UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

ESTADO DEL ARTE DE LOS MÉTODOS DE SEGURIDAD DE DATOS APLICADOS EN INTERNET DE LAS COSAS

Trabajo de titulación previo a la obtención del
Título de Ingeniero e Ingeniera de Sistemas

AUTORES: JOHANN ENRIQUE OVIEDO FÉLIX

MAYRA VANESSA PIZARRO ALOMOTO

TUTOR: MANUEL RAFAEL JAYA DUCHE

Quito-Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros Johann Enrique Oviedo Félix, con documento de identificación N° 1722957360 y Mayra Vanessa Pizarro Alomoto con documento de identificación N° 1719997833 manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos 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.

Quito, 24 de febrero del año 2023.

Atentamente,

Mayra Vanessa Pizarro Alomoto

1719997833

Johann Enrique Oviedo Félix

1722957360

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

Nosotros, Mayra Vanessa Pizarro Alomoto con documento de identificación N° 1719997833 y Johann Enrique Oviedo Félix y N° 1722957360 , expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Artículo Académico : Estado del arte de los métodos de seguridad de datos aplicados en internet de las cosas, el cual ha sido desarrollado para optar por el título de: Ingenieros de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

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

Quito, 24 de febrero del año 2023.

Atentamente,

Mayra Vanessa Pizarro Alomoto

1719997833

Johann Enrique Oviedo Félix

1722957360

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Manuel Rafael Jaya Duche con documento de identificación N° 1710631035, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ESTADO DEL ARTE DE LOS MÉTODOS DE SEGURIDAD DE DATOS APLICADOS EN INTERNET DE LAS COSAS, realizado Mayra Vanessa Pizarro Alomoto con documento de identificación N° 1719997833 y Johann Enrique Oviedo Félix con documento de identificación N°1722957360, 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.

Quito, 24 de febrero del año 2023.

Atentamente,

Ing. Manuel Rafael Jaya Duche, MSc
1710631035

AGRADECIMIENTO

Ante todo, queremos agradecer a Dios por brindarnos salud, fuerza y sabiduría para completar esta importante etapa de nuestra vida académica. Sin Su bendición, esto no habría sido posible.

Queremos expresar nuestro sincero agradecimiento a nuestros hogares, por su amor, apoyo y comprensión incondicional a lo largo de todo este proceso. A nuestros padres, por ser guías y ejemplos en todo momento, por enseñarnos valores y principios que nos han ayudado a crecer como personas.

A nuestras familias y amigos, por ser fuente de motivación y aliento en los momentos difíciles.

Y de manera muy especial agradecemos a nuestro tutor Ing. Manuel Rafael Jaya Duche por la asesoría profesional impartida durante el proceso de titulación.

Hoy celebramos el éxito en haber completado un logro académico de gran importancia, que será la base para futuros éxitos y logros. Estamos todos juntos orgullosos de nuestro arduo trabajo y dedicación.

Mayra Vanessa Pizarro Alomoto

Johann Enrique Oviedo Félix

ESTADO DEL ARTE DE LOS MÉTODOS DE SEGURIDAD DE DATOS APLICADOS EN INTERNET DE LAS COSAS

STATE OF THE ART OF DATA SECURITY METHODS APPLIED TO THE INTERNET OF THINGS

Mayra Pizarro[1], Johann Oviedo[2], Manuel Jaya [3]

Resumen

El propósito de esta investigación es crear el estado del arte de técnicas y procesos usados en el ámbito de la ingeniería, utilizando un mapeo sistemático enfocado a los métodos de seguridad de datos aplicados en Internet de las Cosas. El trabajo recopila documentos a partir del 2017 utilizando mapeo sistemático de literatura y una revisión sistemática aplicando el método PRISMA, cumpliendo el rigor metodológico y de la calidad. Obteniendo uno de los métodos más usados como cifrado utilizado en un 52,8% en las empresas, también la monitorización de anomalías y detección de intrusiones, el control de acceso basado en roles, gestión de claves y autenticación de dispositivos y usuarios, además protocolos que se utilizan para establecer la comunicación y la transferencia de información de manera segura entre distintos dispositivos, como MQTT, que es utilizado por el 38.3% para la comunicación de datos en tiempo real, JWT, AMQP, DDS y HTTP, que es utilizado por el 70% de los desarrolladores de IoT, acompañando estos mecanismos con buenas prácticas y ser conscientes de las consecuencias negativas de la mala práctica, garantizando la seguridad de datos en los dispositivos IoT.

Palabras clave: PRISMA, Seguridad de Datos, Detección de intrusiones, Internet de las cosas (IoT).

Abstract

The purpose of this research is to create the state of the art of techniques and processes used in the field of engineering, using a systematic mapping focused on data security methods applied in the Internet of Things. The work collects documents from 2017 using systematic literature mapping and a systematic review applying the PRISMA method, complying with methodological rigor and quality. Obtaining one of the most used methods as used by 52.8% in companies, also anomaly monitoring and intrusion detection, role-based access control, key management and device and user authentication, in addition protocols used to establish communication and transfer information securely between different devices, such as MQTT, which is used by 38.3% for real-time data communication, JWT, AMQP, DDS and HTTP, which is used by 70% of IoT developers, accompanying these mechanisms with good practices and being aware of the negative consequences of bad practice, guaranteeing data security in IoT devices.

Keywords: PRISMA, Data Security, Intrusion Detection, Internet of Things (IoT)

[1] Estudiante de Ingeniería de Sistemas- Universidad Politécnica Salesiana, Egresado-UPS-sede Quito. Autor para correspondencia: Johann Enrique Oviedo Félix joviedo@est.ups.edu.ec y Mayra Vanessa Pizarro Alomoto mpizarroa@est.ups.edu.ec

[2] Magister en Redes de Información y Conectividad, Ingeniero en Electrónica y Telecomunicaciones, Profesor de Ingeniería en Sistemas-UPS-sede Quito

Email: mjaya@ups.edu.ec

1. INTRODUCCIÓN

La amalgama del mundo físico y el digital en la Internet tradicional preparó el camino para el futuro Internet de los objetos (IoT). La IoT se concibe como un modelo de red para llenar el vacío existente entre el mundo cibernético y el físico cuyo concepto central conectar a Internet a través de redes cableadas o inalámbricas todos aquellos objetos que nos rodean y que cuentan con capacidad de comunicación, tales como etiquetas de identificación por radiofrecuencia, dispositivos móviles, sensores, actuadores, entre otros[1].

La IoT ayuda a optimizar los procesos mediante el análisis avanzado de datos y es el catalizador de nuevos segmentos de mercado al aprovechar sus características ciber físicas, dando lugar a aplicaciones y servicios transversales [2], sin embargo, presentan ciertas debilidades en la seguridad. Por seguridad se hace referencia al grado de resistencia o protección de la infraestructura y las aplicaciones de IoT. Muchos de estos dispositivos son objetivos fáciles para la intrusión porque dependen de muy pocos recursos externos [3].

En ese sentido, dado el incipiente crecimiento del número de dispositivos que se conectan a la IoT, genera que el intercambio de datos sea cada vez más rápido, motivo por el cual, es empleado por grandes industrias lo que ha generado preocupación debido a que los ciberdelincuentes están poniendo su atención en ella, quienes buscan acceder a información de manera ilícita atacando a las vulnerabilidades y amenazando a los dispositivos [4].

Las vulnerabilidades son debilidades o fallas en el sistema informático que compromete la seguridad de la información [5] por lo que bajo este contexto, la seguridad se vuelve más difícil debido a las características de los dispositivos, que incluyen una escala extremadamente grande, un diseño de bajo coste, limitaciones de recursos, heterogeneidad de los dispositivos, preferencia de las funciones sobre la seguridad, mayores requisitos de privacidad y una gestión de la confianza más difícil [6].

La seguridad de los datos son entonces las medidas para proteger la privacidad digital ante situaciones de fallas parciales o totales, esto es importante cuando la información es el principal activo con el que se cuenta [7]. Es importante aclarar que la seguridad de datos es la protección de la información sin importar el medio donde se encuentre, este puede ser de tipo físico, pero para IoT puede ser magnético u otro medio digital, por el contrario, la seguridad informática se centra en la protección de la infraestructura tecnológica, es decir, hardware y software [4].

En el mismo contexto, los ataques que son más frecuentes son los DDos (Denegación de servicios distribuidos), espionaje, vigilancia y ransomware [4]. Al hablar de DDos se entienden como las amenazas simples pero que logran su fin, por ello las empresas la usan como filtro para medir el grado de funcionamiento de sus sistemas de seguridad, pero los delincuentes del internet lo emplean para el robo de información o daño de equipos.

Respecto al espionaje y vigilancia lejos de perseguir el daño a los equipos se centra en el acceso no permitido a la información de las entidades, accesos a los sistemas de vigilancia para realizar espionaje. Debido a que los dispositivos IoT son de uso muy cotidiano no tienen módulos de seguridad fuertes por tanto los hackers los toman como puntos débiles.

Otro tipo de ataque es el ransomware, consiste en el robo de la información y pérdida de acceso a los datos por parte del dueño original, esto hace posible los robos financieros. Su principal modalidad es la infección de los dispositivos por medio de links, correos electrónicos, documentos Word, o PDF que redirecciona a la página con malware.

En definitiva, a pesar de ser una tecnología nueva, el tema de la seguridad es débil en comparación con otra tecnología menos actual debido a que aún no está perfeccionada.

En el escenario actual de Internet, existen varios protocolos y tecnologías disponibles para abordar la mayor parte de los inconvenientes relacionados con la seguridad de las redes inalámbricas, pero las herramientas existentes siguen teniendo una restricción en su aplicación en el ámbito del IoT debido a las limitaciones de los nodos de hardware y las redes de sensores Inalámbricas. Otra razón es que los protocolos de seguridad convencionales devoran grandes cantidades de memoria y recursos informáticos [8].

Según la norma ISO/IEC 27001:2013, la seguridad de la información se ocupa de salvaguardar la confidencialidad, la integridad y disponibilidad de la información [9].

Los principales métodos o mecanismos deben ser implementados en los sistemas de información que permita mantener los principios mencionados anteriormente por la norma ISO/IEC 27001:2013 y coincidiendo con referencias son: cifrado, firma digital, control de acceso, integridad de datos y control de encaminamiento, cifrado, autenticación de dispositivos y usuarios, control de acceso basado en roles, gestión de claves, monitorización de anomalías y detección de intrusiones [10] [11].

Sin embargo, deben tomarse en cuenta buenas prácticas de seguridad, estas son acciones que contribuyen a evitar los ataques cibernéticos, y por otro lado de no seguirlas estas son consideradas como malas prácticas y son las que repercuten de forma negativa en la seguridad [12].

Mediante un estado del arte es posible agrupar diversos estudios referentes a los métodos de seguridad de datos aplicados actualmente en Internet de la Cosas, con el fin de obtener información concisa la cual puede ser usada a futuro reduciendo tiempos de búsqueda y logrando conocer el estado actual en la que se encuentra esta investigación.

Por lo expuesto en la presente sección, el propósito global del actual artículo consiste en desarrollar el estado del arte de técnicas y procesos usados en el ámbito de la ingeniería, utilizando una revisión sistemática de literatura enfocado a los métodos de identificación de intrusos en IoT para la seguridad de datos.

2. METODOLOGÍA

Una revisión bibliográfica exhaustiva sobre un tema establece una base firme para el avance de los conocimientos. Identifica la investigación existente y las áreas en las que es necesario investigar.

Es por mencionado que esta investigación se desarrolla en base de un mapeo sistemático de literatura (SMS) y la revisión sistemática de literatura siguiendo la guía del método PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses). Esta metodología hace posible documentar de forma transparente el motivo de la revisión, qué acciones se ejecutaron y qué se encontró [13], con el fin de localizar y agregar las mejores pruebas disponibles sobre la seguridad de datos aplicados en internet de las cosas.

1.1. Proceso de la metodología aplicada

El proceso seguido para dar consecución consta de 6 pasos que respaldan a esta revisión sistemática, los cuales se describen a continuación.

Paso 1: Formulación de la pregunta u objetivo de la revisión.

Responde a la realización, recopilación de información, para formar un estado del arte de los métodos de seguridad de datos aplicados en internet de las cosas.

RQ1: ¿Cuántos documentos y en qué bases de datos existen en relación con la temática?

RQ2: ¿Cuáles son las vulnerabilidades y amenazas más comunes en ambiente IoT, en relación con la seguridad?

RQ3: ¿Cuáles son los mecanismos de seguridad IoT para mitigar amenazas y vulnerabilidades?

RQ4: ¿Qué protocolos de ciberseguridad y modelos de arquitectura de comunicación pueden ser aplicados en entornos IoT?

RQ5: ¿Cuáles son las medidas de seguridad recomendadas, así como las estrategias de control y protección, para las tecnologías de hardware y software?

RQ6: ¿Se puede ejemplificar un escenario de pruebas la importancia de los métodos de seguridad en los dispositivos IoT?

Paso 2: Descripción de las fuentes y métodos empleados para la búsqueda

Para la localización y búsqueda de estudios primarios, se utilizaron varias bases de datos documentales, para ello se accedió a las bases que son accesibles por medio del internet, entre ellos están:

i) Scopus.
ii) Springer Link.
iii) IEEE Xplore.
iv) Pro Quest.
v) Science Direct.

Paso 3: Establecimiento y uso de criterios para seleccionar los estudios.

Para la selección de los documentos de carácter científico se han establecido varios criterios para su consideración, así:

Palabras clave:

La búsqueda se realizó combinando varias palabras clave sobre el artículo sobre firewall o antivirus, infraestructura de clave pública PKI, Pentesting; Intrusion Prevention Systems (IPS), Intrusion Detection Systems IDS, Transfer learning algorithm y sus traducciones al idioma inglés. Para ampliar los horizontes y encontrar un mayor número de estudios, se utilizaron las cadenas de búsqueda booleanas descritas en anexos la Tabla 3.

Criterios de inclusión:

I1: Estudios publicados desde 2017.
I2: Estudios publicados en bases de datos como Scopus, Springer Link, IEEE Xplore, Pro Quest, y Science Direct.
I3: Estudios publicados en inglés y español.
I4: Estudios que contengan las palabras clave.

Criterios de exclusión:

Se consideran los siguientes:

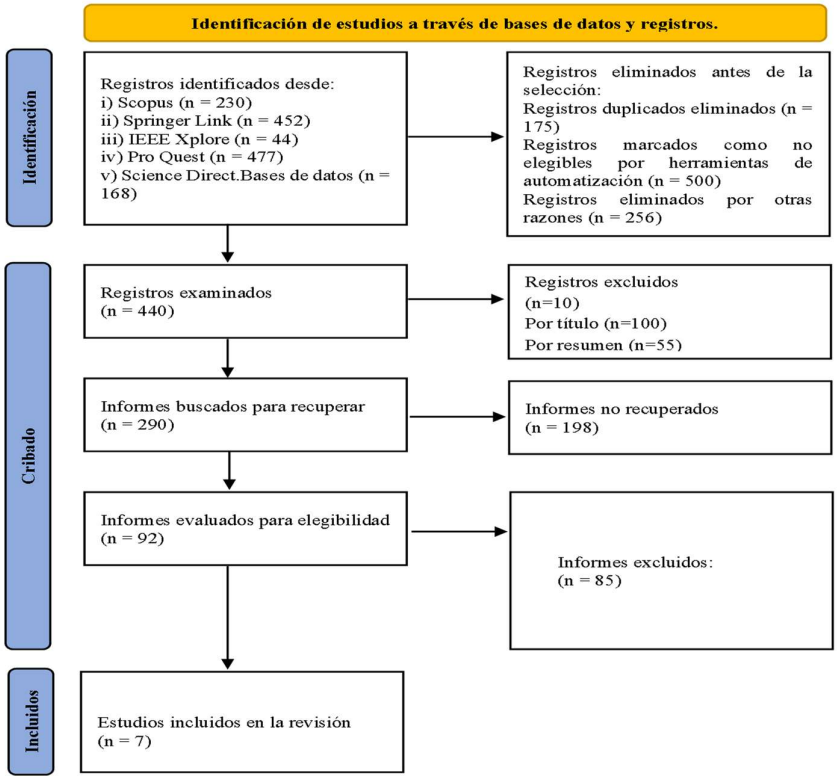
E1: Estudios publicados antes de 2017.
E2: Estudios que no estén indexados en las bases de datos mencionadas.
E3: Estudios que no posean su texto completo.

Paso 4: Análisis crítico de los estudios.

La metodología PRISMA establece la lista de comprobación, para verificar si se ha cumplido con los documentos requeridos o si no se ha realizado. Los siguientes filtros de revisión se utilizan para la selección de estudios primarios, los mismos que se han dividido en siete secciones:

1. Título.
2. Resumen.
3. Introducción.
4. Métodos.
5. Resultados.
6. Discusión
7. Financiación.

Paso 5: Cribado y selección de investigaciones



Posterior a la selección de las investigaciones se aplicó los criterios de inclusión y exclusión, este proceso se detalla en la

Figura 1. Proceso para la selección de artículos

Fuente: Elaborado por el autor

Paso 6: Conclusiones e inferencias sobre los resultados.

Se concluye enunciando las principales inferencias que desprenden en este caso de los métodos de seguridad de datos aplicados en internet de las cosas.

3. RESULTADOS Y DISCUSIÓN

A continuación, se va a presentar y discutir los resultados obtenidos en el trabajo de investigación. Se resumirán los hallazgos más importantes y se analizarán los datos obtenidos, con el objetivo de responder a las preguntas de investigación planteadas en el trabajo.

3.1. Resultados

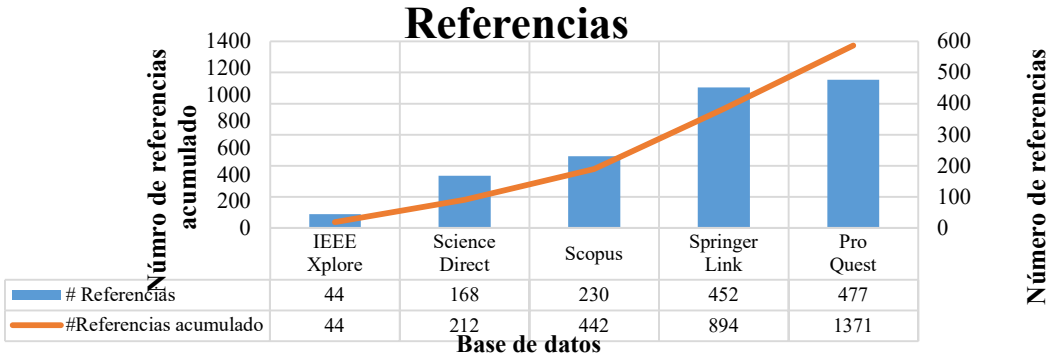


Figura 2. Número de documentos en cada base de datos

Fuente: Elaborado por el autor

RQ1: *¿Cuántos documentos y en qué bases de datos existen en relación con la temática?*

El propósito de esta investigación fue la revisión de la literatura existente que trata sobre los métodos de seguridad de datos aplicados en internet de las cosas.

Inicialmente al aplicar la estrategia en las bases de datos seleccionadas se han identificado un total de 1371 documentos referenciales, los que se encuentran especificados en estos la Figura 2.

RQ2: *¿Cuáles son las vulnerabilidades y amenazas más comunes en ambiente IoT, en relación con la seguridad?*

Las vulnerabilidades y amenazas identificadas en las referencias que están asociadas a la gran variedad de dispositivos del internet de las cosas (IoT) son:

- Contraseñas débiles o en texto plano.
- Servicios de red inseguros.
- Interfaz insegura.
- Ausencia de mecanismo fiable de actualización firmware.
- Librerías inseguras o desactualizadas.
- Deficiente protección de datos personal o privada.
- Almacenamiento y trasferencia de datos insegura.
- Falta de gestión de dispositivos.
- Parámetros por defecto inseguros.

RQ3: *¿Cuáles son los mecanismos de seguridad IoT para mitigar amenazas y vulnerabilidades?*

En consecuencia, a la definición de riesgos, amenazas y vulnerabilidades asociadas a los dispositivos y entorno IoT,

existen varios mecanismos de protección que se deben considerar para mitigarla, se establecen los siguientes métodos que se describen en la Tabla 1.

Tabla 1. Métodos de seguridad de información

Método	Descripción
Cifrado	Cifra los datos en origen y los descifra en el destino, lo que proporciona un alto nivel de privacidad.
Autenticación de dispositivos y usuarios	Verifica la identidad de los dispositivos y los usuarios que acceden a los datos de IoT.
Control de acceso	Procedimientos para garantizar los derechos de acceso a los datos (privilegios).
Gestión de claves	Gestiona las claves de cifrado.
Monitorización de anomalías y detección de intrusiones	Análisis de datos para detectar patrones anómalos en el tráfico de IoT y alertar a los administradores de seguridad.

Nota. Adaptado de artículos [10] [11]

Se señala ciertas acciones de problemas específicos como son:

- ***Contraseñas débiles o en texto plano como:***
  - Empleo de contraseñas fuertes.
  - Control de acceso granular: acceso basado en roles (RBAC).
  - Protección de credenciales: método shadow password en Linux/Unix.
  - Recuperación segura de contraseñas [14].
- ***Servicios de red inseguras como:***
  - Bloqueo de la capa de puerta de enlace de servicio [14].
- ***Interfaz insegura como:***
  - Web no susceptible a XSS, SQL O CSRF.
  - Bloqueo de cuenta tras 3 a 5 intentos.
  - Bloqueo de comportamientos anormales [14].

- ***Ausencia de mecanismo fiable de actualización firmware como:***
  - Aseguramiento de acceso a actualizaciones
  - Verificación de fuente e integridad de actualizaciones [14].
- ***Librerías inseguras o desactualizadas como:***
  - Verificación de última versión de componentes.
  - Configuración adecuada de componentes [14].
- ***Deficiente protección de datos personal o privada como:***
  - Asegurar el anonimato en la recolección de datos.
  - No identificación de datos.
  - Control y autorización de acceso basado en roles [14].
- ***Almacenamiento y trasferencia de datos insegura como:***
  - Cifrado mediante TLS, cifrado handshake [14].
- ***Falta de gestión de dispositivos***
  - Separación de usuarios normales o administrativos, cifrado en reposo y en tránsito [14].
- ***Parámetros por defecto inseguros como:***
  - Configuración adecuada de permisos, cambio de contraseñas en cuentas predeterminadas activas [14].

Además, según una encuesta realizada por Eclipse Foundation en 2021 a expertos en IoT señala que el cifrado es el método de seguridad más utilizado en las soluciones IoT, siendo utilizado por el 52,8% de los encuestados. La autenticación de dispositivos y usuarios también es común, siendo utilizada por el 29,8% y el 26,8% de los encuestados, respectivamente. El control de acceso basado en roles se utiliza por el 22,8% de los encuestados y la gestión de claves, aunque es un método de seguridad importante, es utilizada por un porcentaje menor de encuestados. [15]

RQ4: *¿Qué protocolos de seguridad y modelos de arquitectura de comunicación pueden ser aplicados en entornos IoT?*

A través de la exploración en las bases de datos Scopus, Springer Link, IEEE Xplore, Pro Quest, Science Direct, se

presentan los protocolos de seguridad aplicados para la prevención de vulnerabilidades.

- ***Seguridad MQTT (Advanced Message Queuing)***

Modelo	•Publicación/Suscripción
Transporte	•TCP/IP
Seguridad	•SSL/TLS
Esquema de seguridad	•Cliente-Servidor

Figura 3. Protocolo Seguridad MQTT (Advanced Message Queuing)

Fuente: Elaboración propia a partir de Castro B [15]

Este protocolo es usado en centros de monitoreo de alarmas sistemas IoT con dispositivos como el ESP8266 o Raspberry Pi [16].

- ***Seguridad JWT (JSON Web Token)***

Modelo	•Petición/Respuesta
Transporte	•TCP/IP
Seguridad	•TLS
Esquema de seguridad	•Interfaz uniforme

Figura 4. Seguridad JWT (JSON Web Token)

Fuente: Elaboración propia a partir de Castro B [15]

JSON Web Token, se usa en aplicaciones REST, de recursos de origen cruzado y frameworks, impresoras universales (UP) [17].

- ***Seguridad AMQP (Advanced Message Queuing Protocol)***

Modelo	•Intercambio de mensajes
Transporte	•TCP/IP
Seguridad	•TLS
Esquema de seguridad	•Cliente-Servidor

Figura 5. Seguridad AMQP (Advanced Message Queuing Protocol.

AMQP puede ser aplicado en sistemas con domótica e IoT [15].

- ***Seguridad DDS (Data Distribution Service)***

Modelo	•Publicación/Suscripción
Transporte	•TCP/IP
Seguridad	•TLS/DTLS
Esquema de seguridad	•Cacheable

Figura 6. Seguridad DDS (Data Distribution Service).

Fuente: Elaboración propia a partir de Castro B [15]

- Como sensores, actuadores, Broker, CPU [18].
- DDS es adecuado para aplicaciones que necesitan la transferencia de datos en tiempo real, tales como vehículos autónomos, gestión de redes inteligentes, caso del control del tráfico aéreo, robótica, sistemas de transporte, generación de electricidad, entre otros [19].

- ***Seguridad HTTP (Hypertext Transfer Protocol)***

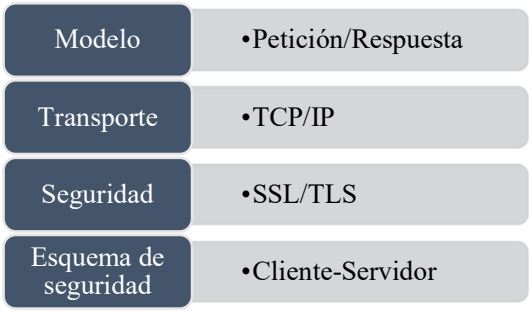


Figura 7. Seguridad HTTP (Hypertext Transfer Protocol)

Fuente: Elaboración propia a partir de Castro B [15]

Se emplea en dispositivos combinados de sensores accionadores, hardware y software, transporte de datos, facturación, Marketplace de datos, dispositivos y tecnologías como Azure IoT Hub [20].

A continuación, se sintetizan protocolos de seguridad con sus características.

Tabla 2. Resumen de protocolos y características

Protocolo	MQTT	JWT	AMQP	DDS	HTTP
Modelo	Publicación/Suscripción	Petición/Respuesta	Intercambio de mensajes	Publicación/Suscripción	Petición/Respuesta
Transporte	TCP/IP	TCP/IP	TCP/IP	TCP/IP	TCP/IP
Seguridad	SSL/TLS	TLS	TLS	TLS/DTLS	SSL/TLS
Esquema de seguridad	Cliente Servidor	Interfaz uniforme	Cliente Servidor	Cacheable	Cliente Servidor

Nota. Adaptado de Castro B [15].

En los protocolos la encuesta Eclipse Foundation IoT Developer Survey 2021 realizada a expertos en IoT muestra que el protocolo MQTT fue el protocolo de comunicación más utilizado, con un 44,1%, el protocolo HTTP fue utilizado con un 36,1%, AMQP fue utilizado por el 10,3%, DDS: fue utilizado por el 3,7% de los encuestados, JWT fue utilizado por el 1,7% y es importante saber que no suman el 100% porque existen otros protocolos nombrados en la encuesta [15]

RQ5: ¿Cuáles *son las medidas de seguridad recomendadas, así como las estrategias de control y protección, para las tecnologías de hardware y software?*

Las buenas prácticas en el ámbito de la seguridad de la información contribuyen a una mayor estabilidad de una empresa, por tanto, la implementación del control en el acceso lógico y físico permite delimitar las entradas y salidas y administrar según las exigencias de seguridad [21].

- ***Prácticas de seguridad física en:***
  - Dispositivos, aplicaciones, sistemas IoT: termostatos, cerraduras, detectores de humo, sistemas de videovigilancia.
  - Buenas prácticas: Control de accesos, Vigilancia 24/7, Climatización de dispositivos, Protección contra siniestros.

- ***Prácticas de seguridad lógica en:***
  - Dispositivos, aplicaciones, sistemas IoT: mensajería, Data center, smartphone.
  - Vulnerabilidad: ciberataques
  - Buenas prácticas: DLP Solución de prevención de pérdida de datos, Segmentación de redes y equipos críticos, IPS, Sistema de prevención de intrusos, Gestión del acceso, Firewalls físicos y virtuales, DRP plan de recuperación de desastres, Gestión de riesgos.
  - Algoritmos propios de cifrado, vpn para dispositivos.

RQ6: *¿Se puede ejemplificar en un escenario de pruebas la importancia de los métodos de seguridad en los dispositivos IoT?*

Gracias a los servicios y técnicas disponibles en la web, se han encontrado evidencias a manera de ejemplos de los temas estudiados, estos se describen a continuación.

Se ha tomado una representación a nivel del país Ecuador, donde se puede visualizar los puertos informáticos en Ecuador que son más comúnmente utilizados, pero también son más propensos a ser atacados o vulnerados en términos de seguridad.

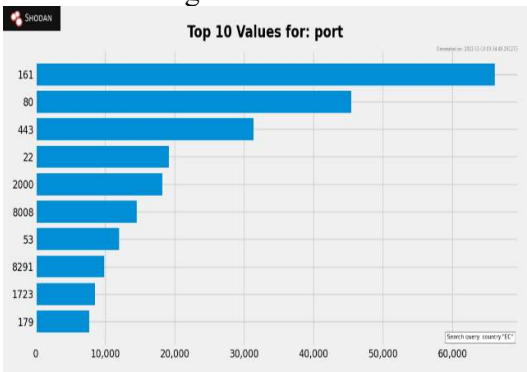


Figura 8. Puertos informáticos más utilizados y vulnerados en el Ecuador

Por lo cual, se determina que el país tiene un índice alto de vulnerabilidad de información sensible por puertos abiertos con lo más reportado y se comprobó con los datos de la Figura 10 de anexos de Ecucert que es el Centro de Respuesta a Incidentes Informáticos del Ecuador.

Visto anteriormente existen malas prácticas en las instalaciones de equipos como credenciales por defecto como se evidencia en la Tabla 6 generando que los dispositivos sean vulnerables para la extracción de información, para comprender los siguientes escenarios que se van a plantear es importante conocer que en internet ya existen diferentes maneras de recolectar información con el objetivo de encontrar direcciones, puertos y con ello dispositivos en donde se puede tener información sensible y sin protección subida en internet.

Las herramientas empleadas para el análisis de escenarios son:

- **Shodan**: es un motor de búsqueda de dispositivos vulnerables.
- **Google dorks:** técnica informática que aplica operadores para el filtrado de información en el buscador de Google.
- **VPN:** red privada virtual, solución que dirige el tráfico de Internet de forma que la dirección IP se oculta y los datos se cifran para una mayor seguridad.
- **Navegador brave:** navegador rápido y seguro cuya ventaja es el bloqueo de anuncios que surgen al realizar una búsqueda, y que atenta contra la privacidad, otras de sus ventajas es el bloqueo del almacenamiento de datos por terceros.

Dentro de estas herramientas se encontraron varios sitios vulnerables en los cuales se enfocan en dos escenarios principalmente:

En el primer escenario que se puede ver en la Figura 11 y Figura 12 de los anexos se encontró un servidor publicado en la web que pertenece a un plantel educativo sin seguridad, lo cual permitiría acceder a varios documentos, configuraciones y estructuras de bases de datos.

En la Figura 13, de los anexos se puede visualizar una cámara sin seguridad en la que se podría obtener información en tiempo real e información sensible de una organización.

Cabe recalcar que con esta información encontrada para una persona

que tenga malas intenciones podría sacar provecho y realizar estafas o extorciones y es muy preocupante ya que si se realiza un estudio más profundo los resultados serían de un nivel crítico, en el cual un atacante podría sacar mucho más provecho de la información sin seguridad a más organizaciones.

3.2. Discusión

Los artículos encontrados se han sujeto al cribado conforme a los criterios de inclusión y exclusión además de las cadenas de investigación establecidas. De la base de datos recopilada se han depurado varios de ellos porque se encontraron duplicados en varias bases de datos. Así mismo, de manera más específica se han descartado referencias por no mantener concordancia con el tema y/o no mantener información específica obteniendo así después de esta revisión un total de 290 archivos.

Posteriormente también se han encontrado documentos que resultan inaccesibles pues requieren de un pago para acceder a su revisión, por lo tanto, no han sido recuperados, derivando así en 92 artículos para elegibilidad.

Finalmente, después del análisis especifico mediante la ejecución de la estrategia de búsqueda establecida por la metodología PRISMA, se han seleccionado varios estudios que se consideran que tienen hallazgos esenciales por la calidad de información detallados en la Tabla 3, donde cada estudio aporta con información de la seguridad con inteligencias artificiales, sistemas de detección (IDS), estrategias de validación, etc., donde sí bien es cierto son muy válidas y altamente eficaces pero algunas poco utilizadas y explotadas, estos estudios abarcan las variables de estudio considerando su estrecha relación al tema y con alta calidad metodológica, todo este procedimiento se evidencia en la Figura 1

En este mapeo sistemático de literatura y revisión sistemática de literatura se han abordado aspectos de seguridad para los dispositivos IoT donde se observa:

- Cuando se trata de configurar métodos y protocolos de seguridad para IoT, es importante tener en cuenta ciertas prácticas recomendadas para garantizar la máxima seguridad posible. Por ejemplo, es importante asegurarse de que se estén utilizando las últimas versiones de los métodos y protocolos de seguridad, ya que estas a menudo contienen correcciones de seguridad críticas. Estas prácticas relacionadas en la Tabla 1 donde se detalla la vulnerabilidad por cada mala práctica, otorgando al practicante menor riesgo y mayor seguridad.

En cuanto a los métodos de seguridad, podemos mencionar que el más utilizado es el cifrado y en cuanto al protocolo MQTT a pesar de la disponibilidad de estos métodos y protocolos de seguridad, todavía existen vulnerabilidades y amenazas de seguridad en los dispositivos IoT.

Dentro de las tecnologías que usan los dispositivos IoT dependerá de funciones y requisitos específicos, entre las más utilizadas se encuentran:

- Sensores: recopilan datos sobre el entorno o a los objetos conectados.
- Redes Inalámbricas: hay que tomar en cuenta que se dividen en características para el alcance y consumo de energía entre ellas se incluyen Wi-Fi, Bluetooth, Zigbee y LoRaWAN.
- Sistemas operativos embebidos: versiones ligeras de sistemas operativos para recursos limitados.
- Plataformas en la nube: procesamiento y almacenamiento de datos con servicios como el análisis de datos y la visualización en tiempo real.[23]

Las medidas de seguridad adoptadas en los dispositivos IoT pueden disminuir las vulnerabilidades existentes, aunque no garantizan una seguridad completa. Es importante que los usuarios finales tomen medidas para proteger sus dispositivos y datos, y que haya colaboración entre fabricantes, investigadores y usuarios para prevenir el aumento de amenazas y vulnerabilidades. Es fundamental aplicar medidas de seguridad para asegurar la protección de la información y la privacidad de los usuarios en los dispositivos IoT. [16]

4. CONCLUSIONES

La cantidad de documentos encontrados durante el proceso de investigación muestra la relevancia y el interés en la seguridad de los dispositivos IoT. El hecho que se hayan podido descartar algunos documentos mediante la metodología utilizada demuestra la importancia de tener un enfoque sistemático y riguroso al realizar un estado del arte. Gracias a la creciente cantidad de dispositivos IoT en uso en todo el mundo, se encuentra información disponible sobre este tema que sugiere prestar cada vez más atención a la seguridad de los dispositivos IoT, lo que a su vez puede contribuir a la generación de nuevos conocimientos y avances.

La seguridad en el entorno IoT es esencial para proteger los datos de los usuarios, existen ciertas vulnerabilidades como el almacenamiento, transferencia insegura de datos y la falta de seguridad en dispositivos, hace necesario aplicar medidas de seguridad para disminuir estos riesgos. Es importante adoptar enfoques proactivos de seguridad, implementar mecanismos de autenticación y encriptación fuertes, monitorear constantemente y actualizar firmware para prevenir amenazas como DDoS, malware y robos de identidad.

Entre las medidas más destacadas para reducir estos riesgos y resguardar los datos de los usuarios, se incluyen el cifrado, autenticación de dispositivos y usuarios, gestión de claves, el control de acceso, monitorización de anomalías y detección de intrusiones. Además, es necesario abordar problemas específicos como contraseñas débiles, servicios de red inseguros, interfaces inseguras, falta de gestión de dispositivos, parámetros por defecto inseguros y falta de seguridad física de dispositivos.

En el transcurso de la investigación en diversas bases de datos, se han identificado varios protocolos de seguridad aplicables en el ambiente IoT, incluyendo MQTT, JWT, AMQP, DDS y HTTP. Cada uno de ellos tiene diferentes características, como el tipo de modelo de comunicación, transporte y esquema de seguridad. La encuesta Eclipse Foundation IoT Developer Survey 2021 muestra que MQTT es el protocolo más utilizado en el entorno IoT, seguido de HTTP y AMQP. Es importante seguir investigando y evaluando nuevos protocolos de seguridad para elevar la protección de los datos en el ambiente IoT y seguir fortaleciendo la ciberseguridad en este campo en constante evolución. Para garantizar la seguridad de los dispositivos IoT y prevenir un aumento en las vulnerabilidades y amenazas, es esencial contar con una colaboración entre fabricantes, investigadores y usuarios. La aplicación de estas medidas de seguridad y la vigilancia a los problemas específicos ayudarán a garantizar la seguridad en el ambiente IoT y a prevenir el aumento de vulnerabilidades y amenazas en el futuro.

Para asegurar la estabilidad y protección de una empresa, es esencial llevar a cabo buenas prácticas de seguridad de la información. Existen dos aspectos importantes en cuanto a la seguridad: la física y la lógica, deben ser consideradas para mantener la seguridad de los dispositivos, aplicaciones y sistemas IoT.

La seguridad física incluye el control de accesos, vigilancia 24/7, climatización de dispositivos y protección contra siniestros. Por otro lado, la seguridad lógica incluye la gestión de riesgos, IPS, segmentación de redes y equipos críticos, sistema de prevención de intrusos, gestión del acceso, DRP plan de recuperación de desastres y DLP solución de prevención de pérdida de datos, firewalls físicos y virtuales. Además, se recomiendan algoritmos propios de cifrado y vpn para dispositivos.

Se ha podido exponer gracias a herramientas disponibles en internet que existen sitios y dispositivos vulnerables demostrando la importancia de los métodos, protocolos y mecanismos para tener información segura para evitar robos, estafas y extorsiones. Aunque se han logrado avances en este ámbito, todavía existen importantes desafíos por abordar, como la diversidad de los dispositivos y la falta de una regulación estandarizada. En consecuencia, es necesaria una continua investigación y mejora en la seguridad de IoT para asegurar una protección eficaz de la información y fomentar la confianza en estos sistemas.

5. Referencias

[1] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal y S. W. Kim, «Multimedia Internet of Things: A comprehensive survey,» *IEEE Access,* vol. 8, pp. 8202-8250, 2020.

[2] C. Maple, «Security and privacy in the internet of things,» *Journal of cyber policy,* vol. 2, nº 2, pp. 155-184, 2017.

[3] A. J. Onumanyi, A. M. Abu-Mahfouz y G. P. Hancke, «Cognitive radio in low power wide area network for IoT applications: Recent approaches, benefits and challenges,» *IEEE Transactions on Industrial Informatics,* vol. 16, nº 12, pp. 7489-7498, 2019.

[4] A. C. Morales-Suárez, S. S. Díaz-Ávila and M. Á. Leguizamón-Páez, "Mecanismos de seguridad en el internet de las cosas," *Revista Vínculos:Ciencia,Tecnología y Sociedad,* vol. 16, no. 2, pp. 288-297, 2019.

[5] M. Jiménez, «Vulnerabilidades que afectan la seguridad de la información,» piranirisk.com, 2022. [En línea]. Available: https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion.

[6] J. Dazine, A. Maizate y L. Hassouni, «Internet of things security,» *2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD),* 2018.

[7] J. Figueroa-Suárez, R. Rodríguez-Andrade, C. Bone-Obando y J. Saltos-Gómez, «La seguridad informática y la seguridad de la información,» *Polo del Conocimiento,* vol. 2, nº 12, pp. 144-155, 2017.

[8] B. S. Krishna y T. Gnanasekaran, «A systematic study of security issues in Internet-of-Things (IoT),» de *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, IEEE, 2017, pp. 107-111.

[9] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala y S. Elkhediri, «CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Technique,» *2nd International Conference on Computer Applications & Information Security ,* 2019.

[10] P. Várlaki y P. Baranyi, «Cognitive and spiritual revolution of the tenth century — Constantine porphyrogenitus and his hidden world: Part I. The Great Monarch's hidden world in the great medieval mystical writings,» *IEEE,* 2017.

[11] M. O. Farooq y A. & Kamal, «Security in internet of things: Opportunities and challenges. In 2018 14th International Conference on Emerging Technologies,» *IEEE,* 2018.

[12] Bidaidea , «¿Qué es la seguridad informática?. Buenas Prácticas,» ciberseguridadbidaidea.com, 2022. [En línea]. Available: https://ciberseguridadbidaidea.com/que-es-seguridad-informatica/.

[13] M. . J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou y J. Glanville, «Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas,» *Revista Española de Cardiología,* vol. 74, nº 9, pp. 790-799, 2021.

[14] A. López Naranjo, «Análisis de amenazas IOT en un sistema domótico,» Repositorio Pontificia Universidad Católica del Ecuador, Ambato, 2022.

[15] Eclipse Foundation., «IoT Developer Survey 2021,» 2021.

[16] B. Castro, «Modelos de seguridad, acciones y ptrotocolos para la prevencion de vulnerabilidades de la seguridad de la informacion mediante las tecnologías IoT y ARPI RESTFUL,» Universidad Politécnica Salesiana, Guayaquil, 2022.

[17] L. Llamas, «¿QUÉ ES MQTT? SU IMPORTANCIA COMO PROTOCOLO IOT,» Ingeniería, Informática y diseño, 2019. [En línea]. Available: https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/.

[18] B. Santos, A. Buck y M. Jim, «Recuperación de tokens de acceso de impresora de impresión universal (UP),» Microsoft, 2022. [En línea]. Available: https://learn.microsoft.com/es-es/universal-print/hardware/universal-print-oem-printer-device-token.

[19] K. Pérez Leones, «Estudio y análisis del protocolo de mensajería avanzado en el internet de las cosas para aplicación en el campo de la domótica,» Repositorio Universidad Católica de Santiago de Guayaquil, Guayaquil, 2019.

[20] I. Porro Sáez, «IoT: protocolos de comunicación, ataques y recomendaciones,» incibe-cert.es, 2019. [En línea]. Available: https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones.

[21] Azure, «Protocolos y tecnologías de IoT,» Microsoft, 2022. [En línea]. Available: https://azure.microsoft.com/es-es/solutions/iot/iot-technology-protocols/.

[22] F. Silva, L. Segadas and E. Kowask, "Gestión de la seguridad de la información," Red Cedia, Bogotá, 2022.

[23] A. Bassi, «Introducción a Protocolos IoT,» 2021. [En línea]. Available: https://www.gotoiot.com/pages/articles/iot_protocols_intro/index.html.

[24] B. Posey, «Privacidad de datos, seguridad de datos y protección de datos,» 2022. [En línea]. Available: https://www.computerweekly.com/es/definicion/Privacidad-de-datos-

seguridad-de-datos-y-proteccion-de-datos.

[25] F. Sánchez, «Mejores prácticas de seguridad física y lógica,» SmartTech, 2020. [En línea]. Available: https://blog.smartekh.com/10-mejores-pr%C3%A1cticas-de-seguridad-f%C3%ADsica-y-l%C3%B3gica-para-proteger-a-tu-data-center.

[26] R. Nagaraju, J. Toriano Pentang, S. Abdufattokhov, R. CosioBorda, N. Mageswari and G. Uganya, "Attack prevention in IoT through hybrid optimization mechanism and deep learning framework," *Measurement: Sensors,* no. 24, pp. 1-10, 2022.

[27] A. Khraisat y A. Alazab, «A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges,» *Cybersecur,* vol. 18, nº Cybersecur, p. 4, 2021.

[28] B. A. Tama, S. Y. Lee y S. Lee, «A Systematic Mapping Study and Empirical Comparison of Data-Driven Intrusion Detection Techniques in Industrial Control Networks,» *Arch Computat Methods Eng,* vol. 1, nº 1, pp. 1-28, 2022.

[29] N. Oliveira, I. Praça, E. Maia y O. Sousa, «Intelligent Cyber Attack Detection and Classification for Network-Based Intrusion Detection Systems,» *Applied Sciences; Basel,* vol. 11, nº 4, pp. 1-21, 2021.

[30] KAMALDEEP, M. DUTTA y J. GRANJAL, «Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms,» *IEEE Access,* vol. 8, pp. 127272-127312, 2020.

[31] S. Hajiheidari, K. Wakil, M. Badri and N. J. Navimipour, "Intrusion detection systems in the Internet of things: A comprehensive investigation," *Computer Networks,* vol. 160, pp. 165-191, 2019.

[32] W. Yao, S. Guozi, C. Xiaochun and Y. Jialea, "An Intrusion Detection System for the Internet of Things Based on the Ensemble of Unsupervised Techniques," *Wireless Communications and Mobile Computing,* vol. 1, no. 1, pp. 1-11, 2022.

[33] I. Salas y Á. García, «Seguridad en la Internet de las cosas,» Universitat Oberta de Catalunya (UOC), 2019.

[34] Eclipse Foundation, «Eclipse Foundation IoT Developer Survey 2021,» 2021.