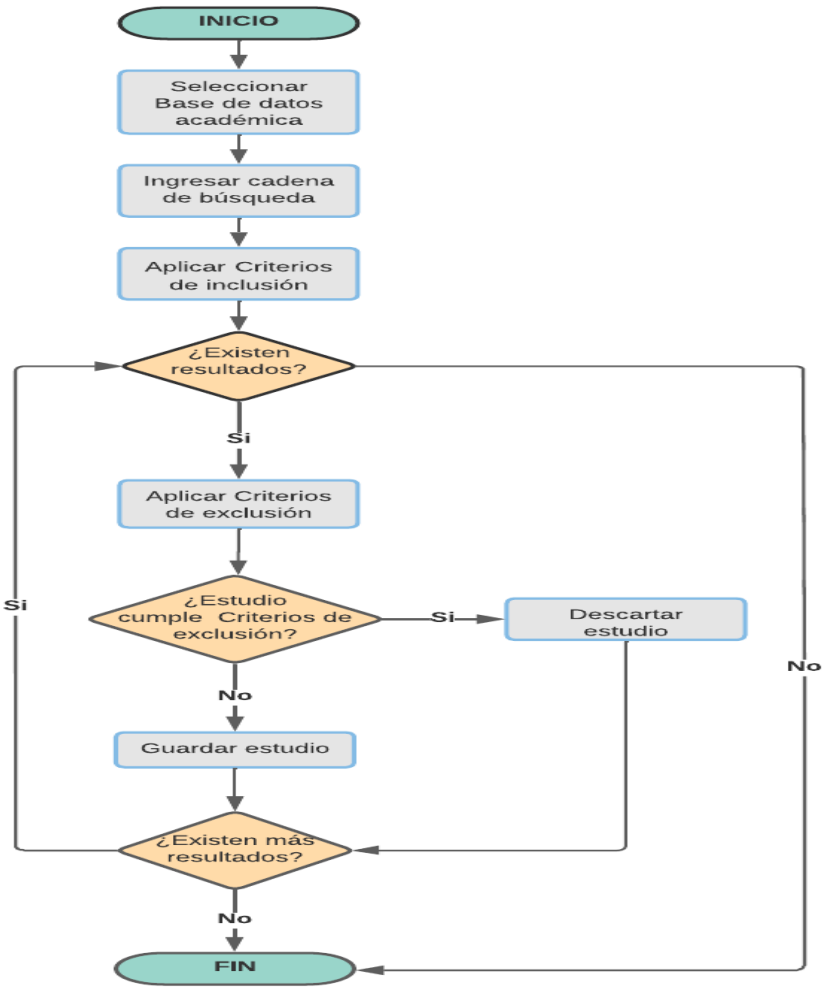

Figura 9 Diagrama de proceso para la selección de estudios primarios (Fuente propia)

Como resultado del proceso, Figura 9, aplicado en cada una de las bases de datos: WoS, Scopus, IEEE Digital Library y Google Scholar, usando como primer filtro el año de publicación (2016-2020), idioma y títulos; se obtuvieron un total de 1366 estudios relacionados con el tema sobre seguridad, IoT y Edge/Fog Computing; después se procedió a eliminar los estudios duplicados quedando una lista de 794; finalmente se aplicó una revisión por

resúmenes y palabras clave a cada uno de los estudios, quedando una lista de 136 para el análisis en esta etapa. La descripción de los resultados puede verse en la Tabla 8. Es importante recalcar que la búsqueda y obtención de la documentación se dio por finalizado el 29 de noviembre del 2020.

Tabla 8. Clasificación de los artículos resultantes

Base de datos	Encontrados	Duplicados	Revisados	Rechazados	Seleccionados
Wos	341	19	322	259	63
Scopus	496	293	203	172	31
IEEE Digital Library	516	253	263	225	38
Google Scholar	13	7	6	2	4
Total	1366	572	794	658	136

Después de realizar la selección de los estudios primarios fue necesario obtener los documentos completos para poder realizar la evaluación de la calidad de los mismo, esta sub-fase se lleva acabo más adelante.

De acuerdo a la Tabla anterior se han seleccionado 136 estudios de los cuales, en la Figura 10, se presenta el porcentaje por cada base de datos.

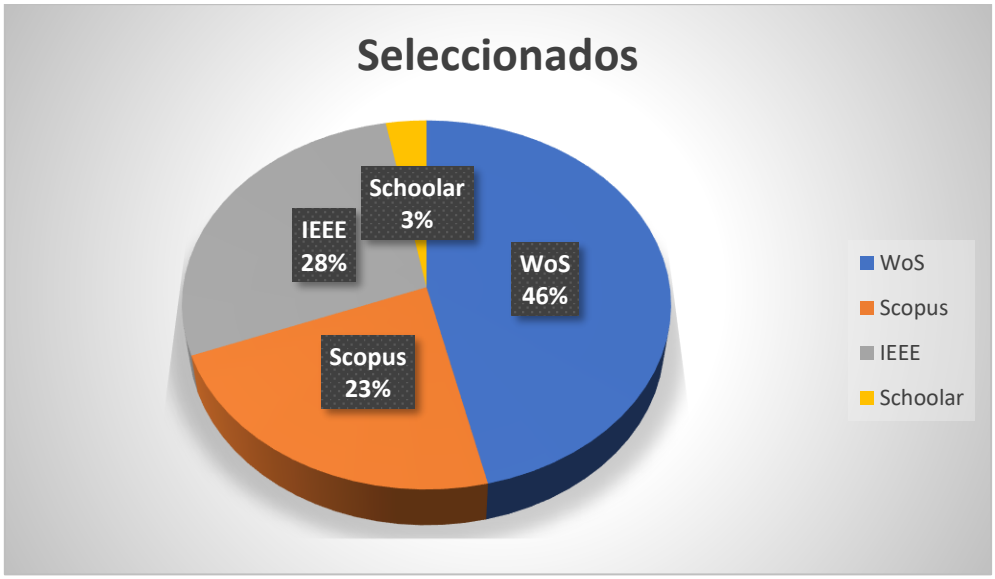

Figura 10. Porcentaje de estudios seleccionados (Imagen propia)

6.2.1.3. Evaluación de la calidad del estudio

Esta sub-fase es complementaria a la anterior. Además de los criterios de inclusión y exclusión es importante evaluar la calidad de los estudios primarios para minimizar el sesgo del estudio e incrementar la validez del mismo según [49]. Los criterios de inclusión y exclusión agregan aspectos de calidad a los estudios como: relevancia del estudio, calidad de las fuentes bibliográficas, relevancia y prestigio académico de los autores [11].

Para evaluar la calidad de los estudios seleccionados para la presente SLR se elaboró una lista de verificación de evaluación de la calidad que debe cumplir cada estudio para ser considerado valido. La lista se puede verificar en la Tabla 9.

Tabla 9. Lista de verificación de evaluación de la calidad

N°	Preguntas
1	¿El estudio aborda los problemas de seguridad en IoT?
2	¿El estudio aborda los problemas de seguridad de IoT basado en Edge Computing o Fog Computing?
3	¿El estudio menciona las características de Edge Computing o Fog Computing?
4	¿El estudio menciona alguna solución para mitigar los problemas de seguridad del IoT y Edge Computing o Fog Computing?

Después de haber formulado la lista de preguntas para la verificación de la evaluación de la calidad se debe dar un valor a cada estudio de acuerdo a cuantas preguntas responda, (véase la Tabla 10).

Tabla 10. Valores de calificación para el control de calidad del estudio

Selección	Calificación
Si	1
Parcialmente	0.5
No	0.0

Se asigna un valor de 1 si la respuesta es “Si”, 0,5 si la respuesta es “Parcialmente” y 0.0 si la respuesta es “No”. La puntuación total por cada artículo da un valor de 4, por lo cual el valor de corte para que un artículo pueda ser aprobado para su análisis es de 2 puntos.

Se aplicaron los parámetros antes descritos a cada uno de los 136 estudios seleccionados (**Ver anexo 1**).

Los estudios que obtuvieron un puntaje igual o mayor a 2 en los parámetros de calidad fueron 50 los cuales han sido seleccionados para extraer la información (Ver Tabla 11).

Tabla 11. Estudios seleccionados

N°	Titulo	Base de datos	Año
ES01	Passban IDS: Un sistema inteligente de detección de intrusos basado en anomalías para dispositivos IoT Edge	**Wos**	**2020**
ES02	Hacia una Internet de los objetos asistida por el borde: Desde la perspectiva de la seguridad y la eficiencia	**Wos**	**2019**
ES03	Marco controlado por la SDN asistida por la niebla para la detección duradera de anomalías en una red IoT	**Wos**	**2018**
ES04	Un marco basado en la computación en la niebla para la preservación de la privacidad en entornos IoT	**Wos**	**2020**
ES05	Blockchain en el borde: rendimiento de las redes de IoT con recursos limitados	**Wos**	**2020**
ES06	Garantizar la prueba de autenticidad de los dispositivos IoT Edge mediante la tecnología Blockchain	**Wos**	**2018**
ES07	Diseño de un mecanismo eficiente de detección de ataques Sinkhole en el despliegue de IoT basado en el borde	**Wos**	**2020**
ES08	Sistema de detección de intrusos basado en redes neuronales artificiales para nodos de la niebla del Internet de las cosas	**Wos**	**2020**
ES09	FOCUS: Un sistema de seguridad basado en la informática de niebla para el Internet de las cosas	**IEEE**	**2018**
ES10	Hacia la prevención de IoT-DDoS mediante computación de borde	**Scopus**	**2018**
ES11	Servicio de autorrecuperación que asegura el servidor de borde en la red IoT contra el ataque de ransomware	**Scopus**	**2020**
ES12	Autenticación basada en Blockchain con tolerancia a fallos para la computación en la niebla habilitada para IoT	**Scopus**	**2020**
ES13	Metodología en tiempo real para mejorar la ciberseguridad en el Internet de las Cosas utilizando la computación de borde durante la amenaza de ataque	**Scopus**	**2019**
ES14	FlowGuard: Un mecanismo inteligente de defensa de borde contra los ataques DDoS de IoT	**Scopus**	**2020**
ES15	Un marco de mitigación de anomalías para el IoT utilizando la computación en la niebla	**Wos**	**2020**
ES16	RAD-EI: Un esquema de detección de ataques de enrutamiento para el entorno del Internet de las Cosas basado en el borde	**Wos**	**2019**
ES17	Esquema de autenticación Protean: Una técnica de autenticación dinámica con límite de tiempo para nodos de borde de IoT en despliegues exteriores	**Wos**	**2019**
ES18	LDAKM-EIoT: Mecanismo ligero de autenticación de dispositivos y gestión de claves para el despliegue de IoT basado en el borde	**Wos**	**2019**

ES19	Detección de ataques de botnets en el borde del IoT basada en la representación dispersa	**Wos**	**2019**
ES20	Combinación de AntibIoTic con Fog Computing AntibIoTic 2.0	**IEEE**	**2019**
ES21	Una estrategia de mitigación distribuida contra los ataques DoS en Edge Computing	**IEEE**	**2019**
ES22	Mejora de la seguridad en un esquema de autenticación ligero con arquitectura de computación en la niebla anónima	**IEEE**	**2020**
ES23	Eccbap: un protocolo de autenticación seguro basado en ECC para dispositivos de borde del IoT	**Scopus**	**2020**
ES24	Biosec: Un marco de autenticación biométrica para la comunicación segura y privada entre dispositivos de borde en IoT e Industria 4.0	**Scopus**	**2020**
ES25	Un esquema de autenticación eficiente basado en la cadena de bloques para proteger los dispositivos IoT habilitados para la niebla	**Scopus**	**2020**
ES26	Un marco integrado seguro para los sistemas del Internet de las cosas asistidos por la niebla	**IEEE**	**2021**
ES27	Estudio sobre cuestiones de seguridad y privacidad en la Internet de los objetos asistida por Edge Computing	**Scholar**	**2021**
ES28	Seguridad en el Internet de las cosas asistido por el borde: retos y soluciones	**Scopus**	**2020**
ES29	Gestión segura de datos distribuidos para la computación en la niebla en aplicaciones de IoT a gran escala: Una solución basada en Blockchain	**Scopus**	**2020**
ES30	Aprendizaje federado con preservación de la privacidad en Fog Computing	**IEEE**	**2020**
ES31	Autenticación mutua y acceso autorizado a los datos entre la niebla y el usuario	**IEEE**	**2020**
ES32	Estudio sobre el análisis seguro de datos en la computación de borde	**IEEE**	**2019**
ES33	Un mecanismo para asegurar las aplicaciones habilitadas para IoT en la capa de niebla	**Wos**	**2019**
ES34	Seguridad de la computación en la niebla para las aplicaciones del Internet de las cosas: Desafíos y soluciones	**Wos**	**2018**
ES35	Un marco de seguridad impulsado por los bordes para la Internet inteligente de los objetos	**Scopus**	**2020**
ES36	Problemas de seguridad y privacidad y soluciones para la niebla	**IEEE**	**2020**
ES37	Lógica difusa y arquitectura segura basada en la niebla para el Internet de las cosas (FLFSIoT)	**Scopus**	**2020**
ES38	Huellas dactilares de los servicios de borde y de nube en el IoT	**Scopus**	**2020**
ES39	Seguridad y privacidad para IoT y Paradigma de la computación en la niebla	**Wos**	**2020**

ES40	Una encuesta: Integración de IoT y computación de niebla	**Wos**	**2018**
ES41	Retos de seguridad en la niebla y el IoT, tecnología Blockchain y soluciones de árbol celular: una revisión	**Wos**	**2020**
ES42	IMPACT: Detección de ataques de suplantación de identidad a través de Edge Computing utilizando autocodificador profundo y abstracción de características	**IEEE**	**2020**
ES43	Defensa del borde definida por software contra los DDoS basados en el IoT	**Wos**	**2017**
ES44	Seguridad de los dispositivos de borde de bajos recursos para los sistemas de IoT	**Wos**	**2018**
ES45	Cuestiones de seguridad y privacidad en el entorno del IoT impulsado por la niebla	**Scholar**	**2019**
ES46	Ransomware dirigido: Una nueva amenaza cibernética para el sistema de borde del Internet industrial de las cosas de Brownfield	**Wos**	**2019**
ES47	Detección de datos falsos para redes de niebla y del Internet de las cosas	**Wos**	**2019**
ES48	Ataque adaptativo de colisión de texto plano en AES enmascarado en Edge Computing	**IEEE**	**2019**
ES49	Mitigación de los ataques DoS en la capa EDGE de IoT para preservar los temas de Qos y la energía de los nodos	**Scopus**	**2020**
ES50	Programación de flujos de trabajo científicos en entornos de niebla múltiple mediante modelos de Markov y un algoritmo híbrido de enjambre SALP	**IEEE**	**2020**

Después de aplicar la evaluación de la calidad a cada estudio se obtiene un total de 50 estudios para analizar, la descripción de las cifras por cada base de datos se muestra en la Tabla 12.

Tabla 12. Estudios válidos para el análisis

Base de datos	Encontrados	Seleccionados	Válidos
Wos	341	63	22
Scopus	496	31	14
IEEE Digital Library	516	38	12
Google Scholar	13	4	2
Total	**1366**	**136**	**50**

Una vez aplicada la evaluación de calidad a cada estudio se puede verificar que las bases de datos relevantes WoS y Scopus son las que aportan un mayor porcentaje de estudios para desarrollar la SLR. (véase la Figura 11).

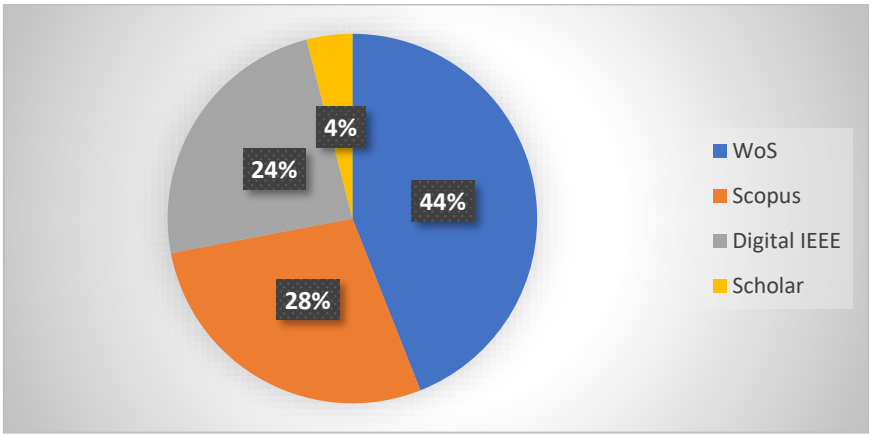

Figura 11. Porcentaje de estudios aceptados (Fuente propia).

6.2.1.4. Extracción y seguimiento de datos

Para el desarrollo de esta sub-fase se extrajo la información de cada uno de los estudios seleccionados; para lo cual, se diseñó un formulario para la extracción de datos, este se muestra en la Tabla 13. Este formulario contiene información básica del estudio (título, autor(es), referencia y año de publicación); además, contiene el resumen y la información relevante de acuerdo a las preguntas de investigación, también se le asignó un código de identificación (ES#).

Tabla 13. Formulario para la extracción de datos

#	**Descripción**	**Detalle**	**Código**: ES0
1	**Información bibliográfica**	**Título**	Nombre del estudio
		Autor	Nombre del autor (es)
		Referencia	Número referencia correspondiente a la bibliografía
		Año	Año de publicación del estudio
2	**Resumen**	Resumen general del estudio	
3	**Información relevante**	Información relevante para complementar el resumen	

El desarrollo del formulario por cada estudio se muestra en el **anexo 2** desde la Tabla 23 hasta la Tabla 72.

6.2.2. Síntesis y monitoreo de datos

En base a Kitchenham [50] la síntesis de datos consiste en comparar y resumir los resultados de los estudios primarios incluidos. Generalmente la síntesis es descriptiva, pero también se puede complementar con un resumen cuantitativo. En esta sub-fase se tabulará la información

extraída de acorde a las preguntas de investigación, con la finalidad de que los resultados sean legibles y comprensibles para los demás.

6.2.2.1. Vista general de los estudios seleccionados

En la Tabla 14, se presenta el resumen del proceso de selección de estudios de cada etapa. Las búsquedas realizadas generaron un total de 1569, obteniendo 1366 estudios al aplicar los criterios de inclusión y exclusión, de los cuales se registraron 512 duplicados, es decir el número de estudios revisados fueron 794, a los cuales se les aplicó una revisión por resúmenes y palabras clave, quedando una lista de 136 estudios para aplicar la evaluación de calidad quedando como resultado final una lista de 50 estudios válidos los cuales servirán para dar respuesta a la problemática propuesta.

Tabla 14. Síntesis de resultados de selección de estudios primarios

Base de datos	Total	Encontrados	Duplicados	Revisados	Seleccionados	Válidos
Wos	477	341	19	322	63	22
Scopus	542	496	293	203	31	14
IEEE Digital Library	524	516	253	263	38	12
Google Scholar	26	13	7	6	4	2
Total	1569	1366	572	794	136	50

En la Tabla 15, se puede observar que los estudios seleccionados con mayor puntuación de calidad y mayormente citados son los de la base de datos Web of Science.

Tabla 15. Información de calidad de estudios seleccionados

Cita	Puntuación total de calidad	año	Base de datos	Citado
[51]	3	2018	WoS	14
[52]	2	2020	WoS	3
[45]	3	2020	WoS	4
[53]	3	2020	WoS	47
[54]	2.5	2020	WoS	2
[55]	2	2019	WoS	23
[8]	2.5	2018	WoS	4

[56]	2	2018	WoS	6
[57]	4	2018	WoS	13
[44]	3	2018	WoS	6
[58]	3	2020	WoS	6
[59]	3	2020	WoS	5
[60]	2	2020	WoS	9
[61]	2	2019	WoS	11
[62]	3	2019	WoS	4
[63]	2	2019	WoS	14
[64]	3	2019	WoS	7
[65]	2	2019	WoS	2
[66]	2	2019	WoS	49
[67]	3	2019	WoS	52
[68]	3	2017	WoS	71
[21]	2	2018	WoS	388
[69]	3	2019	Scholar	4
[70]	3	2020	Scholar	5
[71]	3	2018	Scopus	47
[72]	3	2020	Scopus	1
[7]	3	2020	Scopus	9
[73]	2	2020	Scopus	0
[74]	3	2020	Scopus	3
[75]	2	2020	Scopus	0
[5]	2	2020	Scopus	0
[76]	2	2020	Scopus	0
[77]	2	2020	Scopus	11
[78]	2	2020	Scopus	0
[79]	2.5	2020	Scopus	1
[80]	2	2020	Scopus	2
[81]	3	2020	Scopus	0
[82]	2	2020	Scopus	3
[83]	2	2019	IEEE	22
[84]	3	2019	IEEE	2
[85]	3	2020	IEEE	13
[86]	2	2020	IEEE	0
[87]	2	2020	IEEE	17
[88]	4	2020	IEEE	0
[89]	2	2020	IEEE	1
[90]	3	2020	IEEE	0

[91]	3	2020	IEEE	5
[92]	2	2019	IEEE	1
[93]	3	2018	IEEE	8
[94]	2	2019	IEEE	5

En la Figura 12, se presenta la cantidad de estudios seleccionados por año de publicación, la selección se hizo desde el año 2016 al 2020, de los cuales una vez aplicados los criterios de inclusión, exclusión y evaluación de calidad quedaron únicamente desde el año 2017 al 2020. Se observa que existe un crecimiento de investigaciones con respecto al tema abordado notando que el año 2020 existe el mayor número de documentos seleccionados aun cuando las últimas consultas se realizaron el 29 de noviembre del 2020.

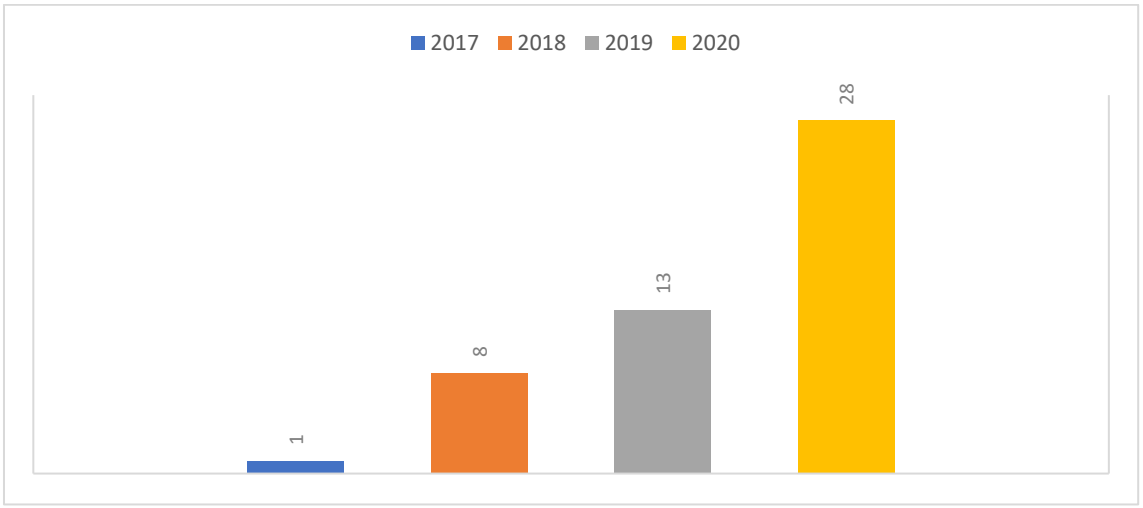

Figura 12. Artículos seleccionados por año de publicación (Fuente propia).

Luego de extraer la información de cada estudio seleccionado se presenta en la Figura 13, el porcentaje de los problemas abordados en los mismos, dando como resultado que los problemas mayormente abordados son: ataque de denegación de servicio (DoS) con el 12%, ataque de denegación de servicio distribuido (DDoS) con el 11%, ataque de hombre en el medio con el 10%, ataque de suplantación de identidad con el 7%, ataques de repetición y Colisión con el 6%.

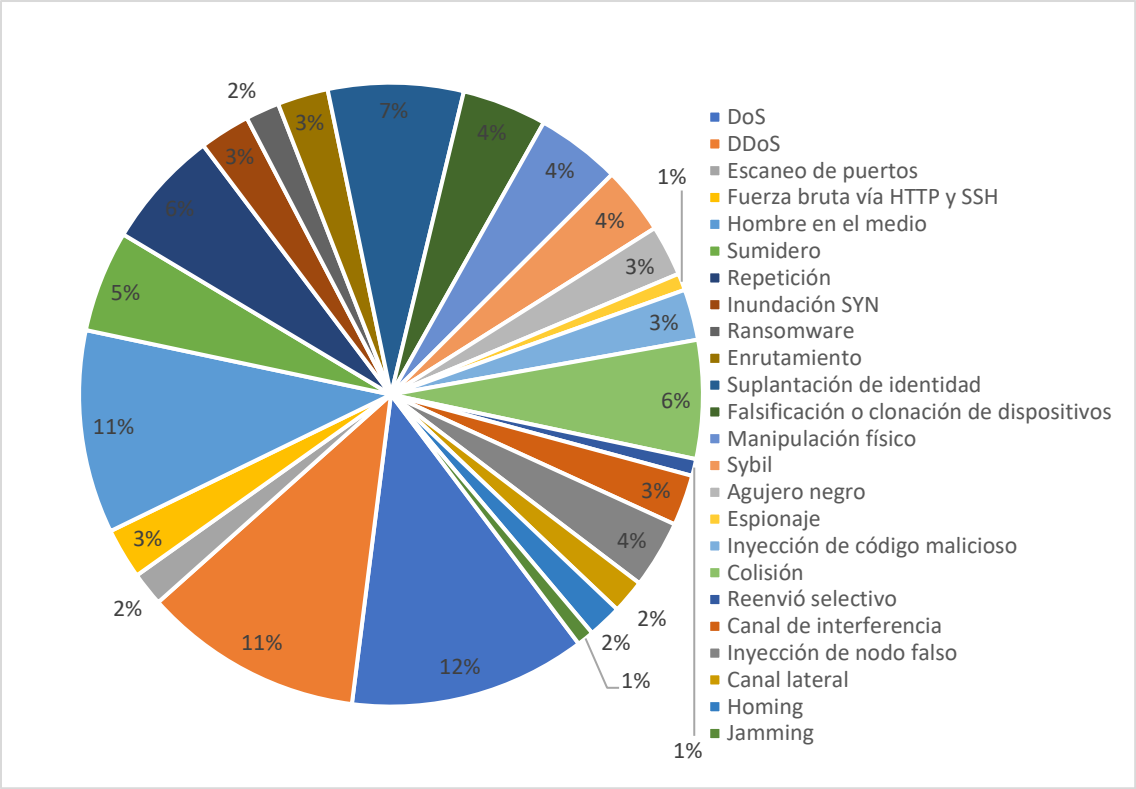

Figura 13. Problemas de seguridad abordados en los estudios analizados (Fuente propia).

6.2.2.2. Respuesta a las preguntas de investigación

Se obtuvieron un conjunto de 50 estudios seleccionados, los mismos que dieron respuesta a dichas preguntas.

6.2.2.2.1. RQ1: ¿Cómo los problemas de seguridad que presenta actualmente el IoT afectan al Edge Computing?

Para dar respuesta a esta pregunta de investigación en la Tabla 16 se presenta los problemas de seguridad que padece el IoT y como estos afectan al Edge Computing, adicional a esto se presenta las soluciones propuestas que se han podido identificar en algunos de los estudios analizados.

Tabla 16. Tabla de respuesta a la pregunta RQ1

Código de artículo de problemas	Problema de seguridad IoT	Como afectan al Edge Computing	Código de artículos de soluciones	Soluciones propuestas
ES03, ES04, ES08, ES15, ES21, ES24, ES27, ES29, ES35, ES36, ES37, ES39, ES40, ES43, ES44, ES47, ES49	**Ataque DoS**	Debido a la limitación de recursos informáticos, de redes y de almacenamiento en un solo nodo Edge, es bastante vulnerable a los ataques de denegación de servicio (DoS), este ataque afecta directamente al dispositivo Edge y a las aplicaciones y servicios que están alojados en él, el adversario desde una máquina o dirección IP genera cantidades masivas de peticiones saturando el servicio hasta lograr que este nodo Edge no tenga capacidad de respuesta y empiece a negar las peticiones a sus usuarios.	ES03	En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque de seguridad dentro de Edge Computing, sin embargo, los autores proponen un sistema de detección y prevención de intrusiones (IDPS) impulsado por redes definidas (SDN) asistido por Fog para redes IoT. Una disposición de Fog Computing colocada con la red de IoT, equipa al IDPS propuesto para la identificación oportuna de varios modelos de ataque DoS casi en tiempo real para la neutralización efectiva de las amenazas mediante el control de SDN, este control instala reglas de recopilación en los conmutadores que componen la capa de acceso de la red necesaria para la detección oportuna de actividades maliciosas inusuales en toda la red.
ES02, ES08, ES09, ES10, ES13, ES14, ES19, ES20, ES28, ES32,	**Ataque DDoS**	Este ataque afecta al dispositivo Edge de una forma similar al ataque DoS con la diferencia que utiliza múltiples dispositivos y varias conexiones a internet llamados botnets para realizar varias solicitudes a un nodo Edge o a un servicio,	ES08	Se identificó una solución diseñada para Fog Computing. Una metodología ABA-IDS (Sistema de Detección de Intrusos con Análisis de Comportamiento de Anomalías) utilizando Redes Neuronales Artificiales (RNA), el enfoque

ES39, ES43, ES50		saturándolo y forzándolo a cerrarse de modo que el nodo no admita ninguna otra solicitud de los usuarios legítimos. Para el administrador es complicado de detectar ya que las solicitudes vienen de diferentes IP's, como consecuencia no puede bloquear la IP que realiza la solicitud como se haría en el ataque DoS.		propuesto permite desplegar métodos de seguridad capaces de detectar cuando un nodo Fog ha sido comprometido, y luego tomar las acciones necesarias para asegurar la disponibilidad de las comunicaciones. La metodología propuesta incluye el uso de un perfil basado en características extraídas del nodo y alimentadas a Redes Neuronales Artificiales, configuradas para caracterizar con precisión las operaciones normales del nodo Fog a pesar de su complejidad debido al esquema adaptativo, y también tiene la capacidad de detectar anomalías debidas a cualquier tipo de fuentes como usos indebidos, ciberataques o fallos del sistema, con una alta tasa de detección y bajas falsas alarmas, teniendo además, una sobrecarga insignificante en términos de tiempo de ejecución, memoria y utilización de la CPU.
			ES09	Se identificó una solución diseñada para Fog Computing. Proponen un sistema de seguridad basado en Fog Computing, llamado FOCUS, este sistema adopta una unidad de análisis de tráfico, una unidad de desafío-respuesta y un firewall para proteger eficazmente el servidor VPN,

				específicamente, la unidad de análisis de tráfico analiza el tráfico de la red que intenta acceder al sistema IoT, para ello, adopta la clasificación del árbol de decisiones para distinguir las solicitudes legítimas de los ataques maliciosos. Los tráficos de la red se clasifican en dos categorías que son confiables y sospechosas, en función de una serie de atributos, como el comportamiento en ráfagas de tráfico, el recuento de flujos, la paralelidad del flujo y el recuento de paquetes de flujo. Luego, la unidad de desafío-respuesta y firewall generará una pregunta de desafío variable en el tiempo y la enviará a las fuentes de tráfico sospechosas. Si la IP de origen ha sido falsificada o si la fuente es un bot, no podrá responder con la respuesta correcta. Las fuentes sospechosas que no puedan responder adecuadamente a la pregunta de seguridad no podrán acceder al servidor VPN y serán bloqueadas por el firewall. De esta forma, los bots y sus ataques DDoS pueden filtrarse, mejorando así la seguridad del servidor VPN y de todo el sistema IoT. FOCUS se implementa de una manera altamente distribuida en la computación en la niebla, lo que

				mejora aún más la seguridad de los clientes de IoT en el borde.
			ES10	Presentan ShadowNet, una arquitectura que convierte el borde en la primera línea de defensa contra IoT-DDoS. En primer lugar, las funciones de borde adecuadas se implementan en la infraestructura de borde distribuida, en nombre de una aplicación de backend de IoT que busca protección. El papel de estas funciones de borde es esbozar los perfiles de la transmisión de tráfico de IoT desde una ubicación de borde determinada. En segundo lugar, la función de borde establece una ruta rápida entre ella y un servicio web ShadowNet especial. La función de borde utiliza la ruta rápida para enviar pequeños paquetes de sombra con información derivada localmente sobre el tráfico de IoT al servicio web ShadowNet. ShadowNet puede luego agregar esa información sobre el tráfico de IoT distribuido en varios nodos de borde, detectar un ataque inminente de IoT-DDoS y responder con alguna acción defensiva proactiva.
			ES13	Presenta un sistema de detección de intrusiones para detectar ataques DDoS, este sistema escanea y filtra el flujo de paquetes

				maliciosos en tiempo real en las redes de internet IoT utilizando políticas básicas de procesamiento de eventos complejos. La arquitectura del IDS está diseñada para implementarse en el borde de la red por lo tanto se logra la privacidad, seguridad, ancho de banda y tiempo de respuesta deseados. La arquitectura del sistema propuesto se divide en tres niveles diferentes. 1. Escáner: Monitorea y almacena los datos de la red en caso de que ocurra algún evento. 2. Procesador: Este actúa en dos subcapas 2.1: Analizador: Analiza las características de los datos. 2.2: Detección: Determina el tipo de ataque de intrusión para alimentar la entrada a una función específica para actuar. 3. Respuesta: Utiliza políticas complejas de procesamiento de eventos e invoca un módulo de respuesta contra cualquier ataque de intrusión o datos maliciosos y bloquea ese flujo de datos o servicio en particular.
			ES14	Proponen un esquema de defensa denominado FlowGuard, un eficaz esquema de detección, identificación, clasificación y mitigación de ataques DDoS que aprovecha dos técnicas

				cooperativas de aprendizaje automático, a saber, LSTM y CNN. FlowGuard consta de dos componentes principales: Filtro de flujo y manejador de flujo; el primero mantiene las reglas de filtración de flujo generadas por el manejador de flujo y se encarga de la detección de ataques DDoS, mientras que el segundo analiza los flujos sospechosos para la identificación y clasificación de ataques DDoS y la generación de reglas de filtración haciendo uso de algoritmos de aprendizaje automático en evolución. FlowGuard opera en los servidores de borde más cercanos a la red de IoT, y todos los paquetes que pasan a través de los servidores de borde deben ser inspeccionados por el filtro de flujo, que es el encargado de pasar los flujos que no se consideran maliciosos según las reglas de filtración.
			ES20	Se identificó una solución para implementar en Fog Computing. -Los autores proponen ANTIBIOTIC 2.0, un antimalware que se basa en la Fog Computing para asegurar los dispositivos IoT, es un gusano blanco que infecta dispositivos IoT que son vulnerables y crea una botnet de sistemas seguros, protegiéndolos contra el malware de

				IoT. La idea de ANTIBIOTIC 2.0 es utilizar un nodo Fog o una federación de nodos Fog para supervisar y desinfectar los dispositivos conectados a él, permitiendo que solo los seguros accedan a Internet. Para ello, el nodo Fog carga en cada dispositivo IoT un "anti-malware" también llamado (Bot ANTIBIOTICO). En primer lugar, el bot saniza el dispositivo, es decir, lo limpia de malware y otras posibles amenazas. A continuación, el bots asegura el dispositivo, es decir, identifica las vulnerabilidades de seguridad del dispositivo y actúa contra ellas (por ejemplo, cerrando puertos, cambiando las credenciales de acceso, actualizando el firmware, etc.). Si un dispositivo se reinicia o se desconecta temporalmente, volverá a estar protegido de forma automática en cuanto esté disponible, sin necesidad de realizar ninguna configuración manual sobre él.
			EE50	Se propone un algoritmo de optimización híbrida, que comprende tanto la optimización de enjambre de partículas (PSO) como el algoritmo Salp Swarm (SSA), para resolver el problema de programación de flujo de trabajo en varios entornos de computación de niebla. Se proponen dos modelos discretos de la cadena

				Markov para cada entorno de computación de niebla para abordar los efectos de los ataques DDoS en ellos. El primer modelo Markov calcula el ancho de banda de red disponible promedio para cada niebla y el segundo modelo markov encuentra el número promedio de máquinas virtuales (VM) disponibles para cada niebla; los modelos abordan diferentes niveles de ataques DDoS.
ES01, ES03	**Escaneo de puertos**	El atacante a través de un programa escanea automáticamente todos los puertos de un dispositivo IoT o nodo Edge que esté conectado a una red con el fin de encontrar puertos abiertos o con fallas de seguridad, una vez que el atacante haya podido ingresar a la red del dispositivo o nodo Edge puede robar la información confidencial del usuario.	ES01	Proponen un Sistema de Detección de Intrusiones (IDS) inteligente llamado Passban, se basa en una técnica de aprendizaje automático para conocer el comportamiento normal del sistema. Utiliza el aprendizaje automático supervisado y no supervisado para su entrenamiento. Después de la fase de entrenamiento, utiliza el modelo aprendido para detectar eventos anómalos que ocurren en el tráfico de red entrante, además, fue diseñado expresamente para ser alojado y ejecutado directamente por un dispositivo de borde típico, es decir, aprovecha al máximo la computación de borde, con respecto a su capacidad de detección, Passban es capaz de detectar casi todo el tráfico malicioso con tasas muy bajas de

				falsos positivos y precisiones relativamente altas.
ES01, ES33, ES41	**Ataque de fuerza bruta vía HTTP y SSH**	Los ataques de fuerza bruta dirigidos a un dispositivo Edge, se llevan a cabo probando cada combinación posible que el usuario podría usar como contraseña. Para validar si la contraseña es correcta o no, verifica si hay errores en la respuesta del dispositivo. Una vez descifrada la contraseña, el atacante puede llegar a tomar el control completo de dicho dispositivo.	ES01	-Recomienda utilizar firewall de comunicaciones para detectar este tipo de ataque. Es decir, si en pocos segundos teneos 60 intentos fallidos de login desde una misma IP origen, el firewall debería cortar las comunicaciones desde esta IP. -El administrador debe conocer que a medida que aumenta la longitud de una contraseña, el tiempo empleado para encontrar la contraseña correcta también aumenta rápidamente. Eso significa que las contraseñas cortas son bastante fáciles de descifrar.
ES04, ES05, ES09, ES12, ES18, ES25, ES33, ES34, ES36, ES37, ES38, ES40, ES41	**Hombre en el medio o escucha clandestina**	El atacante logra interceptar la comunicación entre un dispositivo IoT y un nodo Edge o entre dos nodos Edge sin ser detectado, una vez que el atacante interrumpe la conexión de sus víctimas toma el lugar de apoderado obteniendo acceso a la información que se está enviando entre los nodos Edge legítimos; a través del uso de alguna técnica para descifrar mensajes puede leerlos o modificar la información y hacer uso de ella a su conveniencia antes de enviarla a su destinatario y desaparecer.	ES12	En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque de seguridad dentro de Edge Computing, sin embargo, se identificó una solución basada en Fog Computing. -Proponen un nuevo esquema de control de acceso basado en la tecnología Blockchain para proporcionar autenticación segura y control de acceso a dispositivos IoT basados en Fog Computing. Cada entidad de la red se autentica en la cadena de bloques a través de la billetera, lo que permite una comunicación segura en un

				entorno descentralizado. Blockchain utilizan la criptografía asimétrica como medio para asegurar y garantizar las transacciones entre los usuarios. Cada entidad en estos sistemas posee un par de claves públicas y privadas. Este par de claves proporciona un aumento de la seguridad y protege de los piratas informáticos. Las claves públicas se publican en la red Blockchain y son compartidas por otras entidades. Cada entidad de la red tiene una dirección que se deriva de la clave pública mediante una función hash. Estas direcciones son medios para recibir y enviar activos en la red. Actúan como identidades seudónimas, que no revelan información personal o de identificación. Las claves privadas no están disponibles públicamente y solo debe conservarlas el propietario. Además, Blockchain utiliza el concepto de firma digital que se basa en claves privadas para garantizar la identidad y autenticación del usuario. Cuando dos partes intercambian algo en la red Blockchain, deben proporcionar una firma digital mediante el uso de claves privadas. Este proceso, por un lado, garantiza los objetivos de seguridad, incluida la integridad, la autenticación y el no repudio, y por

				otro lado protege contra el ataque de hombre en el medio. Además, la naturaleza descentralizada de Blockchain nos ofrece un entorno altamente robusto y resistente al ataque DDoS, porque este último se basa en un servidor centralizado.
ES07, ES24, ES26, ES32, ES39, ES41	**Ataque de sumidero (Sinkhole)**	El ataque de sumidero se lleva a cabo a través de un nodo Edge malicioso, que puede ser un router, este interrumpe el tráfico de la red al atraer a los nodos Edge legítimos mostrándoles una ruta más corta para llegar al destino, una vez que los datos que están siendo transferidos por los nodos Edge legítimos ingresan al nodo Edge malicioso este puede filtrar, alterar e incluso desaparecer los datos, además, es capaz de causar otro tipo de ataques como el ataque de reenvío selectivo. Al ocurrir este ataque el nodo Edge receptor, es decir, la estación base no recibe la información requerida o puede recibir información parcial o modificada. Esto da como resultado una reducción del rendimiento de la red y una degradación de la eficiencia y fiabilidad de la comunicación.	ES07	Proponen un esquema de detección de intrusiones denominado SAD-EIoT para proteger el entorno de IoT basado en Edge (EIoT) contra el ataque de sumideros. En SAD-EIoT, los nodos de borde ricos en recursos (servidores de borde) realizan la detección de diferentes tipos de nodos atacantes de sumideros con la ayuda del intercambio de mensajes. SAD-EIoT hace la detección del ataque sumidero en dos fases. En la primera fase aplica el algoritmo de “existencia de nodos atacantes de sumidero”, este utiliza parámetros como la identidad del nodo, el recuento de saltos desde un sensor de nodo Edge, la energía restante de los nodos y la información de rango. Un nodo es malicioso si el valor umbral del recuento de saltos para la red es menor que el recuento de saltos del sensor desde el nodo Edge. Si valor de energía restante en un nodo IoT es menor que la energía

				del nodo que transmite. Si el rango de un sensor IoT no pertenece a los valores más altos o más bajos de los rangos de los nodos de sensor. Un nodo pierde algo de energía cada vez que transmite o recibe paquetes y el nodo de borde conoce el estado inicial de la batería de todos los nodos. Si un nodo atacante proporciona un estado del batería modificado al nodo de borde, a su vez ese nodo de borde puede calcular el valor de la energía. Al finalizar esta fase, prepara una lista de nodos sospechosos de ser atacantes. La fase dos, utiliza el algoritmo de "confirmación de existencia de nodos atacantes. Para ello debe identificar varios casos: si un nodo envía un mensaje a un nodo vecino y este nodo después de un determinado tiempo no recibe ni el mensaje de respuesta ni el mensaje de datos se conforma que es una falla en el nodo, pero si, al contrario, el nodo recibe un mensaje de respuesta, pero no el mensaje de datos es identificado como nodo atacante de sumidero. En otro caso, si el nodo recibe el mensaje de respuesta y de datos, se comprueba la integridad de los datos mediante un algoritmo hash, si la integridad no se mantiene es tratado como un nodo atacante que

				ha modificado el mensaje de datos. Además, si el nodo recibe tanto el mensaje de respuesta y el mensaje de datos, pero la calidad de la red no está a la altura este verifica que no haya ocurrido un reenvió selectivo, es decir, que el atacante haya envía solo los paquetes UDP y retenido los paquetes TCP, para esto si el recuento de paquetes para un servicio concreto (es decir, TCP) no supera el valor umbral de recuento de paquetes en un periodo de tiempo determinado, se considera que el nodo si es un nodo atacante de sumidero. Una vez que ha completado las dos fases se obtiene una lista de nodos atacantes de sumidero que contiene las entradas de los tipos de nodos atacantes de sumidero que existen en la red, también, envía un mensaje de alarma a otros dispositivos IoT legítimos, a continuación, estos nodos legítimos eliminan las entradas de los nodos atacantes de sumidero de su lista de vecinos y comienzan a enviar sus paquetes a las otras posibles rutas disponibles.
ES08, ES12, ES18, ES22, ES25, ES33, ES41	**Ataque de repetición**	En el ataque de repetición, un nodo Edge maliciosa mantiene la red ocupada capturando un mensaje y enviándolo múltiples veces al	ES25	En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque de seguridad dentro de Edge Computing, sin embargo, se identificó una

		destino creando confusión en los nodos Edge receptores del mensaje.		solución diseñada para Fog Computing. Proponen un esquema basado en Blockchain, utilizando el contrato inteligente Ethereum para el acceso seguro de autenticación de usuario a dispositivos IoT habilitados para Fog. Cada participante se identifica en la red con una dirección Ethereum única y también se asocia con una clave pública y privada. Los principales enfoques son el uso de contratos inteligentes, la ejecución de eventos y habilitar dispositivos Fog para permitir que solo los usuarios autenticados accedan a los dispositivos de IoT. En Ethereum, los eventos se transmiten a todos los participantes y mineros cuando se activa un evento en un contrato inteligente. En caso de cualquier violación de las condiciones predefinidas del contrato inteligente, los eventos rebotan inmediatamente y revierten la condición a un estado óptimo anterior. Los principales participantes incluyen administradores, usuarios finales, dispositivos IoT habilitados para Fog, Blockchain con EVM (máquina virtual Ethereum) que ejecuta el contrato inteligente. El esquema cumple con las tríadas CIA definidas por los requisitos de seguridad de

				Confidencialidad, Integridad y Disponibilidad de los dispositivos IoT. El contrato inteligente está desarrollado utilizando el lenguaje Solidity con Remix-IDE y se prueban sus funcionalidades en dos redes de prueba Test RPC (Ganache) y Rinkeby Test Network. El análisis de vulnerabilidades de seguridad del contrato inteligente se realizó en la herramienta de análisis ChainSecurity. El esquema fue comparado con otros esquemas existentes, dando como resultado que el esquema está libre de fallos de punto único (SPF), y tiene altos niveles de confianza.
ES01, ES08, ES29	**Ataque de inundación SYN**	Una inundación SYN (ataque semiabierto) afecta a los nodos Edge de una forma similar al ataque de denegación de servicio (DDoS) consumiendo sus recursos, y como consecuencia dando de baja sus servicios. Este proceso se da a través de un atacante, que envía un gran volumen de paquetes SYN al nodo Edge, a menudo con direcciones IP falsas. el nodo responde a cada una de las solicitudes de conexión y deja abierto un puerto, listo para recibir la respuesta. Mientras el nodo espera el último paquete ACK, que nunca llega, el atacante continúa enviando paquetes SYN. La llegada de cada paquete SYN	ES01	Sobrescribir la conexión semiabierta más antiguas cuando se hayan llenado los registros pendientes. Esta estrategia requiere que las conexiones legítimas puedan establecerse por completo en menos tiempo del que tardan en llenarse los registros pendientes con paquetes SYN maliciosos. Esta estrategia de defensa puede llegar a fallar cuando el volumen de ataque aumenta o si el tamaño de los registros pendientes es demasiado pequeño para ser práctico.

		nuevo provoca que el nodo Edge mantenga temporalmente una nueva conexión de puerto abierto. Una vez utilizados todos los puertos disponibles, el nodo Edge ya no puede funcionar con normalidad.		
ES11, ES46	**Ransomware**	Si se inyecta un ransomware en un servidor Edge bajo el ataque de inyección de malware, el servidor dejaría de aceptar datos de dispositivos IoT, de modo que, no se realizaría ningún procesamiento para el sistema IoT causando una pérdida de datos que impide que el sistema tome decisiones críticas, por lo tanto, degrada el rendimiento del sistema. Atacar los servidores Edge en lugar de los dispositivos IoT tiene un impacto más significativo en los sistemas IoT porque ataca directamente al lugar donde se encuentra toda la información recolectada por los dispositivos IoT para ser procesada.	ES11	Para atenuar el daño causado por el ransomware en el servidor de borde se propone un método de recuperación automática (SRS). El SRS es un servicio del sistema que se ejecuta a nivel del kernel, monitorizando la actividad del sistema de archivos en un servidor de borde. Si se detecta cualquier actividad sospechosa en el almacenamiento, se comprueba la firma del ransomware; si la firma se encuentra en cualquier archivo de datos de IoT, los archivos de datos deben ser encriptados inesperadamente. Para resolver esta situación, SRS toma una acción inmediata para recuperar el archivo cifrado, recuperando su copia de seguridad del nodo de respaldo. Si no hay ninguna actividad sospechosa, el SRS continúa enviando los datos de IoT al nodo de copia de seguridad.
			ES46	Mantener a un atacante fuera de la red y el sistema no es suficiente si hay un atacante altamente calificado y un interno malicioso, ya

				que pueden acceder al firewall de próxima generación y lograr sus objetivos de todos modos. Por lo tanto, es de gran importancia monitorear y seguir el CKC de un ataque para determinar y comprender lo que está ocurriendo en la red. El sistema debe emplear varias herramientas de monitoreo, incluido un sistema de detección de intrusiones (IDS) que puede monitorear, recopilar datos, analizar y detectar un ataque de manera temprana. El sensor IDS debe implementarse en todas las interfaces de la puerta de enlace de borde. Otra solución que presenta el estudio es el uso de dispositivos de recuperación y respaldo en una red aislada (red air-gap). La copia de seguridad y la recuperación deben utilizar servidores en una red de espacio aéreo que esté físicamente aislada de la red infestada
ES16, ES41, ES45	**Ataque de enrutamiento**	Los nodos Edge atacantes de enrutamiento tienen la capacidad de desviar e interrumpir el flujo normal de tráfico. Estos nodos Edge maliciosos no envían los paquetes (mensajes) al nodo Edge destinatario y solo envían paquetes a sus nodos Edge atacantes colaboradores creando un bucle. Por lo tanto, el nodo Edge destinatario no obtiene la información	ES16	Proponen un esquema de detección de ataques de enrutamiento para el entorno de IoT basado en el borde, llamado RAD-EI. RAD-EI puede detectar nodos atacantes de enrutamiento, este trabajo lo realiza en dos fases. En la "fase 1", primero identifica los "nodos atacantes sospechosos" en la red mediante el "algoritmo de existencia del nodo atacante de

		correspondiente o la obtiene de forma parcial. Esto afecta aún más el rendimiento general de la comunicación del entorno de IoT basado en el borde.		enrutamiento (algoritmo 1)", que utiliza los parámetros, como la identidad del nodo (IDSi) y la energía restante (RENSi) en el nodo. Un nodo de sensor IoT (Si) se identifica como un "nodo sospechoso de enrutamiento atacante" si la condición “la energía restante es menor que el valor umbral de energía restante para ese nodo, RENSi <RENSi θ” se cumple. El algoritmo 1 proporciona una lista de los nodos atacantes sospechosos, SN1, si se detectan en la red. En la fase 2, se ejecuta el “algoritmo de confirmación del nodo atacante de enrutamiento (algoritmo 2)”. Para cumplir para esto, se utiliza la lista de nodos sospechosos, SN1 que se obtiene el algoritmo 1. Si el nodo de borde ENj no recibe mensajes de un nodo Si, verifica si el nodo Si es un "nodo atacante de enrutamiento o si hay otros problemas en el entorno (por ejemplo, falla del nodo)". ENj envía “mensajes de consulta de estado y datos Msdq” al nodo Si, y el contador de tiempo de espera aumenta cada vez. Si el tiempo de espera expira y ENj no recibe "mensaje de respuesta (Msr) y mensaje de datos (Md) del nodo Si", se contempla que Si es un nodo de falla. De lo contrario, si ENj recibe el "mensaje de respuesta (Msr)", pero no recibe

				el "mensaje de datos (Md)", Si se detecta como el nodo atacante de enrutamiento.
ES18, ES22, ES23, ES24, ES34, ES36, ES37, ES42	**Ataque de suplantación de identidad**	El ataque de suplantación de identidad llega a afectar a un nodo Edge cuando logra obtener la clave de sesión almacenada en el nodo y consigue ser aceptado por la puerta de enlace, de esta manera lograra beneficiarse de los servicios proporcionados por los nodos Edge, o se hace pasar por un nodo Edge legítimo para ofrecer servicios falsos o de phishing a los usuarios.	ES18	Propone un mecanismo ligero de gestión de claves autenticadas para el entorno del IoT basado en el borde denominado (LDAKM-EIoT) que proporciona protección contra diferentes ataques de suplantación. Si un atacante intenta crear un mensaje de solicitud de autenticación válido en nombre de una parte comunicante, el nodo Edge para calcular los mensajes de respuesta, utiliza los secretos a largo y corto plazo, que debe proporcionarlos el dispositivo IoT y al no poseer estos valores secretos, no es capaz de crear un mensaje de autenticación válido en nombre del auténtico dispositivo IoT.
			ES22	Se propone un esquema de autenticación seguro para la capacidad de generación dinámica de claves. El cual consiste en que los dispositivos de comunicación intercambian ID y números aleatorios para el registro y, a continuación, generan información anónima. Durante el proceso de autenticación, el dispositivo en la nube (por ejemplo, el servidor) utiliza la información del seudónimo para que coincida con los números aleatorios registrados. Ambos dispositivos utilizan el protocolo con

				tales números aleatorios para generar claves de sesión y entregar números aleatorios actualizados. Este protocolo utiliza hash, clave simétrica y técnica de generación de claves dinámicas de capa física para lograr ese objetivo, que no sólo es anónimo y ligero, sino que también se puede aplicar para cada dispositivo en toda la arquitectura FC, para hacer que los nodos perimetrales, los nodos de niebla y el servidor en la nube se autentiquen entre sí y hagan que la transmisión de datos sea más segura.
			ES42	Presenta un modelo IDS ligero basado en ML, denominado IMPACT (IMPersonation Attack detection) utilizando un autocodificador profundo y una abstracción de características. Este modelo se basa en el aprendizaje profundo de entidades con la máquina vectorial de soporte lineal basada en degradado (SVM) para implementarse y ejecutarse en dispositivos con recursos limitados al reducir el número de entidades mediante la extracción y selección de entidades a través de un codificador automático apilado (SAE), información mutua (MI) y contenedor C4.8. El IMPACT está entrenado en

				el Dataset de Intrusión Wi-Fi del Egeo (AWID) para detectar ataques de suplantación.
ES05, ES06, ES17, ES32, ES34, ES36	**Ataque de falsificación o clonación de dispositivos**	Un ataque de hardware hacia un nodo Edge puede ocurrir con la manipulación física de un dispositivo o a través de la introducción de un dispositivo clonado en el sistema o nodo Edge. Los dispositivos impostores representan amenazas graves; la mayoría de los dispositivos Edge de bajo costo se pueden falsificar o clonar fácilmente. Es imprescindible identificar el abastecimiento de los dispositivos Edge de forma única y verificar su validez periódicamente en tiempo de ejecución.	ES06	Implementar la tecnología Blockchain para autenticar los dispositivos Edge restringidos y de bajo costo; utilizando funciones físicamente inclonables (PUFs) basadas en SRAM para generar huellas digitales únicas (ID de dispositivo). Los fabricantes registrados cargan un hash criptográfico de cada ID de dispositivo en una instancia de cadena de bloques accesible globalmente (almacén de clave-valor o contrato inteligente). Al registrar un dispositivo localmente, el usuario final verifica si el hash está presente en esa cadena de bloques. Los dispositivos se pueden autenticar periódicamente para evitar la clonación del dispositivo.
			ES17	Para mitigar el ataque de clonación de dispositivos, proponen un mecanismo de generación de claves eficiente, donde las credenciales de autenticación se generan sobre la marcha y se intercambian de forma segura entre la puerta de enlace y los nodos de borde con una sobrecarga computacional mínima en dispositivos de IoT con recursos limitados

				llamado “Protean”. El esquema de autenticación de Protean se basa en vectores de inicialización mínimos. Tiene poca dependencia de las claves almacenadas estáticas durante todo el ciclo de autenticación. El esquema Protean es computacionalmente menos intensivo en los recursos del dispositivo porque involucra operaciones de cómputo livianas como funciones hash, operaciones XOR y también encriptación AES en el lado de la puerta de enlace, mientras que los nodos de borde solo realizarán encriptación AES. El esquema de autenticación de Protean utiliza AES tanto para el cifrado de carga útil como para cifrar las credenciales de autenticación intercambiadas entre la puerta de enlace y el nodo de borde. El consumo de energía mediante el cifrado AES es insignificante en comparación con sus contrapartes. El almacenamiento seguro de las credenciales por sí solo no es suficiente para la seguridad de las claves, ya que deben intercambiarse con fines de autenticación. Los atacantes que escuchan la comunicación pueden hacerse con las credenciales encriptadas y aún pueden usarlas para autenticar un dispositivo malicioso al

				reproducir las mismas. Por lo tanto, la necesidad de cambiar las claves dinámicamente e intercambiarlas de manera suficientemente segura es una necesidad en el paradigma de IoT. Con el esquema de Protean, se vuelve difícil para un atacante adivinar o manipular la secuencia de eventos seguida por el esquema, ya que el IDS alojado en la puerta de enlace decide dinámicamente la vida útil de las claves. Como muchos esquemas de autenticación existentes, el mecanismo propuesto no requiere almacenar ningún valor de clave estática en el dispositivo. En cambio, las claves cambian dinámicamente y se comparten de forma segura para evitar la reproducción de mensajes y los ataques de clonación de dispositivos.
ES18, ES24, ES32, ES39, ES40	**Ataque de manipulación físico**	Los nodos Edge al estar ubicados en entornos remotos y sin protección son vulnerables a sufrir ataques de hardware y software, el atacante al tener acceso físico a los dispositivos Edge que conforman el nodo puede robarlos, dañarlos, modificar su programación, cambiar el sistema operativo y extraer información criptográfica valiosa. El objetivo del atacante es lograr obtener información que pueda ser usada en un futuro, como pueden ser las claves, este tipo de ataque		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque.

		puede causar daños permanentes en los nodos Edge.		
ES26, ES32, ES34, ES39	**Ataque Sybil**	Un nodo Edge malicioso se hace pasar por un gran número de clientes o nodos Edge legales para controlar o comprometer todo el marco de la computación de borde. Cada nodo Edge malicioso actúa como intermediario para robar la información privada de los clientes, al ingresar muchos nodos maliciosos a la red y enviar grandes cantidades de datos logran bloquear la comunicación de otros dispositivos Edge con la red, es un ataque similar al DoS.	ES26	Proponen un marco de control de acceso basado en atributos y monitoreo de comportamiento basado en la confianza. El marco propuesto consta de dos componentes, el componente de seguridad (SC) y el componente de administración de confianza (TMC). SC garantiza la confidencialidad, integridad, autenticación y autorización de los datos a través de un esquema ABE ligero basado en curvas elípticas. TMC evalúa el rendimiento de las entidades de Fog-IoT mediante un modelo de confianza basado en un conjunto de características de comunicación de red y QoS. Posteriormente, la confianza se incrusta como un atributo dentro de las directivas de control de acceso de SC, lo que garantiza que solo las entidades de confianza tengan acceso a los recursos de niebla.
ES26, ES37, ES39	**Ataque de agujero negro**	El atacante crea un nodo Edge malicioso, a través del cual, altera la información de enrutamiento de la red con el objetivo de atraer todos los paquetes al nodo Edge malicioso, éste nodo recibe los paquetes y de manera sigilosa los deshecha de la red, es decir los paquetes que ingresan al nodo Edge malicioso desaparecen.	ES26	
ES32	**Ataque de espionaje**	Es un tipo de ataque de hombre en el medio, el atacante se coloca en medio de la comunicación entre dos nodos Edge legítimos, un nodo emisor y un receptor, al momento en el que el nodo Edge emisor desea encriptar un mensaje para que el envío sea seguro, este envía un mensaje		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque.

		de saludo y pide la clave pública del nodo Edge receptor, el atacante se interpone e intercepta el mensaje de respuesta con la clave pública del nodo Edge receptor la conserva y envía su propia clave pública, de este modo el nodo Edge emisor cree que es la clave real y procede a enviar el mensaje encriptado con la clave pública del nodo atacante, el cual, lo descifra y lee la información importante y lo reenvía al nodo Edge receptor y desaparece, en este tipo de ataque el objetivo del atacante no es modificar la información sino enterarse del contenido.		
ES28, ES41, ES44, ES47	**Inyección de código malicioso**	El atacante accede físicamente al nodo Edge eh inyecta un código malicioso (es decir, virus, malware, caballo de Troya) en el nodo Edge, de este modo el atacante obtiene acceso a red y puede hacer que la red pierda recursos y, por lo tanto, que los servicios no estén disponibles. Una vez infectados los nodos Edge el atacante podría obtener el control total del nodo Edge o incluso el control de todo el sistema incluso cundo ya no tenga acceso físico al mismo.	ES47	En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque de seguridad dentro de Edge Computing, sin embargo, proponen un novedoso IDS, denominado DataIDS, diseñado específicamente para redes Fog/IoT, basado en el análisis de datos físicos (detectados) para reconocer mejor las vulnerabilidades contra los dispositivos finales. Las mediciones realizadas por los sensores se envían a la unidad Fog (FU), que procesa localmente los flujos de datos, y si se detecta un comportamiento anómalo, puede dar la alarma y gestionar las correspondientes contramedidas adecuadas. DataIDS puede

				integrarse fácilmente en los nodos Fog sin afectar significativamente a su rendimiento, ya que permite que un nodo Fog controle un número muy elevado de dispositivos IoT y lance una alarma y las contramedidas correspondientes si uno o varios dispositivos sufren un ataque. Para complementar el enfoque de DataIDS, se utiliza un árbol de ataques para seleccionar la acción adecuada a realizar, que puede abarcar desde el simple descarte de los datos de los sensores atacados, aislar los dispositivos atacados, descartar sus datos, autenticar un sensor y sus datos hasta una reconfiguración completa de la red.
ES26, ES27, ES30, ES34, ES35, ES37, ES40, ES48	**Ataque de Colisión**	Este ataque puede afectar numerosos nodos Edge, dispositivos IoT y nodos Edge con dispositivos IoT, al coludirse dos o más dispositivos IoT o nodos Edge para aumentar su capacidad de ataque. La colisión se produce cuando la misma frecuencia utiliza diferentes nodos para comunicarse al mismo tiempo.	ES26	El marco de control de acceso basado en atributos y monitoreo de comportamiento basado en la confianza, utilizado para mitigar el ataque Sybil y ataque de agujero negro, también está diseñado para hacerle frente a este tipo de ataque.
ES41	**Ataque de reenvió selectivo**	Un atacante crea un nodo Edge malicio que falsifica la información de enrutamiento para hacer que los nodos Edge envíen sus paquetes por él, una vez que este nodo Edge malicioso intercepta los mensajes puede modificarlos,		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque.

		eliminarlos o hacer un reenvío selectivo solo de ciertos mensajes .		
ES32, ES35, ES36	**Ataque al canal de interferencia**	Un atacante envía una gran cantidad de mensajes falsos tratando de consumir los canales de comunicación y los recursos informáticos hasta agotarlos, de esta manera, logra que los dispositivos IoT no puedan comunicarse con los nodos Edge.		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque
ES27, ES41, ES44, ES45	**Inyección de nodo falso**	Un atacante puede colocar físicamente un nodo Edge falso entre dos o más nodos Edge legítimos, de esta manera el atacante obtiene acceso a la red y puede controlar todo el flujo de datos desde y hacia los nodos y su funcionamiento. Puede hacer que el nodo deje de transmitir los datos reales y, por lo tanto, destruye toda la red.		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque
ES31, ES41	**Ataque de canal lateral**	El atacante utilizando técnicas particulares (es decir, análisis de tiempo, energía, fallos y Análisis electromagnético) en los dispositivos de cifrado de un sistema IoT, de esta manera puede recuperar y recopilar la clave de cifrado que se utiliza para cifrar y descifrar los datos.		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque
ES34, ES39	**Ataque Homing**	El atacante estudia el tráfico de la red para deducir la localización de los nodos Edge principales es decir los nodos coordinadores por ejemplo los router o los vecinos de la estación		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque

		base. El objetivo del atacante es obtener dicha información para deshabilitar esos nodos.		
ES34	**Ataque Jamming**	El atacante produce una denegación del servicio a usuarios autorizados, atascando el canal de comunicación con una cantidad abrumadora de información errónea con el fin de que ningún otro dispositivo Edge pueda utilizarlo, es un tipo de ataque DoS.		En los estudios analizados no se encontró ninguna solución propuesta para mitigar este ataque

6.2.2.2.2. RQ2. ¿Cuáles son las características del Edge Computing que generan problemas de seguridad en dispositivos IoT?

El Edge Computing tiene varias características importantes, estas son: Conocimiento de la ubicación, distribución geográfica, arquitectura descentralizada, soporte de movilidad, infraestructura heterogénea, escalabilidad, baja latencia, bajo consumo de banda ancha, aporta una gran eficiencia, bajo costo de inversión, mayor accesibilidad, consumo energético reducido, soporte de aplicaciones IoT a gran escala, soporte de procesamiento más cerca al origen (proximidad) y seguridad de la información. Cada una de estas características brinda ventajas importantes al Edge para la implementación con el IoT. Pero también algunas de ellas introducen nuevos desafíos de seguridad ya que ya que aportan para que se produzcan ataques de seguridad. Para dar respuesta a la pregunta planteada se describe cada característica y su vulnerabilidad, (Ver Tabla 17).

Tabla 17. Tabla de respuesta a la pregunta RQ2

Código de artículos	Característica	Problema de seguridad
ES26, ES32, ES34, ES40, ES45	**Conocimiento de la ubicación**	Esta característica aparte de brindarle ventajas al Edge Computing también introduce desafíos de seguridad, recordemos que un nodo Edge generalmente le envía su carga al nodo Edge más cercano por lo que el nodo Edge que recibe la carga ya tiene una idea de la ubicación de ese nodo. Además, si un nodo Edge usa múltiples nodos para descargar, entonces la trayectoria completa de la red puede ser revelada. Si este proceso ocurre en cadena, se puede rastrear fácilmente un conocimiento aproximado sobre la red completa. Esto le facilita el trabajo al atacante para que pueda ejecutar fácilmente un ataque Haming y apagar los nodos Edge principales, además, puede ejecutarse todo tipo de ataques de enrutamiento e inundación.
ES32, ES34, ES40	**Distribución geográfica**	Los nodos Edge están desplegados en varias posiciones, como autopistas, carreteras, supermercados, museos, etc. Debido a que están implementados en lugares remotos y sin protección los nodos Edge son propensos a sufrir diferentes tipos de ataques de seguridad como son: ataques de manipulación física, inyección de nodo falso e inyección de código malicioso.

ES26, ES32, ES34, ES36, ES45	**Arquitectura descentralizada**	La implementación de Edge Computing puede tener diferentes proveedores de servicios debido a las distintas necesidades de implementación, esto puede generar un problema de falta de autenticación y control de acceso que abre la puerta a diferentes ataques de seguridad como, DoS, DDoS, suplantación de identidad, ataque de interferencia. Básicamente, la descentralización y el aprovisionamiento de servicios de baja latencia crean una barrera para la autenticación segura.
ES26, ES32, ES34, ES36, ES41, ES45	**Soporte de movilidad**	La movilidad del usuario exige que los dispositivos IoT se desconecten con frecuencia de un nodo Edge de confianza y se unan a otro nodo durante el transcurso, al conectarse al nuevo nodo se pierde la confiabilidad ya que se ingresa a un nuevo nodo del cual no se tiene conocimiento de su comportamiento ya que es muy difícil recopilar información relacionada con el comportamiento de todos los nodos Edge; un dispositivo IoT celular o computador puede estar dentro de un vehículo para recopilar la información del tráfico, durante el recorrido este puede ser interceptado por un atacante que puede lanzar un ataque de canal lateral y obtener las claves de cifrado y descifrado de los datos ya que al conectarse y desconectarse constantemente de diferentes nodos la gestión de claves se convierte en un desafío. Por lo tanto, la confiabilidad entre todos los nodos Edge en la red es un tema crítico.
ES27, ES28, ES40	**Escalabilidad**	Una red distribuida como es Edge Computing debe enfrentar diferentes problemas, primeramente, la heterogeneidad de los dispositivos, que tienen diferentes limitaciones de rendimiento y energía además de la confiabilidad en las conexiones, debido a estas limitaciones no es posible implementar métodos de seguridad en todos los dispositivos y como consecuencia algunos de ellos serán vulnerables a cualquier tipo de ataque de seguridad.
ES27, ES34, ES44	**Consumo energético reducido**	La mayoría de los dispositivos Edge dependen de baterías pequeñas para funcionar debido a limitaciones de tamaño. Los atacantes intentarán agotar la batería de un dispositivo periférico por cualquier medio posible. Por

		ejemplo, esto podría implicar obligar al nodo a ejecutar subrutinas que consumen energía. Otro método bajo el ataque DoS es la privación del sueño. En este tipo de ataque, el atacante envía numerosas solicitudes que parecen legítimas obligándolo a responder impidiendo que el nodo duerma y, por tanto, no conserva energía.

6.3. Objetivo 3: Desarrollar el informe de presentación de resultados de la RSL.

Para el cumplimiento de este objetivo, se desarrolló un artículo científico en el que se muestra los resultados obtenidos en todo el proceso de la SLR, relacionados con los problemas de seguridad que actualmente presenta el IoT y que afectan directamente al Edge Computing; así como, las características de este nuevo paradigma que afectan los dispositivos IoT; el mismo que servirá para ser presentado en una revista científica o en un congreso**. (Véase anexo 3**.)

7. Discusión

El desarrollo del presente TT denominado “Exploración de los problemas de seguridad que presenta el IoT en el contexto del Edge Computing”, se basó en la realización de tres objetivos específicos, encaminados al cumplimiento del objetivo general. A continuación, se detalla la discusión por cada objetivo planteado. La sección 1 explica la discusión de los resultados contrastándolos con la literatura relacionada del objeto de estudio; la sección 2 presenta la valoración científica, técnica, económica y ambiental del TT.

7.1. Desarrollo de la propuesta alternativa

7.1.1. Objetivo 1: Planificar la Revisión Sistemática de Literatura (SLR) definiendo la pregunta de investigación y el protocolo de revisión

Para dar cumplimiento al primero objetivo, primeramente, se identificó la necesidad de realizar la SLR, a continuación, se especificaron las preguntas de investigación que guiaron toda la revisión (ver, Tabla 3). Para asegurar que la SLR sea única y brinde una contribución útil a la comunidad científica, se realizó una búsqueda general de revisiones sistemáticas de literatura relacionadas en las cuatro bases de datos; dentro de los resultados se obtuvo un conjunto de 11 trabajos que tienen relación con la temática de interés, de los cuales [22] presenta algunas cuestiones de seguridad y privacidad del IoT asistido por el Edge, [43] habla sobre las mejoras que introduce la integración de IoT con Edge Computing respecto a latencia, consumo de ancho de banda y consumo de energía, en [44] menciona los beneficios de la combinación de ambas tecnologías; además, menciona los ataques de seguridad más comunes, DoS, hombre en el medio y Colisión; por otro lado, en el estudio [45] analiza el panorama general de la seguridad en Fog y el uso de Blockchain como posible solución; finalmente, en el estudio [46] se presenta un análisis sobre el IoT basado en Fog, la arquitectura y algunas amenazas a la seguridad. De la misma manera, el resto de estudios se encuentran realizados a nivel general; es decir, conceptualizan el IoT, Edge/Fog y cuestiones de seguridad; constatando de tal manera que no existen investigaciones que ya hayan respondido a las preguntas de investigación que se plantearon para este TT. Para la búsqueda de los estudios se seleccionaron cuatro bases de datos científicas, las cuales se eligieron por la calidad de artículos que se encuentran alojados en las mismas. Para estructurar las cadenas de búsqueda, primeramente, se establecieron las palabras clave aplicando los criterios semánticos del mentefacto conceptual; luego, se relacionaron a través de los operadores booleanos AND, OR, NOT. También, se construyeron y probaron varias cadenas de búsqueda, de este modo, se eligió la cadena que arrojó mejores resultados. Se definieron los criterios de inclusión y exclusión con ayuda del mentefacto conceptual. Finalmente, se preparó un formulario de extracción de datos utilizando la herramienta de gestión bibliográfica Mendeley, para la identificación y eliminación de documentos duplicados entre fuentes de búsqueda se utilizó la herramienta de Parsifal, para organizar y facilitar el análisis de la

documentación se crearon Tablas con información de acuerdo a la pregunta de investigación, título y base de datos a la que pertenece cada artículo.

7.1.2. Objetivo 2: Identificar y analizar los estudios que abordan los problemas de seguridad en IoT en el contexto del Edge Computing

Para el desarrollo de este objetivo, primeramente, se elaboró un diagrama de flujo (ver, Figura 9) con el proceso de selección de estudios, que sirvió de guía para llevar a cabo la búsqueda manual en cada una de bases de datos, de la misma manera, se aplicó el proceso de filtrado a través de los criterios de inclusión, exclusión y la eliminación de los duplicados, obteniendo como resultado 136 estudios para el análisis. Posteriormente, se desarrolló el control de calidad de los estudios primarios para así seleccionar los estudios definitivos para el análisis de la información, en este aspecto se formularon cuatro preguntas para el control de calidad con un peso específico de respuesta para cada una (Si=1, Parcialmente=0.5, No=0), haciendo el corte de valoración de 2, para la aceptación de cada estudio, obteniendo como resultado final 50 estudios; de los cuales se procedió hacer la extracción de la información más relevante. Finalmente, en la síntesis de datos, se llevó a cabo el análisis exhaustivo de cada uno de los estudios para dar respuesta a las preguntas de investigación. Se identificó que la base de datos WoS es la que proporcionó la mayor cantidad de documentación relevante para el desarrollo de la presente investigación; además, de ser la fuente que contiene más citas bibliográficas con respecto a las otras bases de datos. Asimismo, se identificó y se analizó 24 ataques de seguridad que padece actualmente el IoT y que heredaría el Edge Computing ya que es una extensión de la Cloud; entre los cuales, se determinó que los ataques más comunes son: el ataque DoS, DDoS y el hombre en el medio con el 12%, 11% y 10% respectivamente, comparando dicha información con otros estudios [6], [70] el ataque DDoS se mantiene como uno de los ataques más comunes, así mismo, tomando en cuenta que la investigación realizada en estos estudios, analiza sólo un espectro reducido de problemas de seguridad mientras que en la presente investigación se analizó un espectro amplio de 24 problemas de seguridad. También se constató que existen pocos estudios que investiguen a fondo los problemas de seguridad, en su mayoría lo hacen de forma general a manera de conceptualización. En virtud de lo antes expuesto, en los estudios [45],[58],[61], [62], [65], [66], [68], [71], [72], [7], [81], [85] se analizan ciertos problemas o en algunos casos un problema en específico, como el ataque de sumidero, ransonware, enrutamiento, inyección de código malicioso, DoS, DDoS, suplantación de identidad y colisión; sin embargo, existen otros problemas de seguridad los cuales se mencionan en muy pocos estudios e incluso en uno solo, como es el caso del ataque Jamming y Homing. De igual manera, en lo que respecta a las soluciones planteadas en los estudios analizados la gran mayoría están propuestas para mitigar el ataque DDoS. Dichas soluciones van desde metodologías, sistemas de seguridad basados en Fog Computing, esquemas de detección, identificación, clasificación y mitigación

de ataques, antimalware y Sistemas de Detección de Intrusiones. Asimismo, en los estudios [45], [52], [57], [75], [5], [79] proponen el uso de Blockchain para la autenticación y el control de acceso de dispositivos IoT asistidos por el Edge.

Por otra parte, una de las limitantes para desarrollar la investigación fue, la poca existencia de estudios que abordan las características de Edge Computing; si bien es cierto, que existen varios trabajos que contextualizan las características de Edge y las ventajas que se obtendrían al implementar el IoT en Edge; sin embargo, no se centran en estudiar a fondo los problemas de seguridad que algunas de estas le introducirán al IoT, en este aspecto, fue necesario analizar exhaustivamente cada una de las características presentes en los estudios [44], [45], [21], [69], [70], [74], [83], [88]. Finalmente, se determinó que el conocimiento de la ubicación, la distribución geográfica, la arquitectura descentralizada, el soporte de movilidad, la escalabilidad y el consumo energético reducido son las características que servirían de punto de entrada para que se produzcan ataques de seguridad en IoT basado en Edge Computing.

7.1.3. Objetivo 3: Desarrollar el informe de presentación de resultados de la RSL

Para el cumplimiento de este objetivo, se elaboró un artículo científico en el que sé plasmo los resultados obtenidos durante todo el proceso de la SLR. Los resultados expuestos a través de este artículo de revisión servirán como referencia para los investigadores interesados en estudiar, integrar y diseñar soluciones para estas tecnologías (IoT basado en Edge/Fog Computing).

7.2. Valoración técnica, económica, ambiental y social

Para la elaboración del presente Trabajo de Titulación fue necesario hacer uso de tres aspectos.

7.2.1. Valoración técnica

Los recursos técnicos utilizados para el desarrollo del TT se basan en el uso de la herramienta de gestión bibliográfica Mendeley para organizar toda la información recolectada de las diferentes bases de datos científicas, la herramienta de Parsifal que permitió gestionar el proceso de desarrollo de la revisión sistemática, simplificando y automatizando procesos que ayudan a desarrollar la investigación de una manera ordenada, el uso de la herramienta de diagramación Lucidchart, para el desarrollo de los diagramas y esquemas del TT.

7.2.2. Valoración económica

En el desarrollo del presente trabajo de titulación, fue necesaria la inversión de talento humano, recursos tecnológicos, recursos materiales e imprevistos los mismos que se presentan a continuación, en la Tabla 18 a la Tabla 21.

7.2.2.1. Recursos para talento humano

El desarrollo del TT involucró la asesoría de un docente de la carrera como figura de director de trabajo de titulación, cuyo costo es asumido por la Universidad Nacional de Loja.

El tiempo empleado para el desarrollo del presente Trabajo de Titulación es de 800 horas.

Tabla 18. Recursos humanos

Personal	Tiempo (Horas)	Precio/Hora ($)	Valor total ($)
Investigador(alumno)	800	$3	$2,400
Director de TT	350	$12,50	$4,375
Subtotal			$6,775.00

7.2.2.2. Recursos técnicos

Los recursos de hardware y software utilizados para el desarrollo del trabajo de titulación se muestran a continuación en la Tabla 19, representa los bienes necesarios que debe adquirir y asumir el tesista para el desarrollo sin inconvenientes del TT.

Tabla 19. Recursos técnicos

Recurso	Cantidad	Valor unitario	Valor Total
Hardware			
Laptop Toshiba	1	$1,000	$1,000
Pendrive	1	$8,00	$8,00
Impresiones	3	$30,00	$90,00
Software			
Base de datos científicas	4	0,00	$0,00
Mendeley	1	0,00	$0,00
Parsifal	1	$0,00	$0,00
Google Drive	1	$0,00	$0,00
Lucichart	1	$0,00	$0,00
Firma electrónica	1	$22,40	$22,40
		Subtotal	$ 1,120.40

7.2.2.3. Recursos materiales

Para la culminación del trabajo de titulación fue necesario adquirir el servicio de internet y transporte, cuyo valor total es asumidos por el tesista. Los cuales se desglosan a continuación.

Tabla 20. Recursos materiales

Recursos	Cantidad	Valor unitario ($)	Valor total ($)
Internet	12 meses	$20,00	$240,00
Transporte	1 día	$15,00	$30,00
Suministros de oficina	-	$66,00	$66,00
		Subtotal	$336,00

7.2.2.4. Costo aproximado del proyecto

Tomando en cuenta cada uno de los totales y subtotales de las Tablas anteriores se pudo calcular el costo aproximado para el desarrollo del TT. Para imprevistos se tomó un 10% del valor total del presupuesto, los cuales se agregaron al valor total del TT, como se describe en la siguiente Tabla 21.

Tabla 21. Costo aproximado del proyecto

Recursos	Subtotal
Recursos humanos	$6,775.00
Recursos tecnológicos	$1,120.00
Recursos materiales	$336,00
Subtotal ($)	8,231.00
Gastos imprevistos (10%)	$823.10
Total	$9,054.10

7.2.2.5. Valoración ambiental

El presente TT se realizó en su totalidad con recursos tecnológicos y digitales que no tienen un mayor impacto al medio ambiente, además que se tuvo un bajo consumo de recursos materiales como impresiones entre otros que puedan llegar a perjudicar al medio ambiente.

8. Conclusiones

Una vez finalizado el trabajo de titulación, se obtiene las siguientes conclusiones:

- Los problemas de seguridad encontrados y analizados en el IoT como son: ataque DoS, DDoS, hombre en el medio, suplantación de identidad, repetición, colisión, manipulación física, inyección de nodo falso y clonación de dispositivos también afectan y son los más frecuentes en Edge Computing, debido a que este paradigma nace gracias a la existencia de IoT y se implementa sobre la base del mismo, el cual en sí tiene muchas fallas de seguridad, además, de estar conectado a Internet que no es seguro, por lo tanto, la computación perimetral heredaría todos los problemas que engloban IoT.
- Las características del Edge Computing generan también una serie de problemas de seguridad que se han podido identificar dentro de esta investigación, debido a que características como la distribución geográfica, la descentralización, el consumo energético reducido, la escalabilidad y el soporte de movilidad, aumentan la superficie de ataque en el mundo real ya que en algunos casos no se puede implementar la protección de seguridad necesaria tanto a nivel de hardware como de software en los dispositivos IoT.
- A pesar de que Edge Computing ofrece grandes ventajas al IoT aún no se puede afirmar que sea la tecnología que solucionará todos los problemas que padece actualmente la Cloud, debido a que esta tecnología aún se encuentra en investigación; sin embargo, este paradigma demuestra ser muy prometedor ya que se constituye como una alternativa para implementar aplicaciones que requieren de respuestas seguras e inmediatas, también optimiza la carga de los datos que se envían a los servidores centralizados y mejora la privacidad de los datos al evitar que estos viajen fuera de red.
- Los mecanismos de seguridad ampliamente estudiados y utilizados en la computación tradicional no pueden ser implementados directamente en Edge Computing, debido que en su mayoría requieren bastante capacidad computacional; así mismo, debido a la heterogeneidad de los dispositivos que conforman los nodos Edge en los diferentes entornos de aplicación, no es posible diseñar mecanismos de seguridad genéricos para todos los entornos de Edge Computing.

9. Recomendaciones

En base al Trabajo de Titulación desarrollado, se realiza las siguientes recomendaciones:

- Previo al desarrollo de una investigación relacionada con Edge Computing o Fog Computing, se debe estudiar las arquitecturas de referencia (OpenFog y Multiaccess Edge Computing) las cuales permitirán conocer a profundidad el funcionamiento de este nuevo paradigma de la computación.
- Realizar una investigación exploratoria antes de iniciar una SLR para identificar las limitaciones existentes con respecto a documentación y acceso a la información. También elaborar el mentefacto conceptual para organizar las ideas fundamentales que se deben cubrir con el desarrollo de la investigación.
- Utilizar la metodología para la revisión sistemática de literatura aplicada a la ingeniería y educación propuesta por Torres-Carrión, puesto que es una adaptación de Kitchenham y Bacca la cual divide el proceso de la investigación en tres fases bien detalladas facilitando de esta manera el proceso de revisión sistemática, además, presenta una descripción general de la aplicación del método en un caso real que sirve como guía para el investigador que no tiene experiencia en realizar SLR.
- Utilizar herramientas de vanguardia que apoyan el desarrollo de revisiones sistemáticas de literatura como Parsifal, que permite identificar y descartar de forma efectiva los documentos que se encuentran duplicados en las diferentes bases de datos.

9.1. Trabajos futuros

- Realizar una investigación sobre el uso de Blockchain como mecanismo de seguridad para solucionar los problemas asociados con la computación perimetral o Edge Computing.
- Realizar una investigación sobre las principales plataformas para Edge Computing tanto privativas como de código abierto para identificar qué servicios y mecanismos de seguridad se pueden implementar.
- Realizar un análisis del control de acceso de grano fino y grano grueso para determinar cuál es el más conveniente para ser implementado en sistemas Edge.

10. Bibliografía

[1] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data Security and Privacy-Preserving in Edge Computing Paradigm : Survey and Open Issues,” *IEEE Access*, vol. 6, no. Idc, pp. 18209–18237, 2018, doi: 10.1109/ACCESS.2018.2820162.

[2] L. S. Vailshery, “statista: Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030.” 2021, [Online]. Available: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.

[3] B. Jovanović, “Internet of Things statistics for 2021 – Taking Things Apart @ dataprot.net.” 2021, [Online]. Available: https://dataprot.net/statistics/iot-statistics/#:~:text=Key IoT statistics,surpass 25.4 billion in 2030.&text=The consumer IoT market is,at a CAGR of 17%25.

[4] M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, “Edge Computing Perspectives : Architectures , Technologies , and Open Security Issues,” *2019 IEEE Int. Conf. Edge Comput.*, pp. 116–123, doi: 10.1109/EDGE.2019.00035.

[5] O. Mounnan, A. El Mouatasim, O. Manad, T. Hidar, A. A. El Kalam, and N. Idboufker, “Privacy-Aware and Authentication based on Blockchain with Fault Tolerance for IoT enabled Fog Computing,” *2020 5th Int. Conf. Fog Mob. Edge Comput. FMEC 2020*, pp. 347–352, 2020, doi: 10.1109/FMEC49853.2020.9144845.

[6] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, “Edge Computing Security: State of the Art and Challenges,” *Proc. IEEE*, vol. 107, no. 8, 2019, doi: 10.1109/JPROC.2019.2918437.

[7] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, “FlowGuard: An Intelligent Edge Defense Mechanism against IoT DDoS Attacks,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9552–9562, 2020, doi: 10.1109/JIOT.2020.2993782.

[8] A. Rauf, R. A. Shaikh, and A. Shah, “Security and privacy for IoT and fog computing paradigm,” *2018 15th Learn. Technol. Conf. L T 2018*, pp. 96–101, 2018, doi: 10.1109/LT.2018.8368491.

[9] P. M. Bocco Marcela , Cruz José, “Métodos de investigación en ingeniería del software.Pdf.” 2014.

[10] O. Kaiwartya *et al.*, “Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects,” *IEEE Access*, vol. 4, pp. 5356–5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[11] P. V. Torres-Carrion, C. S. Gonzalez-Gonzalez, S. Aciar, and G. Rodriguez-Morales, “Methodology for systematic literature review applied to engineering and education,” *IEEE Glob. Eng. Educ. Conf. EDUCON*, vol. 2018-April, no. April, pp. 1364–1373, 2018, doi: 10.1109/EDUCON.2018.8363388.

[12] F. J. Rodríguez Sedano, “Uso De Herramienta on-Line Para La Elaboración De Una Revisión Sistemática De La Literatura (Slr),” 2019, doi: 10.5281/zenodo.2603914.

[13] M. D. Medina Barroso, “Edge computing para IoT,” 2019, [Online]. Available: http://hdl.handle.net/10609/91207.

[14] G. Premsankar, M. Di Francesco, and T. Taleb, “Edge Computing for the Internet of Things: A Case Study,” *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1275–1284, 2018, doi: 10.1109/JIOT.2018.2805263.

[15] A. Hameed and A. Alomary, “Security issues in IoT: A survey,” *2019 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2019*, pp. 1–5, 2019, doi: 10.1109/3ICT.2019.8910320.

[16] G. B. W. Atlam, Hany F, Robert J. Walters, “Fog Computing and the Internet of Things : A Review,” pp. 1–18, 2018, doi: 10.3390/bdcc2020010.

[17] J. S. Ros, N. Rodríguez, M. Montiveros, M. Murazzo, and M. M. Garabetti, “Análisis de las Topologías IoT en Entornos Fog Computing mediante simulación,” pp. 90–100, 2018, [Online]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/69946/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y.

[18] P. Sethi and S. R. Sarangi, “Internet of Things : Architectures , Protocols , and Applications,” vol. 2017, 2017.

[19] D. C.-M. J. LÓPEZ-DE-ARMENTIA, “El Internet de las Cosas y la sostenibilidad medioambiental- revistaingenieria deusto.” [Online]. Available: https://revistaingenieria.deusto.es/tag/iot/.

[20] I. Sittón, R. S. Alonso, L. Múñoz, and S. Rodríguez, “Arquitecturas de Referencia Edge Computing para la Industria 4.0: una revisión,” 2019.

[21] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing Fog Computing for Internet of Things Applications: Challenges and Solutions,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 601–628, 2018, doi: 10.1109/COMST.2017.2762345.

[22] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things,” *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–18, 2020, doi: 10.1109/JIOT.2020.3015432.

[23] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge Computing: Vision and Challenges,” *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, 2016, doi: 10.1109/JIOT.2016.2579198.

[24] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things : Architecture , Enabling Technologies , Security and Privacy , and Applications,” vol. 4662, no. c, pp. 1–17, 2017, doi: 10.1109/JIOT.2017.2683200.

[25] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, “ETSI White Paper #11

Mobile Edge Computing - A key technology towards 5G," *ETSI White Pap. No. 11 Mob.*, vol. 11, no. 11, pp. 1–16, 2015, [Online]. Available: http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf.

[26] D. Satria, D. Park, and M. Jo, "Recovery for overloaded mobile edge computing," *Futur. Gener. Comput. Syst.*, vol. 70, pp. 138–147, 2017, doi: 10.1016/j.future.2016.06.024.

[27] Y. Jararweh, A. Doulat, O. Alqudah, E. Ahmed, M. Al-Ayyoub, and E. Benkhelifa, "The future of mobile cloud computing: Integrating cloudlets and Mobile Edge Computing," *2016 23rd Int. Conf. Telecommun. ICT 2016*, 2016, doi: 10.1109/ICT.2016.7500486.

[28] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, 2018, doi: 10.1109/JIOT.2017.2750180.

[29] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018, doi: 10.1109/COMST.2018.2849509.

[30] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017, doi: 10.1109/COMST.2017.2705720.

[31] R. Architecture, "Multi-access Edge Computing (MEC)," vol. 1, pp. 1–21, 2019.

[32] OpenfogConsortium, "OpenFog Reference Architecture for Fog Computing Produced," *Ref. Archit.*, no. February, pp. 1–162, 2017.

[33] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog Computing for the Internet of Things : A Survey," vol. 19, no. 2, 2019.

[34] F. Liu, G. Tang, Y. Li, Z. Cai, X. Zhang, and T. Zhou, "A Survey on Edge Computing Systems and Tools," *Proc. IEEE*, pp. 1–24, 2019, doi: 10.1109/JPROC.2019.2920341.

[35] J. Liang, F. Liu, S. Li, and Z. Cai, *A Comparative Research on Open Source Edge Computing Systems*, vol. 11633 LNCS. Springer International Publishing, 2019.

[36] LFEDGE, "Akraino Edge Statck. https://www.akraino.org." [Online]. Available: https://www.lfedge.org/projects/akraino/.

[37] H. Ning, Y. Li, F. Shi, and L. T. Yang, "Heterogeneous edge computing open platforms and tools for internet of things," *Futur. Gener. Comput. Syst.*, vol. 106, pp. 67–76, 2020, doi: 10.1016/j.future.2019.12.036.

[38] Oktaviani.J, "Azure IoT Edge Documentation," *Sereal Untuk*, vol. 51, no. 1, p. 51, 2018.

[39] Z. Galvis, "Tipos de Investigación," 2006.

[40] Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007.

[41] Cisco, “Cisco Annual Internet Report - Cisco,” 2020. https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html (accessed Jun. 17, 2020).

[42] Petticrew y Roberts, *Systematic Reviews in the Social Sciences*. 2006.

[43] W. Yu *et al.*, “A Survey on the Edge Computing for the Internet of Things,” *IEEE Access*, vol. 6, pp. 6900–6919, 2017, doi: 10.1109/ACCESS.2017.2778504.

[44] M. Jalasri and D. L. Lakshmanan, “A survey: Integration of iot and fog computing,” *Proc. 2nd Int. Conf. Green Comput. Internet Things, ICGCIoT 2018*, pp. 235–239, 2018, doi: 10.1109/ICGCIoT.2018.8753010.

[45] N. S. Khan and M. A. Chishti, “Security challenges in fog and iot, blockchain technology and cell tree solutions: A review,” *Scalable Comput.*, vol. 21, no. 3, pp. 515–541, 2020, doi: 10.12694:/scpe.v21i3.1782.

[46] R. Verma and S. Chandra, “A Systematic Survey on Fog steered IoT: Architecture, Prevalent Threats and Trust Models,” *Int. J. Wirel. Inf. Networks*, no. 0123456789, 2020, doi: 10.1007/s10776-020-00499-z.

[47] L. Codina, A. Morales-Vargas, R. Rodríguez-Martínez, and M. Pérez-Montoro, “Uso de Scopus y Web of Science para investigar y evaluar en comunicación social: análisis comparativo y caracterización,” *Index Comun.*, vol. 10, no. 3, pp. 235–261, 2020, doi: 10.33732/ixc/10/03usodes.

[48] D. Yang, A. N. Zhang, and W. Yan, “Performing literature review using text mining, Part I: Retrieving technology infrastructure using Google Scholar and APIs,” *Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017*, vol. 2018-Janua, pp. 3290–3296, 2017, doi: 10.1109/BigData.2017.8258313.

[49] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering - A systematic literature review,” *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[50] B. Kitchenham, “Procedures for Performing Systematic Literature Reviews,” *Jt. Tech. Report, Keele Univ. TR/SE-0401 NICTA TR-0400011T.1*, p. 33, 2004, [Online]. Available: https://pdfs.semanticscholar.org/2989/0a936639862f45cb9a987dd599dce9759bf5.pdf.

[51] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, “Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network,” *IEEE Access*, vol. 6, no. November, pp. 73713–73723, 2018, doi: 10.1109/ACCESS.2018.2884293.

[52] S. Misra, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan, “Blockchain at the Edge: Performance of Resource-Constrained IoT Networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 174–183, 2021, doi: 10.1109/TPDS.2020.3013892.

[53] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, “Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices,” *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, 2020, doi: 10.1109/JIOT.2020.2970501.

[54] D. E. D. Abou-Tair, S. Büchsenstein, and A. Khalifeh, “A fog computing-based framework for privacy preserving IoT environments,” *Int. Arab J. Inf. Technol.*, vol. 17, no. 3, pp. 306–314, 2020, doi: 10.34028/iajit/17/3/4.

[55] J. Ni, X. Lin, and X. S. Shen, “Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives,” *IEEE Netw.*, vol. 33, no. 2, pp. 50–57, 2019, doi: 10.1109/MNET.2019.1800229.

[56] S. Shapsough, F. Aloul, and I. A. Zualkernan, “Securing Low-Resource Edge Devices for IoT Systems,” *2018 Int. Symp. Sens. Instrum. IoT Era, ISSI 2018*, no. September, 2018, doi: 10.1109/ISSI.2018.8538135.

[57] U. Guin, P. Cui, and A. Skjellum, “Ensuring Proof-of-Authenticity of IoT Edge Devices Using Blockchain Technology,” *Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree*, pp. 1042–1049, 2018, doi: 10.1109/Cybermatics_2018.2018.00193.

[58] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, “Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment,” *Sensors (Switzerland)*, vol. 20, no. 5, pp. 1–27, 2020, doi: 10.3390/s20051300.

[59] J. Pacheco, V. H. Benitez, L. C. Felix-Herran, and P. Satam, “Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes,” *IEEE Access*, vol. 8, pp. 73907–73918, 2020, doi: 10.1109/ACCESS.2020.2988055.

[60] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, “An anomaly mitigation framework for iot using fog computing,” *Electron.*, vol. 9, no. 10, pp. 1–24, 2020, doi: 10.3390/electronics9101565.

[61] M. Al-Hawawreh, F. Den Hartog, and E. Sitnikova, “Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things,” *IEEE Internet Things J.*, vol. 6, no. 4, pp. 7137–7151, 2019, doi: 10.1109/JIOT.2019.2914390.

[62] M. Wazid, P. Reshma Dsouza, A. K. Das, V. Bhat K, N. Kumar, and J. J. P. C. Rodrigues, “RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment,” *Int. J. Commun. Syst.*, vol. 32, no. 15, pp. 1–20, 2019, doi: 10.1002/dac.4024.

[63] S. Sathyadevan, K. Achuthan, R. Doss, and L. Pan, “Protean Authentication Scheme-A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments,” *IEEE Access*, vol. 7, pp. 92419–92435, 2019, doi:

10.1109/ACCESS.2019.2927818.

[64] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, “LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based iot deployment,” *Sensors (Switzerland)*, vol. 19, no. 24, pp. 1–21, 2019, doi: 10.3390/s19245539.

[65] R. Fantacci, F. Nizzi, T. Pecorella, L. Pierucci, and M. Roveri, “False data detection for fog and internet of things networks,” *Sensors (Switzerland)*, vol. 19, no. 19, pp. 1–19, 2019, doi: 10.3390/s19194235.

[66] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, “Botnet attack detection at the IoT edge based on sparse representation,” *Glob. IoT Summit, GIoTS 2019 - Proc.*, pp. 1–6, 2019, doi: 10.1109/GIOTS.2019.8766388.

[67] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, “A mechanism for securing IoT-enabled applications at the fog layer,” *J. Sens. Actuator Networks*, vol. 8, no. 1, 2019, doi: 10.3390/jsan8010016.

[68] M. Ozcelik, N. Chalabianloo, and G. Gur, “Software-Defined Edge Defense Against IoT-Based DDoS,” *IEEE CIT 2017 - 17th IEEE Int. Conf. Comput. Inf. Technol.*, pp. 308–313, 2017, doi: 10.1109/CIT.2017.61.

[69] R. Verma and S. Chandra, “Security and Privacy Issues in Fog driven IoT Environment,” *Int. J. Comput. Sci. Eng.*, vol. 7, no. 5, pp. 367–370, 2019, doi: 10.26438/ijcse/v7i5.367370.

[70] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, 2021, doi: 10.1109/JIOT.2020.3015432.

[71] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, “Towards IoT-DDoS prevention using edge computing,” *USENIX Work. Hot Top. Edge Comput. HotEdge 2018, co-located with USENIX ATC 2018*, 2018.

[72] I. S. Lei, S. K. Tang, I. K. Chao, and R. Tse, “Self-recovery service securing edge server in iot network against ransomware attack,” *IoTBDS 2020 - Proc. 5th Int. Conf. Internet Things, Big Data Secur.*, no. January, pp. 399–404, 2020, doi: 10.5220/0009470303990404.

[73] X. Qiu, B. Rong, J. Ben-Othman, S. Han, and M. Kodach, “An Edge-Driven Security Framework for Intelligent Internet of Things,” *IEEE Netw.*, vol. 34, no. 5, pp. 6–7, 2020, doi: 10.1109/MNET.2020.9199784.

[74] S. Shen, K. Zhang, Y. Zhou, and S. Ci, “Security in edge-assisted Internet of Things: challenges and solutions,” *Sci. China Inf. Sci.*, vol. 63, no. 12, pp. 1–14, 2020, doi: 10.1007/s11432-019-2906-y.

[75] Z. Chen, H. Cui, E. Wu, Y. Li, and Y. Xi, “Secure Distributed Data Management for Fog

Computing in Large-Scale IoT Application: A Blockchain-Based Solution," *2020 IEEE Int. Conf. Commun. Work. ICC Work. 2020 - Proc.*, pp. 0–5, 2020, doi: 10.1109/ICCWorkshops49005.2020.9145381.

[76] D. Kim, V. Andalibi, and L. J. Camp, "Fingerprinting edge and cloud services in IoT," *Proc. - 2020 13th Syst. Approaches to Digit. Forensic Eng. SADFE 2020*, pp. 13–21, 2020, doi: 10.1109/SADFE51007.2020.00011.

[77] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices," *Pervasive Mob. Comput.*, vol. 67, p. 101194, 2020, doi: 10.1016/j.pmcj.2020.101194.

[78] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, "BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0," *IEEE Consum. Electron. Mag.*, vol. 2248, no. c, 2020, doi: 10.1109/MCE.2020.3038040.

[79] J. K. Mudhar, S. Kalra, and J. Malhotra, "An Efficient Blockchain Based Authentication Scheme to Secure Fog Enabled IoT Devices," *Indo - Taiwan 2nd Int. Conf. Comput. Anal. Networks, Indo-Taiwan ICAN 2020 - Proc.*, pp. 75–80, 2020, doi: 10.1109/Indo-TaiwanICAN48429.2020.9181356.

[80] T. A. Ahanger, U. Tariq, and M. Nusir, "Real-Time Methodology for Improving Cyber Security in Internet of Things Using Edge Computing During Attack Threats," *Second Int. Conf. Smart Syst. Inven. Technol.*, no. Icssit, pp. 293–297, 2019.

[81] F. De Rango, M. Tropea, and P. Fazio, "Mitigating DoS attacks in IoT EDGE Layer to preserve QoS topics and nodes' energy," *IEEE INFOCOM 2020 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2020*, pp. 842–847, 2020, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162902.

[82] S. R. Zahra and M. A. Chishti, "Fuzzy logic and Fog based Secure Architecture for Internet of Things (FLFSIoT)," *J. Ambient Intell. Humaniz. Comput.*, 2020, doi: 10.1007/s12652-020-02128-2.

[83] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, 2019, doi: 10.1109/JIOT.2019.2897619.

[84] A. N. I. O. T. Ic, M. De Donno, and N. Dragoni, "Combining A NTIB I O T IC with Fog Computing : ANTIBIOTIC 2.0," pp. 1–6, 2019.

[85] S. J. Lee *et al.*, "IMPACT: Impersonation Attack Detection via Edge Computing Using Deep Autoencoder and Feature Abstraction," *IEEE Access*, vol. 8, pp. 65520–65529, 2020, doi: 10.1109/ACCESS.2020.2985089.

[86] M. Arun, S. Balamurali, B. S. Rawal, Q. Duan, R. L. Kumar, and B. Balamurugan, "Mutual authentication and authorized data access between fog and user based on

blockchain technology," *IEEE INFOCOM 2020 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2020*, pp. 37–42, 2020, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162915.

[87] C. Zhou, A. Fu, S. Yu, W. Yang, H. Wang, and Y. Zhang, "Privacy-Preserving Federated Learning in Fog Computing," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10782–10793, 2020, doi: 10.1109/JIOT.2020.2987958.

[88] A. K. Junejo, N. Komninos, and J. A. McCann, "A Secure Integrated Framework for Fog-Assisted Internet-of-Things Systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6840–6852, 2021, doi: 10.1109/JIOT.2020.3035474.

[89] O. H. Ahmed, J. Lu, A. M. Ahmed, A. M. Rahmani, M. Hosseinzadeh, and M. Masdari, "Scheduling of scientific workflows in multi-fog environments using markov models and a hybrid salp swarm algorithm," *IEEE Access*, vol. 8, pp. 189404–189422, 2020, doi: 10.1109/ACCESS.2020.3031472.

[90] M. Mukherjee, M. A. Ferrag, L. Maglaras, A. Derhab, and M. Aazam, "Security and privacy issues and solutions for fog," *Fog Fogonomics Challenges Pract. Fog Comput. Commun. Networking, Strateg. Econ.*, pp. 353–374, 2020, doi: 10.1002/9781119501121.ch14.

[91] L. Wang, H. An, and Z. Chang, "Security Enhancement on a Lightweight Authentication Scheme with Anonymity Fog Computing Architecture," *IEEE Access*, vol. 8, pp. 97267–97278, 2020, doi: 10.1109/ACCESS.2020.2996264.

[92] Y. Ding, Y. Shi, A. Wang, X. Zheng, Z. Wang, and G. Zhang, "Adaptive Chosen-Plaintext Collision Attack on Masked AES in Edge Computing," *IEEE Access*, vol. 7, pp. 63217–63229, 2019, doi: 10.1109/ACCESS.2019.2916553.

[93] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, and Z. Ye, "FOCUS: A fog computing-based security system for the Internet of Things," *CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf.*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/CCNC.2018.8319238.

[94] G. Potrino, F. De Rango, and P. Fazio, "A Distributed Mitigation Strategy against DoS attacks in Edge Computing," *Wirel. Telecommun. Symp.*, vol. 2019-April, pp. 1–7, 2019, doi: 10.1109/WTS.2019.8715543.

11. Anexos

11.1. Anexo 1: Artículos evaluados con las preguntas de calidad

En la siguiente Tabla se muestra la aplicación de la evaluación de calidad aplicada a cada artículo.

Tabla 22. Aplicación de preguntas de calidad

N° Artículo	P1	P2	P3	P4	Puntaje
1	1	1	0.0	1	**3**
2	0.5	0.5	1	0.0	**2**
3	1	1	1	0.0	**3**
4	1	1	0.0	1	**3**
5	0.5	0.5	0.0	0.0	**1**
6	1	1	0.5	0.0.	**2.5**
7	1	1	0.0	0.0	**2**
8	0.5	0.5	0.5	0.0	**1.5**
9	1	1	0.5	0.0	**2.5**
10	1	1	0.0	0.0	**2**
11	0.5	0.0	0.0	0.0	**0.5**
12	1	1	1	1	**4**
13	1	1	1	0.0	**3**
14	1	0.5	0.0	0.0	**1.5**
15	0.5	0.0	0.0	0.0	**0.5**
16	0.5	0.5	0.0	0.5	**1.5**
17	0.0	0.0	1	0.0	**1**
18	1	1	1	0.0	**3**
19	1	1	1	0.0	**3**
20	0.5	0.5	0.0	0.5	**1.5**
21	0.5	0.0	1	0.0	**1.5**
22	0.5	0.0	0.0	0.0	**0.5**
23	0.5	0.5	0.0	0.0	**1**
24	0.5	0.0	0.0	0.0	**0.5**
25	1	0.0	0.0	0.0	**1**
26	0.5	0.0	0.0	0.0	**0.5**
27	0.0	0.5	0.0	0.0	**0.5**
28	0.5	0.5	0.0	0.0	**1**
29	1	1	0.0	1	**3**
30	0.5	0.5	0.0	0.0	**1**
31	1	1	0.0	1	**3**
32	0.0	0.5	0.5	0.0	**1**
33	0.5	0.0	0.0	0.0	**0.5**

34	0.5	0.5	0.0	0.0	**1**
35	1	1	0.0	0.0	**2**
36	0.5	0.5	0.0	0.5	**1.5**
37	0.0	0.5	0.0	0.0	**0.5**
38	0.5	0.5	0.0	0.0	**1**
39	0.5	0.5	0.0	0.5	**1.5**
40	0.5	0.5	0.0	0.5	**1.5**
41	1	1	0.0	0.0	**2**
42	1	1	0.0	1	**3**
43	1	1	0.0	0.0	**2**
44	1	1	0.0	1	**3**
45	1	1	0.0	0.0	**2**
46	0.5	0.5	0.0	1	**1.5**
47	1	0.0	0.0	0.0	**1**
48	1	1	0.0	0.0	**2**
49	0.5	0.5	0.0	0.5	**1.5**
50	0.5	0.0	0.0	1	**1.5**
51	0.5	0.5	0.0	0.0	**1**
52	0.5	0.5	0.5	0.0	**1.5**
53	0.5	0.0	0.0	0.5	**1**
54	0.5	0.0	0.0	1	**1.5**
55	1	1	1	0.0	**3**
56	0.5	0.5	0.5	0.0	**1.5**
57	0.5	0.5	0.5	0.0	**1.5**
58	0.5	0.5	0.0	0.5	**1.5**
59	0.5	0.5	0.0	0.5	**1.5**
60	0.5	0.0	0.0	1	**1.5**
61	0.5	0.5	0.0	0.5	**1.5**
62	0.5	0.0	0.0	0.0	**0.5**
63	1	1	0.0	1	**3**
64	0.5	0.5	0.0.	0.5	**1.5**
65	0.5	0.5	1	0.0	**2**
66	0.5	0.0	0.0	1	**1.5**
67	0.5	0.5	0.0	0.0	**1**
68	1	1	0.0	1	**3**
69	1	0.0	0.0	0.5	**1.5**
70	0.5	0.0	0.0	1	**1.5**
71	1	1	0.0	1	**3**
72	0.5	0.5	0.5	0.0	**1.5**

73	1	1	0.0	1	**3**
74	0.5	0.5	0.0	0.5	**1.5**
75	0.5	0.5	0.0	0.0	**1**
76	1	1	0.0	0.0	**2**
77	0.5	0.5	0.0	0.0	**1**
78	1	1	1	0.0	**3**
79	1	1	0.0	0.0	**2**
80	1	1	0.0	0.0	**2**
81	0.5	0.5	0.0	0.5	**1.5**
82	1	1	0.0	0.0	**2**
83	1	1	0.0	0.0	**2**
84	1	1	0.0	0.5	**2.5**
85	1	0.5	0.0	0.0	**1.5**
86	1	1	0.0	0.0	**2**
87	0.5	0.0	0.0	1	**1.5**
88	0.5	0.5	0.0	0.5	**1.5**
89	1	1	0.0	1	**3**
90	0.5	0.0	0.0	1	**1.5**
91	0.5	0.0	0.0	1	**1.5**
92	0.0	0.5	0.0	1	**1.5**
93	0.5	0.5	0.0	0.5	**1.5**
94	1	1	0.0	0.0	**2**
95	0.5	0.5	0.0	0.5	**1.5**
96	1	1	0.0	0.0	**2**
97	0.5	0.0	0.0	1	**1.5**
98	0.5	0.0	0.0	1	**1.5**
99	0.5	0.5	0.0	0.0	**1**
100	0.5	0.5	0.0	0.5	**1.5**
101	0.5	0.5	0.0	0.0	**1**
102	0.5	0.5	0.0	0.5	**1.5**
103	0.5	0.5	0.0	0.5	**1.5**
104	0.5	0.5	0.0	0.5	**1.5**
105	0.0	1	0.0	0.0	**1**
106	1	1	1	0.0	**3**
107	1	0.5	0.0	0.0	**1.5**
108	0.5	0.5	0.0	0.5	**1.5**
109	1	1	0.0	1	**3**
110	0.5	0.0	0.0	1	**1.5**
111	0.5	0.5	0.0	0.5	**1.5**

112	0.0	1	0.0	0.0	**1**
113	0.5	0.5	0.0	0.5	**1.5**
114	0.5	0.5	0.0	0.0	**1**
115	05	0.5	0.0	0.5	**1.5**
116	0.0	0.5	0.0	0.5	**1**
117	0.5	0.5	0.5	0.0	**1.5**
118	0.0	0.0	0.0	0.0	**0**
119	1	1	0.0	0.0	**2**
120	0.0	0.5	0.0	1	**1.5**
121	0.5	0.5	0.0	1	**2**
122	0.0	0.5	0.0	1	**1.5**
123	1	1	0.0	0.0	**2**
124	0.5	0.5	0.0	0.5	**1.5**
125	1	1	1	1	**4**
126	0.5	0.5	0.0	0.5	**1.5**
127	1	1	0.0	0.0	**2**
128	0.5	0.5	0.0	0.5	**1.5**
129	1	1	1	0.0	**3**
130	1	1	0.0	1	**3**
131	1	1	0.0	0.0	**2**
132	0.5	0.5	0.0	0.0	**1**
133	0.5	0.5	0.0	0.5	**1.5**
134	1	1	0.0	1	**3**
135	0.5	0.5	0.0	0.5	**1.5**
136	1	1	0.0	0.0	**2**

11.2. Anexo 2: Formularios de extracción de datos

En las siguientes Tablas se muestra la información extraída de cada uno de los estudios seleccionados.

Tabla 23. Resultado del artículo ES01

#	Descripción	Detalle	Código: ES01
1	Información bibliográfica	Título	Passban IDS: Un sistema inteligente de detección de intrusos basado en anomalías para dispositivos IoT Edge
		Autores	Eskandari, Mojtaba, Janjua, Zaffar Haider, Vecchio, Massimo, Antonelli, Fabio
		Referencia	[53]
		Año	2020
2	Resumen del artículo	En este estudio proponen un Sistema de Detección de Intrusiones (IDS) inteligente Passban capaz de proteger los dispositivos IoT que están conectados directamente a él; demostrando que es capaz de detectar varios tipos de tráfico malicioso, incluido el escaneo de puertos, fuerza bruta vía HTTP y SSH, y ataques de inundación SYN, con tasas muy bajas de falsos positivos y precisiones satisfactorias. Además, mediante Machine Learning usando dos técnicas de clasificación iForest y LOF lograron puntuaciones F1 (métrica para medir el rendimiento de un algoritmo de clasificación) mayor al 90% en algunos ataques y otros oscilan entre 79% y 99%. En cuanto a uso de recursos de hardware demostraron que se puede ejecutar en placas de puerta de enlace IoT económicas como la Raspberry Pi 3 modelo B con una interfaz de red de 40 a 50Mb/s.	
3	Información relevante	Cuando el sistema está bajo un ataque inundación SYN, los recursos computacionales de la puerta de enlace se agotan y, por lo tanto, la tasa de detección de Passban es menor que su tasa de detección para otros tipos de ataques.	

Tabla 24. Resultado del artículo ES02

#	Descripción	Detalle	Código: ES02
1	Información bibliográfica	Título	Hacia una Internet de los objetos asistida por Edge: Desde la perspectiva de la seguridad y la eficiencia
		Autores	Ni, Jianbing, Lin, Xiaodong, Shen, Xuemin Sherman
		Referencia	[55]
		Año	2019
2	Resumen del artículo	En este estudio se examina y explora la arquitectura de la Computación de Borde Móvil (MEC), ya que MEC enfrenta variedad de ataques cibernéticos en los protocolos de comunicación WPA2 y TLS1.0; como ejemplo están los ataques DDoS, ya que un atacante es capaz de inundar un nodo Fog con solicitudes de datos innecesarios; como resultado, este nodo Fog no tendría recursos suficientes para gestionar con normalidad sus dispositivos. Para evitar la corrupción de los dispositivos durante la transmisión se añaden firmas digitales, además se requieren cálculos adicionales para ser cifrados de extremo a extremo, para evitar la fuga de datos; mediante la agregación segura de datos, cada dispositivo antes de enviar sus datos a los nodos de niebla primero los encripta usando un esquema criptográfico homomórfico, como el criptosistema Paillier, BGN, El Gamal o BGV.	
3	Información relevante	Existe redundancia en la gran cantidad de datos producidos por los dispositivos, para esto se incorpora la deduplicación segura de datos para permitir que los intermediarios detecten y descarten los datos replicados de diferentes dispositivos sin tener ningún conocimiento sobre los datos.	

Tabla 25. Resultado del artículo ES03

#	Descripción	Detalle	Código: ES03
1	Información bibliográfica	Título	Marco controlado por la SDN asistid por Fog para la detección duradera de anomalías en una red IoT
		Autores	Shafi, Qaisar, Basit, Abdul, Qaisar, Saad Koay, Abigail, Welch, Ian
		Referencia	[51]
		Año	2018
2	Resumen del artículo	Este estudio presenta algunos ataques hacia dispositivos IoT que se deben atenuar: DoS, escaneo de puertos, escaneo de red, flujos alfa y multitud de cenizas. Así mismo, propone una solución basada en la implementación de un marco de detección de intrusiones asistido por niebla en el borde agregando una capa de administración sobre la niebla que se encarga de la escala de la red de IoT y asigna los recursos computacionales necesarios para la detección de ataques. Este plano de gestión también se coordina con el plano de control impulsado por SDN (Redes definidas por software)	

		de la red de IoT para instalar reglas de flujo adecuadas para la mitigación de ataques. Otra solución propuesta está basada en la arquitectura de SDN que proporciona capacidad de programación y flexibilidad para varios entornos de red, por ejemplo, Edge y Core. El entorno basado en SDN responde a los cambios en la red debido a su naturaleza adaptativa, utilizando el equilibrio de carga y la aplicación de políticas en el paradigma SDN.
3	Información relevante	La arquitectura de Sistema de Prevención y Detección de Intrusiones (IDPS) propuesta en este estudio, emplea clasificadores de aprendizaje automático que, después de entrenar sobre el conjunto de datos UNSW-NB15, pueden detectar múltiples amenazas e invocar el controlador SDN para instalar dinámicamente medidas preventivas. El controlador SDN instala reglas de flujo adecuadas en los conmutadores del borde de la red para controlar la interrupción del tráfico de ataque.

Tabla 26. Resultado del artículo ES04

#	**Descripción**	**Detalle**	**Código: ES04**
1	Información bibliográfica	Título	Un marco basado en Edge Computing para la preservación de la privacidad en entornos IoT
		Autores	Abou-Tair, Dhiah El Diehn, Büchsenstein, Simon, Khalifeh, Ala'
		Referencia	[54]
		Año	2020
2	Resumen del artículo	En este estudio, se propone un marco de protección de seguridad y privacidad, que utiliza la Fog y la Cloud Computing junto con dispositivos de IoT. El marco consiste en un conjunto de dispositivos IoT conectados con el proveedor de servicios a través de una capa intermedia que consiste en un conjunto de dispositivos Fog, los cuales son responsables de establecer conexiones seguras con el proveedor de servicios en la nube, tomando en consideración la privacidad del usuario. Si se da un ataque a la capa Fog el pirata informático puede deshabilitar la comunicación entre esta capa, el dispositivo IoT y la capa de la cloud, afectando así la confiabilidad del sistema y provocando un ataque DoS, sin embargo, no podrá acceder a la información del usuario ya que está encriptada en el dispositivo IoT; es similar a lo que ocurriría si el ataque va dirigido al servidor de seguridad o la cloud ya que esta información esta encriptada, finalmente, si el atacante consigue acceder a los datos de la nube, estos no le servirían ya que no puede utilizar los ID de los usuarios para solicitar datos, ni descifrarlos sin su subclave asociada y almacenada en el servidor de seguridad.	

		Por lo tanto, la capa Fog y los dispositivos de IoT son las partes más críticas que pueden verse comprometidas, siendo importante que deban monitorearse, actualizarse, mantenerse e inspeccionarse para evitar ser expuestos a fallos de seguridad.
3	Información relevante	Un punto débil en la conexión de los dispositivos IoT y Fog es la dependencia de Bluetooth como tecnología inalámbrica, siendo insegura especialmente en el proceso de emparejamiento, ya que establece información clave en ambos dispositivos; este proceso es vulnerable al ataque (MITM).Existen algunos métodos para prevenir esta amenaza potencial como usar un emparejamiento fuera de banda como, por ejemplo, Near Field Communication (NFC), que tiene un rango pequeño de aproximadamente 10 cm, siendo mucho más seguro ante cualquier ataque MITM.

Tabla 27. Resultado del artículo ES05

#	**Descripción**	**Detalle**	**Código: ES05**
1	Información bibliográfica	Título	Blockchain en el borde: rendimiento de las redes de IoT con recursos limitados.
		Autores	Misra, Sudip, Mukherjee, Anandarup, Roy, Arijit, Saurabh, Nishant, Rahulamathavan, Yogachandran, Rajarajan, Muttukrishnan
		Referencia	[52]
		Año	2020
2	Resumen del artículo	En la investigación realizada en este estudio se presenta una solución basada en el uso de Blockchain para la seguridad de los datos en los dispositivos IoT, vulnerabilidades como: contraseñas débiles o codificadas, segmentos de red inseguros, interfaces mal protegidas, mecanismos de acceso a datos no seguros, mecanismos de transferencia de datos inseguros y otros desafíos, hacen que la mayoría de los dispositivos de IoT sean propensos a una fácil manipulación y ruptura. El trabajo propuesto establece la viabilidad de usar dispositivos IoT cotidianos como nodos de Blockchain y se pueden usar como nodos para diferentes marcos de Blockchain. Esta implementación, además, permite la integración de características de seguridad de cifrado basado en atributos (ABE) y otros algoritmos de cifrado sobre la cadena de bloques propuesta a través de contratos inteligentes. Como Blockchain está formado por una cadena de bloques de tal manera que mientras más nodos trabajen en la cadena de bloques abra mayor seguridad en caso de que el servidor de tiempo o cualquier mensaje generado a partir de él se vea comprometido o alterado, los nodos de IoT que forman la cadena de bloques se disociarán, lo	

		que provocará la ruptura de la cadena de bloques y se evitara que se lleve a cabo alguna acción maliciosa.
3	Información relevante	Las características que poseen los dispositivos IoT en Edge, se enfocan principalmente en garantizar conectividad de bajo consumo y computación básica, una parte significativa de estos dispositivos Edge es que no posee suficiente poder de procesamiento o recursos para albergar mecanismos de seguridad de red convencionales lo que los convierte en dispositivos vulnerables a cualquier problema de seguridad.

Tabla 28. Resultado del artículo ES06

#	**Descripción**	**Detalle**		**Código: ES06**
1	Información bibliográfica	Título	Garantizar la prueba de autenticidad de los dispositivos IoT Edge mediante la tecnología Blockchain	
		Autores	Guin, Ujjwal, Cui, Pinchen, Skjellum, Anthony	
		Referencia	[57]	
		Año	2018	
2	Resumen del artículo	En este estudio los autores proponen el uso de la tecnología Blockchain(distributed ledger) para resolver la amenaza de dispositivos impostores, ya que cualquier dispositivo restringido y de bajo costo puede ser falsificado o clonado, la tecnología propuesta en este artículo se emplea para llevar a cabo la autenticación de los dispositivos, identificando cada dispositivo perimetral de forma única sin necesidad de que los usuarios finales se pongan en contacto con el fabricante del dispositivo original para obtener información de procedencia como la identidad, esta arquitectura de infraestructura Blockchain de identidad global, permite que los fabricantes registren sus dispositivos de borde, una vez registrados, cualquier persona puede acceder a su identidad desde cualquier lugar. También se ha propuesto implementar una infraestructura Blockchain "con permiso local" para autenticar dispositivos perimetrales de forma regular en sus entornos implementados principalmente para evitar la amenaza de reemplazar un dispositivo perimetral por una contraparte clonada/manipulada, un administrador local puede registrar un dispositivo perimetral auténtico en su conjunto de datos almacenado en esta cadena de bloques. Otra forma de garantizar la autenticidad de un dispositivo perimetral de bajo costo es mediante la tecnología PUF has, a través de la verificación de un ID de dispositivo inclonable, que se puede generar a partir de una memoria SRAM a bordo, para evitar el costo de la memoria no volátil programable en dispositivos de borde de bajo costo.		
3	Información relevante	Debido a ciertas características que poseen los dispositivos Edge IoT no se puede garantizar la seguridad y autenticidad; estas características son: baja		

		potencia, memoria limitada, carecen de direcciones MAC en sus protocolos inalámbricos, la restricción de potencia limita la funcionalidad de cifrado de los nodos del sensor, lo que conduce a una comunicación mal cifrada o a ningún cifrado en absoluto

Tabla 29. Resultado del artículo ES07

#	**Descripción**	**Detalle**	**Código: ES07**
1	Información bibliográfica	Título	Diseño de un mecanismo eficiente de detección de ataques Sinkhole en el despliegue de IoT basado en Edge
		Autores	Pundir, Sumit, Wazid, Mohammad, Singh, Devesh Pratap, Das, Ashok Kumar, Rodrigues, Joel J.P.C., Park, Youngho
		Referencia	[58]
		Año	2020
2	Resumen del artículo	Los estudios proponen un esquema de detección de intrusiones para proteger el entorno Internet de las Cosas basado en el Borde (EIoT) contra el ataque de sumideros, que se denomina SAD-EIoT. En SAD-EIoT, los nodos de borde ricos en recursos (servidores de borde) realizan la detección de diferentes tipos de nodos atacantes de sumideros con la ayuda del intercambio de mensajes. Además, el análisis de seguridad de SAD-EIoT se lleva a cabo para demostrar su resistencia frente a varios tipos de SHA. SAD-EIoT alcanza una tasa de detección de alrededor del 95,83% y una tasa de falsos positivos del 1,03%, que son considerablemente mejores que otros esquemas existentes relacionados.	
3	Información relevante	El rendimiento de la comunicación IoT basada en Edge se degrada muy rápidamente bajo la presencia de varios nodos atacantes de sumideros. La mayoría de los esquemas existentes para la detección de nodos sinkhole no son efectivos, ya que no pueden identificar todos los tipos posibles de ataques en EIoT. Además, los esquemas de detección de intrusos existentes tienen otras limitaciones, como la ineficacia en términos de costes de comunicación y cálculo.	

Tabla 30. Resultado del artículo ES08

#	Descripción	Detalle		Código: ES08
1	Información bibliográfica	Título	Sistema de detección de intrusos basado en redes neuronales artificiales para nodos Fog del Internet de las cosas	
		Autores	Pacheco, Jesus, Benitez, Victor H, Felix-Herran, Luis C, Satam, Pratik	
		Referencia	[59]	
		Año	2020	
2	Resumen del artículo	El ataque de denegación de servicio distribuido (DDoS) es un tipo de amenaza de gran importancia para la de niebla. Los autores proponen una metodología ABA-IDS (Sistema de Detección de Intrusos con Análisis de Comportamiento de Anomalías) utilizando Redes Neuronales Artificiales (RNA) para proteger los nodos Fog (Gateways) y los dispositivos IoT contra los ciberataques; ABA modela el comportamiento habitual de un sistema, de forma que sea capaz de identificar cualquier comportamiento anormal, es decir, un ataque al sistema objetivo que está modelando. La metodología propuesta se centra en la disponibilidad de la pasarela segura para reconocer posibles amenazas que puedan afectar a su funcionalidad, impidiéndole entregar la información donde se requiere		
3	Información relevante	El desempeño del enfoque fue medido contra ataques como el ataque de repetición, inundación y DoS en un testbed de IoT. Los resultados obtenidos demuestran que la metodología ABA-IDS propuesta puede ser utilizada para desplegar métodos de seguridad capaces de proteger la funcionalidad normal de los dispositivos IoT y Fog. El enfoque fue capaz de detectar con éxito anormalidades conocidas y desconocidas, como los ciberataques aplicados a los nodos finales de IoT, mostrando una alta tasa de detección (hasta el 93%) con bajas falsas alarmas (menos del 3,3%), mientras que introduce una baja sobrecarga (hasta el 13% de sobrecarga de tiempo de ejecución).		

Tabla 31. Resultado del artículo ES09

#	Descripción	Detalle		Código: ES09
1	Información bibliográfica	Título	FOCUS: Un sistema de seguridad basado en la informática de niebla para el Internet de las cosas	
		Autores	Alharbi, Salem Rodriguez, Peter Maharaja, Rajaputhri Iyer, Prashant Bose, Nivethitha Ye, Zilong	
		Referencia	[93]	
		Año	2018	
		Revista	EEE Annual Consumer Communications and Networking Conference	
2	Resumen del artículo	Los ataques cibernéticos como hombre en el medio y denegación de servicio distribuida (DDoS) son amenazas típicas para el IoT. Los autores proponen un sistema de seguridad basado en FOg CompUting, llamado FOCUS para mitigar estos problemas se seguridad, este sistema adopta una protección de seguridad de dos niveles. Primero, el sistema FOCUS usa una VPN para asegurar los canales de comunicación a los dispositivos IoT. Segundo, FOCUS aplica una autenticación de desafío-respuesta para filtrar los ataques maliciosos sospechosos y proteger el servidor VPN contra posibles ataques DDoS, lo que mejora aún más la seguridad del sistema IoT. FOCUS adopta una unidad de análisis de tráfico, una unidad de desafío-respuesta y un firewall para proteger eficazmente el servidor VPN contra ataques DDoS. Más específicamente, la unidad de análisis de tráfico aplica la clasificación del árbol de decisiones para distinguir las solicitudes legitimas de los ataques maliciosos para detectar dicho patrón de tráfico e informar las fuentes de tráfico sospechosas de malware a la unidad de desafío-respuesta para la autenticación. Luego, la unidad de respuesta al desafío inicia un mensaje de desafío para autenticar la identificación de las fuentes de tráfico sospechosas. Las fuentes sospechosas que no puedan responder adecuadamente a la pregunta de seguridad no podrán acceder al servidor VPN y serán bloqueadas por el firewall.		
3	Información relevante	En comparación con la solución en la nube tradicional, FOCUS ofrece algunos beneficios de la siguiente manera. Primero, FOCUS maneja todas las solicitudes a la VPN y la unidad de autenticación de desafío-respuesta en el Fog o Edge, que está cerca de los usuarios de IoT. Por lo tanto, FOCUS logra un tiempo de respuesta mucho menor que el de la solución en la nube, lo cual es de vital importancia para el sistema de IoT que requiere comunicaciones en tiempo real.		

Tabla 32. Resultado del artículo ES10

#	Descripción	Detalle		Código: ES10
1	Información bibliográfica	Título	Hacia la prevención de IoT-DDoS mediante Edge Computing	
		Autores	Bhardwaj, Ketan, Miranda, Joaquin Chung, Gavrilovska, Ada	
		Referencia	[71]	
		Año	2018	
2	Resumen del artículo	Los ataques DDoS son cada vez más grandes, complejos y frecuentes, que pueden resultar un obstáculo para la adopción de IoT, los autores presentan ShadowNet como un enfoque para prevenir ataques IoT-DDoS a nivel de aplicación aprovechando la computación perimetral para implementar funciones de borde que recopilan información sobre el tráfico entrante y comunican esa información a través de una ruta rápida con un servicio de detección cercano limitando así el impacto de dichos ataques. ShadowNet, una arquitectura que convierte el borde en la primera línea de defensa contra IoT-DDoS, alcanza sus objetivos de la siguiente manera. En primer lugar, las funciones de borde adecuadas se implementan en la infraestructura de borde distribuida, en nombre de una aplicación de backend de IoT que busca protección. El papel de estas funciones de borde es esbozar los perfiles de la transmisión de tráfico de IoT desde una ubicación de borde determinada. En segundo lugar, la función de borde establece una ruta rápida entre ella y un servicio web ShadowNet especial. La función de borde utiliza la ruta rápida para enviar pequeños paquetes de sombra con información derivada localmente sobre el tráfico de IoT al servicio web ShadowNet. ShadowNet puede luego agregar esa información sobre el tráfico de IoT distribuido en varios nodos Edge, detectar un ataque inminente de IoT-DDoS y responder con alguna acción defensiva proactiva.		
3	Información relevante	El rendimiento de ShadowNet en la prevención de ataques IoT-DDoS dependerá de su capacidad para implementar funciones de borde de mitigación a tiempo. Este enfoque no solo protege los servicios web al detectar IoT-DDoS 10 veces más rápido que los enfoques existentes, además, evita que el 82% del tráfico ingrese a la infraestructura de Internet, reduciendo el daño causado por el DDoS.		

Tabla 33. Resultado del artículo ES11

#	**Descripción**	**Detalle**		**Código: ES11**
1	Información bibliográfica	Título	Servicio de autorrecuperación que asegura el servidor de borde en la red IoT contra el ataque de ransomware	
		Autores	Lei, In San, Tang, Su Kit, Chao, Ion Kun, Tse, Rita	
		Referencia	[72]	
		Año	2020	
2	Resumen del artículo	Los servidores Edge en las redes de IoT normalmente son accesibles al público, cualquier falla o error de implementación puede ponerlos en riesgo de sufrir una serie de ataques cibernéticos, incluido el ataque de ransomware que es considerado actualmente como una de las amenazas de red más graves para los servidores de borde. La madurez del ransomware incluso ha alcanzado un nuevo nivel que puede atacar a millones de computadoras a la vez por lo que se necesitan medidas de defensa razonables para que los servidores de borde reduzcan la posibilidad de ser atacados. En esta investigación proponen un método de recuperación automática, llamado Servicio de recuperación automática (SRS), para aliviar el daño por ransomware en un servidor de borde, SRS puede detectar firmas de ransomware y recuperar archivos de víctimas automáticamente; Su objetivo es monitorear archivos importantes por un servicio del sistema si se detecta ransomware, SRS recupera los archivos infectados restaurando la copia de seguridad correspondiente de los datos sin procesar no se produciría ninguna interrupción en el funcionamiento del servidor de borde.		
3	Información relevante	SRS es un servicio del sistema que se ejecuta a nivel del kernel y monitorea la actividad del sistema de archivos en un servidor Edge, si se detecta alguna actividad sospechosa en el almacenamiento, este verifica la firma del ransomware, si la firma se encuentra en algún archivo de datos de IoT, los archivos de datos deben cifrarse inesperadamente, si confirma que el servidor está bajo el ataque de ransomware, SRS toma una acción inmediata para recuperar el archivo encriptado, recuperando su copia de respaldo del nodo de respaldo. Si no hay actividad sospechosa, SRS continúa enviando datos de IoT al nodo de respaldo.		

Tabla 34. Resultado del artículo ES12

#	Descripción	Detalle		Código: ES12
1	Información bibliográfica	Título	Autenticación basada en Blockchain con tolerancia a fallos para la computación en la niebla habilitada para IoT	
		Autores	Mounnan, Oussama, Mouatasim, Abdelkrim, Manad, Otman Hidar, Tarik,Kalam, Anas Abou, Idboufker, Noureddine.	
		Referencia	[5]	
		Año	2020	
2	Resumen del artículo	En este estudio, se propone un nuevo esquema de cadena de bloques basado en la autenticación y la privacidad para la Fog compitung habilitada para IoT con tolerancia a fallas. Se propone un sistema de autenticación en el que se utilizará una cadena de bloques para mantener, registrar y administrar dispositivos IoT, nodos Fog, propietarios de datos y usuarios. La solución se presenta en dos procesos. El primero se refiere al propietario de los datos, que administra los dispositivos de IoT y define la política implementada en la cadena de bloques a través del contrato inteligente, y el segundo se refiere a los usuarios o solicitantes de acceso que desean acceder a un dispositivo de IoT. El propietario de los datos se autentica con su billetera en la cadena de bloques, lo que le proporciona el par de claves necesario (público y privado), este par de claves es crucial para la autenticación y firma de transacciones. Los usuarios que solicitan acceso a un recurso deseado, primero se autentica con su billetera, este último recupera los atributos y los encripta, luego los envía con la solicitud al recurso de destino como una transacción		
3	Información relevante	Los sistemas Blockchain utilizan la criptografía asimétrica como medio para asegurar y garantizar las transacciones entre los usuarios. Cada entidad en estos sistemas posee un par de claves (públicas y privadas). Además, Blockchain utiliza el concepto de firma digital que se basa en claves privadas para garantizar la identidad y autenticación del usuario. Este proceso, por un lado, garantiza los objetivos de seguridad, incluida la integridad, la autenticación y el no repudio, y por otro lado protege contra el ataque Man-In-The-Middle y el ataque de repetición. Además, la naturaleza descentralizada de Blockchain nos ofrece un entorno altamente robusto y resistente al ataque DDoS, porque este último se basa en un servidor centralizado.		

Tabla 35. Resultado del artículo ES13

#	**Descripción**	**Detalle**	**Código: ES13**
1	Información bibliográfica	Título	Metodología en tiempo real para mejorar la ciberseguridad en el Internet de las Cosas utilizando la computación de borde durante la amenaza de ataque
		Autores	Ahanger, Tariq Ahamed, Tariq, Usman, Nusir
		Referencia	[80]
		Año	2019
2	Resumen del artículo	En el IoT moderno, uno de los ataques más comunes y simples de hacer es el ataque DDoS (Denegación de servicio distribuida) también conocidos como ataques Zombie. Aquí se presenta un sistema de detección de intrusiones para detectar ataques distribuidos de denegación de servicio que permitirá una vigilancia y escaneo en tiempo real de flujos de paquetes maliciosos en tiempo real en redes de Internet de las cosas utilizando políticas básicas de procesamiento de eventos complejos. Se ha utilizado los conceptos centrales de la informática de borde para diseñar la arquitectura del sistema al cambiar todo el procesamiento del sistema de detección de intrusiones al borde de la red, lo que generalmente se realiza en un servidor base. Por lo tanto, al reubicar IDS, se logra la privacidad, seguridad, ancho de banda y tiempo de respuesta deseados. El sistema de detección de intrusos escanea, filtra los flujos de datos de las inundaciones de datos de la red como entrada y procesa, analiza la información luego genera un informe utilizando políticas complejas de procesamiento de eventos. Para verificar el rendimiento exacto del sistema diseñado en el borde de la red, Se usa ocho computadoras y un conjunto de Raspberry sobre el sistema diseñado para valorar el desempeño.	
3	Información relevante	Los resultados obtenidos después de experimentos rigurosos demostraron que el rendimiento del mecanismo sugerido es mucho mejor que los sistemas de detección de intrusos existentes anteriormente en casi todos los campos clave básicos durante el estudio comparativo. Los resultados obtenidos también demuestran que el procesamiento de eventos complejos es apropiado y suficiente para los servicios y aplicaciones de IoT que tratan con una gran cantidad de flujos de datos y necesitan procesarlos	

Tabla 36. Resultado del artículo ES14

#	Descripción	Detalle		Código: ES14
1	Información bibliográfica	Título	FlowGuard: Un mecanismo inteligente de defensa de borde contra los ataques DDoS de IoT.	
		Autores	Jia, Yizhen, Zhong, Fangtian, Alrawais, Arwa, Gong, Bei, Cheng, Xiuzhen	
		Referencia	[7]	
		Año	2020	
2	Resumen del artículo	Los ataques DDoS dirigidos a dispositivos de IoT pueden provocar graves daños en los meta-sistemas de IoT. Los dispositivos de IoT vulnerables son los posibles objetivos de ataque para formar botnets, las magnitudes de los ataques lanzados son enormes y tales ataques podrían interrumpir fácilmente cualquier objetivo, incluidos los potentes servidores equipados con estrategias altamente protegidas. En este estudio proponen FlowGuard, un eficaz esquema de detección, identificación, clasificación y mitigación de ataques DDoS que aprovecha dos técnicas cooperativas de aprendizaje automático, a saber, LSTM y CNN. FlowGuard consta de dos componentes principales: Filtro de flujo y Manejador de flujo; El Filtro de flujo incluye dos módulos, Filtración de flujo y Detección de ataques DDoS, que sirve como un cortafuegos de seguridad siempre activo con la responsabilidad de distinguir de manera eficiente los flujos de red benignos de los maliciosos y detectar las amenazas de posibles ataques DDoS, mientras que el controlador de flujo también incluye dos módulos, a saber, identificación de ataques DDoS y clasificación de ataques DDoS, que es responsable de identificar y clasificar con precisión los flujos de ataques DDoS desconocidos.		
3	Información relevante	FlowGuard fue evaluado con un conjunto de datos de ataque mixto que contiene varios tipos de ataques DDoS, y los resultados indican que FlowGuard podría lograr precisiones superiores al 98,9% en la identificación de ataques y más del 99,9% en la clasificación de ataques sin afectar obviamente las operaciones de red regulares. En comparación con las técnicas clásicas y basadas en el prendizaje automático mencionadas anteriormente, FlowGuard no implica ningún sistema complicado ni ejerce presión computacional sobre los dispositivos de IoT lo que lo hace ideal para ser implementado en los mismos.		

Tabla 37. Resultado del artículo ES15

#	Descripción	Detalle		Código: ES15
1	Información bibliográfica	Título	Un marco de mitigación de anomalías para el IoT utilizando Fog Computing.	
		Autores	Lawal, Muhammad Aminu, Shaikh, Riaz Ahmed, Hassan, Syed Raheel.	
		Referencia	[60]	
		Año	2020	
2	Resumen del artículo	Los autores presentan un marco híbrido que utiliza el paradigma de la computación en la niebla para mitigar los ataques de botnes. El marco emplea dos módulos, que son módulos IDS basados en firmas y basados en anomalías; En primer lugar, emplea el IDS basado en firmas que utiliza la función de similitud de las fuentes de ataque en los ataques de botnet para crear una lista negra de (direcciones IP) para la detección oportuna de ataques, este módulo asegurará el 100% de precisión en la detección de ataques conocidos a través de su fuente. En segundo lugar, utiliza un IDS basado en anomalías que utiliza un clasificador de impulso extremo para garantizar la detección de ataques con alta precisión y bajas tasas de falsos positivos. Por lo tanto, el marco garantiza una red de IoT segura. El módulo basado en firmas emplea una lista negra de IP que se actualiza con las fuentes de ataque detectadas por el módulo basado en anomalías para garantizar una detección rápida cuando estos ataques se ejecutan nuevamente, mientras que el módulo basado en anomalías utiliza un algoritmo de aumento de gradiente extremo para clasificar el flujo de tráfico de la red en normal o anormal. La utilización del módulo basado en firmas en el marco de análisis del flujo de tráfico de la red asegura una detección rápida de las fuentes de ataque conocidas, reduciendo así la sobrecarga operativa y el tiempo de clasificación en el módulo IDS basado en anomalías.		
3	Información relevante	Para probar el marco propuesto se utilizaron diferentes tipos de ataques: Ataques de sondeo en sus dos tipos, escaneo de puertos y huellas dactilares del sistema operativo. Los resultados obtenidos demuestran que el módulo basado en firmas detecta ataques más rápido que el módulo basado en anomalías. Del mismo modo, el módulo basado en anomalías puede detectar diferentes tipos de ataques con un rendimiento satisfactorio.		

Tabla 38. Resultado del artículo ES16

#	Descripción	Detalle	Código: ES16
1	Información bibliográfica	Título	RAD-EI: Un esquema de detección de ataques de enrutamiento para el entorno del Internet de las Cosas basado en Edge
		Autores	Wazid, Mohammad, Reshma Dsouza, Poonam, Das, Ashok Kumar, Bhat K, Vivekananda, Kumar, Neeraj Rodrigues, Joel J.P.C.
		Referencia	[62]
		Año	2019
2	Resumen del artículo	Se centran en la creación de una solución para mitigar el ataque de enrutamiento en el entorno de IoT usando el borde. Un nodo malicioso o nodo atacante de enrutamiento interrumpe el flujo normal del trafico al enviar los paquetes a los nodos atacantes vecinos. Por lo tanto, los paquetes se mueven en un bucle en un caso, mientras que, en el otro caso, un nodo atacante envía paquetes a algún nodo atacante colaborador vecino, y no reenvía estos paquetes al nodo de borde y los retiene solo consigo mismo. La presencia de nodos atacantes, disminuye el rendimiento de la red, aumenta el retardo de extremo a extremo, disminuye la tasa de entrega de paquetes y otros parámetros también se ven afectados. La solución propuesta en este artículo se basa en el diseño de un esquema de detección de intrusiones para la detección de ataques de enrutamiento en un entorno de IoT basado en el borde llamado RAD-EI. RAD-EI realiza la detección de anomalías en dos fases. En la fase 1 se detecta la existencia de nodos atacantes mediante el uso del algoritmo de existencia de nodos atacantes de enrutamiento. En la fase 2 se confirma la existencia de los nodos sospechosos ya sean nodos normales o nodos atacantes que realizan un ataque de enrutamiento mediante el uso del algoritmo de confirmación del nodo del atacante de enrutamiento.	
3	Información relevante	Para demostrar su resistencia frente a los ataques de enrutamiento, RAD-EI logra alrededor del 95.0% de tasa de detección y 1.23% de tasa de falsos positivos que son notablemente mejores que otros esquemas existentes relacionados. Además, en RAD-EI, los sensores de IoT con recursos limitados requieren los gastos generales mínimos de comunicación y computación, y el algoritmo de detección de intrusiones se ejecuta solo en el nodo de borde rico en recursos.	

Tabla 39. Resultado del artículo ES17

#	Descripción	Detalle		Código: ES17
1	Información bibliográfica	Título	Esquema de autenticación Protean: una técnica de autenticación dinámica con límite de tiempo para nodos Edge de IoT en despliegues exteriores.	
		Autores	Sathyadevan, Shiju, Achuthan, Krishnashree, Doss, Robin, Pan, Lei	
		Referencia	[63]	
		Año	2019	
2	Resumen del artículo	Debido al fácil acceso físico de los dispositivos, los ataques comunes, incluida la clonación de dispositivos o el robo de claves secretas almacenadas en un nodo de borde, son algunos de los ataques más comunes en las implementaciones de IoT. Este documento se centra en el desarrollo de un esquema de autenticación extremadamente ligero para dispositivos finales restringidos que forman parte de una LAN de IoT determinada. La autenticación se produce entre el dispositivo final y la puerta de enlace que actúa como un dispositivo informático de borde. El esquema de autenticación de Protean se basa en vectores de inicialización mínimos. Tiene poca dependencia de las claves almacenadas estáticas durante todo el ciclo de autenticación. El proceso de autenticación almacena un vector de inicialización en la ubicación de la memoria protegida junto con el ID de hardware en el nodo de borde y se mantendrá una copia del mismo en la puerta de enlace, que se usa solo durante el proceso de reconocimiento inicial. El esquema Protean es computacionalmente menos intensivo en los recursos del dispositivo porque involucra operaciones de cómputo livianas como funciones hash, operaciones XOR y también encriptación AES en el lado de la puerta de enlace, mientras que los nodos de borde solo realizarán encriptación AES. Las claves intercambiadas pueden almacenarse en una EEPROM segura o en una ubicación de memoria protegida que no sea susceptible a ataques de clonación o volcados de memoria. Con el esquema de Protean, se vuelve difícil para un atacante adivinar o manipular la secuencia de eventos seguida por el esquema, ya que el IDS alojado en la puerta de enlace decide dinámicamente la vida útil de las claves.		
3	Información relevante	El esquema propuesto genera un impacto mínimo en los recursos como el consumo de energía. Protean en resistente a los ataques de repetición, ataques de suplantación de identidad, ataque de clonación de dispositivos, ataque de captura de nodos u hombre en el medio.		

Tabla 40. Resultado del artículo ES18

#	Descripción	Detalle		Código: ES18
1	Información bibliográfica	Título	LDAKM-EIoT: Mecanismo ligero de autenticación de dispositivos y gestión de claves para el despliegue de IoT basado en Edge	
		Autores	Wazid, Mohammad, Das, Ashok Kumar, Shetty, Sachin Rodrigues, Joel J.P.C., Park, Youngho	
		Referencia	[64]	
		Año	2019	
2	Resumen del artículo	El entorno del IoT basado en Edge proporciona muchas ventajas sobre el entorno informático tradicional, pero al mismo tiempo, también presenta problemas de seguridad y privacidad. Primero los mensajes que se intercambian entre el dispositivo IoT, el nodo de borde y el servidor en la nube deben estar protegidos contra varios ataques conocidos como repetición, hombre en el medio, suplantación y adivinación de contraseñas fuera de línea o en línea. Por otro lado, los protocolos de autenticación existentes tienen fallos de seguridad que los hacen vulnerables a algunos ataques de privilegiados, adivinación de contraseñas en línea y fuera de línea. Finalmente, en entorno del IoT basado en el borde, existe la posibilidad de que algunos dispositivos del IoT sean robados/capturados físicamente por el adversario el cual utiliza un ataque de análisis de energía para obtener los datos de la memoria de los dispositivos IoT. Como solución proponen un mecanismo de autenticación ligera y gestión de claves para el entorno del IoT basado en el borde (LDAKM-EIoT). Utilizan varias operaciones eficientes, como exclusive-OR (XOR) y funciones hash criptográficas resistentes a las colisiones.		
3	Información relevante	El análisis de seguridad detallado y la verificación de seguridad formal llevados a cabo por la herramienta ampliamente utilizada "Automated Validation of Internet Security Protocols and Applications (AVISPA)" demuestran que el LDAKM-EIoT propuesto es seguro contra varios vectores de ataque que existen en la infraestructura del entorno del IoT basado en el borde como son los ataques de repetición, ataque del hombre en el medio (MITM), diferentes ataques de suplantación, ataques de privilegiados, proporciona protección contra los ataques de captura física de dispositivos IoT.		

Tabla 41. Resultado del artículo ES19

#	Descripción	Detalle	Código: ES19
1	Información bibliográfica	Título	Detección de ataques de botnets en el borde del IoT basada en la representación dispersa
		Autores	Tzagkarakis, Christos, Petroulakis, Nikolaos, Ioannidis, Sotiris.
		Referencia	[66]
		Año	2019
2	Resumen del artículo	Los ataques provocados por botnet son muy comunes dentro del IoT. En este estudio presentan un mecanismo de diagnóstico para la detección instantánea de ataques de botnet de IoT, con el objetivo final de minimizar el impacto del ataque mediante el aislamiento inmediato de los dispositivos de IoT comprometidos ubicados en el borde de IoT. Este método está basado en un marco de representación de escasez que utiliza una regla de umbral de error de reconstrucción para identificar el tráfico de red malicioso en el borde de IoT que proviene de dispositivos de IoT comprometidos. La detección de ataques de botnet se realiza en base a datos de tráfico de red de IoT benignos de pequeño tamaño y, por lo tanto, no se tiene conocimiento previo sobre los datos de tráfico de IoT maliciosos. En primer lugar, se emplea una regla de umbral de error de reconstrucción basada en un marco de representación escasa para la detección de ataques de botnet de IoT, asumiendo que solo se usa una cantidad muy limitada de datos de entrenamiento y prueba para lidiar con restricciones computacionales bajas, así como con reacción rápida. En segundo lugar, se adopta un algoritmo codicioso de recuperación dispersa, denominado búsqueda de coincidencia ortogonal, ya que implica solo dos ajustes de hiperparámetros, es decir, la constante de umbral y el nivel de dispersión.	
3	Información relevante	Como resultado de las capacidades computacionales limitadas que gobiernan los dispositivos periféricos de IoT, están muy interesados en proporcionar un procedimiento algorítmico que utilice la menor cantidad posible de datos de entrenamiento y prueba para implementar un detector de ataques de botnet de IoT preciso.	

Tabla 42. Resultado del artículo ES20

#	Descripción	Detalle		Código: ES20
1	Información bibliográfica	Título	Combinación de AntibIoTic con la informática de niebla AntibIoTic 2.0.	
		Autores	Ic, A Ntib I O T, Donno, Michele De Dragoni, Nicola	
		Referencia	[84]	
		Año	2019	
2	Resumen del artículo	Desde el punto de vista de la seguridad, la creciente adopción de dispositivos IoT en todos los aspectos de nuestra sociedad ha expuesto a las empresas y los consumidores a una serie de amenazas, como los ataques de denegación de servicio distribuidos (DDoS). Para hacer frente a este problema de seguridad del IoT los autores proponen ANTIBIOTIC 2.0, un antimalware que se basa en Fog Computing para asegurar los dispositivos IoT, es un gusano blanco que infecta dispositivos vulnerables y crea una botnet de sistemas seguros, protegiéndolos contra el malware del IoT. La idea de ANTIBIOTIC 2.0 es utilizar un nodo Fog o una federación de nodos Fog para supervisar y desinfectar los dispositivos conectados a él, permitiendo que solo los seguros accedan a Internet. Para ello, el nodo Fog carga en cada dispositivo IoT un anti-malware (también llamado Bot ANTIBIOTICO) que los sanea y asegura, y reporta información en vivo de vuelta al nodo Fog de acuerdo a la información recibida de cada dispositivo IoT, así como del modo de funcionamiento establecido para ANTIBIOTIC 2.0, el nodo de la niebla decide si el host puede conectarse a Internet.		
3	Información relevante	ANTIBIOTIC 2.0 está diseñado para funcionar en diferentes escenarios sin necesidad de acceder y configurar manualmente cada dispositivo IoT. Basta con introducir un nodo Fog o una federación de nodos Fog en la red deseada y realizar la primera configuración. Después, el sistema empieza a funcionar y a asegurar la red IoT de forma transparente para el usuario. Hasta donde sabemos, ANTIBIOTIC 2.0 es el primer antimalware basado en Fog para IoT.		

Tabla 43. Resultado del artículo ES21

#	Descripción	Detalle		Código: ES21
1	Información bibliográfica	Título	Una estrategia de mitigación distribuida contra los ataques DoS en Edge Computing.	
		Autores	Potrino, Giuseppe, Rango, Floriano De Fazio, Peppino	
		Referencia	[94]	
		Año	2019	
2	Resumen del artículo	Proponen una estrategia distribuida para mitigar ataques de denegación de servicio (DoS) contra el nodo Fog en un contexto de computación de borde en el que los nodos intercambian mensajes a través del protocolo Message Queue Telemetry Transport (MQTT). El nodo de niebla utiliza un sistema de detección de intrusiones del host para dejar caer mensajes hasta que se alcanza la capacidad del búfer para otorgar prioridad a los mensajes. Los nodos ligeros utilizan una estrategia de envío de mensajes adaptativo para ayudar al nodo de niebla en el proceso de descongestión porque funciona mejor que el envío de mensajes estáticos. También se mitiga la manipulación de datos y la escucha clandestina mediante el uso de criptografía de curva elíptica (ECC).		
3	Información relevante	El sistema de seguridad propuesto fue validado mediante la implementación de un simulador impulsado por eventos capaz de recopilar datos que se pueden utilizar para generar algunos gráficos. Las simulaciones realizadas muestran que el AMS propuesto es más adecuado para un contexto de red de niebla para mitigar los ataques DoS al nodo Fog. En conclusión, si esta mitigación se realiza de forma distribuida puede ser más escalable.		

Tabla 44. Resultado del artículo ES22

#	Descripción	Detalle		Código: ES22
1	Información bibliográfica	Título	Mejora de la seguridad en un esquema de autenticación ligero con arquitectura de Fog Computing anónima	
		Autores	Wang, Lin, An, Haonan, Chang, Zhuo	
		Referencia	[91]	
		Año	2020	
2	Resumen del artículo	Este documento propone un esquema de autenticación seguro para la capacidad de generación dinámica de claves, que puede mejorar la seguridad de toda la red heterogénea sin las restricciones en los tipos de dispositivos, atributos y protocolos de comunicación. La autenticación es un problema importante para la seguridad de FC, ya que los servicios se ofrecen a los usuarios finales a gran escala por los nodos de niebla frontal. Proponemos un método de autenticación escalable ligero con anonimato para la arquitectura de computación de niebla. Este modelo se enfrentará a		

		los siguientes desafíos: 1) Se puede utilizar para los dispositivos de toda la arquitectura FC. 2) Es ligero y tiene un menor consumo de energía para adaptarse a las características de la mayoría de los nodos de IoT. 3) Puede garantizar la generación dinámica de claves de sesión y el anonimato para proporcionar una mayor seguridad. En respuesta a los desafíos anteriores, el método aprovecha el protocolo de autenticación anónima y la generación de claves dinámicas de capa física para satisfacer los requisitos de autenticación y cifrado en la arquitectura FC. Este método utiliza cifrado simétrico para cifrar algunos datos confidenciales y utiliza el resultado hash de la combinación de algunos números aleatorios y clave secreta dinámica generada por ambos lados como nuestra clave de sesión. El seudónimo se actualiza en cada momento de la autenticación para garantizar el anonimato. Este protocolo no sólo es anónimo y ligero, sino que también se puede aplicar a los escenarios de autenticación entre sensores y puertas de enlace. También se puede extender a la arquitectura FC para la autenticación de dispositivos y la actualización de claves.
3	Información relevante	El método propuesto es resistente a diferentes ataques como son: ataque de repetición, ataque resistencia, ataque de suplantación. Los resultados del análisis muestran que los protocolos propuestos pueden prevenir muchos ataques y garantizar la seguridad de los datos entre dispositivos inalámbricos en la arquitectura FC con una sobrecarga más baja.

Tabla 45. Resultado del artículo ES23

#	**Descripción**	**Detalle**	**Código: ES23**
1	Información bibliográfica	Título	ECCbAP: un protocolo de autenticación seguro basado en ECC para dispositivos de Edge del IoT
		Autores	Rostampour, Samad, Safkhani, Masoumeh, Bendavid, Ygal, Bagheri, Nasour
		Referencia	[77]
		Año	2020
2	Resumen del artículo	En este estudio se evalúa un protocolo autenticación seguro basado en Criptografía de Curva Elíptica (ECC) llamado (ECCbAP) este protocolo es resistente al ataque de hombre en el medio, ataque de reproducción, ataque de suplantación, este protocolo utiliza ECC para cubrir una mayor variedad de dispositivos integrados. Dado que el servidor no es un dispositivo restrictivo, es posible aumentar su costo computacional en comparación con los dispositivos integrados. ECCbAP tiene dos fases, i) Fase de registro ii) Fase de inicio de sesión y autenticación. En la fase de registro para iniciar una comunicación, el dispositivo integrado debe registrarse en el servidor, cualquier dispositivo se registra en el servidor a través de un canal seguro	

		una vez y, después, para cada sesión, solo se autentica en función de la fase de autenticación e inicio de sesión del protocolo a través de un canal seguro. En la fase de inicio de sesión y autenticación para compartir una nueva clave secreta con el servidor el dispositivo integral genera un numero aleatorio el cual es buscado en la base de datos segura del servidor si encuentra alguna coincidencia este autentica el dispositivo
3	Información relevante	Dado que la mayoría de los protocolos basados en ECC obligan al dispositivo integrado a utilizar las funciones hash y ECC para aumentar la complejidad y la seguridad, esta propuesta solo requiere el módulo ECC, lo que lo convierte en una opción adecuada para entornos restringidos, como las etiquetas de identificación por radiofrecuencia (RFID) o Bluetooth Low, Sensores de energía (BLE).

Tabla 46. Resultado del artículo ES24

#	**Descripción**	**Detalle**	**Código: ES24**
1	Información bibliográfica	Título	BioSec: Un marco de autenticación biométrica para la comunicación segura y privada entre dispositivos de Edge en IoT e Industria 4.0
		Autores	Golec, Muhammed, Gill, Sukhpal Singh, Bahsoon, Rami Rana, Omer.
		Referencia	[78]
		Año	2020
2	Resumen del artículo	Se propone un método biométrico llamado BioSec para proporcionar autenticación en IoT integrada con electrónica de consumo de vanguardia mediante autenticación de huellas dactilares. BioSec garantiza una comunicación segura y privada entre dispositivos de borde en IoT e Industria 4.0. La autenticación del usuario es esencial para proteger la privacidad de los datos personales. Tradicionalmente, la autenticación de usuarios en IoT se realizaba con sistemas de contraseña basados en PIN. Sin embargo, los sistemas biométricos han comenzado a usarse debido a las debilidades de la contraseña basada en PIN, como ser olvidada, robada y compartida, los datos biométricos no se pueden modificar en caso de robo porque tienen características únicas de la persona y crean serios problemas de privacidad en caso de fuga. La seguridad de los datos biométricos tanto en los canales de transmisión como en las bases de datos se garantiza mediante el método de cifrado estándar.	
3	Información relevante	La disponibilidad del sistema aumentará mediante la autenticación biométrica porque los usuarios no tendrán que llevar consigo un token o una contraseña que deban recordar.	

Tabla 47. Resultado del artículo ES25

#	Descripción	Detalle		Código: ES25
1	Información bibliográfica	Título	Un esquema de autenticación eficiente basado en la cadena de bloques para proteger los dispositivos IoT habilitados para Fog	
		Autores	Mudhar, Jaideep Kaur, Kalra, Sheetal, Malhotra, Jyoteesh	
		Referencia	[79]	
		Año	2020	
2	Resumen del artículo	En este estudio, se propone un esquema basado en Blockchain descentralizado para el acceso autenticado seguro a dispositivos IoT habilitados para niebla. El sistema propuesto es completamente seguro, descentralizado, independiente de terceros confiables y resistente, cumple con las tríadas CIA definidas por los requisitos de seguridad de confidencialidad, integridad y disponibilidad de los dispositivos de IoT. El esquema utiliza el contrato inteligente Ethereum Blockchain y Smart Contract para verificar firmas, aprobar tickets y emitir tokens a usuarios autenticados. Cada participante se identifica en la red con una dirección Ethereum única y también se asocia con una clave pública y privada. La implementación del contrato inteligente se lleva a cabo usando programación de solidez en Remix-IDE y se prueban sus funcionalidades usando Test RPC Ganache y Rinkeby Test Network. El análisis de las vulnerabilidades de seguridad del contrato inteligente se realiza en la herramienta ChainSecurity Analysis. Se realiza una comparación del esquema propuesto con los esquemas existentes, demostrando que el esquema está libre de fallas de punto único (SPF) y tiene altos niveles de confianza debido a la transparencia.		
3	Información relevante	El esquema propuesto elimina la necesidad de un tercero confiable y proporciona transacciones para mantener registros de todo el mapeo de dispositivo Fog, mapeo de dispositivo de usuario y tokens emitidos. También es resistente a los ataques repetición y escucha.		

Tabla 48. Resultado del artículo ES26

#	Descripción	Detalle		Código: ES26
1	Información bibliográfica	Título	Un marco integrado seguro para los sistemas del Internet de las cosas asistidos por Fog	
		Autores	Junejo, Aisha Kanwal, Komninos, Nikos, McCann, Julie A.	
		Referencia	[88]	
		Año	2021	
2	Resumen del artículo	La mitigación de los ataques internos, como, blackhole (agujero negro), sinkhole (agujero de gusano o sumidero), sybil y Colisión, siempre ha sido un desafío y en su mayoría llevado a cabo por los nodos que se hacen pasar por legítimos. En este estudio se propone un marco con control de acceso basado en atributos y monitoreo de comportamiento basado en la confianza para abordar los desafíos mencionados anteriormente. El marco propuesto consta de dos componentes, el componente de seguridad (SC) y el componente de administración de confianza (TMC). SC garantiza la confidencialidad, integridad, autenticación y autorización de los datos. TMC evalúa el rendimiento de las entidades de Fog-IoT mediante un modelo de confianza basado en un conjunto de características de comunicación de red y QoS. Posteriormente, la confianza se incrusta como un atributo dentro de las directivas de control de acceso de SC, lo que garantiza que solo las entidades de confianza tengan acceso a los recursos de niebla. Los resultados muestran que SC y TMC son ligeros y adecuados para dispositivos con recursos limitados.		
3	Información relevante	Los sistemas basados en niebla también se enfrentan a problemas de confianza porque, a diferencia de los servidores Cloud los nodos Fog se encuentran en entornos remotos y sin protección, lo que los hace vulnerables a ataques de manipulación y captura de nodos. Las características de la computación de niebla, a saber, el conocimiento de la ubicación, la movilidad y la arquitectura descentralizada, también introducen desafíos de confianza. Sin red centralizada, los nodos de niebla pueden unirse y salir del sistema con frecuencia, principalmente debido a la incapacidad de proporcionar calidad de servicio (QoS), equilibrio de carga, compromiso del dispositivo o error de usuario/operador.		

Tabla 49. Resultado del artículo ES27

#	Descripción	Detalle		Código: ES27
1	Información bibliográfica	Título	Estudio sobre cuestiones de seguridad y privacidad en la Internet de los objetos asistida por Edge Computing	
		Autores	Alwarafy, Abdulmalik, Al-Thelaya, Khaled A, Abdallah, Mohamed Schneider, Jens, Hamdi, Mounir.	
		Referencia	[70]	
		Año	2020	
2	Resumen del artículo	En la siguiente encuesta los autores hacen mención de los posibles ataques de seguridad a los que están expuestos los dispositivos IoT asistidos por Edge Computing, a saber, dentro de ataque de inyección de hardware y software malicioso se encuentra (el ataque de replicación de nodo, ataque de troyano de hardware, ataque de camuflaje y nodos EC maliciosos), ataque de interferencia, dentro del ataque de denegación de servicios distribuidos tenemos (ataque DoS, ataque de privación del sueño y ataque de agotamiento de batería), ataque físico o manipulación, ataque de espionaje o rastreo, ataque de canal lateral o fuera de la red, en la categoría de ataques de información de enrutamiento se encuentra (agujeros negros, agujeros grises, agujeros de gusano), ataques de falsificación, control de acceso no autorizado y ataque de repetición o ataque de frescura. El paradigma de IoT asistido por EC es una combinación de recursos y dispositivos heterogéneos fabricados por varios proveedores. Dado que no existe un marco generalmente acordado ni políticas estándar para la implementación de este paradigma, todavía hay muchas amenazas a la seguridad y la privacidad sin detectar. Además, los dispositivos Edge se distribuyen y dispersan en áreas amplias y abiertas; por lo tanto, el control centralizado de estos dispositivos Edge puede resultar difícil. Si uno de los nodos Edge se ve comprometido, los intrusos pueden usarlo como un punto de entrada a la red de IoT asistida por EC.		
3	Información relevante	Dado que los datos son el elemento principal de los sistemas de IoT, deben protegerse durante la transmisión, el cálculo y el almacenamiento. El desarrollo del paradigma de IoT asistido por EC apuntó básicamente a aliviar la latencia y reducir la transferencia de datos entre servidores en la nube y dispositivos de borde de IoT. En el IoT asistido por EC, los nodos de borde son responsables de llevar a cabo una parte importante de las tareas de procesamiento al recibir información de otros nodos de borde y enviar la salida a los usuarios finales o servidores en la nube. Por lo tanto, parte de la transmisión de datos de entrada y salida a través de la red todavía está expuesta y necesita protección..		

Tabla 50. Resultado del artículo ES28

#	Descripción	Detalle		Código: ES28
1	Información bibliográfica	Título	Seguridad en el Internet de las cosas asistido por Edge: retos y soluciones	
		Autores	Shen, Shuaiqi, Zhang, Kuan, Zhou, Yi, Ci, Song	
		Referencia	[74]	
		Año	2020	
2	Resumen del artículo	En el siguiente estudio presentan un análisis sobre las principales características y desafíos de seguridad del IoT asistido por Edge. Los autores afirman que el IoT asistido por Edge emerge para proporcionar servicios con reconocimiento de ubicación y descargar tareas computacionales a los nodos del borde cerca de los dispositivos del IoT. Sin embargo, todavía existen una serie de desafíos de seguridad debido a las vulnerabilidades inherentes de los nodos del borde y la naturaleza sensible de los datos recopilados. Las características del IoT asistido por Edge mencionadas en este estudio son: baja latencia, conocimiento de la ubicación, heterogeneidad y descarga. Las características inherentes del borde, como el conocimiento de la ubicación y la flexibilidad de descarga de cómputo, complican aún más la situación de seguridad. En las aplicaciones de IoT asistidas por el borde, los nodos del borde están a cargo de la mayoría de las funciones informáticas básicas, como la autenticación, la autorización, el análisis de datos, la descarga de tareas y el almacenamiento de datos. Los principales desafíos de seguridad que enfrenta el IoT asistido por el borde incluyen el ataque DDoS y el ataque de inyección de malware. Debido a la limitación de la potencia computacional, los dispositivos de IoT y los nodos Edge de bajo nivel apenas pueden protegerse con un firewall tradicional, lo que los hace más vulnerables a los ataques de inyección tanto del lado del cliente como del lado del servidor.		
3	Información relevante	La seguridad de la IoT asistida por Edge aún carece de una solución universal, ya que la mayoría de los esquemas se enfocan en abordar uno o pocos tipos particulares de ataques, pero no se adaptan a la mayoría de los otros ataques. Por lo tanto, es un desafío incorporar varios esquemas de seguridad para proteger toda la arquitectura de IoT de manera unificada.		

Tabla 51. Resultado del artículo ES29

#	Descripción	Detalle		Código: ES29
1	Información bibliográfica	Título	Gestión segura de datos distribuidos para la computación en la niebla en aplicaciones de IoT a gran escala: Una solución basada en Blockchain	
		Autores	Chen, Zunming, Cui, Hongyan, Wu, Ensen, Li, Yuanxin Xi, Yu.	
		Referencia	[75]	
		Año	2020	
2	Resumen del artículo	Uno de los desafíos esenciales es la solución de administración de datos distribuidos de la aplicación de IoT a gran escala y los datos masivos que contiene. En este documento los autores proponen una arquitectura novedosa para la gestión segura de datos distribuidos en aplicaciones IoT gran escala. Es una plataforma escalable de gestión de datos distribuidos de varios niveles que se integra con un servicio de almacenamiento fuera de la cadena, que utiliza criptografía de clave pública y Blockchain para el control de acceso y el seguimiento de la procedencia de los datos para garantizar el almacenamiento seguro de los datos y resistir los ataques externos en la computación en la niebla. El modelo del sistema se propone para manejar los problemas de coordinación e integración de la gestión de datos de los nodos Fog distribuidos geográficamente. Está dividido lógicamente en dos partes: gestión del almacenamiento de datos y gestión de la seguridad de los datos, respectivamente. La gestión de seguridad de los datos resuelve la autenticación y autorización escalables en un escenario multiinquilino y la gestión del almacenamiento se ocupa de la eficiencia y eficacia del control de acceso a los datos en los nodos de niebla.		
3	Información relevante	La solución propuesta funciona bien para defenderse contra el acceso no autorizado de manera efectiva en una aplicación de IoT a gran escala y potencia la trazabilidad y procedencia del linaje de datos, escala bien con la pérdida del rendimiento de la comunicación y la computación manteniéndose en un rango aceptable.		

Tabla 52. Resultado del artículo ES30

#	**Descripción**	**Detalle**	**Código: ES30**
1	Información bibliográfica	Título	Aprendizaje federado con preservación de la privacidad en Fog Computing
		Autores	Zhou, Chunyi, Fu, Anmin, Yu, Shui, Yang, Wei, Wang, Huaqun, Zhang, Yuqing
		Referencia	[87]
		Año	2020
2	Resumen del artículo	En este estudio, los autores proponen un esquema de aprendizaje federado que preserva la privacidad en la computación Fog. Este diseño combina modos de entrenamiento centralizados y distribuidos para hacerlo más práctico, lo que también puede resolver el problema de la formación ineficiente causada por la brecha significativa entre los dispositivos IoT en la cantidad de datos y potencia informática. Además, aprovecha la privacidad diferencial, cegador y cifrado homomórfico Paillier para equipar el esquema con la capacidad de resistir ataques de datos, ataques de modelos y ataques de Colisión. Por un lado, puede proteger contra un nodo Fog revelador de privacidad o un servidor de parámetros maliciosos. Por otro lado, también puede evitar que varias entidades maliciosas infieran en los parámetros del modelo de un nodo Fog específico.	
3	Información relevante	El análisis de seguridad demuestra que el esquema propuesto puede garantizar la seguridad de los datos y la seguridad del modelo, y resistir completamente los ataques de Colisión. Los experimentos simulan dos escenarios basados en el conjunto de datos FashionMNIST y muestran que el esquema es eficiente para hacer frente a múltiples distribuciones de datos. Especialmente, con la misma precisión y baja sobrecarga informática, este esquema puede ahorrar mucho tiempo de entrenamiento en comparación con los trabajos existentes.	

Tabla 53. Resultado del artículo ES31

#	Descripción	Detalle		Código: ES31
1	Información bibliográfica	Título	Autenticación mutua y acceso autorizado a los datos entre Fog y el usuario	
		Autores	Arun, M., Balamurali, S., Rawal, Bharat S., Duan, Qiang Kumar, R. Lakshmana, Balamurugan, Balusamy	
		Referencia	[86]	
		Año	2020	
2	Resumen del artículo	Uno de los retos esenciales para la seguridad de la computación Fog es la autenticación entre los servidores Fog que ofrecen servicios y los usuarios Fog. Esta confirmación de seguridad es crítica ya que se ofrece un gran número de usuarios en la computación Fog. Para dar solución a este desafío de seguridad, los autores en este estudio proponen un método de autenticación mutua entre los usuarios de borde y los servidores Fog sin necesidad de infraestructuras de clave pública (PKI). Lo que un usuario necesita tener es solo una clave maestra durante mucho tiempo y, con esto, el usuario puede autenticarse mutuamente con cualquier servidor Fog existente o recién unido. El método hace que los servidores Fog almacenen una clave secreta por usuario y el usuario realiza encriptaciones/desencriptaciones basadas en hash, el usuario crea un índice seguro de encriptación y cifrado de datos que luego son descifrados por el usuario y los servidores autorizados. El sistema propuesto se apoya en la técnica Blockchain para lograr la integridad de los datos cuando se transfieren datos confidenciales entre los dispositivos de Edge y los nodos. Las transacciones entre los nodos se registran en los bloques que son hash para que todos los nodos Edge y Fog estén rodeados por un sistema seguro. Cuando un servidor Edge malicioso entra en la red, se identifica basándose en el libro de contabilidad mantenido en los nodos.		
3	Información relevante	La tecnología Blockchain incorporada en el sistema facilita el mantenimiento de la integridad y la identificación de un nodo malicioso cuando entra en la red. El historial de transacciones en los bloques y su valor hash, aunque es transparente, permite hacer un seguimiento de cualquier nueva entrada en el sistema. Cualquier alteración del hash de los bloques indica la entrada ilegal y proporciona un sistema distribuido Edge-Fog a prueba de manipulaciones.		

Tabla 54. Resultado del artículo ES32

#	Descripción	Detalle	Código: ES32
1	Información bibliográfica	Título	Estudio sobre el análisis seguro de datos en Edge Computing
		Autores	Liu, Dan, Yan, Zheng, Ding, Wenxiu, Atiquzzaman, Mohammed.
		Referencia	[83]
		Año	2019
2	Resumen del artículo	El estudio proporciona un análisis en profundidad de las amenazas a la seguridad en la computación de borde, y las características distintivas del borde. Las características principales del borde son: la conciencia de ubicación, distribución geográfica, baja latencia, soporte de aplicaciones IoT a gran escala, arquitectura de red, hardware (heterogéneos) y movilidad. El borde se enfrenta a problemas de seguridad debido a algunas de estas características como la distribución geográfica la heterogeneidad y baja latencia principalmente, por otro lado, dado que Edge Computing se considera una extensión de la Cloud Computing, hereda algunos problemas de seguridad de la Cloud, además, introduce nuevos riesgos de seguridad debido a sus propias características, estos problemas de seguridad son: ataque físico, ataque de inyección de información, ataque de manipulación de servicios, ataque Sybil, ataque Sinkhole, ataque de espionaje, ataque al canal de interferencia, ataque de manipulación, ataque de denegación de servicio distribuido (DDoS) .	
3	Información relevante	Para lograr una analítica de datos segura, es indispensable desplegar mecanismos de seguridad. Lamentablemente, debido a los recursos restringidos de los dispositivos de borde, los típicos mecanismos de seguridad propuestos en el marco de la nube para mitigar algunos de los problemas de seguridad antes mencionados no se pueden implementar en el borde debido a sus limitaciones.	

Tabla 55. Resultado del artículo ES33

#	Descripción	Detalle		Código: ES33
1	Información bibliográfica	Título	Un mecanismo para asegurar las aplicaciones habilitadas para IoT en la capa de niebla	
		Autores	Abbas, Nadeem, Asim, Muhammad, Tariq, Noshina, Baker, Thar, Abbas, Sohail	
		Referencia	[67]	
		Año	2019	
2	Resumen del artículo	Este documento propone un nuevo Servicio de seguridad Fog (FSS) para proporcionar seguridad de extremo a extremo en la capa Fog para dispositivos IoT utilizando dos esquemas criptográficos bien establecidos, cifrado basado en identidad y firma basada en identidad. El FSS proporciona servicios de seguridad como autenticación, confidencialidad y no repudio de los dispositivos de IoT en la capa Fog. El mecanismo de seguridad funciona como un Servicio de seguridad Fog (FSS) que ayuda en la autenticación de dispositivos IoT, la confidencialidad de los datos generados por los dispositivos IoT y el no repudio (una garantía de que alguien no puede negar su autenticidad). El esquema propuesto es efectivo contra varios ataques, a saber, ataque de fuerza bruta, hombre en el medio, ataque de repetición, escucha a escondidas, ataque de repudiación.		
3	Información relevante	Existen varias técnicas criptográficas que pueden hacer frente de manera eficaz a diferentes ataques de seguridad, pero no son adecuadas para dispositivos IoT con recursos limitados, ya que implican un alto consumo de recursos.		

Tabla 56. Resultado del artículo ES34

#	Descripción	Detalle		Código: ES34
1	Información bibliográfica	Título	Seguridad de la computación en la niebla para las aplicaciones del Internet de las cosas: Desafíos y soluciones	
		Autores	Ni, Jianbing, Zhang, Kuan, Lin, Xiaodong, Shen, Xuemin Sherman.	
		Referencia	[21]	
		Año	2018	
2	Resumen del artículo	En esta encuesta se presenta algunas amenazas de seguridad y privacidad que los atacantes pueden lanzar para interrumpir la computación de niebla, tales ataques son: Falsificación, Manipulación, Spam, Sybil, Jamming, Escucha, Denegación de servicio (DoS), Colisión, Hombre en el medio, Suplantación. Los dispositivos IoT son las principales fuentes de amenazas de seguridad de la computación niebla. Con el creciente número de dispositivos IoT conectados, la vulnerabilidad de los dispositivos IoT		

		exacerba las preocupaciones de los usuarios sobre la seguridad y la privacidad. Debido a la falta de suficiente protección de seguridad, los dispositivos IoT son vulnerables a ser hackeados, rotos o robados. Estos dispositivos comprometidos pueden convertirse en fuentes poderosas y distribuidas para corromper los servicios normales. Algunas características propias de la computación de niebla ponen en peligro la seguridad de la misma, la niebla tiene cinco características distinguidas; reconocimiento de la ubicación, distribución geográfica, baja latencia, soporte de aplicaciones de IoT a gran escala, descentralización, además tiene varias características generales, incluyendo el soporte de movilidad, predominio de acceso inalámbrico, heterogeneidad, análisis en línea o interacción con la nube.
3	Información relevante	Debido a las amenazas a la seguridad mencionadas anteriormente es crucial construir mecanismos eficientes y eficaces seguros y de preservación de la privacidad en la computación de niebla. Sin la protección adecuada de la seguridad y la privacidad, los usuarios pueden no estar dispuestos a participar en aplicaciones de IoT, lo que impide el éxito de la informática de niebla. Las cuestiones de seguridad en IoT y niebla están en desarrollo. El estudio sobre la seguridad de la informática perimetral sigue siendo un tema abierto y vital en los sistemas inteligentes de IoT.

Tabla 57. Resultado del artículo ES35

#	**Descripción**	**Detalle**	**Código: ES35**
1	Información bibliográfica	Título	Un marco de seguridad impulsado por los bordes para la Internet inteligente de los objetos
		Autores	Qiu, Xuesong, Rong, Bo, Ben-Othman, Jalel, Han, Shuai Kodach, Michel.
		Referencia	[73]
		Año	2020
2	Resumen del artículo	Debido a la apertura de los sistemas inteligentes de IoT, un número sin precedentes de nodos de IoT están conectados a los sistemas. Los usuarios malintencionados pueden atacar los servidores y causar fallas en el sistema, así como enviar información falsa para degradar el rendimiento del sistema. Aunque la informática de borde juega un papel central en la oferta de servicios de manera eficaz y eficiente a los dispositivos de IoT, es vulnerable a varias amenazas de seguridad como: ataques de Colisión, ataques internos, ataques DoS, ataques de malware, ataques de interferencia.	
3	Información relevante	Los autores proponen un mecanismo de detección de intrusiones basado en Q-learning para sistemas IoT inteligentes basados en el borde. En el proceso de Q-learning, los nodos de borde aprenden las acciones efectivas en función de la retroalimentación recibida del entorno. Primero, las	

		operaciones de selección y extracción de características de los dispositivos de IoT se realizan para filtrar los datos por los nodos Edge en la fase de filtrado. En segundo lugar, los datos se etiquetan con diferentes características en la fase de etiquetado. En tercer lugar, se lleva a cabo un entrenamiento de Q-learning para clasificar las características de los dispositivos de IoT en la fase de entrenamiento. Finalmente, la información falsa se detecta en base a la especificación del sistema en la fase de detección. Una vez que recibe una alerta de intrusión, el sistema realiza automáticamente acciones para prevenir o mitigar los ataques.

Tabla 58. Resultado del artículo ES36

#	**Descripción**	**Detalle**	**Código: ES36**
1	Información bibliográfica	Título	Problemas de seguridad y privacidad y soluciones para Fog
		Autores	Mukherjee, Mithun, Ferrag, Mohamed Amine, Maglaras, Leandros, Derhab, Abdelouahid, Aazam, Mohammad
		Referencia	[90]
		Año	2020
2	Resumen del artículo	Este estudio hace un breve resumen de todas las contribuciones de investigación que existen hasta la fecha sobre Fog. En muchos casos, Fog, Cloud y los usuarios residen en diferentes dominios de confianza. Esto trae una enorme amenaza a los datos y servicios de IoT. Aunque, los nodos Fog están generalmente en los protocolos de seguridad acordados, pueden espiar la información personal si hay alguna falta de autenticación adecuada y control de acceso. Como resultado, los servicios de IoT se vuelven vulnerables a los diversos ataques, como falsificación, manipulación de datos, interferencia, denegación de servicio (DoS), hombre en el medio y suplantación. Además, la utilización de los recursos también puede verse comprometida. Básicamente, la descentralización y el aprovisionamiento de servicios de baja latencia crean una barrera para la autenticación segura. Además, la movilidad del usuario exige la unión/salida frecuente hacia/desde el clúster Fog que consta de varios nodos de Fog. Como resultado, la administración de claves se convierte en un problema difícil. Aparte de estos, es muy difícil recopilar información relacionada con el comportamiento de todos los usuarios de Fog; por lo tanto, la fiabilidad entre todos los nodos de Fog en la red es un problema crítico.	
3	Información relevante	Para defenderse de los ataques antes mencionados, es necesario desplegar contramedidas preventivas y de detectives. Las contramedidas preventivas consisten en proteger los sistemas de vulnerabilidades como API inseguras y vulnerabilidades basadas en web. También es importante implementar mecanismos de acceso a la aplicación de políticas contra accesos de datos	

		ilegales, actualizaciones de software regulares y anti-malware. En cuanto a la seguridad de las máquinas virtuales, las contramedidas que se pueden adoptar son las directivas de aislamiento, el endurecimiento del hipervisor, la separación de roles y máquinas virtuales y la abstracción de redes. También hay una necesidad vital de implementar un sistema de detección de intrusiones (IDS) en los diferentes dominios de las redes Fog. El IDS debe supervisar el comportamiento de los hosts, las máquinas virtuales y el tráfico de red. Todas las soluciones de privacidad y seguridad propuestas para la Cloud no son adecuadas para Fog debido a varias características distintas, como la arquitectura descentralizada y distribuida de la computación de niebla, así como una escala más amplia de dispositivos de niebla en el borde de la red.

Tabla 59. Resultado del artículo ES37

#	**Descripción**	**Detalle**		**Código: ES37**
1	Información bibliográfica	Título	Lógica difusa y arquitectura segura basada en Fog para el Internet de las cosas (FLFSIoT)	
		Autores	Zahra, Syed Rameem, Chishti, Mohammad Ahsan	
		Referencia	[82]	
		Año	2020	
2	Resumen del artículo	Esta investigación presenta una categorización detallada de los ataques IoT y la propuesta de una arquitectura segura basada en la lógica difusa y Fog para IoT (FLFSIoT)que funciona en tiempo real. Los ataques están categorizados de la siguiente manera; 1) Ataques que explotan la propiedad del dispositivo, dentro de esta categoría se encuentran los ataques de denegación de servicio distribuida DDoS , 2) ataques basados en protocolos, hay dos tipos; desviación de protocolos e interrupción de protocolos, 3) ataques basados en capas que ocurren tanto en dispositivos como en las redes, incluyen: escuchas, colisión, suplantación, manipulación, ataque de spam/duplicación, hombre en el medio (MiM), ataque de blackhole, ataque de inundaciones. Para abordar estos problemas, proponen el uso de la lógica difusa y la arquitectura segura basada en niebla para IoT (FLFSIoT) para aliviar la incertidumbre de pertenecer a un clúster nítido de un nodo perimetral y para detectar varios ataques clásicos. La arquitectura IoT compatible con Fog se ha utilizado para hacer que FLFSIoT sea intrínsecamente más seguro en comparación con el IoT compatible con la cloud omitiendo la latencia y otros problemas.		
3	Información relevante	FLFSIoT funciona en tiempo real, a diferencia de la mayoría de las técnicas de detección de amenazas disponibles en la literatura que funcionan de manera posterior al ataque. Soporte a la incertidumbre, establecimiento de		

		la confianza, escalable a IoT, trata el tráfico real de ataques, utiliza la arquitectura Fog-IoT, base de reglas difusas computacionalmente menos intensiva. La precisión de detección para el ataque DDoS es del 95% y para el ataque de Colisión el 92%.

Tabla 60. Resultado del artículo ES38

#	**Descripción**	**Detalle**	**Código: ES38**
1	Información bibliográfica	Título	Huellas dactilares de los servicios Edge y Cloud del IoT
		Autores	Kim, Donginn, Andalibi, Vafa, Camp, L. Jean
		Referencia	[76]
		Año	2020
2	Resumen del artículo	En este trabajo, los autores proponen un método amigable con la privacidad para detectar ataques MiTM dirigidos a dispositivos IoT. Cuando los dispositivos de IoT interactúan con un servicio remoto, la integridad o autenticación de ese servicio no está garantizada. Es posible usar phishing para convencer a un usuario de que acepte una conexión a un dispositivo desconocido potencialmente malintencionado. En este trabajo, proponen la construcción de un agente local basado en una raspberry pi llamado Block-Pi este se coloca en la red y el tráfico pasa a través de ella. Luego, Block-Pi ejecuta un análisis de paquetes basado en los datos y la información sobre certificados TLS, servidor de caché DNS, rutas ASN con direcciones IP resueltas, información de WHOIS y datos de PhishTank, para realizar huellas digitales de los servicios Edge. En lugar de enviar todos los datos personales a la red, Block-Pi encuesta fuentes de información remotas centralizadas para listas negras y construcción de modelos, integrando información local para crear un modelo distinto para cada instalación.	
3	Información relevante	El objetivo del método propuesto es asegurar la conexión desde un dispositivo IoT para identificar y mitigar los ataques MiTM sin sacrificar la privacidad de los usuarios. Proponen cambiar el paradigma actual de las huellas dactilares para que los dispositivos en el borde tomen las huellas dactilares colaborativamente de los servicios remotos, identificando las desviaciones de las operaciones normales.	

Tabla 61. Resultado del artículo ES39

#	Descripción	Detalle		Código: ES39
1	Información bibliográfica	Título	Seguridad y privacidad para IoT y el paradigma de la Fog Computing	
		Autores	Mukherjee, Mithun, Ferrag, Mohamed Amine, Maglaras, Leandros, Derhab, Abdelouahid, Aazam, Mohammad	
		Referencia	[8]	
		Año	2020	
2	Resumen del artículo	En este trabajo de investigación se abordan los problemas de seguridad que se presentan en las diferentes capas del IoT y que la computación de niebla heredaría de la nube, estos problemas incluyen, ataque DoS y DDoS, ataque de hombre en el medio, ataque de agujero negro, ataque de inundaciones, ataque de desincronización, ataque homing, ataque de agujero de gusano, ataque sybil y clon, ataque sumidero, ataque RPL, ataque de manipulación física. Una solución identificada en este estudio para abordar algunos de los problemas antes mencionados, es utilizar el cifrado basado en atributos ciphertext-policy (CP-ABE), que es una técnica criptográfica reconocida para garantizar la confidencialidad de los datos y proporciona un control de acceso firme.		
3	Información relevante	Además, los autores presentan un modelo de gestión de confianza basado en el riesgo para el entorno sanitario inteligente con el fin de hacer frente a los problemas relacionados con la seguridad y privacidad en este ecosistema heterogéneo altamente impredecible.		

Tabla 62. Resultado del artículo ES40

#	Descripción	Detalle		Código: ES40
1	Información bibliográfica	Título	Una encuesta: Integración de IoT y Fog Computing	
		Autores	Jalasri, M., Lakshmanan, Dr L.	
		Referencia	[44]	
		Año	2018	
2	Resumen del artículo	Este artículo presenta un estudio de IoT y FC con las amenazas a la seguridad y también los beneficios de su combinación. Las características más destacadas de FC son: Reconocimiento de la ubicación, distribución geográfica, baja latencia, soporte de aplicaciones IoT a gran escala, descentralización; algunas de estas características abren puertas para algunos ataques de seguridad tales como; manipulación, escuchas clandestinos, denegación de servicio, Colisión y hombre en el medio. El objetivo principal de la integración de Fog computing y la IoT es aumentar el rendimiento, la eficiencia y reducir la latencia de respuesta, el procesamiento y el tiempo de almacenamiento. La integración de Fog y IoT proporcionan		

		más seguridad mientras transfieren información a los nodos Fog y también reducen el tráfico de red en lugar de utilizar la Cloud.
3	Información relevante	El estudio presenta los principales desafíos de seguridad y privacidad a los que se enfrenta el IoT y Fog como la autenticación, la verificación de la ubicación y el control de acceso.

Tabla 63. Resultado del artículo ES41

#	**Descripción**	**Detalle**	**Código: ES41**
1	Información bibliográfica	Título	Retos de seguridad Fog y IoT, tecnología Blockchain y soluciones de árbol celular: una revisión
		Autores	Khan, Neelam Saleem, Chishti, Mohammad Ahsan
		Referencia	[45]
		Año	2020
		Revista	Scalable Computing
2	Resumen del artículo	Dado que la mayoría de los dispositivos conectados en red no se autentican mutuamente, los ataques se vuelven inevitables. Teniendo en cuenta la naturaleza muy dinámica de los nodos Fog que siguen uniéndose o saliendo de la capa Fog con mucha frecuencia, las estrictas políticas de seguridad y privacidad actuales adaptadas en el entorno de Cloud Computing no son directamente aplicables debido a la movilidad de los nodos. En esta investigación los autores discuten los problemas de seguridad en IoT como causa de una mala autenticación, que incluyen: manipulación e inyección de código malicioso, inyección de nodo falso y ataque de canal lateral, ataque de información de enrutamiento, reenvío selectivo y ataque de sumidero, ataque de hombre en el medio, ataque de repetición, además, algunas contramedidas propuestas por diferentes investigadores para dar solución a estos problemas. Si bien ciertas soluciones existentes en la Cloud también podrían resolver muchos desafíos de seguridad y privacidad en Fog Computing, pero debido al soporte de movilidad, que es una característica importante en la computación de niebla, es probable que presente muchos desafíos nuevos de seguridad y privacidad.	
3	Información relevante	Aquí proponen el uso de Blockchain para mejorar la seguridad de IoT. Blockchain asegura la integridad y la autenticación de los datos al garantizar que los datos que se transmiten estén criptográficamente protegidos y firmados por el remitente legítimo. Los contratos inteligentes de Blockchain pueden garantizar la autenticación y la privacidad. Cada dispositivo de IoT una vez instalado y conectado a la red Blockchain tendría su GUID único y su par de claves simétricas; por lo tanto, en Blockchain, la distribución y la gestión de claves se eliminan por completo.	

Tabla 64. Resultado del artículo ES42

#	Descripción	Detalle		Código: ES42
1	Información bibliográfica	Título	IMPACT: Detección de ataques de suplantación de identidad a través de Edge Computing utilizando autocodificador profundo y abstracción de características	
		Autores	Lee, Seo Jin, Yoo, Paul D., Taufiq Asyhari, A., Jhi, Yoonchan, Chermak, Lounis, Yeun, Chan Yeob, Taha, Kamal	
		Referencia	[85]	
		Año	2020	
2	Resumen del artículo	En este estudio presenta el diseño y desarrollo un IDS ligero basado en ML adaptado a los dispositivos con recursos limitados. En concreto, el estudio propone un modelo IDS ligero basado en ML, a saber, IMPACT (IMPersonation Attack deteCTion) mediante codificador automático profundo y abstracción de características. Esto se basa en el aprendizaje profundo de entidades con la máquina vectorial de soporte lineal basada en degradado (SVM) para implementar y ejecutarse en dispositivos con recursos limitados al reducir el número de entidades mediante la extracción y selección de entidades mediante un codificador automático apilado (SAE), información mutua (MI) y contenedor C4.8. El IMPACT está entrenado en el Dataset de Intrusión Wi-Fi del Egeo (AWID) para detectar ataques de suplantación.		
3	Información relevante	Los resultados numéricos muestran que el IMPACT propuesto alcanzó una precisión del 98,22% con una tasa de detección del 97,64% y una tasa de falsa alarma del 1,20% y superó a los modelos de referencia existentes.		

Tabla 65. Resultado del artículo ES43

#	Descripción	Detalle		Código: ES43
1	Información bibliográfica	Título	Defensa del borde definida por software contra los DDoS basados en el IoT	
		Autores	Ozcelik, Mert, Chalabianloo, Niaz, Gur, Gurkan	
		Referencia	[68]	
		Año	2017	
		Revista	IEEE Access	
2	Resumen del artículo	En esta investigación presentan un esquema de detección / mitigación orientada al borde contra DDoS en IoT utilizando enfoques SDN y Fog mientras utilizan Mirai como estudio de caso. El mecanismo de detección ECESID implementa dos algoritmos, primero Threshold Random Walk with Credit Based Rate Limiting (TRW-CB) tiene como objetivo detectar la fase de escaneo de malware en un host basándose en la premisa de que la probabilidad de que un intento de conexión sea exitoso debería ser mucho		

		mayor para un host benigno que para uno malicioso. TRW-CB utiliza pruebas de hipótesis secuenciales para decidir si un nodo está infectado. Mantiene una cola de TCP SYN para cada host. Si se recibe TCP RST o se agota el tiempo de espera, TRW-CB lo retira de la cola y aumenta el índice de probabilidad del host para ser declarado infectado; de lo contrario, el índice de probabilidad disminuye. Rate Limiting (RL) es otro algoritmo de detección que utiliza la observación de que un host infectado intenta conectarse a tantos hosts diferentes como sea posible en poco tiempo con el propósito de propagar el virus. Este algoritmo compara las nuevas solicitudes de conexión con una lista de hosts recientemente contactados denominada "conjunto de trabajo". Si la solicitud es para un host que está en el conjunto de trabajo, normalmente se reenvía; de lo contrario, se coloca en una cola de espera. Cada segunda, se saca una conexión de la cola de retardo y se le permite continuar.
3	Información relevante	El sistema esta propuesto para detectar hosts maliciosos y mitigar un posible ataque DDoS en la fase inicial. SDN se utilizó como una solución flexible para dictar nuevas reglas de flujo y actualizarlas dinámicamente cuando fuera necesario. Aunque ECESID está orientado a las variantes de Mirai, su mecanismo de detección se puede configurar y ampliar fácilmente para diferentes amenazas de BotNet. También utilizan la computación de niebla para facilitar ECESID en este entorno. El esquema propuesto mostró que los ataques DDoS de IoT se pueden mitigar usando SDN cuando se acerca al borde usando la computación Fog.

Tabla 66. Resultado del artículo ES44

#	**Descripción**	**Detalle**	**Código: ES44**
1	Información bibliográfica	Título	Seguridad de los dispositivos de Edge de bajos recursos para los sistemas de IoT
		Autores	Shapsough, Shams, Aloul, Fadi, Zualkernan, Imran A.
		Referencia	[56]
		Año	2018
2	Resumen del artículo	El trabajo presentado aquí examina los problemas de seguridad clave en un sistema de IoT con un énfasis especial en los dispositivos de borde. Se utilizó un dispositivo de borde de IoT comercial que utiliza los protocolos MQTT (+ TLS) y CoAP (+ DTLS) para analizar el impacto de estos problemas de seguridad. Se descubrió que este dispositivo periférico era susceptible a ataques de inyección de datos y nodos maliciosos. La inyección de código malicioso no fue posible en este tipo de nodo Edge.	

3	Información relevante	Los dispositivos Edge interactúan directamente con el entorno físico mediante etiquetas RFID, sensores, actuadores y dispositivos integrados. Como componente crítico de cualquier aplicación de IoT, la capa perimetral proporciona un objetivo rico a los atacantes, en el que pueden obtener acceso, comprometer o derribar todo el sistema. Los ataques dirigidos a dispositivos Edge pueden clasificarse en denegación de servicios, recopilación de información o escuchas clandestinas y plantación de nodos maliciosos.

Tabla 67. Resultado del artículo ES45

#	**Descripción**	**Detalle**		**Código: ES45**
1	Información bibliográfica	Título	Cuestiones de seguridad y privacidad en el entorno del IoT impulsado por Fog	
		Autores	Verma, Richa, Chandra, Shalini	
		Referencia	[69]	
		Año	2019	
2	Resumen del artículo	En este estudio se lleva a cabo el análisis de la integración de Fog Computing con el IoT y los problemas a la seguridad relacionados con el entorno de Fog e IoT. Con el crecimiento de la expansión de IoT, entran en juego nuevos problemas de seguridad, mientras que los existentes se vuelven más graves. La autenticación es uno de los principales desafíos incluso es considerado uno de los principales problemas de seguridad, a diferencia de la Cloud donde los centros de datos son propiedad del proveedor de servicios la implementación de Edge puede tener diferentes proveedores lo que hace indispensable la implementación de un mecanismo para autenticar los nodos Edge entre sí y con los dispositivos IoT. Algunos de los problemas de seguridad existentes en el entorno IoT identificados en este estudio son: ataque de nodo falso, ataque de enrutamiento, y Spam.		
3	Información relevante	Debido a los problemas de seguridad antes mencionados es indispensable la implementación de técnicas como el control de acceso y la detección de intrusiones. El principal desafío que persiste en la computación de niebla es diseñar un esquema de control de acceso de tal manera que monitoree todos los tramos entre IoT-Fog-Cloud y también administre la naturaleza de la restricción de recursos. Las técnicas de detección de intrusiones generalmente se implementan en el sistema Fog para combatir ataques como ataque de inundación, ataque interno, ataque a máquinas virtuales, escaneo de puertos, etc. actividades intrusivas mediante el análisis y la supervisión de archivos de registro, la información de inicio de sesión del usuario y la información de control de acceso.		

Tabla 68. Resultado del artículo ES46

#	Descripción	Detalle		Código: ES46
1	Información bibliográfica	Título	Ransomware dirigido: Una nueva amenaza cibernética para el sistema de borde del Internet industrial de las cosas de Brownfield	
		Autores	Al-Hawawreh, Muna, Hartog, Frank Den, Sitnikova, Elena	
		Referencia	[61]	
		Año	2019	
2	Resumen del artículo	Esta investigación presenta un estudio sobre el ataque de ransomware dirigido en las puertas de enlace IIoT. Los autores concluyen que los atacantes encuentran atractivas las puertas de enlace de borde IIoT para dirigir ataques ransomware debido a sus roles y funcionalidades vitales al trabajar con infraestructuras críticas y que la probabilidad de tal ataque es alta. Crean la primera versión de un banco de pruebas de seguridad de ransomware para IIoT y, con fines de prueba, desarrollan una primera versión del objetivo de ransomware en la puerta de enlace de borde de IIoT en un sistema brownfield. En un sistema brownfield, puede haber muchos objetivos atractivos para un ataque de ransomware, como dispositivos físicos, puertas de enlace perimetrales, servidores en la nube e interfaces de usuario final. Las técnicas y tácticas de los atacantes de ransomware dirigidos normalmente se centran en encontrar los objetivos más valiosos, lo más fácil posible y con la menor complejidad posible en el proceso de compromiso. Por lo tanto, vemos la puerta de enlace de borde como un objetivo preferido para los ataques de ransomware en los sistemas IIoT, debido a su ubicación y funcionalidad. Es un punto crítico de falla, ya que es el puente entre el mundo físico (generalmente confiable) y el cibernético (generalmente no confiable), y proporciona varios servicios a los dispositivos físicos y usuarios finales. También es el punto de entrada para cualquier vector de amenaza, el primero en ser atacado y también la primera línea de defensa		
3	Información relevante	La probabilidad de que una puerta de enlace de borde IIoT sea atacada por ransomware puede entenderse cualitativamente al observar el historial reciente de ataques de malware / ransomware en dispositivos, arquitecturas y funcionalidades similares. Por lo tanto, asumimos que la propiedad de Markov de orden superior se mantiene, es decir, la posibilidad de que se produzca un ataque de ransomware dirigido a las puertas de enlace de borde IIoT depende directamente del número y la eficacia de ataques similares en el pasado.		

Tabla 69. Resultado del artículo ES47

#	**Descripción**	**Detalle**	**Código: ES47**
1	Información bibliográfica	Título	Detección de datos falsos para redes de niebla y del Internet de las cosas
		Autores	Fantacci, Romano, Nizzi, Francesca, Pecorella, Tommaso, Pierucci, Laura, Roveri, Manuel
		Referencia	[65]
		Año	2019
2	Resumen del artículo	En este artículo proponen un método de detección de ataques, denominado Sistema de Detección de Intrusiones de Datos (DataIDS), basado en el análisis de datos en tiempo real. Dado que los dispositivos finales tienen principalmente recursos limitados, se introduce la computación en la niebla (FC) para implementar el DataIDS. El FC aumenta las capacidades de almacenamiento, cálculo y procesamiento, lo que le permite detectar rápidamente un ataque con respecto a las soluciones de seguridad en la nube. DataIDS está diseñado específicamente para redes Fog/IoT, basado en el análisis de datos físicos para reconocer mejor las vulnerabilidades contra los dispositivos finales. Las mediciones realizadas por los sensores se envían a la unidad Fog(FU), que procesa localmente los flujos de datos, y si se detecta un comportamiento anómalo, puede dar la alarma y gestionar las correspondientes contramedidas adecuadas, por ejemplo, aislar los dispositivos atacados, descartar sus datos, autenticar un sensor y sus datos, o reconfigurar las direcciones IP. Las características distintivas de DataIDS son: i) la capacidad de detectar una inyección de datos maliciosa mediante el análisis de los flujos de datos adquiridos por los dispositivos y, ii) al mismo tiempo, encontrar los dispositivos que se están comportando mal. La idea clave es construir un gráfico de dependencia analizando la correlación cruzada entre los respectivos flujos de datos de los sensores y utilizar esa información para poner de manifiesto cualquier anomalía en el sistema. Esto permite reaccionar rápidamente ante una amenaza con las acciones apropiadas y/o activar otros mecanismos de análisis destinados a verificar las condiciones de salud de los sensores.	
3	Información relevante	Para complementar el enfoque de DataIDS, proponen un novedoso árbol de ataques con riesgos asociados, costes y nivel de daño potencial al sistema. En función de las amenazas detectadas, el árbol de ataques es un método válido para seleccionar la acción adecuada a realizar, que puede abarcar desde el simple descarte de los datos de los sensores atacados hasta una reconfiguración completa de la red.	

Tabla 70. Resultado del artículo ES48

#	Descripción	Detalle	Código: ES48
1	Información bibliográfica	Título	Ataque adaptativo de colisión de texto plano en AES enmascarado en Edge Computing
		Autores	Ding, Yaoling, Shi, Ying, Wang, An Zheng, Xuexin Wang, Zongyue, Zhang, Guoshuang
		Referencia	[92]
		Año	2019
2	Resumen del artículo	En este artículo presentan un método para la detección de ataques de colisión. Mediante un modelo apropiado, extraen información de la distancia Hamming entre el byte de texto plano actual y el objetivo. Con esta información, reducen el espacio de texto plano candidato en un bucle y detecta una colisión a gran velocidad. Los algoritmos criptográficos empleados en la computación de borde o en cualquier otra aplicación suelen implementarse con contramedidas para defenderse de los ataques de canal lateral. El enmascaramiento es una contramedida muy utilizada. Los autores proponen un nuevo método para explorar la información extra obtenida del ataque de colisión tradicional basado en LSM sobre AES enmascarado. Esta información ayuda a encontrar una colisión a gran velocidad en lugar de buscar exhaustivamente los textos planos. Además, se estudian y comparan algunos modelos como LAD, LADα, CMP. Los resultados experimentales muestran que el método requiere un 2,03% de textos planos y un 5,44% de trazas de ataque de colisión-correlación para detectar una colisión entre dos entradas de cajas S.	
3	Información relevante	Desde la aparición de este problema de seguridad se han presentado muchos algoritmos de detección de colisiones, la mayoría de los cuales enumeran todos los valores del byte de texto plano objetivo para encontrar una colisión. En este estudio establecen una relación entre la distancia euclidiana entre trazos y la distancia de Hamming entre valores, y aprovechan la información de distancia filtrada de los trazos de potencia de encriptación de un texto plano elegido de forma adaptativa para reducir el espacio de texto plano candidato. En consecuencia, la colisión se detecta a gran velocidad. Además, esta mejora es tolerante a los fallos, y su característica de autocorrección promueve la eficacia de los ataques basados en el método de forma significativa.	

Tabla 71. Resultado del artículo ES49

#	**Descripción**	**Detalle**		**Código: ES49**
1	Información bibliográfica	Título	Mitigación de los ataques DoS en la capa EDGE de IoT para preservar los temas de QoS y la energía de los nodos	
		Autores	De Rango, Floriano, Tropea, Mauro, Fazio, Peppino	
		Referencia	[81]	
		Año	2020	
2	Resumen del artículo	El objetivo de este trabajo es modelar y evaluar un nuevo sistema de seguridad IoT en una red de Fog/Edge donde hay nodos ligeros que intercambian mensajes a través del protocolo Message Queue Telemetry Transport (MQTT). Este trabajo tiene como objetivo aumentar la seguridad de este protocolo a nivel aplicación, en particular mitigando la manipulación de datos y las escuchas mediante el uso de criptografía de curva elíptica (ECC), y aplicando diferentes mecanismos de seguridad a los temas de datos. Esta función permite aplicar una política de descarte de paquetes basada en umbrales para preservar la calidad de servicio (QoS) de los temas MQTT. El sistema de seguridad propuesto aplica una política de gestión de colas activa denominada WFSQ-IG y es capaz de distribuir el efecto de los ataques DoS en diferentes colas de TOPICs con los mismos niveles de QoS. La combinación de niveles de QoS aplicada a los TOPIC con diferentes mecanismos de seguridad, combinada con WFSQ, es capaz de reducir el número de paquetes perdidos, preservando el espacio del buffer y sirviendo más solicitudes heredadas. Además, el WFSQ-IG es capaz de garantizar una equidad en la degradación de la QoS para los datos que solicitan los mismos niveles de QoS.		
3	Información relevante	Los problemas de seguridad que enfrenta el IoT, donde el aumento de la conectividad ofrece nuevas oportunidades a los nodos maliciosos haciendo que los dispositivos conectados estén expuestos a la amenaza de ciberataques. Un IDS no puede proteger de la clonación de objetos, la sustitución maliciosa de objetos, sustitución de firmware y extracción de parámetros de seguridad, pero puede ofrecer protección contra: ataque de espionaje, ataque de hombre en el medio, ataque de enrutamiento, ataque DoS, ataque de repetición.		

Tabla 72. Resultado del artículo ES50

#	Descripción	Detalle		Código: ES50
1	Información bibliográfica	Título	Programación de flujos de trabajo científicos en entornos Fog múltiple mediante modelos de Markov y un algoritmo de enjambre salp híbrido	
		Autores	Ahmed, Omed Hassan, Lu, Joan Ahmed, Aram, Mahmood Rahmani, Amir Masoud Hosseinzadeh, Mehdi Masdari, Mohammad	
		Referencia	[89]	
		Año	2020	
2	Resumen del artículo	Este estudio presenta un análisis de los diferentes tipos de ataques DDoS que padece Fog Computing, esto genera un impacto negativo en la programación de flujo de trabajo enviados por IoT. Para hacer frente a estos problemas, se propone un algoritmo de optimización híbrida, que comprende tanto la optimización de enjambre de partículas (PSO) como el algoritmo Salp Swarm (SSA), para resolver el problema de programación de flujo de trabajo en varios entornos de computación de niebla. Se proponen dos modelos discretos de la cadena Markov para cada entorno de computación de niebla para abordar los efectos de los ataques DDoS en ellos. El primer modelo Markov calcula el ancho de banda de red disponible promedio para cada niebla y el segundo modelo markov encuentra el número promedio de máquinas virtuales (VM) disponibles para cada niebla; los modelos abordan diferentes niveles de ataques DDoS.		
3	Información relevante	El algoritmo de optimización propuesto se utiliza para programar flujos de trabajo de IoT en varios entornos de Fog que admiten la red de IoT y minimizan el flujo de trabajo y el número de máquinas virtuales aplicadas Fog. Por lo general, el rendimiento de los entornos de computación de niebla puede verse afectado por ataques DDoS. Para hacer frente a este problema, en este esquema, se han propuesto dos modelos discretos de la cadena Markov para calcular el número medio de máquinas virtuales disponibles para cada entorno de niebla. Con estos modelos de Markov, se puede asignar un número decente de recursos para ejecutar el flujo de trabajo, sin sobreestimar el número de máquinas virtuales en entornos de computación de niebla.		

11.3. Anexo 3: Informe de la revisión

A continuación, se adjunta el informe final de la Revisión Sistemática de Literatura, presentado en forma de artículo científico.

Problemas de seguridad del IoT en el contexto del Edge Computing. Una Revisión Sistemática de Literatura

IoT security issues in the context of Edge Computing. A Systematic Review of Literature

Resumen—**La gran cantidad de dispositivos conectados al internet han ocasionado que el modelo tradicional de computación en la nube (Cloud Computing) se convierta en un cuello de botella. Esto ha motivado en los últimos años el avance de la computación perimetral o de borde (Edge Computing) o computación en la niebla (Fog Computing), la cual brinda capacidades de análisis y procesamiento más cerca de donde se generan los datos. Por la gran cantidad de información que estará expuesta en Edge Computing, surge la necesidad de estudiar a profundidad la seguridad en los escenarios que plantean estos nuevos paradigmas; por tal motivo, el presente trabajo muestra los resultados de una Revisión Sistemática de Literatura (SLR), en la cual, de los 50 estudios analizados se identificaron 24 problemas de seguridad, los cuales se los identifica como ataques que afectan en su gran mayoría al IoT y también son los más frecuentes en Edge Computing, algunos de estos son: el ataque DoS y DDoS, ataque de hombre en el medio, ataque de suplantación de identidad, ataques de repetición, ataque de colusión, ataque de manipulación física, ataque de inyección de nodo falso y clonación de dispositivos; de igual manera, se determinó qué el conocimiento de la ubicación, la distribución geográfica, la arquitectura descentralizada, el soporte de movilidad, la escalabilidad y el consumo energético reducido, son características que aportan para que se produzcan ataques de seguridad.**

Abstract—**The large number of devices connected to the Internet have caused the traditional cloud computing model to become a bottleneck. In recent years, this has motivated the advancement of edge computing or fog computing, which provides analysis and processing capabilities closer to where the data is generated. Due to the large amount of information that will be exposed in Edge Computing, the need arises to study security in depth in the scenarios proposed by these new paradigms; For this reason, the present work shows the results of a Systematic Literature Review (SLR), in which, of the 50 studies analyzed, 24 security problems were identified, which are identified as attacks that mostly affect the user. IoT and are also the most frequent in Edge Computing, some of these are: DoS and DDoS attack, man-in-the-middle attack, phishing attack, replay attacks, collusion attack, physical manipulation attack, fake node injection and device cloning; In the same way, it was determined what: knowledge of the location, geographical distribution, decentralized architecture, mobility support, scalability and reduced energy consumption, are characteristics that contribute to the occurrence of security attacks.**

Keywords – IoT; Internet of Things; Edge Computing; Fog Computing; security; issues; threats; attacks; vulnerability.

INTRODUCCIÓN

El Internet de las cosas (IoT) conecta miles de millones de objetos que generan un volumen significativo de datos los cuales se envían a la nube para su procesamiento, lo que hace que se genere un cuello de botella [1]. Esto afecta de forma directa al tiempo de respuesta de los sistemas de IoT, lo que, en entornos como vehículos inteligentes, monitoreo de salud e industria 4.0 puede provocar problemas críticos [2]. Esto ha provocado el surgimiento del paradigma de Edge/Fog Computing. La idea básica de este paradigma según [3] es: "utilizar una infraestructura descentralizada y semi distribuida en la que los servidores virtualizados, o nodos perimetrales, se implementan en el perímetro de la red. Estos nodos perimetrales coexisten y cooperan entre sí y con sistemas de nube centralizados". Este paradigma tiene el potencial de proporcionar servicios de bajo costo, con suficiente ancho de banda y en tiempo real para respaldar las aplicaciones emergentes de ciudades inteligentes. Sin embargo, las propiedades de la computación perimetral plantean nuevos desafíos de seguridad y privacidad; por lo tanto, las soluciones en este ámbito existentes para la Cloud Computing no se pueden aplicar directamente a Edge Computing debido a sus propiedades específicas, como movilidad, heterogeneidad, gran escala y distribución geográfica [3][4][5]. De modo, que a pesar de que los dominios de servicio y distribución de mercado de IoT están creciendo rápidamente, sus condiciones de seguridad siguen siendo preocupantes. La seguridad es un desafío importante en la computación de borde, debido a que todo el ecosistema no estará controlado por un solo propietario, aún más, los centros de datos Edge son capaces de proporcionar servicios sin depender continuamente de una infraestructura central. Por un lado, el Edge Computing proporciona campos de aplicación muy importantes; y, por otro lado, su surgimiento crea más amenazas de seguridad, ya que aumenta la superficie de ataque [6].

El presente trabajo es una Revisión Sistemática de Literatura (SLR), cuyo objetivo fue identificar los problemas de seguridad del IoT y cómo estos afectan al Edge Computing y las características de este paradigma que generan vulnerabilidades en dispositivos IoT.

METODOLOGÍA

La revisión sistemática de literatura se basa en la metodología planteada por Torres-Carrión [7], aplicada a la ingeniería y educación, la cual, está basada en el protocolo de revisión sistemática de Kitchenham y Bacca [8], dicho proceso se resume en tres fases principales: Planificación de la revisión,

Realización de la revisión e Informe de la revisión. Cada fase contiene diferentes sub-fases o tareas las cuales se describen a continuación.

1. Planificación de la revisión.
   1.1 Identificación de la necesidad de revisión.
   1.1.1 Estado actual del problema de Investigación.
   1.1.2 Preguntas de investigación.
   1.1.3. "Mentefacto conceptual"
   1.1.4. Revisiones sistemáticas relacionadas.
   1.2. Desarrollo de un protocolo de revisión.
   1.2.1. Definición de criterios de inclusión y exclusión.
   1.2.2. Preparación de un formulario de extracción de datos.
   1.2.3. Selección de revistas o bases de datos.
2. Realización de la revisión
   2.1. Identificación de la investigación.
   2.2. Selección de estudios primarios.
   2.3. Evaluación de la calidad del estudio.
   2.4. Extracción y seguimiento de datos.
   2.5. Síntesis y monitoreo de datos.
3. Informe de la revisión
   3.1. Redactar informe de la revisión.

Las fases y sub-fases anteriormente descritas han sido realizadas para cumplir con el propósito planteado en la sección Alcance.

RESULTADOS

Planificación de la revisión

Identificación de la necesidad de una revisión

El propósito de esta SLR surge de la necesidad de conocer el estado actual de la seguridad del IoT con respecto a su integración con el nuevo paradigma Edge Computing, específicamente interesa conocer cuáles son los problemas de seguridad que ambos comparten. Cabe recalcar que a pesar de que Edge Computing es un paradigma que fue introducido por Cisco Company en 2014, no cuenta con los estudios necesarios que aborden de forma precisa la seguridad respecto a su integración con el IoT. A causa de esto, es importante analizar el estado actual de los problemas de seguridad que afectan al IoT bajo el contexto del Edge Computing y también es necesario conocer ciertas características que posee el Edge Computing que causan problemas de seguridad en dispositivos IoT

Preguntas de investigación

A continuación, en la TABLA I se presentan las preguntas de investigación que fueron la base sobre la cual, se guió el desarrollo de dicho estudio.

TABLA I. PREGUNTAS DE INVESTIGACIÓN

	Preguntas de investigación
RQ1	¿Cómo los problemas de seguridad que presenta actualmente el IoT afectan al Edge Computing?
RQ2	¿Cuáles son las características del Edge Computing que generan problemas de seguridad en dispositivos IoT?

El desarrollo de un protocolo de revisión

Diseño del protocolo de búsqueda

Estrategias de búsqueda

El protocolo a implementar es el recomendado por Petticrew y Roberts [9], a través del uso de PICOC (Población, Intervención, Comparación, Resultado y Contexto), se estructuran los cinco componentes para construir la cadena de búsqueda, además, se utilizó la ayuda de la herramienta en línea Parsifal para organizar y seleccionar de mejor manera la documentación.

Fuentes bibliográficas

Para la búsqueda y obtención de la documentación se ha seleccionado las bases de datos científicas más relevantes:

- Web of Science (WoS) (https://www.recursoscientificos.fecyt.es/)
- Scopus (http://www.scopus.com)
- IEEE Digital Library (https://ieeexplore.ieee.org/)
- Google Scholar (https://scholar.google.com/)

Definir palabras claves para el problema de estudio

Con la elaboración del mentefacto conceptual y la definición de los criterios PICOC se obtuvo un conjunto de palabras claves, las mismas que permitieron construir las cadenas de búsquedas, estas son: Internet de las cosas, computación de niebla, computación de borde, niebla, borde, seguridad, problemas, amenazas, ataques, vulnerabilidad. Así como también su traducción al inglés: Internet of things, fog computing, edge computing, fog, edge, security, problems, issues, threats, attacks, vulnerability.

Cadenas de búsqueda

Para una mejor búsqueda y comprensión de la investigación se estableció una cadena relacionando ambos temas, IoT y Edge/Fog Computing. Para evitar el sesgo en la búsqueda se trató de utilizar la sintaxis lo más similar posible en las cuatro bases de datos: WoS, Scopus, IEEE Digital Library y Google Scholar. En la TABLA II se muestran las cadenas de búsqueda con la estructura aplicada a cada base de datos

TABLA II. CADENAS DE BÚSQUEDA

Base de datos	**Cadenas de búsqueda**
Web of Science	(TI = ("Edge Computing" OR "Fog Computing" OR "Edge" OR "Fog") AND TI = ("Internet of Things" OR "IoT") AND TS = ("security" OR "security problems" OR "security issues" OR "threats" OR "attacks" OR "vulnerability"))
Scopus	TITLE ("Edge Computing" OR "Fog computing" OR "Edge" OR "Fog") AND TITLE ("Internet of Things" OR "IoT") AND TITLE-ABS-KEY ("security" OR "security problems" OR "security issues" OR "threats" OR "attacks" OR "vulnerability")

IEEE Digital Library	("Document Title":"Edge Computing" OR "Document Title":"Fog computing" OR "Document Title":"Edge" OR "Document Title":"Fog") AND ("Document Title":"Internet of things" OR "IoT") AND ("Abstract": "security" OR "Abstract":"security problems" OR "Abstract":"security issues" OR "Abstract":"threats" OR "Abstract":"attacks" OR "Abstract": "vulnerability*")
Google Scholar	allintitle: ("Edge Computing" OR "Fog computing" OR Edge OR Fog AND "Internet of things" OR "IoT" AND security) AND "security problems" OR "security issues" OR threats OR attacks OR vulnerability

Criterios de inclusión y exclusión

A continuación, en la TABLA III, se muestran los criterios de inclusión y exclusión que permitieron seleccionar los estudios correctos para dar respuesta a las preguntas de investigación planteadas.

TABLA III. CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios de inclusión	• Los artículos deben estar escritos en inglés. • Los artículos deben estar publicados desde el 2016 al 2020. • Los artículos deben contener problemas de seguridad en IoT, Edge Computing o Fog Computing. • Los artículos cuyo título y resumen contengan las palabras clave. • Se tomarán en cuenta artículos científicos, conferencias, revistas.
Criterios de exclusión	• Todos los artículos que no contengan información sobre seguridad IoT, Edge Computing o Fog Computing. • Todos los artículos que no aporten a resolver las preguntas de investigación. • Todos los artículos que contengan información de seguridad en Cloud Computing. • Todos los artículos que no estén escritos en inglés.

Realizar la revisión

Identificación de la investigación

El objetivo de la presente revisión sistemática de literatura, es dar respuesta a las preguntas de investigación, a través de la búsqueda de estudios primarios que contribuyan con información fiable en torno a los temas de interés.

Selección de los estudios primarios

En la Fig. 1, se muestra el diagrama de flujo del proceso que se realizó para la selección de estudios primarios.

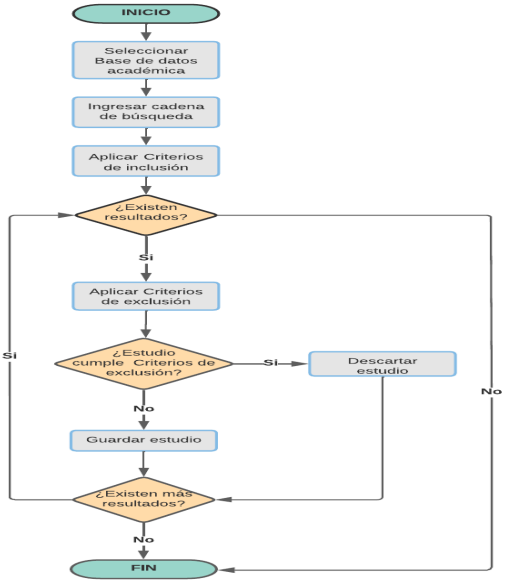

Figura 1. Proceso de Selección de Estudios

En la TABLA IV se presenta un resumen de los estudios que fueron encontrados junto con el número de estudios seleccionados según la base de datos.

TABLA IV. RESUMEN DE ESTUDIOS SELECCIONADOS

Base de datos	Encontrados	Seleccionados
Web of Science	341	63
Scopus	496	31
IEEE Digital Library	516	38
Google Scholar	13	4
Total	1366	136

Evaluación de calidad

Para evaluar la calidad de los estudios seleccionados para la presente SLR se elaboró una lista de verificación de evaluación de la calidad que debe cumplir cada estudio para ser considerado válido.

P1: ¿El estudio aborda los problemas de seguridad en IoT?
P2: ¿El estudio aborda los problemas de seguridad de IoT basado en Edge Computing o Fog Computing?
P3: ¿El estudio menciona las características de Edge Computing o Fog Computing?
P4: ¿El estudio menciona alguna solución para mitigar los problemas de seguridad del IoT y Edge Computing o Fog Computing?

Extracción y monitoreo de datos

Luego de hacer la evaluación de calidad se obtuvo un total de 50 estudios aceptados para el análisis. Estos se detallan a continuación en la TABLA V.

TABLA V. ESTUDIOS SELECCIONADOS

N°	Titulo	Año
ES01	Passban IDS: Un sistema inteligente de detección de intrusos basado en anomalías para dispositivos IoT Edge	2020
ES02	Hacia una Internet de los objetos asistida por el borde: Desde la perspectiva de la seguridad y la eficiencia	2019
ES03	Marco controlado por la SDN asistida por la niebla para la detección duradera de anomalías en una red IoT	2018
ES04	Un marco basado en la computación en la niebla para la preservación de la privacidad en entornos IoT	2020
ES05	Blockchain en el borde: rendimiento de las redes de IoT con recursos limitados	2020
ES06	Garantizar la prueba de autenticidad de los dispositivos IoT Edge mediante la tecnología Blockchain	2018
ES07	Diseño de un mecanismo eficiente de detección de ataques Sinkhole en el despliegue de IoT basado en el borde	2020
ES08	Sistema de detección de intrusos basado en redes neuronales artificiales para nodos de la niebla del Internet de las cosas	2020
ES09	FOCUS: Un sistema de seguridad basado en la informática de niebla para el Internet de las cosas	2018
ES10	Hacia la prevención de IoT-DDoS mediante computación de borde	2018
ES11	Servicio de autorrecuperación que asegura el servidor de borde en la red IoT contra el ataque de Ransomware	2020
ES12	Autenticación basada en Blockchain con tolerancia a fallos para la computación en la niebla habilitada para IoT	2020
ES13	Metodología en tiempo real para mejorar la ciberseguridad en el Internet de las Cosas utilizando la computación de borde durante la amenaza de ataque	2019
ES14	FlowGuard: Un mecanismo inteligente de defensa de borde contra los ataques DDoS de IoT	2020
ES15	Un marco de mitigación de anomalías para el IoT utilizando la computación en la niebla	2020
ES16	RAD-EI: Un esquema de detección de ataques de enrutamiento para el entorno del Internet de las Cosas basado en el borde	2019
ES17	Esquema de autenticación Protean: Una técnica de autenticación dinámica con límite de tiempo para nodos de borde de IoT en despliegues exteriores	2019
ES18	LDAKM-EIoT: Mecanismo ligero de autenticación de dispositivos y gestión de claves para el despliegue de IoT basado en el borde	2019
ES19	Detección de ataques de botnets en el borde del IoT basada en la representación dispersa	2019
ES20	Combinación de AntibIoTic con Fog Computing AntibIoTic 2.0	2019
ES21	Una estrategia de mitigación distribuida contra los ataques DoS en Edge Computing	2019
ES22	Mejora de la seguridad en un esquema de autenticación ligero con arquitectura de computación en la niebla anónima	2020
ES23	Eccbap: un protocolo de autenticación seguro basado en ECC para dispositivos de borde del IoT	2020
ES24	Biosec: Un marco de autenticación biométrica para la comunicación segura y privada entre dispositivos de borde en IoT e Industria 4.0	2020
ES25	Un esquema de autenticación eficiente basado en la cadena de bloques para proteger los dispositivos IoT habilitados para la niebla	2020
ES26	Un marco integrado seguro para los sistemas del Internet de las cosas asistidos por la niebla	2021
ES27	Estudio sobre cuestiones de seguridad y privacidad en la Internet de los objetos asistida por Edge Computing	2021
ES28	Seguridad en el Internet de las cosas asistido por el borde: retos y soluciones	2020
ES29	Gestión segura de datos distribuidos para la computación en la niebla en aplicaciones de IoT a gran escala: Una solución basada en Blockchain	2020
ES30	Aprendizaje federado con preservación de la privacidad en Fog Computing	2020
ES31	Autenticación mutua y acceso autorizado a los datos entre la niebla y el usuario	2020
ES32	Estudio sobre el análisis seguro de datos en la computación de borde	2019
ES33	Un mecanismo para asegurar las aplicaciones habilitadas para IoT en la capa de niebla	2019
ES34	Seguridad de la computación en la niebla para las aplicaciones del Internet de las cosas: Desafíos y soluciones	2018
ES35	Un marco de seguridad impulsado por los bordes para la Internet inteligente de los objetos	2020
ES36	Problemas de seguridad y privacidad y soluciones para la niebla	2020
ES37	Lógica difusa y arquitectura segura basada en la niebla para el Internet de las cosas (FLFSIoT)	2020
ES38	Huellas dactilares de los servicios de borde y de nube en el IoT	2020
ES39	Seguridad y privacidad para IoT y Paradigma de la computación en la niebla	2020
ES40	Una encuesta: Integración de IoT y computación de niebla	2018
ES41	Retos de seguridad en la niebla y el IoT, tecnología Blockchain y soluciones de árbol celular: una revisión	2020
ES42	IMPACT: Detección de ataques de suplantación de identidad a través de Edge Computing utilizando autocodificador profundo y abstracción de características	2020
ES43	Defensa del borde definida por software contra los DDoS basados en el IoT	2017

ES44	Seguridad de los dispositivos de borde de bajos recursos para los sistemas de IoT	2018
ES45	Cuestiones de seguridad y privacidad en el entorno del IoT impulsado por la niebla	2019
ES46	Ransomware dirigido: Una nueva amenaza cibernética para el sistema de borde del Internet industrial de las cosas de Brownfield	2019
ES47	Detección de datos falsos para redes de niebla y del Internet de las cosas	2019
ES48	Ataque adaptativo de colisión de texto plano en AES enmascarado en Edge Computing	2019
ES49	Mitigación de los ataques DoS en la capa EDGE de IoT para preservar los temas de Qos y la energía de los nodos	2020
ES50	Programación de flujos de trabajo científicos en entornos de niebla múltiple mediante modelos de Markov y un algoritmo híbrido de enjambre SALP	2020

Síntesis de los datos

Cada estudio fue analizado para identificar su aporte más relevante y así finalmente obtener la respuesta para las preguntas de investigación inicialmente planteadas (ver, TABLA I).

> *¿Cómo los problemas de seguridad que presenta actualmente el IoT afectan al Edge Computing?*

Para dar respuesta a esta pregunta de investigación a continuación en la TABLA VI se presentan los problemas de seguridad que afectan en su gran mayoría al IoT y también son los más frecuentes en Edge Computing. Para algunos de los problemas se ha podido identificar que ya existen soluciones para mitigarlos; sin embargo, existen algunos problemas de seguridad como son: ataque de manipulación física, espionaje, reenvío selectivo, ataque al canal de interferencia, inyección de nodo falso, canal lateral, homing, jamming; para los cuales, no se identificó ninguna solución dentro de los estudios analizados.

TABLA VI. PROBLEMAS DE SEGURIDAD IoT Y EDGE COMPUTING

Estudios	**Problemas de Seguridad**
[10][11][12][13] [14][15][16][17] [18][19][20][5][21][22][23][24] [25]	Ataque DoS
[26][12][27][28] [29][4][30][31] [32][33][5][22] [34]	Ataque DDoS
[35][10]	Ataque de Escaneo de puertos
[35][36][37]	Ataque de fuerza bruta vía HTTP y SSH
[11][38][27][2] [39][40][36][41] [19][20][21][37]	Hombre en el medio o escucha clandestina
[42][15][43][33] [5][37]	Ataque de sumidero (Sinkhole):
[12][2][39][44][40][36][37]	Ataque de repetición
[35][12][17]	Ataque de inundación SYN
[45][46]	Ataque Ransomware
[47][37][48]	Ataque de enrutamiento
[39][44][49][15][41][19][20][22]	Ataque de suplantación de identidad
[38][50][51][33] [41][19]	Ataque de falsificación o clonación de dispositivos
[15][39] [33][5][21]	Ataque de manipulación físico
[43][33][41][5]	Ataque Sybil
[43][20][5]	Ataque de agujero negro
[33]	Ataque de espionaje
[32][37][23][24]	Inyección de código malicioso
[43][16][52][41] [18][20][53]	Ataque de colusión
[37]	Ataque de reenvío selectivo
[33][18][19]	Ataque al canal de interferencia
[16][37][23][48]	Inyección de nodo falso
[54][37]	Ataque de canal lateral
[41][5]	Ataque Homing

[41]	Ataque Jammin

¿Cuáles son las características del Edge Computing que generan problemas de seguridad en dispositivos IoT?

El Edge Computing tiene varias características importantes, estas son: Conocimiento de la ubicación, distribución geográfica, arquitectura descentralizada, soporte de movilidad, infraestructura heterogénea, escalabilidad, baja latencia, bajo consumo de banda ancha, aporta una gran eficiencia, bajo costo de inversión, mayor accesibilidad, consumo energético reducido, soporte de aplicaciones IoT a gran escala, soporte de procesamiento más cerca al origen (proximidad) y seguridad de la información. Cada una de estas características brinda ventajas importantes al Edge para la implementación con el IoT. Pero también algunas de ellas introducen nuevos desafíos de seguridad ya que aportan para que se produzcan ataques de seguridad.

Para dar respuesta a la pregunta planteada a continuación se describe cada característica y su vulnerabilidad.

TABLA VII. CARACTERÍSTICAS EDGE COMPUTING QUE GENERAN PROBLEMAS DE SEGURIDAD

Estudio	Característica	Descripción
[43][33][41] [21][48]	Conocimiento de la ubicación	Esta característica aparte de brindarle ventajas al Edge Computing también introduce desafíos de seguridad, recordemos que un nodo Edge generalmente le envía su carga al nodo Edge más cercano por lo que el nodo Edge que recibe la carga ya tiene una idea de la ubicación de ese nodo. Además, si un nodo Edge usa múltiples nodos para descargar, entonces la trayectoria completa de la red puede ser revelada. Si este proceso ocurre en cadena, se puede rastrear fácilmente un conocimiento aproximado sobre la red completa. Esto le facilita el trabajo al atacante para que pueda ejecutar fácilmente un ataque Homing y apagar los nodos Edge principales, además, puede ejecutarse todo tipo de ataques de enrutamiento e inundación.
[33][41][21]	Distribución geográfica	Los nodos Edge están desplegados en varias posiciones, como autopistas, carreteras, supermercados, museos, etc. Debido a que están implementados en lugares remotos y sin protección los nodos Edge son propensos a sufrir diferentes tipos de ataques de seguridad como son: ataques de manipulación física, inyección de nodo falso e inyección de código malicioso.
[43][33][41] [19][48]	Arquitectura descentralizada	La implementación de Edge puede tener diferentes proveedores de servicios debido a las distintas necesidades de implementación, esto puede generar un problema de falta de autenticación y control de acceso que abre la puerta a diferentes ataques de seguridad como, DoS, DDoS, suplantación de identidad, ataque de interferencia. Básicamente, la descentralización y el aprovisionamiento de servicios de baja latencia crean una barrera para la autenticación segura.
[43][33][41] [19][37][48]	Soporte de movilidad	La movilidad del usuario exige que los dispositivos IoT se desconecten con frecuencia de un nodo Edge de confianza y se unan a otro nodo durante el transcurso, al conectarse al nuevo nodo se pierde la confiabilidad ya que se ingresa a un nuevo nodo del cual no se tiene conocimiento de su comportamiento ya que es muy difícil recopilar información relacionada con el comportamiento de todos los nodos Edge; un dispositivo IoT celular o computador puede estar dentro de un vehículo para recopilar la información del tráfico, durante el recorrido este puede ser interceptado por un atacante que puede lanzar un ataque de canal lateral y obtener las claves de cifrado y descifrado de los datos ya que al conectarse y desconectarse constantemente de diferentes nodos la gestión de claves se convierte en un desafío. Por lo tanto, la confiabilidad entre todos los nodos Edge en la red es un tema crítico.
[16][32][21]	Escalabilidad	Una red distribuida como es Edge Computing debe enfrentarse a diferentes problemas, primeramente, la heterogeneidad de los dispositivos, que tienen diferentes limitaciones de rendimiento y energía, además de la confiabilidad en las conexiones, debido a estas limitaciones no es posible implementar métodos de seguridad en todos los dispositivos y como consecuencia algunos de ellos serán vulnerables a cualquier tipo de ataque de seguridad.
[16][41][23]	Consumo energético reducido	La mayoría de los dispositivos Edge dependen de baterías pequeñas para funcionar debido a limitaciones de tamaño. Los atacantes intentarán agotar la batería de un dispositivo periférico por cualquier medio posible. Por ejemplo, esto podría implicar obligar al nodo a ejecutar subrutinas que consumen energía. Otro método bajo el ataque DoS es la privación del sueño. En este tipo de ataque, el atacante envía numerosas solicitudes que parecen legítimas obligándolo a responder impidiendo que el nodo duerma y, por tanto, no conserva energía.

CONCLUSIONES

Los problemas de seguridad encontrados y analizados en el IoT afectan también al Edge Computing, debido a que este paradigma nace gracias a la existencia de IoT y se implementa sobre la base del mismo, el cual en sí tiene muchas fallas de seguridad, además, de estar conectado a Internet que no es seguro, por lo tanto, la computación perimetral heredaría todos los problemas que engloban IoT.

Los mecanismos de seguridad ampliamente estudiados y utilizados en la computación tradicional no pueden ser implementados directamente en Edge Computing, debido que en su mayoría requieren bastante capacidad computacional; así mismo, debido a la heterogeneidad de los dispositivos y los diferentes protocolos de comunicación que conforman el Edge Computing, no es posible diseñar mecanismos de seguridad genéricos para todos los entornos.

Las características del Edge Computing generan también una serie de problemas de seguridad que se han podido identificar dentro de esta investigación, lo cual hace que el desafío de crear e implementar mecanismos de seguridad sea mayor.

REFERENCIAS

[1] M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, "Edge Computing Perspectives : Architectures , Technologies , and Open Security Issues," *2019 IEEE Int. Conf. Edge Comput.*, pp. 116–123, doi: 10.1109/EDGE.2019.00035.

[2] O. Mounnan, A. El Mouatasim, O. Manad, T. Hidar, A. A. El Kalam, and N. Idboufker, "Privacy-Aware and Authentication based on Blockchain with Fault Tolerance for IoT enabled Fog Computing," *2020 5th Int. Conf. Fog Mob. Edge Comput. FMEC 2020*, pp. 347–352, 2020, doi: 10.1109/FMEC49853.2020.9144845.

[3] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge Computing Security: State of the Art and Challenges," *Proc. IEEE*, vol. 107, no. 8, 2019, doi: 10.1109/JPROC.2019.2918437.

[4] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism against IoT DDoS Attacks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9552–9562, 2020, doi: 10.1109/JIOT.2020.2993782.

[5] A. Rauf, R. A. Shaikh, and A. Shah, "Security and privacy for IoT and fog computing paradigm," *2018 15th Learn. Technol. Conf. L T 2018*, pp. 96–101, 2018, doi: 10.1109/LT.2018.8368491.

[6] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data Security and Privacy-Preserving in Edge Computing Paradigm : Survey and Open Issues," *IEEE Access*, vol. 6, no. Idc, pp. 18209–18237, 2018, doi: 10.1109/ACCESS.2018.2820162.

[7] P. V. Torres-Carrion, C. S. Gonzalez-Gonzalez, S. Aciar, and G. Rodriguez-Morales, "Methodology for systematic literature review applied to engineering and education," *IEEE Glob. Eng. Educ. Conf. EDUCON*, vol. 2018-April, no. April, pp. 1364–1373, 2018, doi: 10.1109/EDUCON.2018.8363388.

[8] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007.

[9] M. Petticrew and H. Roberts, "Systematic Reviews in the Social Sciences," *Syst. Rev. Soc. Sci.*, 2006, doi: 10.1002/9780470754887.

[10] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, "Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network," *IEEE Access*, vol. 6, no. November, pp. 73713–73723, 2018, doi: 10.1109/ACCESS.2018.2884293.

[11] D. E. D. Abou-Tair, S. Büchsenstein, and A. Khalifeh, "A fog computing-based framework for privacy preserving IoT environments," *Int. Arab J. Inf. Technol.*, vol. 17, no. 3, pp. 306–314, 2020, doi: 10.34028/iajit/17/3/4.

[12] J. Pacheco, V. H. Benitez, L. C. Felix-Herran, and P. Satam, "Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes," *IEEE Access*, vol. 8, pp. 73907–73918, 2020, doi: 10.1109/ACCESS.2020.2988055.

[13] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "An anomaly mitigation framework for iot using fog computing," *Electron.*, vol. 9, no. 10, pp. 1–24, 2020, doi: 10.3390/electronics9101565.

[14] G. Potrino, F. De Rango, and P. Fazio, "A Distributed Mitigation Strategy against DoS attacks in Edge Computing," *Wirel. Telecommun. Symp.*, vol. 2019-April, pp. 1–7, 2019, doi: 10.1109/WTS.2019.8715543.

[15] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, "BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0," *IEEE Consum. Electron. Mag.*, vol. 2248, no. c, 2020, doi: 10.1109/MCE.2020.3038040.

[16] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, 2021, doi: 10.1109/JIOT.2020.3015432.

[17] Z. Chen, H. Cui, E. Wu, Y. Li, and Y. Xi, "Secure Distributed Data Management for Fog Computing in Large-Scale IoT Application: A Blockchain-Based Solution," *2020 IEEE Int. Conf. Commun. Work. ICC Work. 2020 - Proc.*, pp. 0–5, 2020, doi: 10.1109/ICCWorkshops49005.2020.9145381.

[18] X. Qiu, B. Rong, J. Ben-Othman, S. Han, and M. Kodach, "An Edge-Driven Security Framework for Intelligent Internet of Things," *IEEE Netw.*, vol. 34, no. 5, pp. 6–7, 2020, doi: 10.1109/MNET.2020.9199784.

[19] M. Mukherjee, M. A. Ferrag, L. Maglaras, A. Derhab, and M. Aazam, "Security and privacy issues and solutions for fog," *Fog Fogonomics Challenges Pract. Fog Comput. Commun. Networking, Strateg. Econ.*, pp. 353–374, 2020, doi: 10.1002/9781119501121.ch14.

[20] S. R. Zahra and M. A. Chishti, "Fuzzy logic and Fog based Secure Architecture for Internet of Things (FLFSIoT)," *J. Ambient Intell. Humaniz. Comput.*, 2020, doi: 10.1007/s12652-020-02128-2.

[21] M. Jalasri and D. L. Lakshmanan, "A survey: Integration of iot and fog computing," *Proc. 2nd Int. Conf. Green Comput. Internet Things, ICGCIoT 2018*, pp. 235–239, 2018, doi: 10.1109/ICGCIoT.2018.8753010.

[22] M. Ozcelik, N. Chalabianloo, and G. Gur, "Software-Defined Edge Defense Against IoT-Based DDoS," *IEEE CIT 2017 - 17th IEEE Int. Conf. Comput. Inf. Technol.*, pp. 308–313, 2017, doi: 10.1109/CIT.2017.61.

[23] S. Shapsough, F. Aloul, and I. A. Zualkernan, "Securing Low-Resource Edge Devices for IoT Systems," *2018 Int. Symp. Sens. Instrum. IoT Era, ISSI 2018*, no. September, 2018, doi: 10.1109/ISSI.2018.8538135.

[24] R. Fantacci, F. Nizzi, T. Pecorella, L. Pierucci, and M. Roveri, "False data detection for fog and internet of things networks," *Sensors (Switzerland)*, vol. 19, no. 19, pp. 1–19, 2019, doi: 10.3390/s19194235.

[25] F. De Rango, M. Tropea, and P. Fazio, "Mitigating DoS attacks in IoT EDGE Layer to preserve QoS topics and nodes' energy," *IEEE INFOCOM 2020 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2020*, pp. 842–847, 2020, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162902.

[26] J. Ni, X. Lin, and X. S. Shen, "Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives," *IEEE Netw.*, vol. 33, no. 2, pp. 50–57, 2019, doi: 10.1109/MNET.2019.1800229.

[27] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, and Z. Ye, "FOCUS: A fog computing-based security system for the Internet of Things," *CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf.*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/CCNC.2018.8319238.

[28] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, "Towards IoT-DDoS prevention using edge computing," *USENIX Work. Hot Top. Edge Comput. HotEdge 2018, co-located with USENIX ATC 2018*, 2018.

[29] T. A. Ahanger, U. Tariq, and M. Nusir, "Real-Time Methodology for Improving Cyber Security in Internet of Things Using Edge Computing During Attack Threats," *Second Int. Conf. Smart Syst. Inven. Technol.*, no. Icssit, pp. 293–297, 2019.

[30] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet attack detection at the IoT edge based on sparse representation," *Glob. IoT Summit, GIoTS 2019 - Proc.*, pp. 1–6, 2019, doi: 10.1109/GIOTS.2019.8766388.

[31] A. N. I. O. T. Ic, M. De Donno, and N. Dragoni, "Combining A NTIB I O T IC with Fog Computing : ANTIBIOTIC 2.0," pp. 1–6, 2019.

[32] S. Shen, K. Zhang, Y. Zhou, and S. Ci, "Security in edge-assisted Internet of Things: challenges and solutions," *Sci. China Inf. Sci.*, vol.

63, no. 12, pp. 1–14, 2020, doi: 10.1007/s11432-019-2906-y.

[33] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, 2019, doi: 10.1109/JIOT.2019.2897619.

[34] O. H. Ahmed, J. Lu, A. M. Ahmed, A. M. Rahmani, M. Hosseinzadeh, and M. Masdari, "Scheduling of scientific workflows in multi-fog environments using markov models and a hybrid salp swarm algorithm," *IEEE Access*, vol. 8, pp. 189404–189422, 2020, doi: 10.1109/ACCESS.2020.3031472.

[35] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, 2020, doi: 10.1109/JIOT.2020.2970501.

[36] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *J. Sens. Actuator Networks*, vol. 8, no. 1, 2019, doi: 10.3390/jsan8010016.

[37] N. S. Khan and M. A. Chishti, "Security challenges in fog and iot, blockchain technology and cell tree solutions: A review," *Scalable Comput.*, vol. 21, no. 3, pp. 515–541, 2020, doi: 10.12694:/scpe.v21i3.1782.

[38] S. Misra, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan, "Blockchain at the Edge: Performance of Resource-Constrained IoT Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 1, pp. 174–183, 2021, doi: 10.1109/TPDS.2020.3013892.

[39] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based iot deployment," *Sensors (Switzerland)*, vol. 19, no. 24, pp. 1–21, 2019, doi: 10.3390/s19245539.

[40] J. K. Mudhar, S. Kalra, and J. Malhotra, "An Efficient Blockchain Based Authentication Scheme to Secure Fog Enabled IoT Devices," *Indo - Taiwan 2nd Int. Conf. Comput. Anal. Networks, Indo-Taiwan ICAN 2020 - Proc.*, pp. 75–80, 2020, doi: 10.1109/Indo-TaiwanICAN48429.2020.9181356.

[41] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 601–628, 2018, doi: 10.1109/COMST.2017.2762345.

[42] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment," *Sensors (Switzerland)*, vol. 20, no. 5, pp. 1–27, 2020, doi: 10.3390/s20051300.

[43] A. K. Junejo, N. Komninos, and J. A. McCann, "A Secure Integrated Framework for Fog-Assisted Internet-of-Things Systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6840–6852, 2021, doi: 10.1109/JIOT.2020.3035474.

[44] L. Wang, H. An, and Z. Chang, "Security Enhancement on a Lightweight Authentication Scheme with Anonymity Fog Computing Architecture," *IEEE Access*, vol. 8, pp. 97267–97278, 2020, doi: 10.1109/ACCESS.2020.2996264.

[45] I. S. Lei, S. K. Tang, I. K. Chao, and R. Tse, "Self-recovery service securing edge server in iot network against ransomware attack," *IoTBDS 2020 - Proc. 5th Int. Conf. Internet Things, Big Data Secur.*, no. January, pp. 399–404, 2020, doi: 10.5220/0009470303990404.

[46] M. Al-Hawawreh, F. Den Hartog, and E. Sitnikova, "Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 7137–7151, 2019, doi: 10.1109/JIOT.2019.2914390.

[47] M. Wazid, P. Reshma Dsouza, A. K. Das, V. Bhat K, N. Kumar, and J. J. P. C. Rodrigues, "RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment," *Int. J. Commun. Syst.*, vol. 32, no. 15, pp. 1–20, 2019, doi: 10.1002/dac.4024.

[48] R. Verma and S. Chandra, "Security and Privacy Issues in Fog driven IoT Environment," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 5, pp. 367–370, 2019, doi: 10.26438/ijcse/v7i5.367370.

[49] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices," *Pervasive Mob. Comput.*, vol. 67, p. 101194, 2020, doi: 10.1016/j.pmcj.2020.101194.

[50] U. Guin, P. Cui, and A. Skjellum, "Ensuring Proof-of-Authenticity of IoT Edge Devices Using Blockchain Technology," *Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree*, pp. 1042–1049, 2018, doi: 10.1109/Cybermatics_2018.2018.00193.

[51] S. Sathyadevan, K. Achuthan, R. Doss, and L. Pan, "Protean Authentication Scheme-A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments," *IEEE Access*, vol. 7, pp. 92419–92435, 2019, doi: 10.1109/ACCESS.2019.2927818.

[52] C. Zhou, A. Fu, S. Yu, W. Yang, H. Wang, and Y. Zhang, "Privacy-Preserving Federated Learning in Fog Computing," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10782–10793, 2020, doi: 10.1109/JIOT.2020.2987958.

[53] Y. Ding, Y. Shi, A. Wang, X. Zheng, Z. Wang, and G. Zhang, "Adaptive Chosen-Plaintext Collision Attack on Masked AES in Edge Computing," *IEEE Access*, vol. 7, pp. 63217–63229, 2019, doi: 10.1109/ACCESS.2019.2916553.

[54] M. Arun, S. Balamurali, B. S. Rawal, Q. Duan, R. L. Kumar, and B. Balamurugan, "Mutual authentication and authorized data access between fog and user based on blockchain technology," *IEEE INFOCOM 2020 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2020*, pp. 37–42, 2020, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162915.

11.4. Anexo 4: Certificado de inglés

Macará, 20 de septiembre de 2021

Lic. Pablo Días Vaca

DOCENTE BILINGÜE DE LA UNIDAD EDUCATIVA SANTA MARIANA DE JESÚS

CERTIFICA.-

Que he dirigido, revisado y corregido la traducción del resumen del trabajo de titulación denominado **"EXPLORACIÓN DE LOS PROBLEMAS DE SEGURIDAD QUE PRESENTA EL IoT EN EL CONTEXTO DEL EDGE COMPUTING"** desarrollado por la egresada **Nora Cecivel Solano Chamba** con número de cédula **1105652372**.La beneficiada puede hacer uso del mismo como mejor convenga.

Es todo cuanto puedo certificar en honor a la verdad.

.....

Lic. Pablo Días Vaca
CI:1103917330
DOCENTE BILINGÜE DE LA UNIDAD EDUCATIVA SANTA MARIANA DE JESÚS