UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA: COMPUTACIÓN

SOLUCIONES DE CIBERSEGURIDAD CONTRA LOS ATAQUES A REDES IOT EN AMÉRICA LATINA, UNA REVISIÓN SISTEMÁTICA DE LA LITERATURA

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

AUTOR: Andrés Marcelo Celi Sandoya

TUTOR: Mora Saltos Nelson Salomón, Msig.

Guayaquil – Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Andrés Marcelo Celi Sandoya con documento de identificación N° 0931178206 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 10 de agosto del año 2023

Atentamente,

Andrés Marcelo Celi Sandoya
0931178206

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Andrés Marcelo Celi Sandoya con documento de identificación No. 0931178206, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Soluciones de ciberseguridad contra los ataques a redes IoT en América Latina, una Revisión Sistemática de la Literatura", el cual ha sido desarrollado para optar por el título de: Ingeniero en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 10 de agosto del año 2023

Atentamente,

Andrés Marcelo Celi Sandoya
0931178206

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Nelson Salomón Mora Saltos con documento de identificación No. 0909257800, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **Soluciones de ciberseguridad contra los ataques a redes IoT en América Latina, una Revisión Sistemática de la Literatura**, realizado por Andrés Marcelo Celi Sandoya con documento de identificación N° 0931178206, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 10 de agosto del año 2023

Atentamente,

Nelson Salomón Mora Saltos
0909257800

DEDICATORIA

Dedico este trabajo con todo mi cariño y gratitud a mi familia y primos, fuente inagotable de apoyo, amor y motivación. Agradezco infinitamente su comprensión y paciencia en cada momento de mi vida.

A mis profesores y mentores, mi reconocimiento por su sabiduría, orientación y valiosos consejos que han enriquecido mi aprendizaje.

Este trabajo es el fruto del esfuerzo y la pasión que he dedicado a mi formación académica, y espero que contribuya positivamente al conocimiento en nuestro campo de estudio.

A cada persona que ha sido parte de esta travesía, ¡Gracias Totales!

AGRADECIMIENTO

Agradezco a todas las personas que han contribuido de manera significativa en la realización de este artículo académico.

En primer lugar, agradezco a mi familia por su constante apoyo, paciencia y amor incondicional.

También quiero expresar mi sincero agradecimiento a mis amigos y compañeros de estudio, cuya colaboración y ánimo han sido un pilar fundamental en este camino académico. Así mismo a mis amigos fuera de las aulas de clase y las personas que ya no están, gracias por sus lecciones y enseñanzas.

Finalmente, agradezco a la Universidad Politécnica Salesiana por brindarme los recursos y el ambiente propicio para desarrollar este trabajo.

Sin la contribución de todos ustedes, este artículo no habría sido posible. ¡Gracias por ser parte de este logro!

RESUMEN

La seguridad en IoT se considera una necesidad crítica y desafiante, los ataques a las redes IoT ponen en peligro a las personas, economías, empresas, entre otros; y la conectividad de dispositivos heterogéneos y abiertos avizora un entorno para que las amenazas puedan evolucionar. El objetivo general es determinar las soluciones de ciberseguridad contra los ataques a redes Internet of Things a nivel de América Latina mediante la realización de un análisis exhaustivo de la literatura de los años 2018 hasta 2023. De acuerdo a la extracción de datos en los resultados se obtiene de 33 artículos científicos que, el factor de seguridad más referenciada son las vulnerabilidades, la característica de seguridad más referenciada es la disponibilidad, el ataque más común es la denegación de acceso distribuido DDoS, la solución tecnológica más utilizada son los protocolos, la propuesta más diseñada es el framework personalizado; las acciones más realizadas son detectar y monitoreo; el componente que más se protege son los dispositivos, el dominio que más propuestas se presentan es en el industrial. Se concluye que IoT es una tecnología emergente que requiere más atención desde el enfoque de la ciberseguridad efectiva, además que IoT incorpora varias tecnologías en desarrollo como Big Data, Inteligencia Artificial, Blockchain, Cifrado, entre otros.

Palabras claves: Ciberseguridad, Internet de las Cosas, Ataques, seguridad de la información.

ABSTRACT

IoT security is considered a critical and challenging need, attacks on IoT networks endanger people, economies, companies, among others; and the connectivity of heterogeneous and open devices envisions an environment for threats to evolve. The general objective is to determine cybersecurity solutions against attacks on Internet of Things networks in Latin America through a systematic review of the literature between 2018 and 2023. According to the extraction of data in the results it is obtained of 33 articles that, the most referenced security factor are the vulnerabilities, the most referenced security feature is availability, the most common attack is the denial of distributed DDoS access, the most used technological solution are the protocols, the most designed proposal is the custom framework; The most performed actions are detection and monitoring; The component that is most protected are the devices, the domain that most proposals are presented is in the industrial. It is concluded that IoT is an emerging technology that requires more attention from the focus of effective cybersecurity, in addition to IoT incorporates several technologies in development such as Big Data, Artificial Intelligence, Blockchain, Encryption, among others.

Key words: Cybersecurity, Internet of Things, Attacks, Information Security.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

La sociedad actual tiene dependencia de la tecnología IoT (Internet de las cosas), esta tecnología integra los datos del mundo físico y el mundo digital en un entorno que puede ser aprovechado por usuarios y sistemas; esta tecnología se utiliza en entornos como la domótica, la sanidad, el transporte, la energía y el militar. Esta tecnología tiene problemas de seguridad en los diferentes entornos porque cada entorno es complejo y los dispositivos son de varios proveedores o distintos estándares. Las redes IoT se forman por dispositivos que capturan datos, se comunican, interactuar con otros dispositivos, establecen una gran red de objetos y forman una interconexión más amplia y servicios inteligentes. Los ataques cibernéticos obligan a desarrollar soluciones efectivas y consistentes; los dispositivos y aplicaciones informáticas existentes en los entornos IoT no cuentan con diseños para gestionar ni prevenir intrusiones o anomalías, y esto aumenta la curva de ataques dirigidos esta clase de infraestructura (Djenna et al., 2020).

IoT se forma por equipos o dispositivos heterogéneos y las interconexiones consideran la importancia de aplicar ciberseguridad desde las tareas en el diseño de las infraestructuras para las empresas que adopten IoT; los quebrantos en seguridad digital conducen a impactos críticos en los negocios y pérdida de capacidad operativa (Mullet et al., 2021) IoT es omnipresente en los entornos comerciales y gobiernos que están conectados para brindar experiencias y funcionalidades a los usuarios; existe gran cantidad de dispositivos conectados con vulnerabilidades de seguridad y es necesario adoptar conocimiento sobre la seguridad en redes IoT; además es necesario tener habilidades y tiempo para realizar monitoreo de los entornos, y son muchos los dispositivos, alertas y tráfico, y entender los datos que presenten las herramientas de monitoreo (Chavis et al., 2021).

De acuerdo a (S. Zhao et al., 2020), el análisis de ciberseguridad en IoT se orienta en dos tipos de enfoques, el primero se centra en reglas explícitas por la seguridad y políticas, el segundo se centra en tecnologías como Inteligencia Artificial o Machine Learning que buscan patrones extraños.

Algunos problemas de seguridad en IoT son: Insuficientes actualizaciones en grandes entornos IoT son complicadas por el firmware y núcleo de los sistemas operativos heredados con posibles vulnerabilidades a los ataques; Aumento de malware y ransonware que deben ser solucionadas en forma adecuada; Robots que funcionan con las tecnologías emergentes; y ataques a la seguridad y confidencialidad de los datos.

Para el año 2022, el problema principal como ataque más común es el ransonware, el 12% de los ataques cibernéticos se dieron en América Latina, los principales países afectados son Colombia, Brasil, Perú, México y Chile; el ransonware atacó en 32% a nivel de la región a archivos y dispositivos entre ellos dispositivos IoT, las seguridades han aumentado, pero los ataques también han mejorado en tiempos menores a cuatro días. América Latina tiene preferencias por los ataques por dos razones, la primera razón porque la región tiene organizaciones robustas en trayectoria e información, la segunda razón porque la ciberseguridad está en segundo plano a nivel empresarial (IBM-Security, 2023).

En Ecuador, el Centro de Respuesta a Incidentes Informáticos Ecucert que pertenece al Ministerio de Telecomunicaciones y de la Sociedad de la Información, informa que existen 7292 ataques desde enero a abril del año 2022, y el año 2021 existen 15847 alertas de ataques (Ecucert, 2022).

IoT se utiliza en otros entornos como manufactura, educación, salud, hogar, transporte, procesamiento de alimentos, agricultura, entre otros; además IoT se utiliza con otras tecnologías como Big Data, Inteligencia Artificial, Blockchain, Business Intelligence (Alferidah & Jhanjhi, 2020).

La seguridad en IoT se considera una necesidad crítica y desafiante, los ataques a las redes IoT ponen en peligro a las personas, economías, empresas, entre otros; y la conectividad de dispositivos heterogéneos y abiertos avizora un entorno para que las amenazas puedan evolucionar. Las redes distribuidas tienen desafíos significativos en seguridad y resiliencia, estas redes escalables mantienen a los profesionales de la seguridad informática en permanente monitoreo y resguardo de los límites a las aplicaciones informáticas de la empresa (Lam et al., 2022).

Con la gran cantidad de dispositivos IoT conectados, las inquietudes principales son la seguridad y privacidad de los datos obtenidos del mundo real, y que son transmitidos luego procesados. Se considera que la ciberseguridad debe existir en cada nivel de los modelos IoT, es decir, en la conexión del hardware IoT, en la comunicación de red, en la nube, en el procesamiento de datos, en la exposición de los conocimientos, entre otros (Manta-Caro et al., 2020).

Es necesario dar a conocer las soluciones de ciberseguridad que existen en los niveles o sistemas que trabajan en entornos IoT; esta información se la obtiene de los artículos científicos, y este

documento puede servir para futuras investigaciones que deseen diseñar redes IoT e incluir la ciberseguridad en el modelo.

El objetivo general: Determinar las soluciones de ciberseguridad contra los ataques a redes Internet of Things a nivel de América Latina mediante una revisión sistemática de la literatura en los años 2018 hasta 2023.

Objetivos específicos: 1) Identificar artículos científicos para clasificar las propuestas de ciberseguridad en redes IoT mediante revisión bibliográfica. 2) Determinar los ataques, las tecnologías, los dominios, las temáticas y las soluciones que existen de ciberseguridad en redes IoT mediante la revisión de los artículos científicos. 3) Analizar los resultados para conocer las soluciones de ciberseguridad en IoT obtenidos de los artículos científicos mediante el análisis cuantitativo y descriptivo.

Los entornos IoT son un auténtico espacio de batalla de la ciberseguridad, por la gran cantidad de dispositivos y objetos conectados, además con muchas amenazas importantes que incrementa la superficie y el vector de ataque encaminado a esta clase de infraestructura.

2. REVISIÓN DE LITERATURA

2.1. IoT

Los entornos IoT tienen características relevantes como: los dispositivos IoT interactúan y toman datos del mundo físico, y los sensores y actuadores están en la primera línea de los modelos. Los dispositivos IoT cumplen niveles de confiabilidad, rendimiento y resiliencia. Los dispositivos IoT tienen diferentes maneras de gestión, monitoreo y servicio por su ubicación física (Lam et al., 2022).

2.2. Ciberseguridad

Las vulnerabilidades, riesgos, amenazas, confidencialidad, integridad, disponibilidad y autenticación son conceptos vinculantes a la seguridad cibernética operativa (Mullet et al., 2021).

Vulnerabilidades son las debilidades que los invasores pueden explotar para complicar los sistemas, las debilidades pueden localizarse en los procedimientos, en los sistemas o los controles; las vulnerabilidades pueden ser acceso remoto, software y red. Amenaza es cualquier hecho que afecte a las operaciones o los activos o las personas o empresas o sistema mediante accesos no autorizados o violación a información. Riesgo es el nivel de impacto sobre las operaciones o los activos o las personas o empresas como resultado de una amenaza y su probabilidad de suceder; en temas de ciberseguridad, los riesgos se muestran al perder las características como Confidencialidad, Integridad, Disponibilidad y Autenticación.

Disponibilidad es permitir ejecutar las tareas o permitir accesos a los recursos, el recurso puede ser un hardware o software o información. Integridad es mantener la exactitud de la información, los datos deben mantenerse iguales desde su creación, los sistemas o protocolos que son heredados pueden no incluir niveles de seguridad en el diseño. Confidencialidad se mantiene el acceso a los datos solo a las personas correspondientes o dueños de los datos, la amenaza es acceder a datos por terceros. Autenticación es mantener los privilegios y accesos de usuarios hacia los recursos protegidos, la amenaza explota las vulnerabilidades para acceder a los recursos o información; los accesos inadecuados son producto de configuraciones incorrectas y causan daño físico y lógico.

2.3. Ataques a redes IoT

Algunos de los ataques en redes IoT son: 1) Ataque de respuesta que el intruso escucha comunicación o visualiza mensajes. 2) Hombre en el medio que el intruso está en medio de una comunicación entre pares. 3) Ataques de criptoanálisis que descifra los datos o mensajes. 4) Ataques de canal lateral que se basa en la implementación de un sistema. 5) Troyanos de hardware que se dirigen a los circuitos integrados. 6) Ataques encubiertos que el intruso manipula la entrada y salida de un sistema informático. 7) Privación del sueño que agota la fuente de alimentación del dispositivo y evita el modo de ahorro de energía. 8) Sesgo del reloj que desajusta las marcas de tiempo y causa error en los sistemas informáticos que usan marcas de tiempo. 9) Suplantación de identidad que el intruso usa otra identidad. 10) Ataques de reputación del sistema que corrompe el nodo de un sistema informático en modo físico o lógico. 11) Malware que son programas maliciosos que bloquean archivos o dispositivos. 12) Ataque a la integridad de datos que actualiza con datos falsos en un sistema o red o paquete. 13) Denegación de servicio deshabilita los accesos a los recursos de un dispositivo o red o sistema. 14) Escucha a escondidas que roba datos en plena transmisión de una red o dispositivo. 15) Ataques de comando y control que intruso domina el dispositivo mediante comandos. 16) Ingeniería social que el intruso engaña a personas autorizadas para obtener datos clasificados (Xenofontos et al., 2022).

De acuerdo con Arbor Networks, existen 20 mil ataques diarios de DDoS con volúmenes promedio de medio Tbps (Djenna et al., 2020).

2.4. Aplicación de Ciberseguridad en redes IoT

En (Tashtoush et al., 2022) proponen utilizar metodologías ágiles para diseñar y desarrollar sistemas de seguridad, en una primera parte compararon los enfoques ágiles y en una segunda parte los dominios analizados son aplicaciones de transporte, IoT y Ciberseguridad.

En (Lam et al., 2022) se plantea un framework de confidencialidad como referencia para adoptar los requisitos de seguridad y aplicar buenas prácticas y revisiones de seguridad que minimicen los riesgos; aplican la base “seguridad en un entorno de confianza cero” para identificar áreas críticas que gestionan los activos sensibles, además el marco ayuda a identificar y evaluar las áreas de posibles ataques para aplicar las intervenciones de seguridad.

Mejora la ciberseguridad de una infraestructura IoT de gran escala con operación de dispositivos para captura de datos en edificios, los datos capturados sirven para aplicar

aprendizaje automático; la herramienta es de código abierto, utiliza reglas de flujo de red, localización de anomalías con especificación de ubicación de los dispositivos (Hamza et al., 2022).

La propuesta de (S. Zhao et al., 2020) aplica el concepto Inteligencia Computacional que abarca la seguridad en IoT con una arquitectura, análisis de amenazas, análisis de incidentes, gestión de sucesos, detección de intrusos, entre otros; la arquitectura realiza el análisis de seguridad cibernética, contiene las inquietudes de seguridad y aplica algoritmos; la arquitectura puede emplear varios modelos o herramientas con algoritmos de aprendizaje-adaptación-optimización y solucionar problemas de ciberseguridad que serían complicados con algoritmos convencionales.

La propuesta de (Espina et al., 2021) entrega un patrón IoT donde, integra una arquitectura de ciberseguridad en los elementos de la red para certificar los controles y delatar amenazas en los dispositivos portátiles IoT; el modelo busca minimizar las vulnerabilidades existentes en los dispositivos IoT, el modelo está formado por tres capas: negocio, aplicaciones y tecnología; los autores simularon un entorno para verificar el control y seguimiento de los dispositivos.

Para detectar intrusos, ser eficaces y gestionar nuevos tipos de intrusos en redes IoT, el trabajo de (Kandhro et al., 2023) propone un modelo basado en Aprendizaje Profundo para descubrir las vulnerabilidades e infracciones en los sistemas; el modelo detecta amenazas cibernéticas con precisión de 95 %, además aumenta la confiabilidad y eficiencia al descubrir diferentes tipos de ataques, otro punto importante es mantener la confidencialidad e integridad de los sistemas y usuarios.

Machine Learning se utiliza para clasificar los dispositivos que se encuentran en la capa física IoT, y esto resguarda las aplicaciones informáticas que utilizan los datos de la red IoT; esta clasificación auxilia a los ingenieros para que identifiquen y entiendan los desafíos, los requerimientos y los principios de diseño representados para preservar los dispositivos y redes de IoT pensando en las propiedades de la capa física (Boukerche & Coutinho, 2021).

3. METODOLOGÍA

Esta investigación explora los aspectos de ciberseguridad que se utilizan en los modelos Intertnet of Things de diferentes entornos o dominios, se llevará a cabo una revisión sistemática de la literatura (Andrade et al., 2020) basada en orientación de arriba hacia abajo de las soluciones o componentes que mitigan los ataques en los ecosistemas de IoT. La metodología tiene 3 fases: Inicio, Análisis cualitativo y Análisis de resultados, cada fase tiene sus actividades que a continuación se describe como se realiza durante la investigación. Ver figura 1.

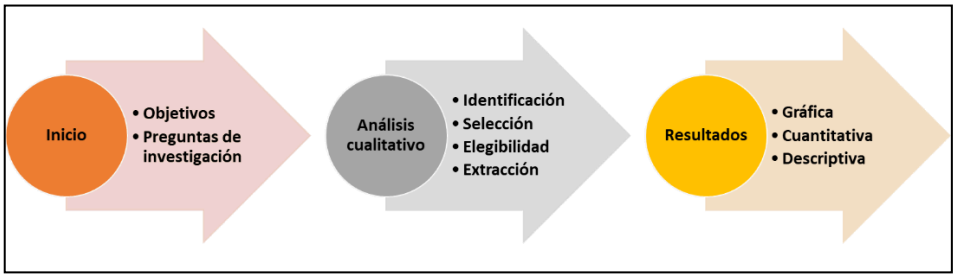

Figura 1. Revisión Sistemática.

1) Inicio: En esta fase se define la meta principal de la revisión sistemática y se definen las preguntas relacionadas al tema o motivo de la investigación.

El objetivo general es explorar y conocer los enfoques de artículos científicos relacionados a soluciones de ciberseguridad en redes IoT.

2) Análisis cualitativo: Para entender los aspectos de ciberseguridad en el contexto de redes IoT, la metodología utiliza el análisis desde arriba hacia abajo; conocer los componentes o estrategias o tecnologías para mejorar la seguridad de la red e identificar los ataques que son frecuentes; la metodología contiene de cuatro actividades: identificación de estudios, selección, análisis de elegibilidad y extracción; se ejecuta la clasificación y elegibilidad, el análisis y extracción se hace con la revisión ciega para minimizar la subjetividad en este proceso de investigación. Identificación de estudios:

a) Clasificación: Las vulnerabilidades, riesgos, amenazas son puertas para los ataques a las redes IoT y esto es importante para entender el desarrollo de la ciberseguridad; se seleccionan artículos de investigación desde el año 2018; se utilizan las bases de datos: Association for Computing Machinery (ACM), IEEE Xplorer, Springer, Web of Science, estas bases corresponden a Sistemas de Información o Ciencias de la Computación o Tecnología. Las palabras clave de búsqueda son: “(Cibersecurity OR IoT OR Latin America)” y “(Cybersecurity OR Internet of Things OR Latin America)”.

b) Criterios de inclusión y exclusión: Los criterios de inclusión son: (i) artículos científicos, (ii) artículos relacionados con ciberseguridad en dominios IoT,

(iii) artículos desde el año 2018, (iv) documentos en idioma inglés. Los criterios de exclusión son: (i) artículos tipo encuestas preliminares o resúmenes, (ii) literatura gris, (iii) libros sobre el tema.

Selección: Se desarrolla durante la investigación y se escoge los artículos de acuerdo a los criterios.

Análisis de elegibilidad: Se desarrolla durante la investigación y se realiza una revisión completa del artículo seleccionado.

Extracción: Se desarrolla durante la investigación y se realiza extracción de datos de cada artículo en una hoja electrónica; los datos son: nombres de ataques, nombres de tecnologías, nombres de dominios, nombres de protocolos, nombres de temáticas, nombres de soluciones.

3) Análisis de resultados: En esta fase se tabulan los datos de la hoja electrónica para generar las respuestas a las preguntas de investigación mediante gráficos, datos cuantitativos y describir la situación encontrada. las preguntas objeto de estudio son:

a. ¿Cuáles serían los Factores de seguridad en IoT?

b. ¿Cuáles son las Características de seguridad en IoT?

c. ¿Cuáles son los Ataques comunes en IoT?

d. ¿Cuáles son las Soluciones Tecnológicas en IoT?

e. ¿Cuáles son las Propuestas en IoT?

f. ¿Cuáles son las Acciones contra los ataques?

g. ¿Cuáles son los Componentes a proteger en IoT?

h. ¿Cuáles son los Dominios utilizados en IoT?

4. RESULTADOS

4.1. Identificación de artículos científicos para clasificar las propuestas de ciberseguridad en redes IoT mediante revisión bibliográfica.

Para cumplir el primer resultado se realizó la revisión bibliográfica, es decir se exploraron artículos científicos relacionados a soluciones de ciberseguridad en redes IoT. Se realizó el análisis cualitativo que ayuda a entender los aspectos de ciberseguridad en el contexto de redes IoT; se realizó la identificación, selección, análisis de elegibilidad y extracción; en la clasificación se buscaron las vulnerabilidades, riesgos, amenazas; luego se utilizaron criterios de exclusión e inclusión. Entonces, se han identificado 101 artículos, luego durante la selección se descartaron 21 artículos por no elegibles y se descartaron 9 artículos porque no son afines al tema, para el análisis de elegibilidad se examina los resúmenes de 71 artículos y luego se excluyen 32 artículos por ser artículos de revisión, se procede a bajar los archivos de los 39

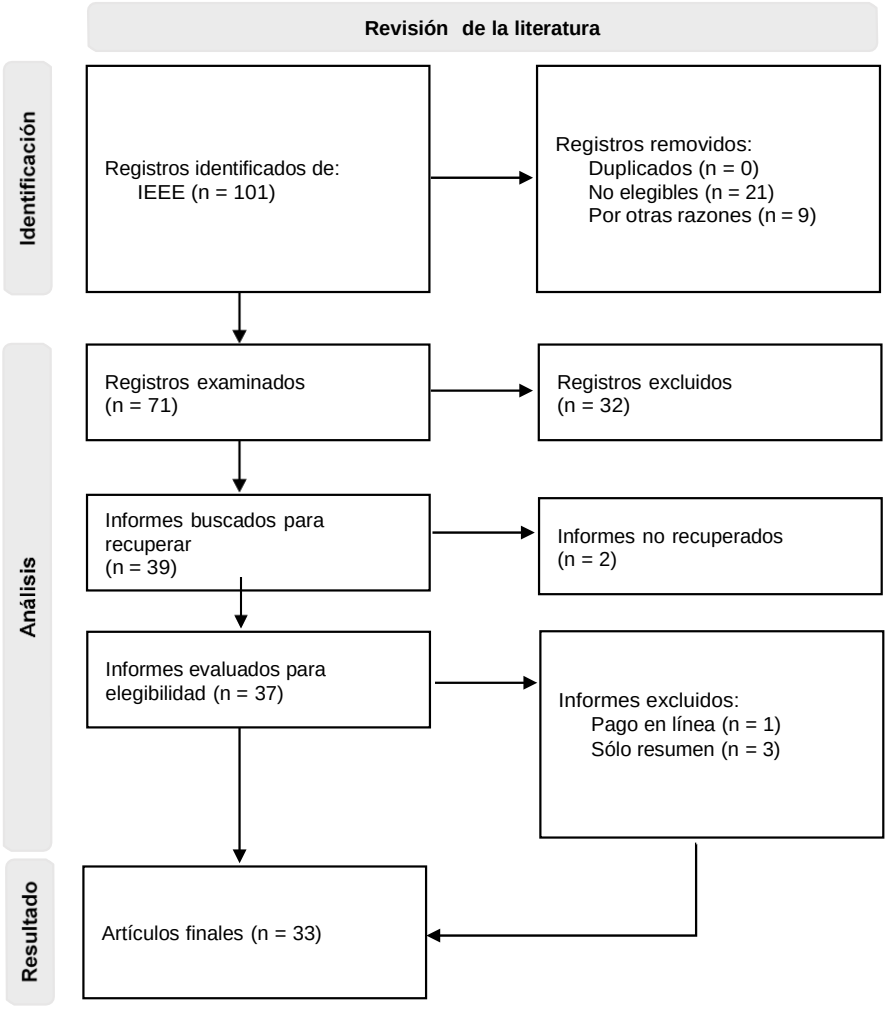

Figura 2. PRISMA de identificación de artículos científicos.

artículos, pero 2 artículos no son recuperables, entre los 37 artículos, 1 artículo se descarta por ser pago y 3 artículos se descartan por ser artículo de una sola página. Son 33 artículos que sirven para realizar el proceso donde extraeremos los datos.

Al extraer o separar de datos, se mantiene una hoja electrónica con los datos analizados de los 33 artículos. La hoja electrónica contiene ocho grupos que se describen a continuación. El primer grupo es llamado Factores de seguridad que contiene: Vulnerabilidades, Riesgos, Amenazas. El segundo grupo es llamado Características de seguridad que contiene: Confidencialidad, Integridad, Disponibilidad y Autenticación. El tercer grupo es llamado Ataques comunes que contiene: DDoS, Ransomware, Malware, Zero-Day, Man in the Middle, Inyeccion, Spoofing, Sniffing, Rogue, Botnet y Otros. El cuarto grupo es llamado Soluciones Tecnológicas que contiene: Inteligencia Artificial, Machine Learning, Blockchain, Protocolos y Cifrado. El quinto grupo es llamado Propuestas que contiene: Firewall, Framework Personalizados, Arquitectura, Norma Estándar y DMZ. El sexto grupo es llamado Acciones que contiene: Detectar, Mitigar, Prevenir, Monitoreo y Proteger. El séptimo grupo es llamado Componentes a proteger que contiene Dispositivos, Red y Almacén de datos. El octavo grupo es llamado Dominios que contiene Industrial, Hogar, Transporte, Educación, Salud y Otros.

La tabla 1 presenta los 33 artículos que se realizó la extracción de datos.

Tabla 1. Artículos científicos extraídos

Referencias	Cant.
(Djenna et al., 2020), (S. Zhao et al., 2020), (Manta-Caro et al., 2020), (Alferidah & Jhanjhi, 2020), (Shin & Seto, 2020), (Datta, 2020), (Giannoutakis et al., 2020)	7
(Mullet et al., 2021), (Chavis et al., 2021), (Espina et al., 2021), (Boukerche & Coutinho, 2021), (Zaghloul et al., 2021), (Arpaia et al., 2021)	6
(Tashtoush et al., 2022), (Lam et al., 2022), (Hamza et al., 2022), (Xenofontos et al., 2022), (Quadar et al., 2022), (Alagappan, Andrews, et al., 2022), (Alagappan, Baptist Andrews, et al., 2022), (Alaali et al., 2022), (Khurshid et al., 2022), (Salazar et al., 2022), (Junior et al., 2022), (Ghimire & Rawat, 2022), (Blagoev & Atanasova, 2022), (Pirbhulal et al., 2022), (Halabi et al., 2022), (H. Zhao & Silverajan, 2022), (Nguyen et al., 2022)	17
(Kandhro et al., 2023), (Thakur, 2023), (Ayavaca-Vallejo & Avila-Pesantez, 2023)	3

Realizado por el autor.

4.2. Determinación de los ataques, las tecnologías, los dominios, las temáticas y las soluciones que existen de ciberseguridad en redes IoT mediante la revisión de los artículos científicos.

En base a los 33 artículos obtenidos producto de la revisión bibliográfica, se obtuvieron soluciones a las preguntas de investigación y se determinaron los porcentajes de: factores de seguridad, características de seguridad, ataques comunes, soluciones tecnológicas, propuestas, acciones, componente a proteger y dominios.

a. ¿Cuáles son los Factores de seguridad en IoT?

El primer grupo llamado Factores de seguridad presenta: las vulnerabilidades en 37%, los riesgos en 27 y las amenazas en 36%, ver figura 3.

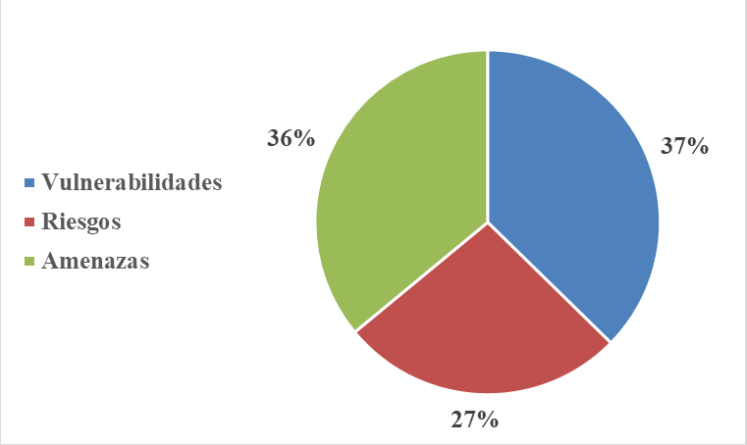

Figura 3. Factores de seguridad.

b. ¿Cuáles son las Características de seguridad en IoT? El segundo grupo llamado Características de seguridad presenta: la confidencialidad en 24%, la integridad en 27%, la disponibilidad en 30% y la autenticación en 19%, ver figura 4.

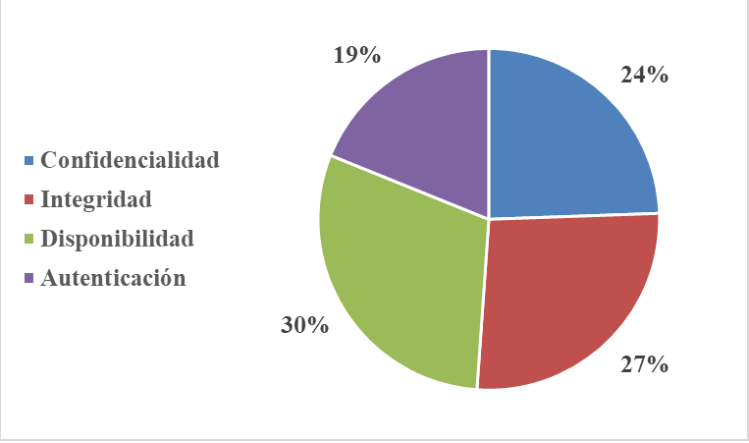

Figura 4. Factores de seguridad.

c. ¿Cuáles son los Ataques comunes en IoT?

El tercer grupo llamado Ataques comunes presenta: DDoS en 29%, Ransomware en 3%, Malware en 11%, Zero-Day en 7%, Man in the Middle en 9%, Inyeccion en 8%, Spoofing en 5%, Sniffing en 7%, Rogue en 1%, Botnet en 4% y Otros en 16%, ver figura 5.

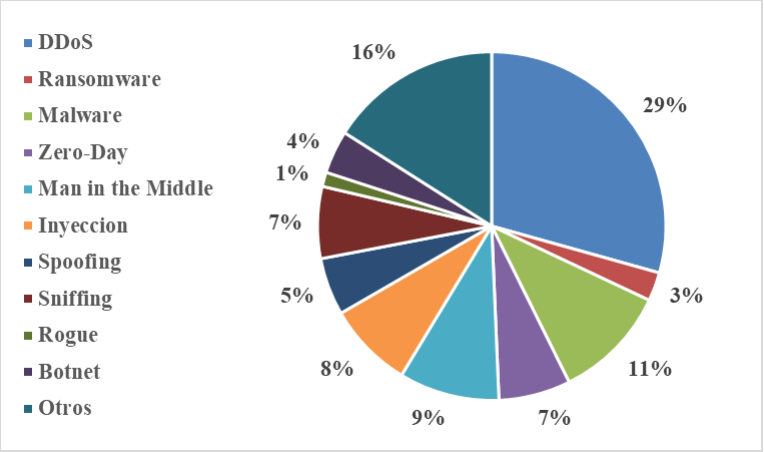

Figura 5. Ataques comunes.

d. ¿Cuáles son las Soluciones Tecnológicas en IoT?

El cuarto grupo llamado Soluciones Tecnológicas presenta: Inteligencia Artificial en 13%, Machine Learning en 22%, Blockchain en 3%, Protocolos en 34% y Cifrado 28%, ver figura 6.

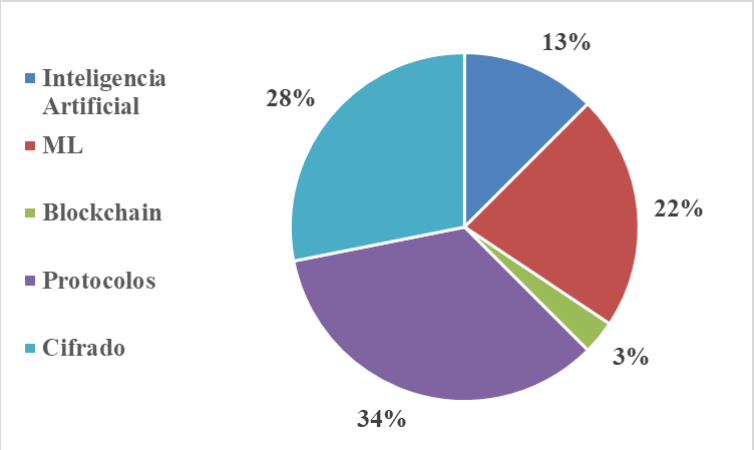

Figura 6. Soluciones tecnológicas.

e. ¿Cuáles son las Propuestas en IoT?

El quinto grupo llamado Propuestas presenta: Firewall en 6%, Framework Personalizados en 51%, Arquitecturas en 23%, Norma Estándar en 17% y DMZ 3%, ver figura 7.

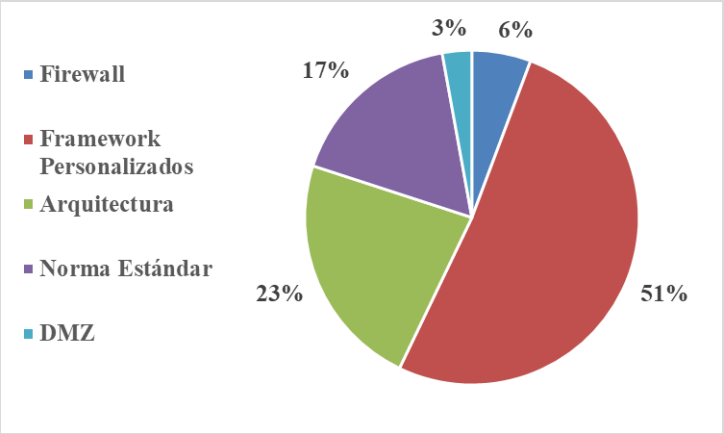

Figura 7. Propuestas.

f. ¿Cuáles serían las Acciones contra los ataques?

El sexto grupo llamado Acciones presenta: detectar en 24%, mitigar en 14%, prevenir en 18%, monitoreo en 24% y proteger en 20%, ver figura 8.

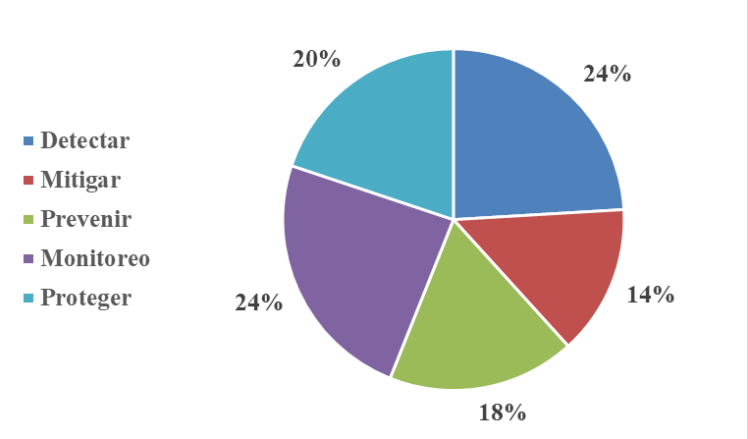

Figura 8. Acciones.

g. ¿Cuáles son los Componentes a proteger en IoT?

El séptimo grupo llamado Componentes a proteger presenta: dispositivos en 49%, red en 35% y almacén de datos en 16%, ver figura 9.

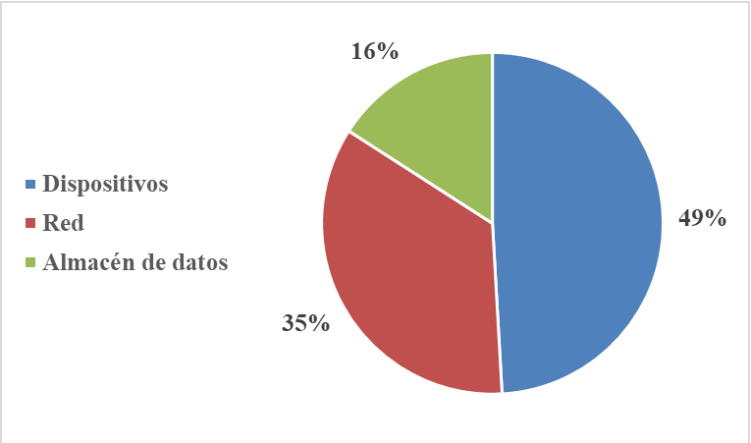

Figura 9. Componentes a proteger.

h. ¿Cuáles son los Dominios utilizados en IoT?

El octavo grupo llamado Dominios presenta: Industrial en 30%, Hogar en 12%, Transporte en 6%, Educación en 9%, Salud en 9% y Otros en 34%, ver figura 10.

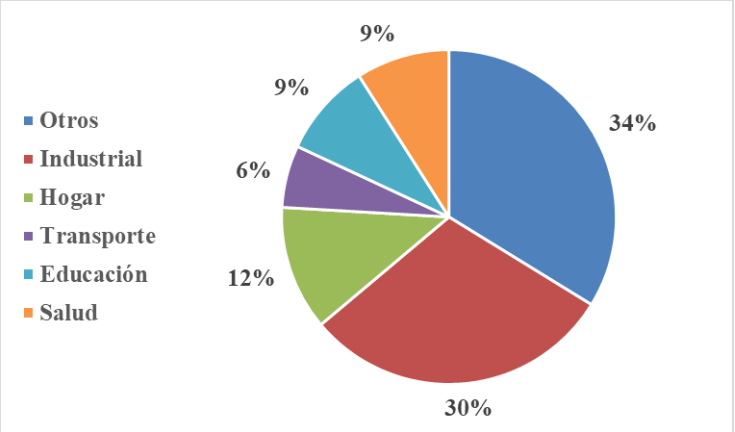

Figura 10. Componentes a proteger.

4.3. Análisis los resultados para conocer las soluciones de ciberseguridad en IoT obtenidos de los artículos científicos mediante el análisis cuantitativo y descriptivo.

De acuerdo a la extracción y tabulación de los datos, se tiene lo siguiente de cada grupo:

El factor de seguridad más referenciada son las vulnerabilidades, es decir que los artículos quieren minimizar las debilidades existentes en los sistemas que pueden ser utilizados por personas con malas intenciones y romper la seguridad; es decir 28 de 33 artículos referencia las vulnerabilidades.

La característica de seguridad más referenciada es la disponibilidad, es decir tratan de maximizar la capacidad de servicios o datos o sistemas, que puedan ser accesibles a cualquier usuario o proceso previamente autorizado, además que la información pueda ser accedida en cualquier momento y evitar la pérdida; es decir 27 de 33 artículos referencia la disponibilidad.

El ataque más común es la denegación de acceso distribuido DDoS, es decir que los artículos tratan de minimizar a los procesos que ataquen a un servidor o servicios desde varios sitios o equipos al mismo tiempo; este tipo de ataque hace el recurso del servido no sea suficiente para atender a los demás, y puede colapsar; el servidor puede caer junto al servicio que ofrece; es decir 22 de 33 artículos nombra el ataque DDoS.

La solución tecnológica más utilizada son los protocolos, es decir que los artículos nombran algún sistema de reglas que aprueban que los objetos de un sistema se comuniquen entre ellos para enviar información por cualquier medio; es decir 11 de 33 artículos utilizaron protocolos.

La propuesta más diseñada es el framework personalizado; es decir los artículos diseñaron entornos o marcos para utilizar un conjunto de prácticas o criterios para mantener en algún estándar o alguna regla, y otros se presentan como herramientas listas para utilizar; es decir 18 de 33 artículos realizaron modelos de ciberseguridad en IoT.

Las acciones más realizadas son detectar y monitoreo; es decir que un grupo de artículos propone detectar el uso no autorizado o detectar posibles ataques o detectar posibles amenazas o detectar intrusos; otro grupo de artículos, no necesariamente los mismos, proponen monitorear o hacer el seguimiento de las actividades anómalas que son detectadas; es decir 23 de 33 artículos proponen estas dos acciones.

El componente que más se protege son los dispositivos, es decir que el hardware IoT mantienen o aplican medidas de seguridad para que la obtención de datos continúe en forma permanente; es decir 30 de 33 artículos utilizan la ciberseguridad para proteger los componentes de primera línea.

El dominio que más propuestas se presentan es en el industrial, independiente de otros, es decir que los artículos se enfocan en las diferentes industrias para aplicar la ciberseguridad en este dominio, aquí existen otra clase de dispositivos que se enfocan en captar datos de una industria o manufacturera en marcha; es decir 10 de 33 artículos aplicaron la seguridad a este dominio.

Otras deducciones: El 24% de los artículos (8) cubren las Vulnerabilidades-Riesgos-Amenazas y Confidencialidad-Integridad-Disponibilidad. El 18% de los artículos (6) cubren los ataques

DDoS y Malware. El 48% de los artículos (16) coinciden en detectar y monitoreo. El 24% de los artículos (8) coinciden en proteger los 3 componentes básicos de IoT que son dispositivos, red y almacén de datos.

Los artículos que utilizan Machine Learning nombran a los algoritmos: SVM, LSTM, Random Forest, kNN, Decision Tree, Bayesian. Otro tipo de ataques encontrados en los artículos son: APT, Browser, red, Web Server, Phishing, Samba, Unknown Instances, Masquerade, Port Scanning, Data forgery, Spam, Malicious attack. Protocolos encontrados en los artículos: AMQP, MQTT, HTTPS, STOMP, CoAP, NetFlow. Los estándares hallados son OWASP (Open Web Application Security Project), ISO/IEC 27017, ISO/IEC 27002, National Institute of Standards and Technology (NIST), European Network and Information Security Agency (ENISA), ISO/IEC 17825, ISO/IEC 27400, NISTIR 8228-8259-8259A, ISO/IEC 29147, ISO/IEC 17065, ISO/IEC 30111. En cifrado se utilizan los algoritmos: Rivest Shamir and Adleman (RSA), Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES).

Las figuras 11 y 12 presentan los 33 artículos tabulados en la hoja electrónica, por cada columna que se hallaba en el documento se marca con 1, por cada columna esta la sumatoria de la columna, por cada grupo se suma para obtener subtotal del grupo, el porcentaje se obtiene dividiendo la sumatoria de la columna para el subtotal del grupo.

Las columnas que se presentan son: grupo Factores de seguridad: A1 Vulnerabilidades, A2 Riesgos, A3 Amenazas. Grupo Características de seguridad: B1 Confidencialidad, B2 Integridad, B3 Disponibilidad, B4 Autenticación. Grupo Ataques comunes: C1 DDoS, C2 Ransomware, C3 Malware, C4 Zero-Day, C5 Man in the Middle, C6 Inyeccion, C7 Spoofing, C8 Sniffing, C9 Rogue, C10 Botnet, C11 Otros. Grupo Soluciones Tecnológicas: D1 Inteligencia Artificial, D2 ML, D3 Blockchain, D4 Protocolos, D5 Cifrado. Grupo Propuestas: E1 Firewall, E2 Framework Personalizados, E3 Arquitectura, E4 Norma Estándar, E5 DMZ. Grupo Acciones: F1 Detectar, F2 Mitigar, F3 Prevenir, F4 Monitoreo, F5 Proteger. Grupo Componentes a proteger: G1 Dispositivos, G2 Red, G3 Almacén de datos. Grupo Dominios: H1 Otros, H2 Industrial, H3 Hogar, H4 Transporte, H5 Educación, H6 Salud.

No	Articulo	Año	Factores de seguridad			Características de seguridad				Ataques comunes											Soluciones Tecnológicas				
			A1	A2	A3	B1	B2	B3	B4	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	D1	D2	D3	D4	D5
1	A Pragmatic Cybersecurity Strategie	2020					1	1	1		1											1			
2	A Review of Cybersecurity Guidelin	2021		1	1	1	1	1	1	1	1		1	1											1
3	A Voice Assistant for IoT Cybersecu	2021					1	1	1	1										1			1		
4	Agile Approaches for Cybersecurity	2022					1	1	1		1														
5	ANT-Centric IoT Security Reference	2022		1	1	1		1												1					1
6	Combining Device Behavioral Mode	2022			1	1		1	1		1												1		
7	Computational Intelligence Enabled	2020	1	1		1		1	1				1	1								1			
8	Consumer, Commercial, and Indust	2022	1	1	1	1	1	1	1	1				1		1									
9	Cybersecurity architecture function	2021	1	1	1	1	1	1	1	1			1												1
10	Cybersecurity as Information Retrie	2020	1	1	1	1	1		1	1							1		1						1
11	Cybersecurity Impact over Bigdata a	2020	1		1	1		1		1					1	1	1	1		1					
12	Design Guidelines for Machine Lear	2021	1		1		1	1	1	1			1				1			1			1		
13	Detection of Real-Time Malicious In	2023	1		1	1	1		1	1								1		1	1				
14	Cybersecurity Issues of IoT in Ambi	2022	1	1	1	1	1	1	1	1								1		1					1
15	Cybersecurity Risks Mitigation in th	2022	1	1	1	1	1	1	1	1	1	1	1	1	1					1			1		1
16	Cybersecurity Risks Quantification i	2022	1	1	1			1		1										1			1		
17	Cybersecurity Threats and Solutions	2022	1		1	1	1	1	1	1							1			1					1
18	Development of IoT Security Exerci	2020	1		1			1	1	1										1					
19	DRAFT - A Cybersecurity Framework	2020	1	1	1		1		1	1															1
20	EU Cybersecurity Act and IoT Certifi	2022	1	1	1	1	1	1		1															
21	A Blockchain Solution for Enhancing	2020		1	1	1	1	1																1	
22	Green IoT System Architecture for A	2021	1		1		1	1							1										1
23	INTEROPERABILITY AND CYBERSECU	2022	1		1	1	1	1	1																
24	IoT Administration Cybersecurity us	2023	1	1	1	1		1		1								1							1
25	Learning Cybersecurity in IoT-based	2022	1		1		1																		1
26	Power Measurement-Based Vulner	2021	1		1	1	1	1							1										
27	Recent Advances on Federated Lear	2022	1	1	1	1	1	1	1	1						1				1	1		1		
28	RNG Entropy Enrichment to Improv	2022	1	1																					1
29	Smart Home IoT Cybersecurity Surv	2023	1	1		1	1	1	1	1			1		1	1					1				1
30	Towards a Novel Framework for Rei	2022	1	1	1	1	1	1																	1
31	Towards Adaptive Cybersecurity for	2022	1	1	1			1	1	1			1	1	1	1					1	1			
32	Visual Cybersecurity Collaboration	2022	1	1	1	1		1		1	1				1						1				1
33	Towards improving explainability, r	2022	1		1			1					1					1					1		
			28	20	27	22	24	27	17	22	2	8	5	7	6	4	5	1	3	12	4	7	1	11	9
			75			90				75											32				
			37%	27%	36%	24%	27%	30%	19%	29%	3%	11%	7%	9%	8%	5%	7%	1%	4%	16%	13%	22%	3%	34%	28%

Figura 11. Revisión literaria parte a.

No	Articulo	Año	Propuestas					Acciones					Componentes a proteger			Dominios					
			E1	E2	E3	E4	E5	F1	F2	F3	F4	F5	G1	G2	G3	H1	H2	H3	H4	H5	H6
1	A Pragmatic Cybersecurity Strategie	2020			1			1	1				1	1	1	1					
2	A Review of Cybersecurity Guidelin	2021					1 1			1			1	1			1				
3	A Voice Assistant for IoT Cybersecu	2021			1			1						1	1				1		
4	Agile Approaches for Cybersecurity	2022					1	1		1			1	1	1					1	
5	ANT-Centric IoT Security Reference	2022			1					1			1	1						1	
6	Combining Device Behavioral Mode	2022			1			1					1	1			1				
7	Computational Intelligence Enabled	2020			1			1				1 1	1	1		1					
8	Consumer, Commercial, and Indust	2022						1	1	1		1	1	1			1				
9	Cybersecurity architecture function	2021				1		1	1			1 1	1	1	1						1
10	Cybersecurity as Information Retrie	2020			1				1			1 1	1	1	1		1				
11	Cybersecurity Impact over Bigdata a	2020							1	1		1	1	1	1	1					
12	Design Guidelines for Machine Lear	2021			1			1		1		1 1	1	1		1					
13	Detection of Real-Time Malicious In	2023				1		1				1	1			1					
14	Cybersecurity Issues of IoT in Ambi	2022					1		1	1		1	1	1			1				
15	Cybersecurity Risks Mitigation in th	2022		1	1			1	1				1	1		1					
16	Cybersecurity Risks Quantification i	2022			1				1			1	1			1					
17	Cybersecurity Threats and Solutions	2022			1			1		1	1	1	1	1			1				
18	Development of IoT Security Exerci	2020				1		1		1	1		1							1	
19	DRAFT - A Cybersecurity Framework	2020				1		1				1 1	1	1	1	1					
20	EU Cybersecurity Act and IoT Certifi	2022			1		1	1	1			1 1	1	1			1				
21	A Blockchain Solution for Enhancing	2020			1							1 1			1			1			
22	Green IoT System Architecture for A	2021				1		1		1		1	1	1	1	1					
23	INTEROPERABILITY AND CYBERSECU	2022			1		1		1			1 1	1							1	
24	IoT Administration Cybersecurity us	2023			1			1		1	1	1	1				1				
25	Learning Cybersecurity in IoT-based	2022				1			1	1	1		1	1					1		
26	Power Measurement-Based Vulner	2021				1					1	1 1	1								1
27	Recent Advances on Federated Lear	2022			1			1	1	1	1	1	1							1	
28	RNG Entropy Enrichment to Improv	2022					1	1			1	1	1	1		1					
29	Smart Home IoT Cybersecurity Surv	2023		1				1	1	1		1	1						1		
30	Towards a Novel Framework for Rei	2022			1			1	1	1	1		1	1	1						1
31	Towards Adaptive Cybersecurity for	2022				1		1	1	1	1	1	1				1				
32	Visual Cybersecurity Collaboration	2022			1			1			1			1			1				
33	Towards improving explainability, r	2022			1			1			1	1	1			1					
			2	18	8	6	1	23	15	17	23	19	30	22	10	11	10	4	2	3	3
			35					97					63			33					
			6%	51%	23%	17%	3%	24%	14%	18%	24%	20%	49%	35%	16%	34%	30%	12%	6%	9%	9%

Figura 12. Revisión literaria parte b.

5. DISCUSIÓN

Internet de las cosas continúa su crecimiento a miles de millones de dispositivos, aunque es vulnerable a los ataques cibernéticos, y puede afectar a la seguridad de cualquier dominio; diferentes ataques de seguridad generan desafíos para los entornos IoT; este documento entrega un pequeño escenario de riesgos cibernéticos en varios dominios.

Puede ser necesario identificar una cantidad más grande de posibles ciberataques y vulnerabilidades, además estudiar los impactos en los dominios ambiental, económico y social; hoy en día, muchas de las plataformas en la nube tienen parámetros de ciberseguridad que son explotados para minimizar el impacto de los ciberataques en cualquier dominio. Otro punto que no se considera en esta investigación, es el ataque a infraestructuras críticas como agua, energía, salud, y que afectan en forma directa a la vida toda persona.

Aquí no se evalúa la ciberseguridad en IoT en los diferentes dominios, tampoco no se consideró problemas de privacidad en los entornos IoT, ni las causas de los ataques. Aunque, es posible enfocarse en la capa de red IoT para combinar o adoptar las propuestas de seguridad de acuerdo a soluciones de Machine Learning.

Los dominios IoT son objetivos atractivos para ciberterroristas, todo ataque es más sofisticado, en especial la denegación de servicio distribuida (DDoS), además que combinan otros modos de operación para esquivar el control de seguridad. De acuerdo a la revisión sistemática, la ciberseguridad adopta inteligencia artificial o algoritmos Machine Learning para proteger los dominios IoT mediante métodos inteligentes para detectar-mitigar-monitorear-prevenir-proteger a los dominios.

Esta investigación puede ser útil para mejorar la ciberseguridad porque entrega un análisis de las redes IoT, puede ser útil para simular una brecha de seguridad o para realizar respuestas de mitigación.

En un trabajo futuro, se propone extender el análisis sobre ataques de ciberseguridad centrado en IoT y sus posibles impactos en los dominios ambientales, económicos y sociales.

6. CONCLUSIÓN

En el presente trabajo, se realizó una revisión exhaustiva de la literatura y se obtuvo 33 artículos científicos que ayudaron a responder las incógnitas sobre ciberseguridad en IoT; el análisis de las preguntas de investigación demuestra que: el factor de seguridad más referenciada son las vulnerabilidades, la característica de seguridad más referenciada es la disponibilidad, el ataque más común es la denegación de acceso distribuido DDoS, la solución tecnológica más utilizada son los protocolos, la propuesta más diseñada es el framework personalizado, las acciones más realizadas son detectar y monitorear, el componente que más se protege son los dispositivos, y el dominio que más referenciado es el industrial.

Se identificaron los factores de seguridad, las características de seguridad, los ataques más comunes, las soluciones tecnológicas, las propuestas diseñadas, las acciones, los componentes que se protegen y los dominios. En total se hallaron 42 características que fueron tabuladas en una hoja electrónica y que respondieron las preguntas de investigación.

Se concluye que IoT es una tecnología emergente que requiere más atención desde el enfoque de la ciberseguridad efectiva, además que IoT incorpora varias tecnologías en desarrollo como Big Data, Inteligencia Artificial, Blockchain, Cifrado, entre otros.

REFERENCIAS

Alaali, A. M., Alateeq, A., & Elmedany, W. (2022). Cybersecurity Threats and Solutions of IoT Network Layer. *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2022*, 250–257. https://doi.org/10.1109/3ICT56508.2022.9990734

Alagappan, A., Andrews, L. J. B., Venkatachary, S. K., Sarathkumar, D., & Raj, R. A. (2022). Cybersecurity Risks Mitigation in the Internet of Things. *Proceedings - 2022 2nd International Conference on Innovative Sustainable Computational Technologies, CISCT 2022*. https://doi.org/10.1109/CISCT55310.2022.10046549

Alagappan, A., Baptist Andrews, L. J., Kumar V, S., Raj, R. A., & D, S. (2022). Cybersecurity Risks Quantification in the Internet of Things. *2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, 154–159. https://doi.org/10.1109/ICRAIE56454.2022.10054330

Alferidah, D. K., & Jhanjhi, N. (2020). Cybersecurity Impact over Bigdata and IoT Growth. *2020 International Conference on Computational Intelligence (ICCI)*, 103–108. https://doi.org/10.1109/ICCI51257.2020.9247722

Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garces, I. (2020). A Comprehensive Study of the IoT Cybersecurity in Smart Cities. *IEEE Access*, *8*, 228922–228941. https://doi.org/10.1109/ACCESS.2020.3046442

Arpaia, P., Bonavolonta, F., Cioffi, A., & Moccaldi, N. (2021). Power Measurement-Based Vulnerability Assessment of IoT Medical Devices at Varying Countermeasures for Cybersecurity. *IEEE Transactions on Instrumentation and Measurement*, *70*, 1–9. https://doi.org/10.1109/TIM.2021.3088491

Ayavaca-Vallejo, L., & Avila-Pesantez, D. (2023). Smart Home IoT Cybersecurity Survey: A Systematic Mapping. *2023 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. https://doi.org/10.1109/ICTAS56421.2023.10082751

Blagoev, I., & Atanasova, T. (2022). RNG Entropy Enrichment to Improve Cybersecurity in IoT and Cloud Services. *2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Ciees*, 1–4. https://doi.org/10.1109/CIEES55704.2022.9990782

Boukerche, A., & Coutinho, R. W. L. (2021). *Design Guidelines for Machine Learning-based Cybersecurity in Internet of Things*. *February*, 393–399. https://doi.org/10.1109/MNET.011.2000396

Chavis, J. S., Doster, M., Feng, M., Zeeshan, S., Fu, S., Aguirre, E., Davila, A., Nyarko, K., Kunz, A., Herriotts, T., Syed, D., Watkins, L., Buczak, A., & Rubin, A. (2021). A Voice Assistant for IoT Cybersecurity. *2021 IEEE Integrated STEM Education Conference (ISEC)*, 165–172. https://doi.org/10.1109/ISEC52395.2021.9764005

Datta, S. K. (2020). DRAFT - A Cybersecurity Framework for IoT Platforms. *2020 Zooming Innovation in Consumer Technologies Conference (ZINC)*, 77–81. https://doi.org/10.1109/ZINC50678.2020.9161441

Djenna, A., Saidouni, D. E., & Abada, W. (2020). A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks. *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6. https://doi.org/10.1109/ISNCC49221.2020.9297251

Ecucert. (2022). *Alertas*. https://www.ecucert.gob.ec/alertas/

Espina, E., Armas-aguirre, J., Manuel, J., & Molina, M. (2021). *Cybersecurity architecture functional model for cyber risk reduction in IoT based wearable devices*. 2021–2024.

https://doi.org/10.1109/CONIITI53815.2021.9619624

Ghimire, B., & Rawat, D. B. (2022). Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. *IEEE Internet of Things Journal*, *9*(11), 8229–8249. https://doi.org/10.1109/JIOT.2022.3150363

Giannoutakis, K. M., Spathoulas, G., & Collen, A. (2020). A Blockchain Solution for Enhancing Cybersecurity Defence of IoT. *IEEE International Conference on Blockchain (Blockchain) A*, 490–495. https://doi.org/10.1109/Blockchain50366.2020.00071

Halabi, T., Bellaiche, M., & Fung, B. C. M. (2022). Towards Adaptive Cybersecurity for Green IoT. *Proceedings of the 2022 IEEE International Conference on Internet of Things and Intelligence Systems, IoTaIS 2022*, 64–69. https://doi.org/10.1109/IoTaIS56727.2022.9975990

Hamza, A., Habibi Gharakheili, H., Pering, T., & Sivaraman, V. (2022). Combining Device Behavioral Models and Building Schema for Cybersecurity of Large-Scale IoT Infrastructure. *IEEE Internet of Things Journal*, *9*(23), 24174–24185. https://doi.org/10.1109/JIOT.2022.3189350

IBM-Security. (2023). *X-Force Threat Intelligence Index*. https://www.ibm.com/mx-es

Junior, A. O., Funchal, G., Queiroz, J., Loureiro, J., Pedrosa, T., Parra, J., & Leitao, P. (2022). Learning Cybersecurity in IoT-based Applications through a Capture the Flag Competition. *2022 IEEE 20th International Conference on Industrial Informatics (INDIN)*, 560–565. https://doi.org/10.1109/INDIN51773.2022.9976079

Kandhro, I. A. L. I., Alanazi, S. M., Ali, F., Kehar, A., Fatima, K., Uddin, M., & Karuppayah, S. (2023). Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures. *IEEE Access*, *11*(January), 9136–9148. https://doi.org/10.1109/ACCESS.2023.3238664

Khurshid, A., Alsaaidi, R., Aslam, M., & Raza, S. (2022). EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. *IEEE Access*, *10*(December), 129932–129948. https://doi.org/10.1109/ACCESS.2022.3225973

Lam, K.-Y., Mitra, S., Gondesen, F., & Yi, X. (2022). ANT-Centric IoT Security Reference Architecture—Security-by-Design for Satellite-Enabled Smart Cities. *IEEE Internet of Things Journal*, *9*(8), 5895–5908. https://doi.org/10.1109/JIOT.2021.3073734

Manta-Caro, C., Fernandez-Luna, J. M., & Fernandez, W. J. (2020). Cybersecurity as Information Retrieval Dimension for Cloud-based Edge-powered IoT Search. *2020 IEEE Latin-American Conference on Communications (LATINCOM)*, 1–6. https://doi.org/10.1109/LATINCOM50620.2020.9282336

Mullet, V., Sondi, P., & Ramat, E. (2021). A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access*, *9*, 23235–23263. https://doi.org/10.1109/ACCESS.2021.3056650

Nguyen, M., La, V. H., Cavalli, R., & de Oca, E. M. (2022). Towards improving explainability, resilience and performance of cybersecurity analysis of 5G/IoT networks. *2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 7–10. https://doi.org/10.1109/ICSTW55395.2022.00016

Pirbhulal, S., Abie, H., & Shukla, A. (2022). Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications. *IEEE Vehicular Technology Conference*, *2022-June*, 1–5. https://doi.org/10.1109/VTC2022-Spring54318.2022.9860581

Quadar, N., Chehri, A., Jeon, G., Hassan, M. M., & Fortino, G. (2022). Cybersecurity Issues of IoT in Ambient Intelligence (AmI) Environment. *IEEE Internet of Things Magazine*, *5*(3), 140–145. https://doi.org/10.1109/IOTM.001.2200009

Salazar, R., Godfrey, T., Winkel, L., Finn, N., Powell, C., Rolfe, B., Seewald, M., Salazar, R., & Winkel, L. (2022). INTEROPERABILITY AND CYBERSECURITY FOR IOT-ENABLED SENSOR DEVICES. *ICAP*.

Shin, S., & Seto, Y. (2020). Development of IoT Security Exercise Contents for Cyber Security Exercise System. *2020 13th International Conference on Human System Interaction (HSI)*, 1–6. https://doi.org/10.1109/HSI49210.2020.9142678

Tashtoush, Y. M., Darweesh, D. A., Husari, G., Darwish, O. A., Darwish, Y., Issa, L. B., & Ashqar, H. I. (2022). Agile Approaches for Cybersecurity Systems, IoT and Intelligent Transportation. *IEEE Access*, *10*, 1360–1375. https://doi.org/10.1109/ACCESS.2021.3136861

Thakur, R. (2023). IoT Administration Cybersecurity using Programmatic Monitoring and Pattern Recognition. *2023 International Conference on Artificial Intelligence and Smart Communication, AISC 2023*, 1210–1214. https://doi.org/10.1109/AISC56616.2023.10085587

Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., & Choo, K.-K. R. (2022). Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. *IEEE Internet of Things Journal*, *9*(1), 199–221. https://doi.org/10.1109/JIOT.2021.3079916

Zaghloul, Z. S., Elsayed, N., Li, C., & Bayoumi, M. (2021). Green IoT System Architecture for Applied Autonomous Network Cybersecurity Monitoring. *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 628–632. https://doi.org/10.1109/WF-IoT51360.2021.9595142

Zhao, H., & Silverajan, B. (2022). Visual Cybersecurity Collaboration and Incident Exchange in Multi-Stakeholder IoT Environments. *2022 IEEE International Conferences on Internet of Things (IThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, 85–92. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics55523.2022.00051

Zhao, S., Li, S., Qi, L., & Xu, L. Da. (2020). Computational Intelligence Enabled Cybersecurity for the Internet of Things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(5), 666–674. https://doi.org/10.1109/TETCI.2019.2941757