FACULTAD DE INGENIERÍA Y COMPUTACIÓN

DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Escuela Profesional de Ciencia de la Computación

Riesgos del Internet de las Cosas y su Relación con los Usuarios

Tesis Presentado por el Bachiller:

Jose Alonso Vides Aguirre Flores

Para Optar el Título Profesional:

Ingeniero Informático

Asesor: Dr. Yván Jesús Túpac Valdivia

UCSP- Universidad Católica San Pablo
Arequipa, agosto de 2022

Dedicado de forma muy especial a mi mejor guía, Dios, a mi esposa e hijos, a mis padres, profesores y amigos.

Abreviaturas

AF *Architectural framework*

API Interfaz de programación de aplicaciones - *Application Programming Interfaces*

ASF *Adaptive software framework*

AWS *Amazon Web Services*

AMQP *Advanced Message Queuing Protocol*

BLE *Bluetooth Low Energy*

CEI Comisión Electrotécnica Internacional

CIA *Confidentiality, integrity and availability*

CMM Modelo de Madurez de Capacidades - *Capability Maturity Model*

CMMI Modelo de Madurez de Capacidades Integrado - *Capability Maturity Model Integrated*

CSRF Falsificación de solicitud entre sitios - *Cross Site Request Forgery*

CVSS Sistema Común de Puntuación de Vulnerabilidad - *Common Vulnerability Scoring System*

CoAP *Constrained Application Protocol*

DDS Servicio de distribución de datos - *Data Distribution Service*

DoS Ataque de servicio - *Denial of Service*

DDoS Ataque de denegación de servicio distribuido - *Distributed Denial of Service*

FAIR *Findable, Accessible, Interoperable, and Reusable* (Encontrables, Accesibles, Interoperables y Reutilizables)

GPS Sistema de Posicionamiento Global - *Global Positioning System*

HTTP Protocolo de Transferencia de Hipertexto - *Hypertext Transfer Protocol*

IoT Internet de las Cosas - *Internet of things*

IEEE *Institute of Electrical and Electronics Engineers*

IoV Internet de los Vehículos - *Internet of Vehicles*

ISO Organización Internacional de Normalización - *International Organization for Standardization*

NIST Instituto Nacional de Estándares y Tecnología - *National Institute of Standards and Technology*

OWASP Proyecto abierto de seguridad de aplicaciones web - *Open Web Application Security Project*

PKI Infraestructura de clave pública - *Public key infrastructure*

RS Revisión Sistemática

RFID Identificación por radiofrecuencia - *Radio Frequency Identification*

SCA Ataques de canal lateral - *Side-Channel Attack*

SQL Lenguaje de consulta estructurada - *Structured Query Language*

SGSI Sistema de Gestión de Seguridad de la Información

TARA Evaluación de amenazas y análisis de soluciones - *Threat Assessment and Remediation Analysis*

TLS Seguridad de la capa de transporte - *Transport Layer Security*

OTA *Over-The-Air*

UIT Unión Internacional de Telecomunicaciones

URI Identificador de recursos uniforme - *Universal Resource Identifier*

WSN *Wireless Sensor Network*

Agradecimientos

Agradezco a mi esposa, quien me brindó su amor, su cariño, su estímulo y su apoyo constante.

A mis hijos quienes me prestaron el tiempo que les pertenecía para terminar y me motivaron siempre con su alegría.

A mi padre Don Vides Aguirre Tapia (QEPD) quien me enseño a luchar para alcanzar mis metas, por su apoyo brindado y haber entregado todo para forjarme como un profesional.

Agradezco a la universidad, mi *alma matter*, por haberme cobijado y brindado la formación que ahora me permitirá ayudar a construir una mejor sociedad.

Agradezco de forma muy especial a mi asesor Dr. Yván Jesus Túpac Valdivia por haberme guiado en esta tesis.

Resumen

El presente estudio tiene por objetivo determinar los riesgos del Internet de las cosas y su relación con los usuarios, con el fin de disminuir los riesgos asociados al uso del Internet de las Cosas (IoT), ya que su funcionamiento no depende de la intervención humana sino de sensores inteligentes que recogen información, la comunican, analizan y actúan ofreciendo nuevas formas de interacción con los usuarios. Sin embargo, esto crea nuevas oportunidades para que esa información se vea comprometida exponiendo información sensible y confidencial de los usuarios y como resultado, podría estar expuesto a riesgos cibernéticos. En este sentido, el IoT radica en la capacidad de agregar datos, que actualmente se generan en diferentes formatos; donde aplicativos y/o sensores se conectan a las redes utilizando diferentes protocolos de comunicación, y sin estándares comunes que rijan el funcionamiento de los dispositivos habilitados para IoT. Según lo expuesto, se considera viable esta investigación ya que busca conocer del IoT, sus generalidades, comunicación, amenazas y vulnerabilidades para determinar los riesgos relacionados a IoT y proporcionar metodologías que optimicen la protección de los datos y la intimidad de los usuarios, así como contrarrestar el espionaje de los datos del IoT, a través de una revisión sistemática, basado en la metodología de Barbara Kitchenham.

Palabras claves: IoT, Seguridad, Dispositivos, Riesgos, Internet, Ataques, Privacidad, Tecnología, Amenaza, Vulnerabilidad, Ciberseguridad.

Abstract

The objective of this study is to determine the risks of the Internet of things and its relationship with users, in order to reduce the risks associated with the use of the IoT, since its operation does not depend on human intervention but on intelligent sensors that collect information, communicate it, analyze it and act offering new forms of interaction with users. However, this creates new opportunities for that information to be compromised exposing users' sensitive and confidential information and as a result, you could be exposed to cyber risks. In this sense, the IoT lies in the ability to aggregate data, which is currently generated in different formats; where applications and/or sensors connect to networks using different communication protocols, and without common standards that govern the operation of devices enabled for the Internet of things. According to the above, this research is considered viable since it seeks to know about the IoT, its generalities, communication, threats and vulnerabilities to determine the risks related to IoT and provide methodologies that optimize data protection and user privacy, as well as counteract espionage of IoT data, through a systematic review, based on the methodology of Barbara Kitchenham.

Keywords: IoT, Security, Devices, Risks, Internet, Attacks, Privacy, Technology, Threat, Vulnerability, Cybersecurity.

Índice general

1. Introducción **2**

1.1. Motivación y Contexto 2

1.2. Planteamiento del Problema 4

1.2.1. Problema general 4

1.3. Objetivos 4

1.3.1. Objetivo General 4

1.3.2. Objetivos Específicos 4

1.4. Metodología 5

1.4.1. Planificación de la Revisión 6

1.5. Delimitaciones 7

1.5.1. Temporal 7

1.5.2. Temática 7

1.6. Organización de la Tesis 7

2. Marco Teórico **8**

2.1. Consideraciones Iniciales 8

2.2. Internet de las cosas (IoT) 8

2.2.1. Ventajas y desventajas de IoT 9

2.2.2. Funcionamiento de IoT 9

2.2.3. Estándares y marcos del IoT 10

2.2.4. Riesgo cibernético 18

2.2.5. Problemas de seguridad y privacidad del IoT 20
2.2.6. Aplicaciones de IoT para consumidores y empresas 24
2.3. Consideraciones Finales 25

3. Revisión Sistemática **26**
3.1. Consideraciones Iniciales 26
3.2. Planificación de la investigación 26
3.2.1. Identificación de la necesidad de revisión 26
3.2.2. Especificación de las Preguntas de investigación 26
3.3. Ejecución de la Revisión 27
3.3.1. Selección de estudios primarios 27
3.3.2. Palabras claves y cadenas de búsqueda 28
3.3.3. Criterios de inclusión y exclusión 28
3.3.4. Selección de las fuentes de búsqueda 29
3.3.5. Selección de estudios primarios 29
3.3.6. Evaluación de la Calidad del Estudio 30
3.3.7. Extracción y síntesis de Datos 30
3.4. Consideraciones Finales 32

4. Análisis **33**
4.1. Consideraciones Iniciales 33
4.2. Desarrollo de la comparativa 33
4.2.1. Amenazas a la seguridad en las aplicaciones del IoT 36
4.2.2. Marcos, metodologías, sistemas y modelos de ciberriesgo 43
4.2.3. Tipos de riesgos del IoT 48
4.2.4. Normas IoT 53
4.3. Discusión 55
4.4. Consideraciones Finales 61

5. Conclusiones y Trabajos Futuros **62**

5.1. Problemas Encontrados 63

5.2. Recomendaciones 63

5.3. Trabajos Futuros 64

Bibliografía **68**

Índice de tablas

1.1. Preguntas de Investigación 6

3.1. Preguntas de Investigación 27
3.2. Palabras Claves o Cadenas de búsqueda 28
3.3. Criterios de Inclusión 28
3.4. Criterios de Exclusión 29
3.5. Fuentes de búsqueda 29
3.6. Resultados del proceso de selección de estudios primarios. 30
3.7. Lista de verificación de evaluación de calidad 30
3.8. Formato extracción de documentos de estudios existentes. 32

4.1. Comparación detallada de los estudios primarios en el ámbito de la seguridad de IoT 36
4.2. Clasificación de los artículos según ataques o vulnerabilidades estudiadas . 40
4.3. Mejoras en la seguridad a través de diferentes técnicas en los sistemas de IoT. 41
4.4. Artículos según el marco de riesgos de la ciberseguridad (CSRF) 41
4.5. Comparación de los marcos de riesgos de la ciberseguridad (CSRF). 42
4.6. COBIT 5 y la alineación de IoT. 46
4.7. OWASP Top 10 2017. 51
4.8. OWASP Top 10 2018. 51
4.9. Resumen de las normas internacionales relativas a la IoT. 55

Índice de figuras

1.1. Estadísticas de dispositivos conectados entre 2018, 2025 y 2030. 3

1.2. Etapas de la revisión sistemática. 5

2.1. Ventajas y desventajas de IoT. 9

3.1. Proceso de selección de estudios primarios. 27

4.1. Riesgos de IoT. 44

4.2. Los 10 riesgos más críticos de OWASP Top 10. 50

Capítulo 1

Introducción

El presente trabajo se inicia con el desarrollo de la motivación y el contexto, que establece el fundamento por el cual se realiza la investigación. Seguidamente, se presenta el planteamiento del problema y su formulación, la cual proporciona información sobre los inconvenientes que se pretende abordar en el desarrollo de este estudio. Posteriormente, se establecen los objetivos de la investigación, así como la definición de la metodología, delimitaciones y por último se presenta la organización del presente documento.

1.1. Motivación y Contexto

La siguiente investigación se justifica ya que busca determinar los riesgos asociados a Internet de las Cosas - *Internet of things* (IoT) y proporcionar herramientas y metodologías que optimicen la protección de los datos y la intimidad de los usuarios, así como contrarrestar el espionaje de los datos asociados al IoT, basado en un estudio bibliográfico y una revisión sistemática que fundamente los hallazgos encontrados, con el fin de comprender las variables en estudio y buscar formas idóneas para lograr protegerse de posibles intrusiones en los sistemas asociados con estas tecnologías, que cada día se encuentran más ligadas a la vida cotidiana a nivel mundial.

El mundo ha ido evolucionando significativamente al pasar de los años, gracias al desarrollo de la tecnología y actualmente con el empleo de teléfonos inteligentes con funcionalidades como la ubicación satelital o la consulta del tráfico vehicular, o monitorear las rutas de las aeronaves en tiempo real, representan actividades que hoy en día se consideran tareas cotidianas que han ido abarcando practicas necesarias en la vida cotidiana [Derawi and Zhang, 2016].

En tal sentido, se pueden destacar entre las tecnologías más resaltantes el IoT, el cual contempla esencialmente la investigación para el desarrollo de la interconexión, a través del internet de diferentes objetos, empleando tecnología inalámbrica como WIFI, bluetooth, radiofrecuencias o por medio de sensores o actuadores presentes en varios dispositivos inteligentes [Bunawan et al., 2019].

Asimismo, esta tecnología ha permitido satisfacer las necesidades de los usuarios en

diferentes áreas. Por lo tanto, es común observar cómo personas encienden la calefacción de sus hogares por medio de teléfonos inteligentes, encender o apagar la iluminación de sus viviendas, también logran vigilar la frecuencia cardiaca por medio de pulseras inteligentes, monitorear sus refrigeradores, los cuales le indican a sus usuarios cuando falta un producto para poder realizar la compra en tiendas on line [Derawi and Zhang, 2016].

En efecto, según cifras de Statista, el cual es un portal de estadísticas en línea alemán comenta que el crecimiento de esta tecnología se espera que, a nivel mundial para el 2025, se encuentren conectados alrededor de 38.600 millones de dispositivos y para el 2030 la cifra ascendería a 50.000 millones de dispositivos conectados, lo que producirá miles de millones de terabytes de información fluyendo a través del internet e interactuando con dispositivos IoT [Statista, 2021].

La figura 1.1 representa la previsión de dispositivos conectados a internet a nivel mundial en 2018, 2025 y 2030 (en miles de millones de unidades). Tomado de [Statista, 2021].

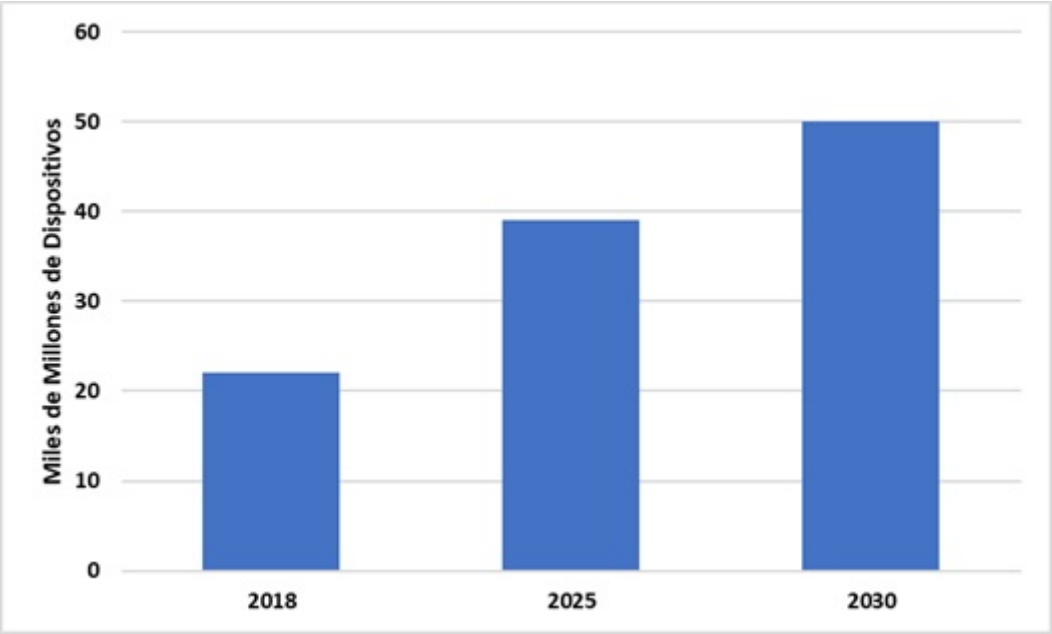

Figura 1.1: Estadísticas de dispositivos conectados entre 2018, 2025 y 2030.

Fuente: [Statista, 2021]

Según lo antes expuesto, el presente estudio tiene por objetivo determinar los riesgos del IoT y su relación con los usuarios, con el fin de conocer de IoT sus generalidades, comunicación, amenazas y metodologías que contrarresten los peligros existentes, ya que su funcionamiento no depende de la intervención humana, sino de sensores inteligentes que recogen información, la comunican, analizan y actúan ofreciendo nuevas formas de interacción con los usuarios. Sin embargo, esto crea nuevas oportunidades para que esa información se vea comprometida, exponiendo información sensible y confidencial de los usuarios y como resultado podría estar expuesto a riesgos cibernéticos. En este sentido, el IoT radica en la capacidad de agregar datos, que actualmente se generan en diferentes formatos y los sensores se conectan a distintas redes utilizando diversos protocolos de comunicación y sin estándares comunes que rijan el funcionamiento de los dispositivos

habilitados para IoT, creando barreras para la interoperabilidad [Cardenas and Hahn, 2019].

1.2. Planteamiento del Problema

1.2.1. Problema general

El problema se puede resumir en la siguiente pregunta:

¿Cuáles son los riesgos del Internet de las Cosas y su relación con los usuarios?

Problemas Específicos

- ¿Cuáles son las incidencias de los riesgos del Internet de las Cosas en la protección de los datos?
- ¿Cuáles son las incidencias de los riesgos del Internet de las Cosas en la protección a la intimidad?
- ¿Cuáles son las incidencias de los riesgos del Internet de las Cosas en la protección del espionaje informático?
- ¿Cómo el establecimiento de medidas de seguridad pueden minimizar los riesgos del Internet de las Cosas?

1.3. Objetivos

1.3.1. Objetivo General

Determinar los riesgos del Internet de las Cosas y su relación con los usuarios.

1.3.2. Objetivos Específicos

- Determinar la incidencia de los riesgos del Internet de las Cosas en la protección de los datos.
- Determinar la incidencia de los riesgos del Internet de las Cosas en la protección a la intimidad.
- Determinar la incidencia de los riesgos del Internet de las Cosas en la protección del espionaje informático.
- Proponer metodologías que ayuden a minimizar los riesgos del Internet de las Cosas a través del uso de tecnologías.

1.4. Metodología

El desarrollo de esta investigación se fundamenta en una revisión documental empírica y teórica, tomando como estudio casos relevantes, relacionados con riesgos cibernéticos asociados al IoT, la información recopilada a través de bases de datos reconocidas como Scopus, Science Direct, *Institute of Electrical and Electronics Engineers* (IEEE), Proquest, entre otros, seguidamente se realiza análisis y discusión de la evidencia recopilada a través de la metodología de Revisión Sistemática (RS) de Barbara Kitchenham.

Para el trabajo de investigación se emplea la metodología de RS de Barbara Kitchenham, la cual esta enfocado en los criterios de inclusión, exclusión, que permitan determinar cuáles son los documentos que cumplen con los requerimientos establecidos para la investigación, así como los que no serán aceptados, adicionalmente se establecerán las estrategias de búsqueda con el fin de realizar las consultas en los portales de información especializados, posteriormente se determinaran los parámetros de evaluación de calidad y por último se efectuara el procedimiento de la extracción y síntesis de datos, que permitan responder las preguntas de investigación que se determinaron con anterioridad para la realización de la investigación.

Para la realización de esta RS se incluyen diferentes actividades independientes, para lo cual el método propone tres fases fundamentales, según la figura 1.2 que se muestra a continuación:

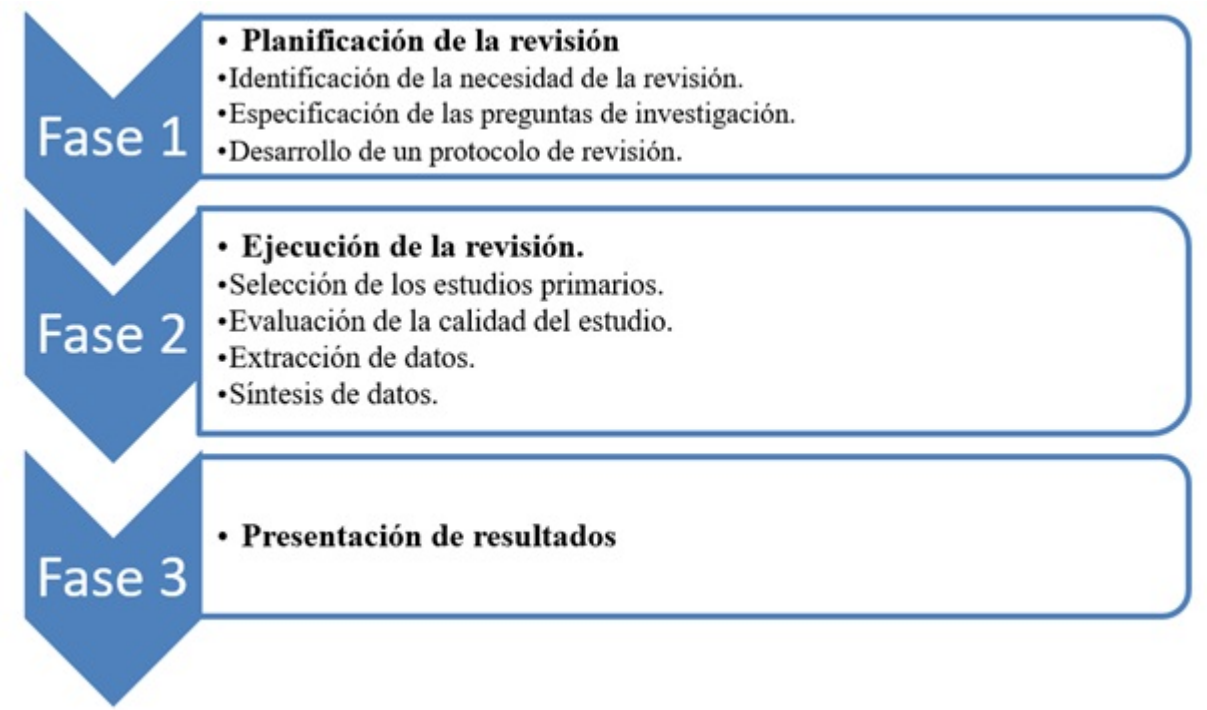

Figura 1.2: Etapas de la revisión sistemática.

Nota: Elaboración propia basado en el modelo de Kitchenham referenciada por [Xiao and Watson, 2017].

1.4.1. Planificación de la Revisión

Siguiendo la metodología de Kitchenham referenciada por [Xiao and Watson, 2017], se presentan una serie de puntos que se irán cumpliendo paso a paso para la consecución del trabajo que se expone a continuación.

Identificación de la necesidad de revisión

En esta etapa se buscaron trabajos cuyo objetivo se asimile al planteado en esta investigación o que responda a las preguntas de investigación planteadas para determinar si existen revisiones de literatura relacionadas con el tema en estudio. Además se revisa si existe variedad de estudios que apliquen para determinar si es pertinente este estudio.

Especificación de las Preguntas de investigación

A continuación, se presenta la tabla 1.1 con las preguntas de investigación que se establecieron como guía para la realización de la RS de la metodología de [Kitchenham, 2007].

ID	Pregunta de Investigación
I1	¿Qué tipos de incidencia de riesgos del IoT en la protección de los datos se han presentado?
I2	¿Qué tipos de incidencia de riesgos del IoT en la protección a la intimidad se han presentado?
I3	¿Qué tipos de incidencia de riesgos del IoT en la protección del espionaje informático se han presentado?

Tabla 1.1: Preguntas de Investigación

Fuente: Elaboración propia

Desarrollo del protocolo de investigación

Se procede a desarrollar el protocolo de revisión para reducir la posibilidad de sesgos, en el protocolo se incluye las preguntas de investigación, fuentes y cadenas de búsqueda, criterios de inclusión y exclusión, dicho protocolo se desarrolla a partir del capítulo 3.

1.5. Delimitaciones

1.5.1. Temporal

Las fuentes de información contempladas para esta investigación están enmarcadas en el periodo comprendido de 2015-2021. Al ser el tema objeto de estudio los riesgos cibernéticos del IoT, se puede establecer como un tema de reciente data. Por lo tanto, se consideró ese periodo de tiempo para la búsqueda de las fuentes bibliográficas.

1.5.2. Temática

Este trabajo de investigación pertenece al campo de la seguridad informática, específicamente sobre la seguridad asociada al IoT, es por ello que se busca determinar la incidencia de los riesgos cibernéticos del IoT y que están expresados en los objetivos específicos y para esto se recopilara información de fuentes secundarias, como artículos, tesis de pre-grado, post-grado y textos relacionados con el tema.

1.6. Organización de la Tesis

El presente trabajo está organizado de la siguiente manera:

- En el **Capítulo 1**, se desarrolla la introducción de la Tesis, definiendo el problema y los objetivos, así como el contexto y motivación por el cual se desarrolla este proyecto, por ultimo los trabajos relacionados que sirven como sustento a la presente Tesis.
- En el **Capítulo 2** se presenta una introducción al estado del arte del IoT, donde se presentan conceptos, las ventajas y desventajas, así como sus estándares y marcos de trabajo, aplicaciones, riesgos y aspectos de seguridad.
- En el **Capítulo 3** se presenta el desarrollo del protocolo de investigación, iniciando con los pasos de la metodología seleccionada para la búsqueda, definición de los portales de búsqueda, definición de la cadena de búsqueda, proceso de inclusión y exclusión de artículos, presentación de artículos seleccionados, análisis de los hallazgos y discusión de los autores.
- En el **Capítulo 4** se presenta el análisis y discusión obtenidos de la revisión, para finalmente dar paso a las conclusiones y recomendaciones de la investigación realizada.
- En el **Capitulo 5**, se muestran las conclusiones a las que se llego, en donde se especifican los problemas encontrados, con algunas recomendaciones a seguir y los posibles trabajos futuros.

Capítulo 2

Marco Teórico

2.1. Consideraciones Iniciales

En la sección 2.2, se explicara los estudios que tienen por objeto el Internet de las cosas (IoT), como sus ventajas y desventajas, su funcionamiento, estandares y marcos, el riesgo cibernético, problemas seguridad y privacidad del IoT y las aplicaciones del IoT para consumidores y empresas. En la sección 2.3, son presentadas las consideraciones finales sobre la revisión de la literatura.

2.2. Internet de las cosas (IoT)

El IoT es una forma de conectar el mundo físico con el mundo digital que incluye todos los dispositivos físicos conectados a Internet, recopilando y compartiendo gran cantidad de datos, es decir, el IoT hace referencia a conectar algún artefacto a una gigantesca red de personas y cosas conectadas, que recolectan e intercambiar datos sobre su uso y el ambiente que las rodea. Por ejemplo, desde microondas inteligentes, que cocinan sistemáticamente los alimentos por el tiempo apropiado, hasta coches auto conducidos [Derawi and Zhang, 2016].

Asimismo, todos los dispositivos IoT están conectados a Internet y disponen de una dirección IP y recopilan datos constantemente. No obstante, para que estos datos sean útiles, primero deben enviarse a la plataforma IoT, que recopila datos de todos los dispositivos conectados y cuando los datos están en la plataforma IoT se procede al análisis con el fin de que el usuario puede extraer los datos que necesita. Estos dispositivos poseen sofisticados sensores que detectan los objetos que se encuentran en su camino, pasando por mecanismos como aparatos fitness para llevar en la muñeca, que miden el ritmo cardíaco y el número de pasos que se han dado en un día, de igual manera estos utilizan esa información para sugerir planes de entrenamiento indicados a cada individuo. Adicionalmente, existen balones de fútbol vinculados que registran la velocidad, distancia a la que se lanzan y registran esas estadísticas por medio de un aplicativo para siguientes entrenamientos [Pathak and Bhandari, 2018].

2.2.1. Ventajas y desventajas de IoT

A continuación, según [Pathak and Bhandari, 2018] en la figura 2.1, se presentan algunas ventajas y desventajas de IoT.

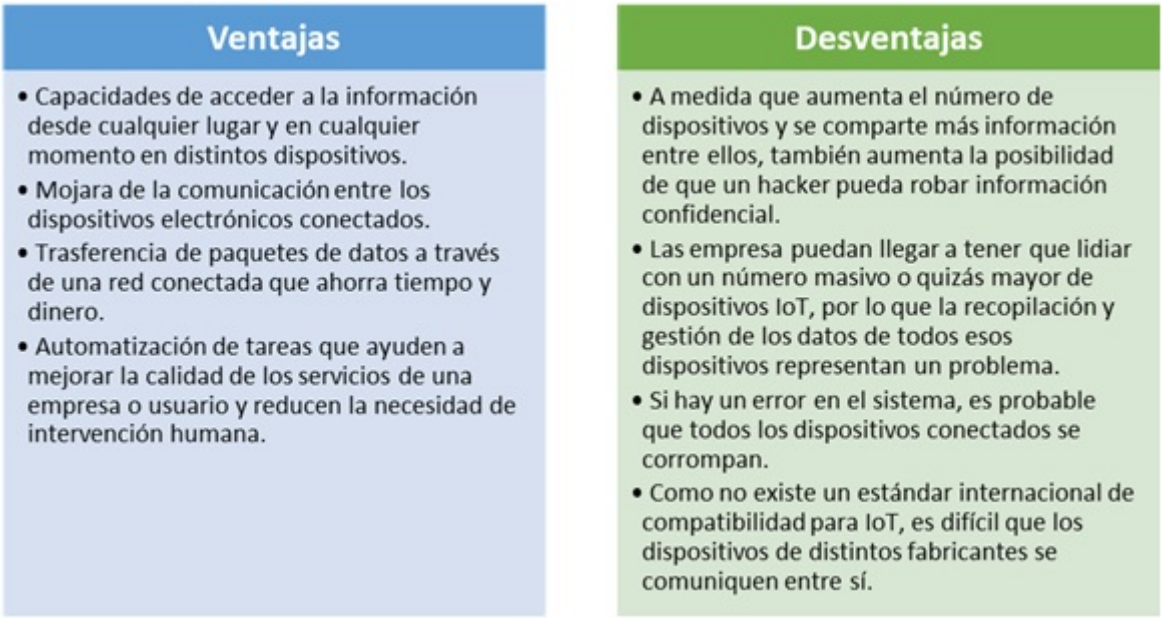

Figura 2.1: Ventajas y desventajas de IoT.

Fuente: Adaptado de [Pathak and Bhandari, 2018]

2.2.2. Funcionamiento de IoT

Los dispositivos y objetos con sensores incorporados se conectan a una plataforma de IoT, que integra los datos de los distintos dispositivos y aplica la analítica para compartir datos importantes con aplicativos diseñadas para atender determinadas necesidades. Asimismo, estas potentes plataformas de IoT pueden determinar exactamente qué información es de utilidad y qué puede ignorarse de forma automática [Pathak and Bhandari, 2018].

Estos datos puede utilizarse para descubrir patrones, realizar asesoramientos y revelar potenciales problemas antes se manifiesten. Por ejemplo, si un negocio de fabricación de automóviles a través de IoT requiere determinar qué componentes opcionales son requeridos, le presentara opciones a elegir como asientos de cuero o llantas de aleación que sean los más idóneos, con el fin de ser asignados para el próximo pedido directo con el fabricante de manera automatizada [Cardenas and Hahn, 2019].

Por otra parte, utilizando la tecnología IoT se puede emplear sensores para revelar qué zonas de una sala de exposición son las más utilizadas y dónde permanecen los clientes por periodos más largos de tiempo o profundizar en información de ventas accesibles, para establecer qué dispositivos se venden con mayor rapidez, por lo que, los datos recopilados por los equipos conectados permiten realizar elecciones ingeniosas sobre los elementos de

los que se encuentran conectados, basados en datos recolectados en el tiempo en que se produce el evento, lo que contribuye con el rendimiento económico y tiempo. Por lo tanto, la información que proporcionan los análisis avanzados permite aumentar la eficacia de los procesos. Igualmente, el propósito de los esquemas inteligentes permiten automatizar ciertas tareas, sobre todo cuando son repetitivas y que consumen mucho tiempo o incluso son peligrosas [Cardenas and Hahn, 2019].

2.2.3. Estándares y marcos del IoT

Los autores Derawi y Zhang [Derawi and Zhang, 2016], indican que existen varios estándares de IoT emergentes, entre ellos se mencionan los siguientes:

IPv6

IPv6 o Protocolo de Internet versión 6 es un protocolo de capa de red que permite que la comunicación tenga lugar a través de la red. IPv6 fue diseñado por Internet Engineering Task Force (IETF) en diciembre de 1998 con el propósito de reemplazar el IPv4 debido al crecimiento exponencial global de usuarios de Internet [Derawi and Zhang, 2016].

El tipo común de dirección IP (se conoce como IPv4, para "versión 4"). A continuación, se muestra un ejemplo de cómo se vería una dirección IP: 25.59.209.224

Una dirección IPv4 consta de cuatro números, cada uno de los cuales contiene de uno a tres dígitos, con un solo punto (.), que separa cada número o conjunto de dígitos. Cada uno de los cuatro números puede oscilar entre 0 y 255, este grupo de números separados crea las direcciones que permiten a todos en todo el mundo enviar y recuperar datos a través de conexiones a Internet. El IPv4 utiliza un esquema de direcciones de 32 bits que permite almacenar 2^{32} direcciones, lo que equivale a más de 4 mil millones de direcciones. Hasta la fecha, se considera el protocolo de Internet principal y transporta el 94 % del tráfico de Internet [Cardenas and Hahn, 2019].

Inicialmente, se asumió que nunca se quedaría sin direcciones, pero la situación actual allana un nuevo camino hacia IPv6, ya que una dirección IPv6 consta de ocho grupos de cuatro dígitos hexadecimales. A continuación se presenta un ejemplo de dirección IPv6: 3001: 0da8: 75a3: 0000: 0000: 8a2e: 0370: 7334

Esta nueva versión de dirección IP se está implementando para satisfacer la necesidad de más direcciones de Internet. Su objetivo era resolver problemas asociados con IPv4. Con un espacio de direcciones de 128 bits, permite 340 mil millones de espacios de direcciones únicos. IPv6 también llamado IPng (Protocolo de Internet de próxima generación) lo que admite un máximo teórico de (2^{128} o 340 sextillones de direcciones) [Derawi and Zhang, 2016].

Tipos de dirección IPv6: Según [Derawi and Zhang, 2016] entre los diferentes tipos de IPv6 se mencionan los siguientes:

- Direcciones unicast: Identifica un nodo único en una red y generalmente se refiere a un solo remitente o un solo receptor.
- Direcciones de multidifusión: Representa un grupo de dispositivos IP y solo se puede utilizar como destino de un datagrama.
- Direcciones Anycast: Se asigna a un conjunto de interfaces que normalmente pertenecen a diferentes nodos.

Ventajas de IPv6: Según [Derawi and Zhang, 2016] entre las ventajas se mencionan las siguientes:

- Fiabilidad.
- Velocidades más rápidas: IPv6 admite multidifusión en lugar de difusión en IPv4. Esta función permite que los flujos de paquetes que consumen mucho ancho de banda (como los flujos multimedia) se envíen a varios destinos a la vez.
- Stringer Security: IPSecurity, que proporciona confidencialidad e integridad de los datos, está integrado en IPv6.
- Eficiencia de enrutamiento.

Desventajas de IPv6: Según [Derawi and Zhang, 2016] entre las desventajas se mencionan las siguientes:

- Conversión: debido al uso generalizado actual de IPv4, será necesario un largo período de tiempo para cambiar completamente a IPv6.
- Comunicación: las máquinas IPv4 e IPv6 no pueden comunicarse directamente entre sí. Necesitan una tecnología intermedia para hacerlo posible.

ZigBee

Según [Cardenas and Hahn, 2019] y [Derawi and Zhang, 2016] es una tecnología inalámbrica desarrollada como un estándar global abierto para abordar las necesidades únicas de las redes inalámbricas de IoT de bajo coste y baja potencia. El estándar Zigbee se basa en la especificación de radio física IEEE 802.15.4 y opera en bandas sin licencia como 2,4 GHz, 900 MHz y 868 MHz.

La especificación 802.15.4 sobre la que opera Zigbee fue ratificada por el Instituto de Ingenieros Eléctricos y Electrónicos IEEE en 2003. Esta es un protocolo de radio basado en paquetes y destinado a dispositivos de bajo coste que funcionan con baterías. El protocolo permite que los dispositivos se comuniquen en una variedad de topologías de red y puede tener una duración de batería de varios años [Cardenas and Hahn, 2019].

Por otra parte, el protocolo Zigbee ha sido creado y ratificado por las empresas miembros de la Zigbee Alliance. Más de 300 fabricantes de semiconductores, empresas tecnológicas, fabricantes de equipos originales y empresas de servicios son miembros de la Zigbee Alliance. Este protocolo fue diseñado para ofrecer una solución de datos inalámbricos fácil de usar, caracterizada por arquitecturas de red inalámbricas seguras y fiabilidad [Cardenas and Hahn, 2019].

El protocolo Zigbee 3.0 está diseñado para comunicar datos a través de entornos de radiofrecuencia ruidosos, habituales en las aplicaciones comerciales e industriales. La versión 3.0 se basa en el estándar Zigbee existente, pero unifica los perfiles de aplicación específicos del mercado para permitir que todos los dispositivos se conecten de forma inalámbrica en la misma red, independientemente de su designación y función en el mercado. Además, un esquema de certificación de Zigbee 3.0 garantiza la interoperabilidad de productos de distintos fabricantes. La conexión de las redes Zigbee 3.0 al dominio IP abre la supervisión y el control desde dispositivos como smartphones y tabletas en una LAN o WAN, incluso en Internet y contribuye con la operabilidad del Internet de las cosas [Cardenas and Hahn, 2019].

Según [Derawi and Zhang, 2016] entre las características del protocolo Zigbee se incluyen las siguientes:

- Compatibilidad con múltiples topologías de red, como las redes punto a punto, punto a multipunto y de malla.
- Bajo ciclo de trabajo, el cual proporciona una larga duración de la batería.
- Baja latencia.
- Espectro ensanchado de secuencia directa (DSSS).
- Hasta 65.000 nodos por red.
- Encriptación AES de 128 bits para conexiones de datos seguras.
- Prevención de colisiones, reintentos y acuses de recibo.

[Derawi and Zhang, 2016] mencionan que Zigbee 3.0 incorpora un "dispositivo base" que proporciona un comportamiento coherente para la puesta en marcha de nodos en una red. Se proporciona un conjunto común de métodos para su funcionamiento, incluido Touchlink, un método de puesta en marcha por proximidad. Adicionalmente, esta ofrece una mayor seguridad en la red y dispone de dos métodos de seguridad que dan lugar a dos tipos de red que se mencionan a continuación:

- Seguridad centralizada: Este método emplea un coordinador/centro de confianza que forma la red y gestiona la asignación de las claves de seguridad de la red y de los enlaces a los nodos que se unen.
- Seguridad distribuida: Este método no tiene coordinador/centro de confianza y está formado por un router. Cualquier nodo del router Zigbee puede proporcionar posteriormente la clave de red a los nodos de unión.

Los autores [Derawi and Zhang, 2016] indican que los nodos adoptan el método de seguridad que utiliza la red a la que se unen. Zigbee 3.0 soporta la creciente escala y complejidad de las redes inalámbricas y hace frente a grandes redes locales de más de 250 nodos. Zigbee también gestiona el comportamiento dinámico de estas redes con nodos que aparecen, desaparecen y vuelven a aparecer en la red y permite que los nodos huérfanos, resultado de la pérdida de un progenitor, vuelvan a unirse a la red a través de otro progenitor. La naturaleza de autor reparación de las redes Zigbee Mesh también permite que los nodos salgan de la red sin que se interrumpa el enrutamiento interno.

La compatibilidad con versiones anteriores de Zigbee 3.0 significa que las aplicaciones ya desarrolladas bajo el perfil Zigbee Light Link 1.0 o Home Automation 1.2 están listas para Zigbee 3.0. El perfil Smart Energy también es compatible con Zigbee 3.0 a nivel funcional, pero Smart Energy tiene requisitos de seguridad adicionales que sólo se abordan dentro del perfil. Por otra parte, la función de actualización *Over-The-Air* (OTA) de Zigbee para las actualizaciones de software durante el funcionamiento del dispositivo garantiza que las aplicaciones de los dispositivos ya desplegados en el campo puedan migrar sin problemas a Zigbee 3.0. La actualización OTA es una funcionalidad opcional que los fabricantes puede incluir en sus productos Zigbee [Derawi and Zhang, 2016].

Redes de malla: Un componente clave del protocolo Zigbee es la capacidad de soportar redes de malla. En una red de malla, los nodos están interconectados con otros nodos, de modo que cada uno de ellos está conectado por múltiples vías. Las conexiones entre los nodos se actualizan y optimizan dinámicamente a través de una tabla de enrutamiento de malla incorporada [Derawi and Zhang, 2016].

Las redes de malla son de naturaleza descentralizada; cada nodo es capaz de auto descubrirse en la red. Además, cuando los nodos abandonan la red, la topología de malla permite a los nodos reconfigurar las rutas de enrutamiento en función de la nueva estructura de la red. Las características de la topología de malla y el enrutamiento ad hoc proporcionan una mayor estabilidad en condiciones cambiantes o en caso de fallo de un solo nodo [Derawi and Zhang, 2016].

Aplicaciones de Zigbee: Zigbee permite un amplio despliegue de redes inalámbricas con soluciones de bajo coste y bajo consumo. Ofrece la posibilidad de funcionar durante años con baterías de bajo coste para una serie de aplicaciones de supervisión y control. Energía inteligente/red inteligente, lectura automática de contadores AMR, controles de iluminación, sistemas de automatización de edificios, monitorización de depósitos, control de HVAC, dispositivos médicos y aplicaciones son sólo algunos de los muchos espacios en los que la tecnología Zigbee está realizando avances significativos [Derawi and Zhang, 2016].

Por otra parte, la empresa Digi es miembro de la Zigbee Alliance y ha desarrollado una amplia gama de soluciones de red basadas en el protocolo Zigbee. Digi XBee 3 es el último de una larga línea de dispositivos que proporcionan una solución fácil de implementar que ofrece funcionalidad para conectarse a una amplia variedad de dispositivos [Derawi and Zhang, 2016].

LiteOS

LiteOS es un sistema operativo de código abierto, interactivo, similar a UNIX, diseñado para redes de sensores inalámbricos. A través de las herramientas que vienen con LiteOS, puede operar una o más redes de sensores inalámbricos de una manera similar a Unix, transfiriendo datos, instalando programas, recuperando resultados o configurando sensores. También puede desarrollar programas para nodos y distribuirlos de forma inalámbrica a los nodos sensores [Kandasamy et al., 2020].

Por otra parte, dentro de la empresa Huawei LiteOS lo consideran como una plataforma de desarrollo de software diseñada para ayudar a desarrollar rápidamente la industria de dispositivos de IoT y la smartificación del hardware de IoT. Asimismo, desde su lanzamiento en 2015, Huawei LiteOS ha ayudado a que muchos productos salgan al mercado, incluidos los teléfonos inteligentes, dispositivos portátiles y chips de IoT de Huawei de alta gama. Hasta la fecha, se han producido 50 millones de dispositivos con tecnología Huawei LiteOS [Kandasamy et al., 2020].

LiteOS está diseñado para ocupar poco espacio, lo que ahorra espacio y reduce la carga del sistema operativo en el dispositivo. El sistema operativo está disponible con una licencia BSD, que es una clase de licencias simples y gratuitas para software de computadora que se desarrolló originalmente en la Universidad de California en Berkeley. LiteOS es compatible con teléfonos inteligentes, dispositivos portátiles, aplicaciones de fabricación inteligente, hogares inteligentes e Internet de los Vehículos - *Internet of Vehicles* (IoV). El sistema operativo también sirve como plataforma de desarrollo de dispositivos inteligentes. La plataforma simplifica el desarrollo y la conectividad de los dispositivos IoT, al tiempo que se centra en mejorar la experiencia del usuario [Kandasamy et al., 2020].

Los protocolos compatibles con los dispositivos de IoT incluyen Zigbee y *Bluetooth Low Energy* (BLE), junto con varias plataformas en la nube. A diferencia del sistema operativo Android Things de Google, LiteOS se puede ejecutar en dispositivos con hardware mucho menos potente. Al mismo tiempo, IoT tiene requisitos distintos en los sistemas operativos en comparación con las PC o los dispositivos móviles. Los sistemas operativos de IoT deben ser modulares; tener una arquitectura actualizable y kernels escalables, consumen poca energía, admite una variedad de protocolos de conexión, diferentes tipos de hardware y soluciones de chip. Adicionalmente, ofrecen capacidades de seguridad en el lado del dispositivo [Kandasamy et al., 2020].

OneM2M

Según [Cardenas and Hahn, 2019] OneM2M es la iniciativa de estándares globales que cubre requisitos, arquitectura, especificaciones API, soluciones de seguridad e interoperabilidad para tecnologías de máquina a máquina e IoT, desarrollados en 2012 integrados por ocho de las organizaciones de desarrollo de estándares más importantes del mundo como lo son:

- Instituto Europeo de Normas de Telecomunicaciones (ETSI), Europa.
- La Asociación de Industrias y Negocios de Radio (ARIB), Japón.

- El Comité de Tecnología de Telecomunicaciones (TTC), Japón.
- Alliance for Telecommunications Industry Solutions (ATIS), EE.UU.
- La Asociación de la Industria de las Telecomunicaciones (TIA), EE.UU.
- Asociación de Normas de Comunicaciones de China (CCSA), China.
- La Asociación de Tecnología de Telecomunicaciones (TTA), Corea

Adicionalmente, Junto con dos consorcios de la industria (GlobalPlatform, OMA SpecWorks) y más de 200 organizaciones miembros. Esta proporciona un marco para respaldar aplicaciones y servicios como la red inteligente, el automóvil conectado, la automatización del hogar, la seguridad pública y la salud desarrollando especificaciones técnicas e informes para garantizar que los dispositivos M2M puedan comunicarse con éxito a escala global [Cardenas and Hahn, 2019].

Data Distribution Service (DDS)

El Servicio de distribución de datos - *Data Distribution Service* (DDS) es un protocolo de middleware y un estándar API para la conectividad centrada en datos de Object Management Group (OMG). Integra los componentes de un sistema, proporcionando conectividad de datos de baja latencia, confiabilidad extrema y una arquitectura escalable que las aplicaciones empresariales y de misión crítica de Internet de las cosas (IoT) necesitan [Reeves and Maple, 2018].

En un sistema distribuido, el middleware es la capa de software que se encuentra entre el sistema operativo y las aplicaciones. Permite que los diversos componentes de un sistema se comuniquen y compartan datos más fácilmente. Simplifica el desarrollo de sistemas distribuidos al permitir que los desarrolladores de software se concentren en el propósito específico de sus aplicaciones en lugar de la mecánica de pasar información entre aplicaciones y sistemas [Reeves and Maple, 2018].

La protección de los entornos de IoT requiere una seguridad que se amplíe desde el borde hasta la nube, en todos los sistemas y proveedores. DDS incluye mecanismos de seguridad que brindan autenticación, control de acceso, confidencialidad e integridad a la distribución de la información. DDS Security utiliza una arquitectura punto a punto descentralizada que proporciona seguridad sin sacrificar el rendimiento en tiempo real [Reeves and Maple, 2018].

Advanced Message Queuing Protocol (AMQP)

El Protocolo de cola de mensajes avanzado o *Advanced Message Queuing Protocol* (AMQP) es un estándar publicado de código abierto para la mensajería asincrónica por cable, esta permite la mensajería encriptada e interoperable entre organizaciones y aplicaciones. El protocolo se utiliza en la mensajería cliente / servidor y en la gestión de dispositivos IoT. Por otra parte, es eficiente, portátil, multicanal y seguro. El protocolo

binario ofrece autenticación y cifrado mediante SASL o TLS, basándose en un protocolo de transporte como TCP. El protocolo de mensajería es rápido y ofrece entrega garantizada con acuse de recibo de los mensajes recibidos. AMQP funciona bien en entornos multi cliente y proporciona un medio para delegar tareas y hacer que los servidores manejen solicitudes inmediatas más rápido. Debido a que AMQP es un sistema de mensajería binaria en streaming con un comportamiento de mensajería estrictamente obligatorio, la interoperabilidad de los clientes de diferentes proveedores está asegurada [Babun et al., 2021].

AMQP permite varios modos de mensajería garantizados que especifican que se envía un mensaje:

- Como máximo una vez (enviado una vez con la posibilidad de que se pierda).
- Al menos una vez (garantizando la entrega con posibilidad de mensajes duplicados).
- Exactamente una vez (garantizando una entrega única).

AMQP fue concebido por John O'Hara de JP Morgan Chase en 2003 e inicio como un esfuerzo cooperativo comenzando con iMatix Corporation. Antes de la versión 1.0 fue lanzado el 30 de octubre º 2011, el grupo de trabajo para AMQP creció a 23 empresas como Bank of America, Barclays, Cisco Systems, Credit Suisse, Deutsche Börse, Goldman Sachs, HCL Technologies Ltd, Progress Software, IIT Software, INETCO Systems Limited, Informática (incluida 29 West), JPMorgan Chase, Microsoft Corporation, my-Channels, Novell, Red Hat, Software AG, Solace Systems, StormMQ, Tervela Inc., TWIST Process Innovations Ltd., VMware y WSO2 [Babun et al., 2021].

Constrained Application Protocol (CoAP)

Es un protocolo que determina cómo pueden funcionar los dispositivos de baja potencia, este se desarrolló originalmente para la transferencia web con nodos y redes restringidas en la Internet de las cosas. El protocolo es una versión notable de Protocolo de Transferencia de Hipertexto - *Hypertext Transfer Protocol* (HTTP) para cumplir con el requisito de IoT de baja sobrecarga y soporte de multidifusión. *Constrained Application Protocol* (CoAP) depende de REST, un principio adoptado de HTTP e integrado en UDP para la transacción. La razón inicial para el desarrollo de este protocolo es para cumplir con el alto requisito de IoT y la necesidad de un protocolo ligero y de baja tasa. En general, las principales características de CoAP son: soporta los requisitos M2M en entornos restringidos, enlace UDP con soporte opcional de peticiones uni-cast y multicast, intercambios de mensajes asíncronos, baja sobrecarga de cabecera y complejidad de análisis, soporta Identificador de recursos uniforme - *Universal Resource Identifier* (URI) y tipo de contenido y disponen de capacidades simples de proxy y caché [Granjal et al., 2015].

La arquitectura de CoAP se divide en dos capas, la de mensajes y de solicitud/ respuesta. La primera capa es responsable de controlar el intercambio de mensajes a través de UDP entre dos puntos finales. Mientras que la segunda capa transporta la petición y la respuesta que contienen el código de método y el código de respuesta para evitar problemas

como la llegada de mensajes que están fuera de orden perdidos o duplicados. Así, CoAP es un mecanismo fiable con características ricas como, simples retransmisiones de parada y espera, detección de duplicados y soporte de multidifusión. CoAP utiliza una cabecera binaria de longitud fija y componentes, y los mensajes se codifican codificados en formato binario simple [Granjal et al., 2015].

LoRaWAN

Long Range Wide Area Network, es un protocolo para WANs diseñado para soportar enormes redes, como las ciudades inteligentes, con millones de dispositivos de baja potencia y a largas distancias. Adicionalmente, es un protocolo de red de área extendida de bajo consumo creado para operar con dispositivos de IoT que funcionen con baterías con alcance regional, nacional y global, su configuración se basa en el cumplimiento de los requisitos de comunicación bidireccional del IoT, seguridad de punto a punto y servicios de localización. Por otra parte, permite que los equipos constatados al IoT envíen pequeñas cantidades de datos con un largo alcance y a una baja velocidad con un consumo mínimo de energía [Reeves and Maple, 2018].

[Reeves and Maple, 2018] indican que, entre los marcos de trabajo de IoT se encuentran los siguientes:

Amazon Web Services (AWS) IoT: Es una plataforma de computación en la nube para IoT. Esta creada para conectar dispositivos inteligentes de forma fácil con la nube de *Amazon Web Services* (AWS) y otros equipos. esta puede recopilar datos de miles de millones de dispositivos y conectarlos a puntos finales para otras herramientas y servicios de AWS, lo que permite a un desarrollador vincular esos datos en una aplicación [Reeves and Maple, 2018].

AWS IoT es compatible con los protocolos de comunicación HTTP, MQTT y WebSockets entre los dispositivos conectados y las aplicaciones en la nube a través de Device Gateway, que proporciona una comunicación bidireccional segura al tiempo que limita la latencia. Device Gateway se escala automáticamente, eliminando la necesidad de que una empresa aprovisione y administre servidores para un sistema de mensajería pub / sub, lo que permite a los clientes publicar y recibir mensajes entre sí [Reeves and Maple, 2018]. AWS requiere que los dispositivos, las aplicaciones y los usuarios se adhieran a políticas de autenticación sólidas a través de certificados X.509, credenciales de AWS Identity and Access Management o autenticación de terceros a través de Amazon Cognito. AWS cifra todas las comunicaciones desde y hacia los dispositivos [Reeves and Maple, 2018].

Arm MbedIoT: Plataforma para crear aplicativos para IoT fundamentados en microcontroladores Arm, esta se centra en la creación e implementación de dispositivos de Internet de las cosas basados en estándares. Ofrece Mbed OS, un sistema operativo gratuito para dispositivos basados en procesadores ARM Cortex-M que consolida los bloques de construcción fundamentales de IoT, el cual es un conjunto integrado de componentes de software. Contiene funciones de seguridad, comunicación y administración de dispositivos para permitir el desarrollo de dispositivos IoT de grado de producción y energéticamente

eficientes; Mbed Device Server, que proporciona productos de software de extremo a extremo que llevan IP y servicios web al nodo final, combinando software de cliente integrado altamente optimizado con una plataforma escalable de administración y aplicación web, entre otras herramientas. ARM Mbed se fundó en 2009 y tiene su sede en Cambridgeshire, Reino Unido [Reeves and Maple, 2018].

Azure IoT Suite de Microsoft: Plataforma que se compone de un grupo de servicios para que los usuarios interactúen y reciban información de sus dispositivos IoT, con la cual se puede monitorear y controlar miles de millones de activos de IoT. En términos más simples, una solución de IoT se compone de uno o más dispositivos de IoT que se comunican con uno o más servicios de back-end alojados en la nube. Un dispositivo de IoT generalmente se compone de una placa de circuito con sensores conectados que usan WiFi para conectarse a Internet [Microsoft, 2021]. Por ejemplo:

- Un sensor de presión en una bomba de aceite remota.
- Sensores de temperatura y humedad en una unidad de aire acondicionado.
- Un acelerómetro en un ascensor.
- Sensores de presencia en una habitación.

Existe una amplia variedad de dispositivos disponibles de diferentes fabricantes para crear una solución. Para la creación de prototipos, se pueden utilizar dispositivos como MXChip IoT DevKit o Raspberry Pi. El Devkit tiene sensores integrados de temperatura, presión, humedad, giroscopio, acelerómetro y magnetómetro. La Raspberry Pi permite conectar muchos tipos diferentes de sensores. Microsoft proporciona SDK de dispositivos de código abierto que se puede utilizar para crear las aplicaciones que se ejecutan en dispositivos. Estos SDK simplifican y aceleran el desarrollo de soluciones de IoT [Microsoft, 2021].

2.2.4. Riesgo cibernético

Es aquel que puede dañar a una organización a través de sus sistemas de información. Según [Petar et al., 2019], el riesgo cibernético es cualquier riesgo asociado con pérdidas financieras, interrupciones o daños a la reputación de una empresa debido a fallas, uso no autorizado o erróneo de sus sistemas de información. Por otra parte, el riesgo cibernético puede tomar varias formas como, por ejemplo, el delito cibernético, el terrorismo cibernético, el espionaje corporativo, los controles de seguridad defectuosos de los proveedores y las amenazas internas son fuentes de riesgo cibernético. Por lo que, esos riesgos pueden tomar formas específicas, como ransomware o ataques de phishing y ataques Ataque de denegación de servicio distribuido - *Distributed Denial of Service* (DDoS), entre otros [Faried and Fajardo, 2017].

Un ataque de denegación de servicio Ataque de servicio - *Denial of Service* (DoS) es un ataque destinado a cerrar una máquina o red, haciéndola inaccesible para los usuarios.

Los ataques DoS logran esto inundando el objetivo con tráfico o enviándole información que desencadena un bloqueo. Entonces, el ataque DoS priva a los usuarios legítimos (es decir, empleados, miembros o titulares de cuentas) del servicio o recurso que esperaban. Por otra parte, los ataques de denegación de servicio distribuido DDoS son una subclase de los ataques de denegación de servicio DoS. Un ataque DDoS involucra múltiples dispositivos en línea conectados, conocidos colectivamente como botnet, que se utilizan para abrumar un sitio web objetivo con tráfico falso. A diferencia de otros tipos de ataques cibernéticos, los ataques DDoS no intentan violar su perímetro de seguridad. Más bien, un ataque DDoS tiene como objetivo hacer que su sitio web y sus servidores no estén disponibles para los usuarios legítimos [Faried and Fajardo, 2017].

El ransomware es un tipo de software malicioso (malware) que amenaza con publicar o bloquear el acceso a datos o a un sistema informático, generalmente cifrándolos, hasta que la víctima paga una tarifa de rescate al atacante. En muchos casos, la demanda de rescate viene con una fecha límite. Si la víctima no paga a tiempo, los datos desaparecen para siempre o el rescate aumenta [Faried and Fajardo, 2017].

El phishing es una forma de fraude en la que un atacante se hace pasar por una entidad o persona de confianza en un correo electrónico u otras formas de comunicación. Los atacantes suelen utilizar correos electrónicos de phishing para distribuir enlaces maliciosos o archivos adjuntos que pueden realizar una variedad de funciones. Algunos extraerán las credenciales de inicio de sesión o la información de la cuenta de las víctimas [Faried and Fajardo, 2017].

¿Qué es la seguridad del IoT?

La seguridad del IoT se refiere a los métodos de protección utilizados para proteger los dispositivos conectados a Internet o basados en la red. El término IoT es increíblemente amplio, y con la continua evolución de la tecnología, el término no ha hecho más que ampliarse. Desde los relojes hasta los termostatos y las consolas de videojuegos, casi todos los dispositivos tecnológicos tienen la capacidad de interactuar con Internet, o con otros dispositivos, de alguna manera.

La seguridad del IoT es el conjunto de técnicas, estrategias y herramientas que se utilizan para proteger estos dispositivos y evitar que se pongan en peligro. Irónicamente, es la conectividad inherente al IoT la que hace que estos dispositivos sean cada vez más vulnerables a los ciberataques.

Dado que IoT es tan amplio, la seguridad de IoT es aún más amplia. Esto ha dado lugar a una variedad de metodologías que caen bajo el resguardo de la seguridad de IoT. La seguridad de la Interfaz de programación de aplicaciones - *Application Programming Interfaces* (API), la autenticación de la Infraestructura de clave pública - *Public key infrastructure* (PKI) y la seguridad de la red son solo algunos de los métodos que los responsables de TI pueden utilizar para combatir la creciente amenaza de la ciberdelincuencia y el ciberterrorismo que tienen su origen en los dispositivos vulnerables de IoT.

2.2.5. Problemas de seguridad y privacidad del IoT

La IoT conecta a miles de millones de dispositivos a internet, los mismos deben estar resguardados debido a su mayor extensión de la zona de ataque, la seguridad y la privacidad que representa la principal preocupación. Para ejemplificar, en 2016, Se presento un ataque de denegación de servicio distribuidos DDoS el cual se denominó Mirai, dejando fuera de servicios miles de dispositivos [Petar et al., 2019].

Por lo tanto, los atacantes accedieron a la red aprovechando dispositivos IoT mal protegidos. En efecto, dado que los dispositivos IoT están estrechamente conectados, todo lo que hace un hacker es explotar una vulnerabilidad para manipular todos los datos, dejándolos inutilizables. Los fabricantes que no actualizan sus dispositivos con regularidad o no lo hacen los dejan sensibles a los ciberdelincuentes [Petar et al., 2019].

Cuando los dispositivos IoT se conectan a internet, están expuestos a diferentes riesgos de seguridad en términos de confidencialidad, integridad y disponibilidad de los datos. Estos dispositivos se vuelven inseguros y vulnerables debido a estos riesgos que pueden ser afectados por atacantes maliciosos. Es por ello que, los dispositivos IoT con sensores inteligentes se han convertido en un objetivo fácil para los atacantes en lo que respecta a la disponibilidad del servicio, el enrutamiento de la red y la autenticación de los nodos [Alharbi et al., 2020].

Adicionalmente, las vulnerabilidades de los dispositivos IoT incluyen el hackeo, la fuga de información, el ataque de virus y la violación de la privacidad. Por lo que, el adversario puede obtener acceso para controlar las funciones de los dispositivos y puede realizar ataques a la red y al dispositivo. Adicionalmente, puede interrumpir, manipular o interceptar los datos que se transmiten y el atacante puede hacerse pasar por usuario interno, a través de algunos medios para controlar los dispositivos IoT. Es así como, los dispositivos IoT se pueden enfrentar a ataques de ciberseguridad como ataques físicos, denegación de servicio DDoS, desvío, reenvío selectivo, ataques de inundación, suplantación de identidad, falsificación, escuchas e interceptación del tráfico de red, entre otros [Alharbi et al., 2020].

Al mismo tiempo, la limitación de la potencia de cálculo, la comunicación y la energía en los dispositivos IoT impide el uso de los mecanismos de seguridad estándar que se utilizan en otros dispositivos informáticos. Los usuarios de los dispositivos IoT no son conscientes de las medidas y prácticas de seguridad, por lo que no son capaces de aplicar los requisitos y procedimientos básicos para la protección de sus dispositivos IoT, como no cambiar la contraseña y el nombre de usuario por defecto. En estos casos, los usuarios se convierten involuntariamente en aliados de los atacantes [Petar et al., 2019].

Es por ello que el IoT consiste en añadir conectividad a Internet a un sistema de dispositivos informáticos, máquinas mecánicas y digitales, objetos, animales o personas interrelacionados. Asimismo, a cada cosa se le proporciona un identificador único y la capacidad de transferir automáticamente datos a través de una red. Permitir que los dispositivos se conecten a Internet, exponiéndolos a una serie de graves vulnerabilidades si no están debidamente protegidos.

En tal sentido, una serie de incidentes de gran repercusión en los que se utilizó un

dispositivo IoT común para infiltrarse y atacar la red más grande ha llamado la atención sobre la necesidad de la seguridad de IoT. Es fundamental para garantizar la seguridad de las redes con dispositivos IoT conectados a ellas. Esto incluye una amplia gama de técnicas, estrategias, protocolos y acciones que tienen como objetivo mitigar las crecientes vulnerabilidades del IoT de las empresas modernas, ya que cuantas más formas tengan los dispositivos de conectarse entre sí, más formas tendrán los actores de amenazas de interceptarlos. Protocolos como el HTTP y las API son sólo algunos de los canales en los que se basan los dispositivos IoT y que los hackers pueden interceptar. Por otra parte, el resguardo del IoT tampoco incluye estrictamente los dispositivos basados en Internet. Los aparatos que utilizan la tecnología Bluetooth también se incluyen como dispositivos IoT, por lo tanto, requieren seguridad. En tal sentido, este tipo de descuidos han contribuido al reciente aumento de las violaciones de datos relacionadas con el IoT.

A continuación, se presentan algunos de los desafíos de seguridad del IoT que siguen representando una amenaza:

Exposición remota

A diferencia de otras tecnologías, los dispositivos de IoT tienen una superficie de ataque particularmente amplia debido a su conectividad con apoyo de Internet. Aunque esta accesibilidad es extremadamente valiosa, también concede a los hackers la oportunidad de interactuar con los dispositivos de forma remota. Por ello, las campañas de hacking como el phishing son especialmente eficaces. La seguridad del IoT, al igual que la seguridad de la nube, tiene que tener en cuenta un gran número de puntos de entrada para proteger los activos [Albataineh and Alsmadi, 2019].

Falta de previsión de la industria

A medida que las empresas continúan con las transformaciones digitales de sus negocios, también lo han hecho ciertas industrias y sus productos. Industrias como la automoción y la sanidad han ampliado recientemente su selección de dispositivos IoT para ser más productivos y rentables. Esta revolución digital. Sin embargo, también ha dado lugar a una mayor dependencia tecnológica que nunca [Danda and Hota, 2016].

Al respecto, aunque normalmente no representa un problema, la dependencia de la tecnología puede amplificar las consecuencias de una violación de datos. Lo que hace que esto sea preocupante es que estas industrias ahora dependen de una pieza de tecnología que es inherentemente más vulnerable. Así pues, no solo los dispositivos IoT, sino que muchas empresas del sector sanitario y de la automoción no estaban preparadas para invertir la cantidad de dinero y recursos necesarios para asegurar estos dispositivos. Por lo tanto, esta falta de previsión de la industria ha expuesto innecesariamente a muchas organizaciones y fabricantes a mayores amenazas de ciberseguridad [Danda and Hota, 2016].

Limitación de recursos

La falta de previsión no es el único problema de seguridad del IoT al que se enfrentan las industrias recién digitalizadas. Otra de las principales preocupaciones de la seguridad del IoT es la limitación de recursos de muchos de estos dispositivos. Es así como, no todos los dispositivos IoT tienen la potencia de cálculo necesaria para integrar sofisticados cortafuegos o software antivirus y algunos apenas tienen la capacidad de conectarse a otros dispositivos. Asimismo, los dispositivos IoT que han adoptado la tecnología Bluetooth han sufrido una reciente oleada de violaciones de datos y el sector del automóvil ha sido uno de los mercados más perjudicados. Por ejemplo, en 2020, un experto en ciberseguridad hackeó un Tesla Model X en menos de 90 segundos aprovechando una enorme vulnerabilidad de Bluetooth. Otros coches que dependen de llaves FOB[1] para abrir y arrancar sus coches han sufrido ataques por razones similares. Debido a esto, los actores de las amenazas han encontrado una forma de escanear y replicar la interfaz de estas llaves tipo FOB para robar los vehículos asociados sin activar una alarma [Derawi and Zhang, 2016].

En tal sentido, si una maquinaria tecnológicamente avanzada como un Tesla es vulnerable a una violación de datos del IoT, también lo es cualquier otro dispositivo inteligente [Derawi and Zhang, 2016].

Contraseñas débiles, adivinables o codificadas

Las contraseñas débiles, predeterminadas y obsoletas son más fácil para los piratas informáticos que buscan atacar e implementar botnets a gran escala y otro malware. La gestión de las contraseñas de los dispositivos a escala es una responsabilidad, especialmente porque los dispositivos de IoT no suelen tener operadores humanos para instigar el cambio de contraseña [Albataineh and Alsmadi, 2019].

Servicios de red inseguros

Cuando se intenta comprometer un punto final de IoT conectado, una de las primeras y más simples áreas de ataque es encontrar debilidades en el modelo de comunicación de la red y en los servicios de red que se ejecutan en el dispositivo. De este modo, los atacantes tratarán de explotar una serie de vulnerabilidades para capturar las credenciales de inicio de sesión, los tokens de comunicación u otros identificadores que el ecosistema de servicios utilizará para identificar el punto final. Por lo tanto, es imperativo asegurar el punto final con las mejores prácticas de la industria [Albataineh and Alsmadi, 2019].

[1]FOB, comúnmente llamado (Key Fob) llavero de control remoto, es una pequeña seguridad de hardware del dispositivo con una función de autenticación utilizado para el control y el acceso seguro a los dispositivos móviles, sistemas informáticos, redes y servicios de datos.

Interfaces inseguras del ecosistema

Para hacer frente a las interfaces inseguras de la web, de la API de backend, de la nube o del móvil en el ecosistema fuera del dispositivo IoT, es necesario contar con un mecanismo sólido y regular para autenticar y autorizar el dispositivo. Por ello, se han desarrollado varios casos de uso para combatir la protección del hardware, el firmware y las comunicaciones de datos de extremo a extremo. Por lo tanto, al garantizar una autenticación fuerte con el punto final, se demuestra que cada dispositivo tiene permiso para comunicarse con el proveedor de servicios IoT y cada vez que los servicios de back-end se comunican con un dispositivo IoT, podrá diferenciar entre un EndPoint válido y un clon forzando al EndPoint a autenticarse. Si el dispositivo no puede hacerlo, KeyScaler puede rechazar el dispositivo [OWASP, 2021].

Falta de un mecanismo de actualización seguro

Las actualizaciones de software y firmware no autorizadas son un importante vector de amenaza para los ciberataques de IoT. Las brechas de IoT pueden tener consecuencias físicas que resultan en la pérdida de datos y también introducen una responsabilidad legal sustancial y erosionan la reputación de la marca de estos dispositivos [OWASP, 2021].

Según [OWASP, 2021], existen tres requisitos de seguridad fundamentales para suministrar actualizaciones de forma segura a los dispositivos IoT:

- Asegurar el acceso a las actualizaciones.
- Verificar el origen de las actualizaciones.
- Verificar la integridad de las actualizaciones.

Insuficiente protección de la privacidad

Respecto a la privacidad de los consumidores y la información personal empieza por proporcionar seguridad desde el principio, esto significa proporcionar seguridad a los datos desde el propio dispositivo final para establecer la confianza en el equipo. Así pues, para garantizar la confianza en el dispositivo, éste debe estar habilitado con la tecnología de seguridad de la autoridad de dispositivos para proporcionar una incorporación en términos de aprovisionamiento, registro y autenticación seguros. De este modo, puede establecerse la confianza en los datos para que el dispositivo pueda enviar datos confidenciales a través de la red, por ello se pueden establecer y gestionar la identidad y la integridad del dispositivo mediante el uso de una política de seguridad de datos de extremo a extremo que garantice la privacidad del consumidor de principio a fin [OWASP, 2021].

Transferencia y almacenamiento de datos inseguros

Los datos se refieren a distintas piezas de información, normalmente formateadas y almacenadas de una manera que concuerde con un propósito específico. Los datos pueden existir en varias formas: como números o texto grabado en papel, como bits o bytes almacenados en la memoria electrónica o como hechos que viven en la mente de una persona. Sin embargo, desde la llegada de la informática a mediados del siglo pasado, los datos se refieren más comúnmente a la información que se transmite o almacena electrónicamente [Arateco and Lorena, 2015].

La protección de los datos es primordial para la integridad de las aplicaciones de IoT. Los datos que alimentan las aplicaciones de IoT dan lugar a acciones y controles automatizados que pueden tener consecuencias físicas peligrosas. Por lo tanto, es fundamental que tanto el origen como el contenido de los datos generados por los dispositivos IoT estén protegidos y sean verificables. Sin embargo, los datos deben ser encriptados desde su creación hasta su consumo, y requieren un mayor nivel de versatilidad e inteligencia criptográfica que el que puede ofrecer el tradicional cifrado de Seguridad de la capa de transporte - *Transport Layer Security* (TLS) unidireccional [OWASP, 2021].

2.2.6. Aplicaciones de IoT para consumidores y empresas

Existen numerosas aplicaciones del mundo real del IoT, que van desde los consumidores, empresarial hasta el IoT industrial y de fabricación (IIoT). Los aplicativos de IoT engloban diversos sectores verticales, como la automoción, las telecomunicaciones y la energía. En el segmento de consumo, por ejemplo, los hogares inteligentes equipados con termostatos inteligentes, electrodomésticos inteligentes, calefacción, iluminación y dispositivos electrónicos conectados pueden controlarse a distancia a través de ordenadores y smartphones [Pathak and Bhandari, 2018].

Por otro lado, los dispositivos vestibles con sensores, estos softwares pueden recolectar y analizar los datos del usuario, remitiendo mensajes a otras tecnologías acerca de los usuarios, con el propósito de hacer la vida más cómoda y fácil. Los dispositivos vestibles igualmente se emplean para la seguridad pública. Por ejemplo, para optimizar los tiempos de respuesta de los socorristas en el transcurso de una emergencia, suministrando rutas perfeccionadas a un lugar o haciendo un seguimiento constante de los signos vitales de los bomberos en lugares con riesgo elevado [Pathak and Bhandari, 2018].

Igualmente, en el ámbito de la sanidad, el IoT ofrece muchas ventajas, entre ellas la posibilidad de hacer un seguimiento más exhaustivo de los pacientes mediante el análisis de los datos generados. Los hospitales pueden utilizar sistemas de IoT para realizar tareas como la gestión de inventarios, tanto de productos farmacéuticos como de instrumental médico [Petar et al., 2019].

Asimismo, los edificios inteligentes presentan avances tecnológicos, que logran determinar a través de sensores información la cual permite realizar funciones de manera automatizada, logrando de esta forma reducir costos en electricidad y aprovechamiento en el uso los sistemas de climatización de los mismos [Petar et al., 2019].

2.3. Consideraciones Finales

Para terminar el análisis de este capítulo, vemos que el IoT es un concepto que se refiere a una interconexión digital de objetos cotidianos con internet, es decir proceso que permite conectar elementos físicos cotidianos al Internet. Es, en definitiva, la conexión de internet más con objetos que con personas. Sin embargo, como se ve en la revisión de la literatura, se puede observar riesgos relacionados con la seguridad y vulnerabilidades en los dispositivos IoT.

Capítulo 3

Revisión Sistemática

3.1. Consideraciones Iniciales

Los fundamentos teóricos para la revisión sistemática se dividen en dos partes. En la sección 3.2, se explicara la etapa de planificación de la investigación. En la sección 3.3, se hablara sobre la ejecución de la revisión, concretamente más sobre el proceso de estudios primarios, palabras claves, cadenas de búsqueda, criterios de inclusión y exclusión, y extracción de datos. En la sección 3.4, son presentadas las consideraciones finales sobre la revisión sistemática.

3.2. Planificación de la investigación

3.2.1. Identificación de la necesidad de revisión

En esta etapa se buscó trabajos cuyo objetivo sea similar al planteado en esta investigación o que responda a las preguntas de investigación formuladas para determinar si existen documentos de literatura relacionados con el tema en estudio, además se revisó si existen variedad de estudios que apliquen para realizar la revisión sistemática en este estudio.

3.2.2. Especificación de las Preguntas de investigación

Se presenta la tabla 3.1 con las preguntas de investigación que se establecieron:

Seguidamente se inicia con el desarrollo del protocolo de revisión y para reducir la posibilidad de sesgos, en el protocolo se incluye las preguntas de investigación, fuentes y cadenas de búsqueda, criterios de inclusión y exclusión.

ID	Pregunta de Investigación
PI1	¿Cuáles son las incidencias de los riesgos del IoT en la protección de los datos?
PI2	¿Cuáles son las incidencias de los riesgos del IoT en la protección a la intimidad?
PI3	¿Cuáles son las incidencias de los riesgos del IoT en la protección del espionaje informático?
PI4	¿Cómo el establecimiento de medidas de seguridad pueden minimizar los riesgos del IoT a través del uso de tecnologías?

Tabla 3.1: Preguntas de Investigación

3.3. Ejecución de la Revisión

En este apartado se comienza con las actividades referentes a la RS a través de una serie de pasos que se describen a seguidamente:

3.3.1. Selección de estudios primarios

A continuación, el proceso de revisión y selección de los estudios primarios se realiza respetando el siguiente esquema presentado en la figura 3.1.

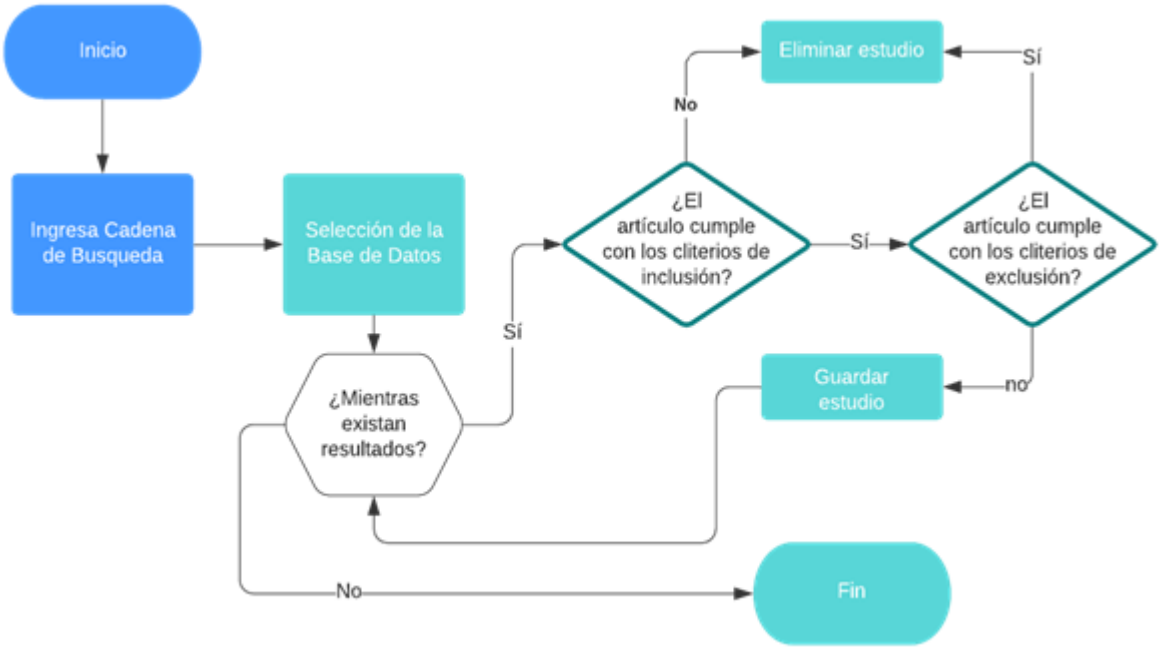

Figura 3.1: Proceso de selección de estudios primarios.

Fuente: elaboración propia.

3.3.2. Palabras claves y cadenas de búsqueda

Se escogieron a partir de una exploración inicial de información en artículos científicos y ponencias. Entre las palabras claves más utilizadas, se pueden indicar:

Cyber AND Risk AND in AND IoT AND Systems Security AND Risk AND Assessment AND in AND Internet AND of AND Things AND Systems

Una vez determinadas las bases de datos y detalladas las palabras claves se efectuaron las posibles consultas empleando los operadores lógicos AND / OR, creando las cadenas de búsqueda que se exponen en la tabla 3.2.

Fuente de Búsqueda	**Codificación**	**Cadena de Búsqueda**
SCOPUS	CB-01	Cyber AND Risk AND in AND IoT AND Systems Security AND Risk AND Assessment AND in AND Internet AND of AND Things AND Systems
SCIENCE DIRECT	CB-02	
IEEE XPLORER	CB-03	
PROQUEST	CB-04	
SEMANTICSCHOLAR	CB-05	
ELSEVIER	CB-06	
SPRINGER LINK	CB-07	
RESEARCHGATE	CB-08	
ACM DIGITAL LIBRARY	CB-09	

Tabla 3.2: Palabras Claves o Cadenas de búsqueda

3.3.3. Criterios de inclusión y exclusión

Los criterios de inclusión y exclusión determinaron un factor clave para la elección de estudios primarios. Dichos criterios se diseñaron con la finalidad de obtener documentos que se relacionen con el tema de investigación, los criterios de inclusión se exponen en la tabla 3.3.

Identificador	**Criterios de Inclusión**
CI-01	Artículos científicos publicados en revistas de alto nivel.
CI-02	Estudios publicados a partir del 2015.
CI-03	Estudios en los que en el título o resumen contenga las palabras claves.
CI-04	Estudios cuyo título tenga relación con el tema de investigación.
CI-05	Estudios en inglés.

Tabla 3.3: Criterios de Inclusión

Los criterios de exclusión se utilizarán para descartar dichos estudios que no fueron relevantes con el objetivo trazado, estos criterios se exponen en la tabla 3.4.

Identificador	Criterios de Exclusión
CE-01	Divulgaciones no oficiales que no persiguen una metodología científica.
CE-02	Estudios publicados antes del 2015.
CE-03	Estudios que en el título o resumen no contenga las palabras claves.
CE-04	Estudios cuyo título no tenga relación con el tema de investigación.
CE-05	Estudios duplicados.

Tabla 3.4: Criterios de Exclusión

3.3.4. Selección de las fuentes de búsqueda

Siguiendo los pasos de la metodología de [Kitchenham, 2007], en la etapa inicial se discurrieron las fuentes de búsqueda plasmadas en la tabla 3.5, las cuales fueron escogidas apoyados en la fiabilidad y confiabilidad del material obtenido a través de las consultas avanzadas.

Fuentes de Búsqueda	URL del Portal
SCOPUS	https://www.scopus.com/
SCIENCE DIRECT	https://www.sciencedirect.com/
IEEE XPLORER	https://ieeexplore.ieee.org/
PROQUEST	https://www.proquest.com/
SEMANTICSCHOLAR	https://www.semanticscholar.org/
ELSEVIER	https://www.elsevier.com/
SPRINGER LINK	https://link.springer.com/
RESEARCHGATE	https://www.researchgate.net/
ACM DIGITAL LIBRARY	https://dl.acm.org/

Tabla 3.5: Fuentes de búsqueda

3.3.5. Selección de estudios primarios

Posteriormente se emplearon los criterios de inclusión expuestos en la tabla 3.3, se consiguió como resultado 29 artículos. Consecutivamente para escoger los estudios primarios se aplicaron los criterios de exclusión que pueden observarse en la Tabla 3.4, que dieron como resultado 9 estudios excluidos, quedando un total de 20 estudios primarios analizados en esta revisión.

A continuación, en la tabla 3.6 puede observarse los resultados:

Cadena de Búsqueda	Estudios Obtenidos	Estudios Incluidos	Estudios Excluidos	Estudios Primarios
CB-01	3	0	0	0
CB-02	14	6	1	5
CB-03	10	7	2	5
CB-04	3	2	2	0
CB-05	4	2	1	1
CB-06	3	2	1	1
CB-07	6	5	1	4
CB-08	5	4	1	3
CB-09	2	1	0	1
Totales	50	29	9	20

Tabla 3.6: Resultados del proceso de selección de estudios primarios.

Fuente: Elaboración propia

3.3.6. Evaluación de la Calidad del Estudio

Se estableció criterios de evaluación de calidad definidos en el estudio, realizado por [Kitchenham, 2007], de los cuales se consideraron los expuestos en la lista de verificación, tabla 3.7, para la selección de los estudios primarios y dirección de la metodología.

N°	Pregunta	SI	N0
Preguntas para selección de estudios primarios			
1	¿Cumple con los criterios de inclusión?	X	
2	¿Se examinó el documento para comprobar que cumple con los criterios de inclusión y exclusión?	X	
3	¿El autor o autores sustentaron el problema de investigación?	X	
4	¿Los estudios utilizados se seleccionaron en relación al problema de investigación y pertenecen a fuentes confiables?	X	
Para la ejecución del Trabajo de Titulación			
1	¿El documento tiene por objetivo determinar los riesgos del IoT y su relación con los usuarios?	X	
2	¿Los documentos guardan relación con los riesgos cibernéticos del IoT?	X	

Tabla 3.7: Lista de verificación de evaluación de calidad

3.3.7. Extracción y síntesis de Datos

La extracción y síntesis de datos consiste en registrar y seleccionar con exactitud la información de los estudios primarios. La tabla 3.8 se diseñó para recopilar los datos generales referente a los documentos de los estudios primarios registrando los puntos referentes a título, año de publicación, referencia, al ser una investigación cualitativa se

utilizan tablas relacionales, gráficas y análisis que permitió agrupar los estudios que más se asemejan, considerando como parámetros las preguntas de investigación.

Estudio Primario	**Titulo**	**Año**	**Referencia**
P1	Evaluación de los riesgos ciberfísicos de los dispositivos energéticos basados en el IoT en las operaciones de la red.	2020	[Cardenas et al., 2020]
P2	Aplicaciones del IoT, retos de seguridad, ataques, detección de intrusiones y visiones de futuro: Una RS.	2021	[Mishra and Pandya, 2021]
P3	Vulnerabilidad en la seguridad del internet de las cosas	2021	[Cárdenas et al., 2020]
P4	Investigación del efecto de la seguridad y la privacidad en el comportamiento de compra de dispositivos IoT.	2021	[Ho-Sam-Sooi et al., 2021]
P5	Un estudio sobre las plataformas de IoT: Perspectivas de comunicación, seguridad y privacidad.	2021	[Babun et al., 2021]
P6	Los retos de IoT en materia de seguridad, ética, privacidad y legislación.	2021	[Karale, 2021]
P7	Estudio de problemas y soluciones de seguridad en el Internet de las cosas IoT.	2021	[Rekha et al., 2021]
P8	Evolución futura de la normalización del ciberriesgo en la Internet de las cosas IoT.	2020	[Radanliev et al., 2020b]
P9	Ciberriesgo de IoT: un análisis holístico de los marcos de evaluación del ciberriesgo, los vectores de riesgo y el proceso de clasificación del riesgo.	2020	[Kandasamy et al., 2020]
P10	Análisis estático para descubrir las vulnerabilidades de IoT.	2020	[Ferrara et al., 2020]
P11	Evaluación de las amenazas a la seguridad de las aplicaciones basadas en el IoT.	2020	[Anand and Sharma, 2020]
P12	Riesgo cibernético en el mundo de la IoT.	2020	[Alharbi et al., 2020]
P13	Riesgo cibernético en los sistemas de IoT.	2019	[Petar et al., 2019]
P14	De la Internet de las amenazas a la IoT: Una arquitectura de ciberseguridad para hogares inteligentes.	2019	[Augusto-Gonzalez et al., 2019]
P15	Amenazas de IoT para la red inteligente: Un marco para analizar los riesgos emergentes.	2019	[Cardenas and Hahn, 2019]
P16	Seguridad de IoT: Una revisión de la arquitectura y las capas de ciberseguridad.	2019	[Ali and El-Medany, 2019]
P17	El valor de los datos personales en IoT: Perspectivas de la industria sobre las concepciones de valor de los consumidores.	2019	[Burgess et al., 2019]

Sigue en la página siguiente.

Estudio Primario	Titulo	Año	Referencia
P18	Anatomía de las amenazas al IoT.	2019	[Makhdoom et al., 2019]
P19	Interoperabilidad de IoT: Consideraciones de seguridad y desafíos en la implementación.	2018	[Reeves and Maple, 2018]
P20	Evaluación de los riesgos de seguridad en los sistemas de la Internet de las cosas.	2017	[Nurse et al., 2017]

Tabla 3.8: Formato extracción de documentos de estudios existentes.

Fuente: Elaboración propia

Seguidamente de haber realizado la búsqueda como indica el protocolo de Kitchenham, se consigue un total de 20 estudios primarios. Utilizando la tabla 3.7 en la metodología, se extrajo la información relevante para este estudio, con la finalidad de continuar con el análisis de los datos.

3.4. Consideraciones Finales

Las revisiones sistemáticas se caracterizan por tener y describir el proceso de elaboración transparente y comprensible para recolectar, seleccionar, evaluar críticamente y resumir toda la evidencia disponible de una forma relevante para este estudio.

Como se puede observar en la secciones anteriores, existen diferentes procesos, cada una con sus características diferentes a la otra. La revisión sistemática proporciona un metodo para recopilar y analizar varios trabajos o estudios, utilizando las mejores fuentes de informacion posibles.

Capítulo 4

Análisis

4.1. Consideraciones Iniciales

En la sección 4.2, se presentara el desarrollo de la comparativa obtenida de los artículos analizados que tienen por objeto el Internet de las cosas (IoT), como son las amenazas a la seguridad en las aplicaciones del IoT, marcos, metodologías, sistemas y modelos de ciberriesgo, tipos de riesgos y normas IoT. En la sección 4.3, se presentara la discusion relacionado al tema de investigación. En la sección 4.4, son presentadas las consideraciones finales.

4.2. Desarrollo de la comparativa

A continuación, se presenta la síntesis obtenida de los artículos analizados y organizados a través de tablas, las cuales resumen los datos relacionados con el tema de investigación, así como las preguntas planteadas anteriormente. De este modo, en la tabla 4.1 se extraen datos iniciales de los estudios seleccionados para determinar el tema estudiado y su relación con la investigación, así como los la descripción empleados en dichos artículos.

Estudio Primario	Tema estudiado	Descripción
P1	Ataques a la red del IoT.	Evaluación de riesgos a través del Modelo eléctrico de Western Electricity Coordination Council (WECC) junto con estadísticas operativas de Recursos energéticos distribuidos (DER) en el IoT. Asimismo, el modelo lógico reproduce la interconectividad a nivel de dispositivo y la interacción de los componentes de software que se encuentran dentro de estas arquitecturas para comprender la viabilidad de los ataques coordinados, mientras que el modelo físico se utiliza para evaluar el impacto de ataque en la red.
P2	Analiza los ataques DDoS.	Revisión sistemática que compara los modelos de detección y prevención de intrusiones para mitigar los ataques DDoS.
P3	Discute sobre la seguridad y vulnerabilidades del IoT.	Revisión bibliográfica que analiza elementos como la privacidad, seguridad y vulnerabilidad.
P4	Efecto de la seguridad y la privacidad en el comportamiento del consumo de dispositivos IoT.	Este artículo realizó un estudio cuantitativo y otro cualitativo, con el fin de analizar los efectos de factores como la seguridad, funcionalidad y el costo de estos dispositivos.
P5	Estudio sobre la comunicación, seguridad y privacidad.	Este documento realizó un análisis de las plataformas de IoT hacia diferentes dominios de aplicación, estableciendo un marco de evaluación que tiene en cuenta siete criterios de comparación técnica diferentes: diseño de la topología, lenguajes de programación, soporte de terceros, soporte de protocolos extendidos, manejo de eventos, seguridad y privacidad.
P6	Estudio sobre seguridad, ética y privacidad del IoT.	El estudio realizó un análisis de los desafíos de seguridad, ética y privacidad a los que se enfrentan los usuarios comunes y examina las leyes, normas actuales y emergentes de la IoT promulgadas por los gobiernos de diferentes países para combatir las vulnerabilidades de esta tecnología.
P7	Discute sobre los problemas de seguridad de IoT y soluciones.	Este estudio analizó la seguridad de IoT con énfasis en la privacidad de la información, la conducta profesional, la honestidad, cifrado, detección de intrusiones y la capacidad de reconocimiento, así como la versatilidad, interoperabilidad y usabilidad de esta tecnología.
P8	Evaluación de riesgos cibernéticos existentes.	El artículo presentó un nuevo modelo que incluye un proceso de diseño con nuevos vectores de evaluación de riesgos, específicos para el ciberriesgo de IoT a través de la revisión de la literatura, el estudio comparativo, el análisis empírico, teórico y epistemológico de estudios de casos.

Sigue en la página siguiente.

Estudio Primario	Tema estudiado	Descripción
P9	Evaluación de Amenazas, Activos y Vulnerabilidades Operacionalmente Críticas.	Este estudio realizó una revisión de las metodologías empleadas en la evaluación de riesgos cibernéticos existentes y su adecuación a los sistemas IoT.
P10	Análisis de las Vulnerabilidades relacionadas al enfoque OWASP.	Este estudio discutió la relación entre las vulnerabilidades y las que menciona la lista OWASP Top 10.
P11	Se discute sobre las amenazas relacionadas a la seguridad y privacidad en aplicaciones de IoT.	Este documento estudió las principales amenazas relacionadas con la privacidad y la seguridad de las aplicaciones basadas en la IoT y ofrece detalle de las técnicas que pueden ayudar a mejorar la seguridad en este tipo de aplicaciones.
P12	Evalúa de seguridad y privacidad del IoT.	El artículo analizó los problemas actuales de seguridad y privacidad en los dispositivos IoT y proponer recomendaciones para la solución de los problemas de ciberseguridad en los dispositivos IoT.
P13	Discute la gestión de riesgos de IoT.	El artículo evalúo la gestión del riesgo de IoT para dar una respuesta a la recuperación de incidentes.
P14	Estudia el marco de seguridad GHOST para la seguridad del IoT.	En este artículo presentó un estudio del marco de seguridad GHOST para los hogares inteligentes basados en IoT, con el propósito de abordar los retos de seguridad, los cuales plantean varios tipos de ataques, como los de red, de dispositivos y de software.
P15	Análisis de los riesgos asociados al empleo del IoT.	En este trabajo realizó un análisis de las amenazas en los despliegues de IoT que podrían suponer un riesgo para el funcionamiento de la red debido a su rápida capacidad de cambio.
P16	Estudio sobre los aspectos relacionados con la privacidad a través del empleo del IoT.	En este artículo efectuó un estudio de la privacidad, sus aspectos y significados para obtener una definición clara de los tipos y formas en que se invade o viola la privacidad.
P17	Evaluación de acerca de la perspectiva del valor de los datos personales relacionada al uso del IoT.	Este estudio realizó una evaluación con las partes interesadas de la industria de la IoT para explorar sus perspectivas sobre las concepciones de los consumidores sobre el valor de los datos personales y dicha tecnología, con el propósito de conocer la perspectiva de industria y los consumidores en cuanto a la comprensión de lo que son los datos personales, su control y el valor de estos, así como la necesidad de una mayor educación y transparencia para los consumidores.

Sigue en la página siguiente.

Estudio Primario	Tema estudiado	Descripción
P18	Estudio sobre las amenazas del IoT enfocado en ataques de Malware.	Este artículo se basó en analizar las amenazas conocidas en las distintas capas de la arquitectura de la IoT, centrándose en la anatomía de los ataques de Malware.
P19	Estudio sobre problemas en la seguridad del IoT.	Este documento examinó el panorama de las normas y orientaciones, los retos de seguridad que se presentan y la dificultad para garantizar su cumplimiento, además examina los problemas que se plantean en la aplicación y propone recomendaciones para la interoperabilidad en la IoT.
P20	Estudio sobre los enfoques actuales relacionados a los riesgos del IoT.	Este artículo analizó las razones por las que los enfoques actuales de evaluación de riesgos no son adecuados para el IoT, destacando la necesidad de nuevos enfoques o adaptaciones para apuntalar la confianza en los sistemas basados en el IoT.

Tabla 4.1: Comparación detallada de los estudios primarios en el ámbito de la seguridad de IoT

Fuente: Elaboración propia

4.2.1. Amenazas a la seguridad en las aplicaciones del IoT

Existen amenazas que pueden comprometer a la seguridad del IOT, entre las encontradas en los artículos analizados se puede mencionar la que afectan la arquitectura de los sistemas como lo representan: la capa de información, capa de middleware, capa de red y la capa de percepción. A continuación, se analiza algunas de las amenazas y problemas más comunes asociados a cada una de estas capas encontrados en el estudio primarios examinados:

En la capa de percepción

Es la capa sensorial de IoT, donde está distingue su alrededor, recibe datos del mundo físico e interactúa con el mismo. Es por ello que, algunos de los sensores más populares son los sensores de cámara, los sensores de humedad, los sensores de temperatura, los sensores químicos, los sensores de detección, entre otros. En esta capa se utilizan tecnologías como *Wireless Sensor Network* (WSN), Sistema de Posicionamiento Global - *Global Positioning System* (GPS), Identificación por radiofrecuencia - *Radio Frequency Identification* (RFID), entre otros. Esta capa es propensa a los ataques que involucran a los nodos de los sensores, a las escuchas, entre otros ataques y que seguidamente se enumeran:

Ataque de inyección de código: Los software de los nodos de IoT se actualizan en el aire, lo que da a cualquier perpetrador la oportunidad de inyectar un código malicioso que puede conducir a acciones no deseadas y a acceder a niveles no autorizados del sistema.

Ataques al arranque: Todos los servicios de seguridad se activan cuando un dispositivo está en modo de trabajo. Pero en el momento de la puesta en marcha o durante el arranque, los hackers pueden atacar los dispositivos de los nodos. Los dispositivos de borde, al ser de baja potencia, tienen un ciclo constante de sueño-despertar y son más vulnerables a estos ataques.

Captura de nodos: En este tipo de ataque, un asaltante adquiere un nodo en un sistema y lo sustituye por su propio nodo como un topo en un sistema que le da acceso a partes o incluso a todo el sistema.

Escuchar a escondidas: Los intrusos pueden sentarse en la red con la intención de escuchar y observar los datos cuando se transmiten entre los diferentes nodos de la red.

Ataques de canal lateral - *Side-Channel Attack* (SCA): Los datos sensibles pueden filtrarse a través de los chips incrustados en los procesadores, entre otros., por medio de innumerables ataques de canal lateral, como los ataques electromagnéticos, de sincronización, entre otros.

Ataques Jamming: El ataque de interferencia es una de las graves amenazas para las redes de sensores inalámbricos Wireless Sensor Networks (WSN) que utilizan el estándar IEEE 802.15.4. En dicho ataque, los jammers, que lanzan el ataque, pueden degradar drásticamente el rendimiento de la red al interferir en la transmisión de paquetes. Por lo tanto, el estudio del ataque de interferencia y sus contramedidas se ha convertido en un aspecto importante de la seguridad de las WSN.

En la capa de red

El papel más importante de esta capa es transferir los datos de la capa de percepción a la capa de middleware, lo que implica una variedad de ataques entre los que se pueden encontrar:

Ataque DDoS (Denegación de servicio distribuida): Como su nombre indica, la denegación de servicio, es donde un atacante envía una gran cantidad de solicitudes no deseadas a los servidores de destino, inundándolos y haciendo que el servicio no esté disponible para los usuarios.

Falsificación de RFID: La información que se transmite a través de una etiqueta RFID[1] puede ser alterada y falsificada, ya que el atacante supera la señal RFID.

Ataques de phishing: El atacante envía un correo electrónico a varios usuarios de una red IoT con la esperanza de que al menos algunos de ellos accedan a ese correo. Una vez que un usuario introduce sus credenciales en el enlace abierto a través de ese correo electrónico, el hacker ha conseguido el acceso total a la red IoT en cuestión.

Ataque Sinkhole: Se trata de una categoría de ataque de enrutamiento en la que se reenvían detalles de enrutamiento falsos a los nodos contiguos, lo que atrae una gran cantidad de tráfico de red. El ataque se genera desde el nodo que tiene ha sido comprometida por el atacante en la red. Este ataque puede ser utilizado para lanzar una variedad de otros ataques.

En la capa de middleware

Esta capa actúa como buffer y tiene dos tareas básicas: una es confirmar la autenticidad del usuario y la segunda es transferir los datos, también puede presentar una variedad de ataques entre los que se mencionan a continuación:

Ataque Man-in-The-Middle: Aquí un intruso juega el papel de hombre que finge ser el usuario legítimo de un sistema IoT, como cuando dos usuarios reales de una red se comunican entre sí cuando en realidad están en conversación directa con un hacker que está hablando con ambos y tiene el poder de controlar y manipular la comunicación.

Ataque de información privilegiada: Este es uno de los ataques más difíciles de identificar porque el autor no es otro que el miembro auténtico del sistema. El atacante puede ser un miembro actual o antiguo con un acceso genérico a los detalles y credenciales del sistema y tiene la capacidad de lanzar diferentes tipos de ataques.

Ataque de inyección SQL: Una de las amenazas más graves para cualquier sistema que puede conducir a la pérdida de datos confidenciales, el acceso no autorizado e incluso el riesgo de violación de toda la red o máquinas individuales. Un atacante inserta ciertas sentencias Lenguaje de consulta estructurada - *Structured Query Language* (SQL) maliciosas en las aplicaciones web vulnerables que tienen interfaces con las bases de datos backend.

[1]Las etiquetas RFID son un tipo de sistema de rastreo que utiliza radiofrecuencia para buscar, identificar, rastrear y comunicarse con artículos y personas. Esencialmente, las etiquetas RFID son etiquetas inteligentes que pueden almacenar una variedad de información, desde números de serie hasta una breve descripción e incluso páginas de datos. Algunas etiquetas incluyen características de seguridad criptográfica para un alto nivel de verificación y autenticación. Estas generalmente se identifican por sus frecuencias de radio: baja frecuencia (LF), alta frecuencia (HF) y ultra alta frecuencia (UHF).

En la capa de aplicación

Esta capa tiene una asociación directa con los usuarios finales y es responsable de prestar los servicios adecuados. Por lo tanto, hay muchas amenazas en juego y entre las cuales se presentan las siguientes:

Ataques de Sniffing Los paquetes de datos pueden ser capturados y los datos sensibles pueden ser extraídos usando Sniffers[2] si hay un mínimo o ningún cifrado en los paquetes de datos cuando están en transmisión.

Robo de datos Los datos o la información que recogen los sensores de los dispositivos IoT son más vulnerables cuando están en tránsito. Las personas con la intención de utilizar las credenciales para uso personal o para revenderlas al mejor postor pueden robar los datos muy fácilmente si no se siguen los protocolos de seguridad adecuados.

Ataque de interrupción del servicio La red de una aplicación se hace inaccesible a los usuarios legítimos, haciendo artificialmente que los servicios estén demasiado ocupados para acceder a ellos.

Reprogramar los ataques Un atacante puede reprogramar muy fácilmente cualquier dispositivo IoT de forma remota si su proceso de programación no está asegurado.

Seguidamente, se presenta en la tabla 4.2 un resumen donde se clasifican los artículos según los tipos de ataques analizados en cada uno de los documentos analizados previamente.

Tipo de ataque o vulnerabilidad	**Nombre del ataque**	**Capa**	**Nro. de artículos**	**REF.**
Ataques físicos	Manipulación de nodos Inyección de código malicioso Inyección de nodos maliciosos Ataque de privación del sueño Ataques Jamming	Capa de percepción	6	P1, P6, P8, P9, P10, P12
Ataques a la red	Spoofing RFID Ataque Man-in-the-middle (MITM) Acceso no autorizado a RFID Ataque Sinkhole Análisis de tráfico Ataque Sybil Espionaje	Capa de red	8	P1, P6, P7, P8. P9, P12, P10, P18

Sigue en la página siguiente.

[2]El Sniffing, es una técnica utilizada para escuchar todo lo que ocurre dentro de una red, esto se suele hacer en redes internas o de intranet, pero también se llega a ver en internet

Tipo de ataque o vulnerabilidad	Nombre del ataque	Capa	Nro. de artículos	REF.
	Flooding			
Ataques de encriptación	Ataque de canal lateral Ataque de criptoanálisis Ataque de inyección SQL Insider attack Ataque Man-in-the-middle (MITM)	Capa de software intermedio	2	P10, P11
Ataques de software	Ingeniería social Virus y troyanos Scripts maliciosos Ataque de suplantación de identidad Ataque de DoS Ataque de DDoS	Capa de Aplicación	8	P1, P2, P3, P6, P9, P12, P15, P18
Ataques de software	Ataque de lógica empresarial Ataque Zero-Day	Capa empresarial	1	P6
Vulnerabilidad	Arquitectura compleja Configuración de seguridad inadecuada Seguridad física Firmware o software inseguro	N/A	4	P1, P9, P10, P16

Tabla 4.2: Clasificación de los artículos según ataques o vulnerabilidades estudiadas

Fuente: Elaboración propia

Posteriormente, se presenta en la tabla 4.3 la recopilación de los mecanismos de seguridad implementados en cada uno de los artículos analizados.

Seguridad	Nro. de artículos	REF.
Sistema de Detección de Intrusiones (IDS) Sistema de Prevención de Intrusiones (IPS)	1	P2
Secure Boot, módulos de plataforma de confianza Autoridad única de certificados SSL Tokens de acceso REST Cifrado de extremo a extremo Autenticación de servicios de directorio Certificados individuales	4	P5, P7, P11, P12
Tecnología de encriptación	2	P7, P11
Tecnología Blockchain	4	P10,P11, P14, P20
Computación en la Niebla	1	P11

Sigue en la página siguiente.

Seguridad	**Nro. de artículos**	**REF.**
Aprendizaje automático	2	P10, P11
Informática de Borde	2	P10, P11

Tabla 4.3: Mejoras en la seguridad a través de diferentes técnicas en los sistemas de IoT.

Fuente: Elaboración propia

En la tabla 4.4 se presenta la clasificación de los artículos según el marco de riesgos de la ciberseguridad Falsificación de solicitud entre sitios - *Cross Site Request Forgery* (CSRF) analizado.

Nombre del CSRF	**Número de artículos**	**REF.**
NIST	4	P8, P9, P15, P20
OCTAVE	3	P8, P9, P20
TARA	2	P8, P9
ISO	4	P8, P9, P19, P20
COBIT 5	1	P9

Tabla 4.4: Artículos según el marco de riesgos de la ciberseguridad (CSRF)

Por otra parte, la diversidad de enfoques para la evaluación del impacto de los ciberriesgos pone de manifiesto la necesidad de normalizarlos. Según [Kandasamy et al., 2020] indica que dentro de la tabla 4.5 se hace referencia a los principios de la *Confidentiality, integrity and availability* (CIA) donde estos tres forman la piedra angular de la infraestructura de seguridad de cualquier organización que refieren a los siguientes:

- **La confidencialidad:** se refiere a los esfuerzos de una organización para mantener sus datos privados o secretos. En la práctica, se trata de controlar el acceso a los datos para evitar la divulgación no autorizada.
- **La integridad:** en el uso cotidiano, se refiere a la cualidad de que algo sea íntegro o completo, esta se trata de garantizar que los datos no hayan sido manipulados y, por lo tanto, se pueda confiar en ellos.
- **Disponibilidad:** los sistemas, las aplicaciones y los datos son de poco valor para una organización y sus clientes si no están accesibles cuando los usuarios autorizados los necesitan. En pocas palabras, la disponibilidad significa que las redes, los sistemas y las aplicaciones están en funcionamiento. Garantiza que los usuarios autorizados tengan acceso oportuno y confiable a los recursos cuando se necesitan.

Nombre del CSRF	**Propietario**	**Áreas de interés del IoT**	**Puntos fuertes**	**Debilidad**	**Industrias utilizadas/ aplicadas**	**CIA cobertura (sí/no)**	**Normas publicadas IoT**
NIST	NIST	Normas, tecnología, asociaciones, publicaciones, inteligencia de mercado y adopción por parte de los gobiernos.	Un marco más valioso en la gestión de los riesgos cibernéticos y excelente para la planificación de desastres y recuperación.	El marco está documentado, pero no es una herramienta automatizada. No hay cuantificación del riesgo.	Empresas de fabricación, seguros, sanidad, finanzas, administraciones públicas y consultoría de seguridad/riesgos.	Si	Si
OCTAVE	Octava Allegro	Activos de información de la organización.	Estandarizado. El cuestionario se dirige a explorar y clasificar las áreas de impacto de la recuperación.	No hay cuantificación del impacto del riesgo método de cálculo de la recuperación.	Hogares inteligentes, dirigido a empresas con recursos limitados.	Si	No
TARA	Intel	Análisis de susceptibilidad a las amenazas y análisis de remediación de riesgos.	Marco predictivo para las exposiciones más cruciales.	No hay cuantificación del impacto del riesgo.	Industria, seguros, sanidad y finanzas.	No	Si
ISO	ISO con 164 organismos nacionales de normalización	Global estandarización de evaluación de riesgos.	Promueve estandarización de riesgo cibernético y sigue la experiencia y los conocimientos internacionales.	Internacional estandarización en requiere un nivel de cumplimiento obligatorio.	Pequeña empresa o corporativa, gobierno o privado.	Si	Si

Tabla 4.5: Comparación de los marcos de riesgos de la ciberseguridad (CSRF).

Fuente: [Kandasamy et al., 2020]

4.2.2. Marcos, metodologías, sistemas y modelos de ciberriesgo

La mayoría de los marcos de ciberseguridad actuales aplican enfoques cualitativos para medir el ciberriesgo [NIST., 2018]. Algunos de los marcos proponen diversos métodos cualitativos, como OCTAVE, que significa Evaluación de Amenazas, Activos y Vulnerabilidades Operacionalmente Críticas y recomienda tres niveles de riesgo (bajo, medio y alto) [Caralli et al., 2007]. Asimismo, metodologías como Evaluación de amenazas y análisis de soluciones - *Threat Assessment and Remediation Analysis* (TARA) [Wynn et al., 2011], son también cualitativas y aplican una plantilla estandarizada para registrar las amenazas del sistema. También existen sistemas que combinan enfoques cualitativos y cuantitativos como la Sistema Común de Puntuación de Vulnerabilidad - *Common Vulnerability Scoring System* (CVSS) [Radanliev, 2014] que proporciona una métrica base modificada para asignar valores métricos a las vulnerabilidades reales. Asimismo, el CVSS aplica las opiniones de los expertos, presentadas en forma de afirmaciones, donde a cada afirmación se le asigna un nivel de riesgo cibernético y los cálculos se evalúan por el nivel global de riesgo de todas las afirmaciones.

Teniendo en cuenta la falta de métodos más precisos, las métricas básicas modificadas representan una herramienta útil para las evaluaciones. Por otra parte, los riesgos cibernéticos de la cadena de suministro también se evalúan con enfoques cualitativos [Radanliev et al., 2020a]. El sistema Exostar [Radanliev et al., 2018], que representa un enfoque cualitativo, proporciona puntos de orientación para evaluar el ciberriesgo de la cadena de suministro. El estado actual de madurez cibernética puede verificarse con el Modelo de Madurez de Capacidades Integrado - *Capability Maturity Model Integrated* (CMMI) [CMMI., 2022], que integra cinco niveles del Modelo de Madurez de Capacidades - *Capability Maturity Model* (CMM) original [Department of Energy, 2021] que permite alcanzar el nivel de madurez de ciberseguridad requerido, el estado cibernético actual puede transformarse en un determinado estado cibernético objetivo aplicando la guía de implementación del marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología [NIST., 2018], este enfoque de la evaluación de riesgos se basa en el marco para la mejora de la ciberseguridad de las infraestructuras críticas y sigue las recomendaciones para la evaluación cualitativa de riesgos, por ejemplo, el enfoque basado en normas o el enfoque de controles internos.

En ese mismo sentido, un enfoque ligeramente diferente para entender el riesgo, es el uso de modelos cuantitativos emergentes de ciberriesgo, como el enfoque del Instituto de Análisis de Factores de Riesgo de la Información [FAIR., 2017]. En efecto, los enfoques cuantitativos están presentes sobre todo en los modelos de ciberseguridad [RiskLens., 2022]. El enfoque *Findable, Accessible, Interoperable, and Reusable* (Encontrables, Accesibles, Interoperables y Reutilizables) (FAIR) es complementario a los marcos de riesgo existentes que se alejan deliberadamente de la modelización cuantitativa, por ejemplo, el Instituto Nacional de Estándares y Tecnología - *National Institute of Standards and Technology* (NIST) que aplica los conocimientos de los modelos cuantitativos existentes, por ejemplo, RiskLens, y Cyber VaR (CyVaR) [FAIR., 2022]. En cierto modo, FAIR complementa el trabajo del NIST y de la Organización Internacional de Normalización -

International Organization for Standardization (ISO) [ISO, 2017], que incluye normas sobre ciberriesgos. Por ejemplo, la ISO 27032 es un marco de colaboración que proporciona recomendaciones específicas para la ciberseguridad, y la ISO 27001 establece requisitos para que las organizaciones establezcan un Sistema de Gestión de Seguridad de la Información (SGSI).

Por lo tanto, solo la ISO 27031 y el NIST proporcionan recomendaciones para la planificación de la recuperación, en la que algunos de los otros marcos y modelos se han centrado menos. Un punto clave a tener en cuenta, es que la estimación del riesgo se utiliza para la planificación de la recuperación, y como tal, la estimación cuantitativa del impacto del riesgo es necesaria para tomar decisiones sobre temas como el seguro de ciberriesgo [Allodi and Massacci, 2017]. Los enfoques de evaluación cuantitativa del riesgo, como [FAIR., 2017], [RiskLens., 2022] y CyVaR [FAIR., 2022], todavía están en desarrollo. Por lo tanto, el marco en la estimación de riesgos actual "también conocido como análisis de riesgos", se basa en las escalas alto, medio, bajo "también conocido como el sistema de semáforos o sistema de colores".

Otro enfoque es el propuesto por el marco COBIT 5 IoT, como un nuevo vector de consumo de ancho de banda donde miles de sensores, o actuadores, tratando de comunicarse con un único servidor, crearán una avalancha de tráfico de datos que puede hacer caer fácilmente los servidores. En la Figura 4.1 se muestran algunos de los riesgos de la IoT, que son los datos y las aplicaciones, el entorno físico, la gestión del cambio, los proveedores y vendedores externos, los empleados internos, la seguridad y la privacidad, la infraestructura y la normativa. Es por ello, que la gestión eficaz de los riesgos de las TI ayuda a mejorar el rendimiento empresarial al vincular los riesgos de la información y la tecnología a la consecución de los objetivos estratégicos de las empresas.

Figura 4.1: Riesgos de IoT.

Fuente: Propia.

El riesgo se define generalmente como la combinación de la probabilidad de un evento y su consecuencia. Sin embargo, COBIT5 ofrece algunas prácticas recomendadas en este ámbito, como:

- Comprender los factores, los beneficios y los destinatarios desde la perspectiva del riesgo.
- Comprender los componentes de las actividades de riesgo.
- Entender cómo utilizar los escenarios de riesgo para los Fundamentos del Gobierno Empresarial de TI (GEIT).
- Entender cómo COBIT 5 para el riesgo se relaciona y se alinea con otros estándares.
- Comprender cómo usar los escenarios de riesgo para GEIT.
- Entender cómo COBIT 5 para Riesgos se relaciona y se alinea con otros estándares.

Una definición general de riesgo es la probabilidad de que no se cumplan las predicciones. Asimismo, el riesgo significa la posibilidad de un daño y una pérdida financiera como resultado del desarrollo de una actividad económica. La tabla 4.6 define el mapeo entre los riesgos asumidos en el ámbito de la IoT. Además, en la última columna de la tabla se enumeran algunas ventajas de COBIT5 en diferentes áreas según la definición de los roles y funciones [Latifi and Zarrabi, 2017].

Riesgos del IoT	**Funciones de COBIT 5**	**Las ventajas de utilizar COBIT 5**
Datos y aplicación	Establece una función de ciclo de vida de la información.	Garantiza que los datos estén protegidos y disponibles cuando y donde la empresa los necesite. Garantizar la fiabilidad de los datos. Medir el rendimiento de los datos.
Entorno físico	Implementación de medidas de seguridad física. Seleccionar y gestionar las instalaciones.	Reducción de las interrupciones de la actividad por daños a los equipos informáticos y al personal.
Gestión del cambio	Evaluar, priorizar y autorizar los cambios.	Mitigación de los riesgos negativos
Terceros proveedores y vendedores	22 acciones de mitigación	Reducción de la pérdida de datos. Disminución de los resultados de las auditorías. Optimización de costes.
Seguridad y privacidad	Apoyo a la misión de la empresa y a la consecución de los objetivos empresariales	La reducción de la complejidad aumenta la rentabilidad.

Sigue en la página siguiente.

Riesgos del IoT	**Funciones de COBIT 5**	**Las ventajas de utilizar COBIT 5**
Infraestructura	Gestión de la infraestructura y las aplicaciones.	Proporcionar una arquitectura de seguridad. Proporcionar una conciencia de seguridad. Proporcionar un desarrollo seguro.

Tabla 4.6: COBIT 5 y la alineación de IoT.

Fuente: [Latifi and Zarrabi, 2017].

GHOST - Protección de los entornos domésticos del IoT con un control de riesgos personalizado y en tiempo real.

En el contexto del mejoramiento de la seguridad de los dispositivos de IoT han surgido nuevos proyectos como GHOST cuyo objetivo principal es desarrollar una aplicación amigable, para mejorar la seguridad y privacidad en un Hogar Digital conectado a IoT, utilizando las tecnologías más avanzadas disponibles para este fin. De esta forma, Ghost contribuye a impulsar el mercado doméstico europeo de IoT, acercando los sistemas de seguridad de última generación para aplicaciones domésticas y basados en tecnologías como Blockchain o la inspección profunda de paquetes a todos los usuarios, independientemente de sus conocimientos previos [Ghost., 2022].

Esta arquitectura tratará de estimular un comportamiento de usuario amigable con la seguridad impuesto por una solución discreta y comprensible para el usuario. En el núcleo de la solución GHOST se encuentra una puerta de enlace de red doméstica inteligente, compatible con una amplia gama de tecnologías cableadas e inalámbricas. Se integrará un conjunto de servicios de seguridad habilitados por software en la puerta de enlace con la finalidad de ofrecer seguridad de nivel corporativo y a los ciudadanos comunes para uso personal en sus hogares. GHOST equipará a los consumidores con su propio conjunto de herramientas de inspección, descubrimiento y decisión de seguridad cibernética, y se plantea cambiar el paradigma de enfoque de seguridad de los flujos de datos entrantes a la conciencia y el control de los datos que salen para el entendimiento de sus usuarios [Ghost., 2022].

Asimismo, el proyecto tiene además el objetivo de aumentar el nivel y la eficacia de la automatización de los servicios de ciberseguridad existentes y mejorar la autodefensa del sistema, al tiempo que da prioridad a la apertura de la "caja negra" de la ciberseguridad a los consumidores y a la creación de confianza a través de herramientas avanzadas. De esta manera, el sistema GHOST se está llevando a cabo mediante el análisis de la infraestructura técnica y los componentes de software existentes que se corresponden con los objetivos del proyecto. Se definieron estudios de usabilidad con el objetivo de establecer modelos mentales de los usuarios finales. Esto permitió abordar de forma sistemática y eficaz el factor humano con el objetivo de facilitar a los usuarios la toma de decisiones adecuadas en relación con las cuestiones de seguridad, privacidad y el uso adecuado de la solución planteada [Ghost., 2022].

Proceso de validación de GHOST

La estrategia de validación definida para GHOST se basa en una triple visión que combina un conjunto completo de pruebas de robustez y de laboratorio; la definición específica de bancos de pruebas realistas y ensayos o pilotos en la vida real. En primer lugar, las pruebas de laboratorio se realizarán con los objetivos de reducir el número de posibles bugs y errores funcionales y de comprobar la estabilidad del hardware. Por lo tanto, Se llevarán a cabo pruebas unitarias sobre cada módulo específico de GHOST definiendo y comprobando un plan de pruebas de aceptación, que incluye pruebas de estabilidad de software y hardware. Tras esta primera fase, se utilizaron dos bancos de pruebas ya funcionales para probar a fondo la funcionalidad de la solución GHOST en un entorno controlado. Los bancos de pruebas diseñados para dos demostradores específicos de hogares inteligentes incluyeron hasta 25 dispositivos agrupados en más de 15 tipos diferentes que fueron conectados y supervisados simultáneamente por el conjunto GHOST. Para tener una visión amplia de los posibles servicios y soluciones, se han incluido en los bancos de pruebas dispositivos como cerraduras inteligentes, dispositivos biomédicos, robots de compañía o luces inteligentes basados en varias soluciones de comunicación (como 802.11, 802.15.4, Z-Wave o Bluetooth Low Energy) [Ghost., 2022].

Según [Ghost., 2022] luego de las evaluaciones efectuadas, refieren que las amenazas potenciales contra el hogar inteligente pueden clasificarse en:

- **(i)** Ataques físicos,
- **(ii)** Daños no intencionados (accidentales),
- **(iii)** Desastres (naturales/ambientales),
- **(iv)** Daños o pérdida de activos informáticos,
- **(v)** Fallos/mal funcionamiento,
- **(vi)** Apagones,
- **(vii)** Espionaje/intercepción/secuestro,
- **(viii)** Actividad/abuso malintencionado,
- **(ix)** Legal.

De todos ellos, los más importantes para GHOST son los grupos (ii), (iv), (vii) y (viii). Cada uno de estos grupos incluye una serie de amenazas que pueden aprovechar las vulnerabilidades relevantes lanzando diferentes ataques. La respuesta de GHOST cuando se enfrenta a los ataques mencionados que conllevan mayores riesgos y/o son más frecuentes se evalúa en el entorno controlado de los bancos de pruebas de GHOST.

Por otra parte, para [Ghost., 2022] comenta que el paradigma de IoT se ha vuelto extremadamente popular en la última década, ya que ofrece la capacidad de crear una infraestructura de red de objetos que siguen diferentes protocolos de red inalámbrica, como Bluetooth, ZigBee y Z-Wave. Por lo tanto, dado que la popularidad de IoT es cada

vez más considerable, la necesidad de proteger la seguridad de IoT se vuelve más urgente e indispensable.

En la solución GHOST, las estadísticas y las técnicas de aprendizaje automático se combinan para fortalecer la seguridad del ecosistema IoT, como se describe a continuación. Cada dispositivo IoT se comunica con la puerta de enlace, esta comunicación entre los dispositivos IoT y la puerta de enlace se registra en la solución GHOST y los datos relacionados son muy útiles para metodologías estadísticas y de aprendizaje automático avanzadas. Por lo tanto, utilizando medidas estadísticas relacionadas con el número y el tamaño de los paquetes de comunicación, junto con la realización de procedimientos estadísticos sofisticados como el Análisis de Componentes Principales, se puede extraer un comportamiento de red para cada dispositivo IoT. Por lo que, los dispositivos IoT podrían agruparse en clústeres/plantillas de comportamiento con el agrupamiento espacial de aplicaciones con ruido basado en la densidad.

El citado procedimiento constituye la fase de formación de esta metodología, mientras que la fase de seguimiento se presenta a continuación. Para cada dispositivo IoT, el tráfico de red actual "en intervalos a corto y largo plazo" se compara con el tráfico de red de su plantilla y si hay una diferencia estadísticamente significativa en el comportamiento, como se muestra en la distancia euclidiana[3] desde el centro de la plantilla, entonces se detecta una posible amenaza. Cuanto mayor sea la distancia desde el centro, más posible será detectar un ataque real y no tener una falsa alarma por parte del algoritmo [Ghost., 2022].

La tecnología IoT emergente, sin duda, requiere metodologías innovadoras para proteger la seguridad de los hogares inteligentes que consisten en muchos y diversos dispositivos IoT. Por esta razón, la solución GHOST explora el mundo de las estadísticas que ofrecen herramientas valiosas para proteger la seguridad del ecosistema IoT y garantizar a los usuarios domésticos inteligentes su privacidad y seguridad [Ghost., 2022].

4.2.3. Tipos de riesgos del IoT

El riesgo cibernético, también denominado riesgo de la tecnología de la información (TI) se define como la probabilidad combinada de un evento no deseable y su nivel de impacto. El riesgo es descrito por el NIST (National Institute of Standards and Technology) de EE. UU. [NIST., 2018]. Como una función de la probabilidad de que una determinada fuente de amenaza ejerza cualquier vulnerabilidad potencial y el impacto resultante de ese evento adverso en las organizaciones. La Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (ISO/IEC) definen el riesgo informático como la posibilidad de que una amenaza explote las vulnerabilidades de los activos y perjudique a las organizaciones [ISO, 2017].

A continuación, se presentan ejemplos de diferentes tipos de riesgos de la IoT:

- **Riesgo ético de IoT:** Se refiere a los efectos adversos imprevistos de las acciones poco

[3]Distancia euclidiana: Es la distancia ordinaria entre dos puntos de un espacio euclídeo, la cual se deduce a partir del teorema de Pitágoras.

éticas que utilizan los dispositivos de IoT. Volkswagen, una empresa de fabricación de automóviles, desarrolló e instaló un software para engañar las pruebas de emisiones de diésel. Esto violó la Ley de Aire Limpio de EE.UU., comprometió las normas de la organización y de la industria, y dio lugar a enormes pérdidas financieras y de reputación [Zhou, 2016].

- **Riesgo para la seguridad y la privacidad del IoT:** Se refiere a la explotación de las vulnerabilidades del sistema para acceder a los activos con la intención de causar daño. En octubre de 2016, la botnet Mirai (especializado malware en IoT) lanzó un ataque DDoS contra DYN que provocó la caída de partes de internet y afectó a Twitter, Netflix, CNN, Reddit y muchos otros [Antonakakis et al., 2017]. Esta categoría incluye también el riesgo de privacidad del IoT, que se refiere a la pérdida temporal o permanente del control de los datos que es perjudicial para la organización. La violación de datos de eBay que ocurrió en el mes de mayo de 2014 hizo que sus registros de clientes, incluyendo las contraseñas, fueran hackeados [Finkle and Seetharaman, 2014].

- **Riesgo técnico del IoT:** Se debe a un fallo de hardware o software debido a un mal diseño, evaluación, entre otros. Recientemente, se ha descubierto que los chips de los ordenadores personales creados en los últimos 20 años contienen fallos de seguridad a nivel de chip. Meltdown es una vulnerabilidad de hardware del microprocesador Intel $\times 86$ que permite a un método fraudulento leer toda la memoria, aunque no esté autorizado a hacerlo. Los problemas de diseño deficiente conllevan riesgos para la privacidad y la seguridad del IoT [Perekalin, 2019].

En este mismo sentido, el Proyecto abierto de seguridad de aplicaciones web - *Open Web Application Security Project* (OWASP) Top 10 se centra en los 10 riesgos más críticos para el ecosistema del IoT (Figura 4.2). La política de OWASP se refiere al Top 10 como un "documento de concienciación" que puede ser adoptado por las industrias para mejorar sus procesos de desarrollo de productos con el fin de minimizar y/o mitigar los riesgos de seguridad más críticos [Ferrara et al., 2020].

A continuación, en la Tabla 4.7 se presenta la primera versión de esta clasificación y se ha actualizado en varias ocasiones. A lo largo de los años, el OWASP Top 10 ha seguido el ritmo de los cambios del mundo de la ciberseguridad y se mantiene en continua evolución, en la que se descubren y explotan nuevas vulnerabilidades tan pronto como se detectan y solucionan las anteriores.

Figura 4.2: Los 10 riesgos más críticos de OWASP Top 10.

Fuente: [Latifi and Zarrabi, 2017].

ID	OWASP Top 10 2017 (seguridad de las aplicaciones)
A1	Inyección
A2	Autenticación rota
A3	Exposición de datos sensibles
A4	Entidades externas XML (XXE)
A5	Control de acceso roto
A6	Mala configuración de la seguridad
A7	Secuencia de comandos en sitios cruzados (XSS)
A8	Deserialización insegura
A9	Uso de componentes con vulnerabilidades conocidas

Sigue en la página siguiente.

ID	OWASP Top 10 2017 (seguridad de las aplicaciones)
A10	Registro y control insuficientes

Tabla 4.7: OWASP Top 10 2017.

Fuente: [Ferrara et al., 2020].

A continuación, en la Tabla 4.8 se resumen las categorías de las 10 principales vulnerabilidades de OWASP IoT de 2018, y su cobertura utilizando el análisis estático y que fueron encontrados en los artículos analizados.

ID	Vulnerabilidades del IoT)	Seguridad de las aplicaciones	Categoría
I1	Contraseñas débiles y difíciles de adivinar	A2	Sistema, software
I2	Servicios de red inseguros		Sistema, software
I3	Interfaces inseguras del ecosistema	A1, A2, A7	Software
I4	Falta de un mecanismo de actualización seguro		Sistema
I5	Uso de componentes inseguros o anticuados	A9	Software
I6	Insuficiente protección de la privacidad	A3	Software
I7	Transferencia y almacenamiento de datos inseguros		Sistema, software
I8	Falta de gestión de dispositivos		Dispositivo, hardware
I9	Configuración insegura por defecto		Dispositivo, hardware
I10	Falta de endurecimiento físico		Dispositivo, hardware

Tabla 4.8: OWASP Top 10 2018.

Fuente: [Ferrara et al., 2020].

Seguidamente, se presenta el Top 10 de IoT de OWASP que proporciona una clasificación genérica de vulnerabilidades al crear una lista que consiste en problemas muy críticos relevantes para los fabricantes, las empresas y los consumidores al mismo tiempo. Seguidamente, según [OWASP, 2021] describen dicha clasificación:

- **I1: Contraseñas débiles, adivinables o codificadas:**

  El uso de credenciales fácilmente forzadas, disponibles públicamente o inalterables, incluyendo puertas traseras en el firmware o en el software del cliente, que conceden acceso no autorizado a los sistemas desplegados.

- **I2: Servicios de red inseguros:**

  Servicios de red innecesarios o inseguros que se ejecutan en el propio dispositivo, especialmente los expuestos a internet, que comprometen la confidencialidad, la integridad/autenticidad o la disponibilidad de la información, o permiten un control remoto no autorizado.

- **I3: Interfaces inseguras del ecosistema:**

  La inseguridad de la interfaz web, de las APIs de apoyo y de las interfaces móviles del ecosistema del IoT aumenta la superficie de ataque del dispositivo o de sus componentes relacionados. Los problemas más comunes son la falta de autenticación/autorización, la falta de cifrado o un cifrado débil, y la falta de filtrado de entrada y salida.

- **I4: Falta de un mecanismo de actualización seguro:**

  La falta de capacidad para actualizar el dispositivo de forma segura, lo que incluye la falta de validación del firmware en el dispositivo, la falta de entrega segura "sin cifrar en tránsito", la falta de mecanismos anti retroceso y la falta de notificaciones de cambios de seguridad debido a las actualizaciones.

- **I5: Uso de componentes inseguros o anticuados:**

  Uso de componentes o bibliotecas de software obsoletos o inseguros que podrían permitir que el dispositivo se viera comprometido. Esto incluye la personalización insegura de plataformas de sistemas operativos y el uso de componentes de software o hardware de terceros procedentes de una cadena de suministro comprometida.

- **I6: Insuficiente protección de la privacidad:**

  Información personal del usuario almacenada en el dispositivo o en el ecosistema que se utiliza de forma insegura, inadecuada o sin permiso.

- **I7: Transferencia y almacenamiento de datos inseguros:**

  Falta de cifrado o de control de acceso a los datos sensibles en cualquier lugar del ecosistema, incluso en reposo, en tránsito o durante el procesamiento.

- **I8: Falta de gestión de dispositivos:**

  Falta de soporte de seguridad en los dispositivos desplegados en la producción, incluyendo la gestión de activos, la gestión de actualizaciones, el desmantelamiento seguro, la supervisión de sistemas y las capacidades de respuesta.

- **I9: Configuración insegura por defecto:**

  Los dispositivos o sistemas se entregan con una configuración por defecto insegura o no tienen la capacidad de hacer que el sistema sea más seguro, restringiendo a los operadores la posibilidad de modificar las configuraciones.

- **I10: Falta de endurecimiento físico:**

  La falta de medidas de endurecimiento físico, que permite a los potenciales atacantes obtener información sensible que puede ayudar en un futuro ataque remoto o tomar el control local del dispositivo.

4.2.4. Normas IoT

Según [Karale, 2021] manifiesta que con el desarrollo del IoT, sus usuarios y fabricantes se preocupan cada vez más por garantizar la seguridad de las personas, los sistemas, los dispositivos, los canales de transmisión de datos, entre otros. Además de la protección física, es necesario garantizar la seguridad de todo el IoT. Para ello, es necesario desarrollar normas en este ámbito y llevar todos los requisitos de seguridad a una única forma universal. Las normas proporcionan a las personas y a las organizaciones una base para la comprensión mutua de la IoT. Las que más contribuyen a este campo son la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI), la Unión Internacional de Telecomunicaciones (UIT) y la Asociación de Normas del IEEE (IEEE-SA). La creación y el uso de la IoT desde diferentes puntos de vista, incluida la garantía de la IoT. A continuación, se presentan en las normas adoptadas en 2012-2018 que se muestran resumidas en la tabla 4.9.

ISO/IEC		
N°	**Estándar**	**Descripción**
1	ISO/IEC 20924:2018 (definición y vocabulario de IoT)	Este documento delimita el Internet de las cosas y proporciona las definiciones y los términos pertinentes que forman la base del IoT.
2	ISO/IEC 21823-1:2019 (Interoperabilidad para sistemas de IoT - Parte 1: Marco)	Ofrece un resumen de la interoperabilidad de los sistemas de IoT, así como un marco de trabajo.
3	ISO/IEC 22417:2017 (casos de uso de IoT)	Identifica casos y escenarios de uso de IoT que se basan en aplicaciones y necesidades de la vida real.
4	ISO/IEC 29161:2016 (Identificación única para el IoT)	Indica las reglas comunes relevantes para la identificación única de cualquier objeto virtual o físico para garantizar la compatibilidad entre varias identidades.
5	ISO/IEC 29181-9:2017 (Red del futuro - Planteamiento del problema y requisitos, Parte 9: Conexión en red de todo)	Describe un modelo conceptual de Networking of Everything (NoE) y sus atributos generales que pueden aplicarse a las futuras redes desde el punto de vista del IoT.
6	ISO/IEC 30141:2018 (arquitectura referencia de IoT)	Proporciona una arquitectura de referencia de IoT normalizada que utiliza técnicas comunes.
UIT		
N°	**Estándar**	**Descripción**
1	Y.4000/Y.2060 (Visión general de la IoT)	Destaca la futura estandarización de la IoT. Seguridad genérica y explícita, también habla de las capacidades.
2	Y.4050/Y.2069 (Términos y definiciones para la IoT)	Indica los términos y definiciones pertinentes aplicables a la IoT para explicar las actividades relacionadas con esta.

Sigue en la página siguiente.

N°	Estándar	Descripción
3	Y.4100/Y.2066 (Requisitos comunes de la IoT)	Proporciona requisitos funcionales para la recopilación y el intercambio de información, procesamiento, manipulación y ordenación de los servicios.
4	Y.4103/F.748.0 (Requisitos comunes para las aplicaciones de la IoT)	En este documento se incluye una lista de requisitos comunes centrados en las aplicaciones de IoT.
5	Y.4552/Y.2078 (Modelos de soporte de aplicaciones de la IoT)	Proporciona los modelos de soporte de aplicaciones configurables, adaptables y fiables con su premisa.
6	Y.4111/Y.2076 (Requisitos y marco basados en la semántica de la IoT)	Contiene necesidades de capacidades de seguridad con la utilización de tecnologías semánticas o de toma de decisiones de seguridad.
7	Y.4113 (Requisitos de la red para el IoT)	Presenta un modelo básico de la red del IoT, cualidades generales, sensores inteligentes, y las vulnerabilidades de la red.
8	Y.4453 (Marco de software adaptable para dispositivos de la IoT)	Aborda el concepto de marco de software adaptable "*Adaptive software framework* (ASF)", identifica los requisitos de alto nivel y proporciona una arquitectura funcional de referencia para los dispositivos IoT.
9	Y.4101/Y.2067 (Requisitos y capacidades comunes de una pasarela para aplicaciones IoT)	Analiza brevemente las pasarelas de IoT, junto con sus requisitos previos, capacidades, marco y casos de uso.
10	Y.4112/Y.2077 (Requisitos de la capacidad plug and play (PnP) del IoT)	Además, se describe la idea de PnP, junto con sus requisitos y componentes, también se analizan las capacidades de protección del cortafuegos, el control de acceso y la pasarela PnP.
11	Y.4401/Y.2068 (Marco funcional y capacidades de la IoT)	Describe las capacidades clave de la IoT que dependen del marco funcional de esta para satisfacer los requisitos de la norma Y.2066
12	Y.4806 (Capacidades de seguridad que apoyan la seguridad de la IoT)	Presenta los peligros para la confidencialidad, la integridad y la disponibilidad que afectan a la seguridad y sugiere métodos para mitigarlos.
IEEE		
N°	**Estándar**	**Descripción**
1	P2413 (*Architectural framework* (AF)" para el IoT)	Caracteriza el AF, incluyendo detalles de diferentes dominios del IoT y proporciona proyecto de seguridad, privacidad y protección denominada la "cuádruple" confianza de calidad.
2	ISO/IEC 21823-1:2019 (Interoperabilidad para sistemas de IoT - Parte 1: Marco)	Caracteriza una estrategia para el intercambio de información, la interoperabilidad y la seguridad de los mensajes en las redes en las que operan los dispositivos IoT. Hace uso de las capacidades de alto nivel del Protocolo Extensible de Mensajería y Presencia.

Sigue en la página siguiente.

N°	Estándar	Descripción
3	P1931.1 (AF para la facilitación de operaciones in situ en tiempo real para el IoT)	Caracteriza un AF, convenciones y APIs para proporcionar facilitación de operaciones In Situ en tiempo real o ROOF, sobre la interoperabilidad, el esfuerzo coordinado y la actividad autogestionada del sistema de IoT.
4	P2668 (Índice de madurez de la IoT: evaluación, calificación y clasificación)	Proporciona la base para medir la madurez de los dispositivos y las cosas de la IoT y define un mecanismo de evaluación mediante un valor indicador Índice de la IoT o "Indicator Value IoT Index (IDex)".

Tabla 4.9: Resumen de las normas internacionales relativas a la IoT.

Fuente: [Miloslavskaya et al., 2019].

4.3. Discusión

Según [Cardenas et al., 2020] los riesgos basados en el IoT presentes en los dispositivos representan un problema en la seguridad, por ejemplo, el aislamiento LAN-WAN puede romperse por reglas de cortafuego deficientes o por equipos vulnerables. Además, algunas tecnologías como bluetooth tienen mecanismos de seguridad limitados que pueden ser explotados si el atacante está cerca. Asimismo, algunos diseños, como las soluciones de gestión centralizada en la nube, pueden convertirse en vectores de entrada, por ejemplo, para enviar una actualización de software comprometida y sobre todo cuando esas interfaces están poco codificadas o se refuerzan débilmente.

Por otra parte, [Mishra and Pandya, 2021] indican que la evolución del IoT ha sido notable y ha allanado el camino para varios esfuerzos en el campo de la tecnología. La seguridad de la IoT desempeña un papel crucial en la progresión de la tecnología, ya que los inversores sólo avanzarán en este ámbito cuando se cumplan las medidas de seguridad más avanzadas. En general, la ciberseguridad funciona según el modelo CIA, es decir, confidencialidad, integridad y disponibilidad. Los atacantes tienden a utilizar las vulnerabilidades de los protocolos de comunicación para lanzar ataques.

En este contexto, los mismos autores destacaron que se necesitan mejores técnicas de mitigación de los ataques, ya que éstos ponen en peligro a una amplia gama de dispositivos que abarcan monitores de bebés, los juguetes inteligentes que presentan una interfaz de usuario con acceso limitado y normalmente pueden funcionar incluso después de formar parte de un ejército de botnets. Con el creciente volumen de dispositivos IoT, existe una necesidad urgente de detectar a tiempo los ataques de Botnet para eliminar los dispositivos comprometidos y a medida que casi todo lo que emplean los usuarios estará conectado a internet, por lo que la seguridad de estos dispositivos es de gran importancia.

Según [Mishra and Pandya, 2021] indican que en la literatura se encuentran dos soluciones principales para prevenir los ataques DDoS, a saber, el Sistema de Detección

de Intrusiones (IDS) y el Sistema de Prevención de Intrusiones (IPS). Además, [Cárdenas et al., 2020] comentan que debido al crecimiento y a los problemas existentes en IoT es necesaria la alianza entre empresas para crear soluciones, que permitan tener una mayor seguridad, y así, más usuarios implementen esta tecnología sin el temor a que su información sea manipulada, ya que este tema involucra a la comunidad en general.

Adicionalmente, [Karale, 2021] subraya la necesidad de una legislación globalizada sobre la IoT y de que el usuario común sea consciente de las amenazas a la seguridad, la ética y la privacidad que imponen los dispositivos modernos de la IoT, porque a medida que el número de dispositivos del IoT sigue aumentando, son blanco de un número cada vez mayor de ataques a la seguridad. Los piratas informáticos están ideando formas más complejas e innovadoras de atacar estos dispositivos para robar y manipular los datos de los usuarios.

Según lo expuesto en el párrafo anterior, el autor considera que la mayoría de las investigaciones sobre las vulnerabilidades del IoT se centran en la seguridad. Sin embargo, las soluciones propuestas en estos trabajos aún no se han aplicado en mayor medida, lo que ha provocado un aumento del número de víctimas relacionadas con la seguridad.

Al mismo tiempo, [Rekha et al., 2021] manifiestan que el IoT es una aplicación innovadora que ya ha logrado avances sustanciales en la optimización del software, en los campos profesionales y para los propios usuarios, el IoT tiene muchas ventajas y utilidades. Sin embargo, a medida que aumentan las aplicaciones y los sistemas de sensores, entre otros, no es posible ignorar la cuestión de la protección, ya que dentro de ese desarrollo también han proliferado hackeos de información.

En este sentido, los mismos autores indicaron que las vulnerabilidades hacen que las empresas realicen esfuerzos tecnológicos en el ámbito de la seguridad y aportan una transformación en el pensamiento y el impulso para desarrollar más controles de protección para asegurar la información de sus clientes, por lo tanto, es importante desarrollar e implementar aplicaciones de IoT adecuadas que puedan garantizar la integridad, seguridad y la honestidad en el empleo de dicha tecnología.

Igualmente, [Alharbi et al., 2020] comentan que la diversidad de dispositivos del IoT contribuyen a efectuar diversas tareas, lo que incrementa cada vez más su empleo en diferentes ámbitos, tanto de la industria como en el hogar, llevando a esta tecnología a ser blanco de atacantes que desean obtener información y datos privados de forma fraudulenta, por lo que estas empresas fabricantes han desarrollado sus propias metodologías de seguridad para mitigar las amenazas. Sin embargo, es de gran importancia establecer reglas universales y parámetros que les permita a estas compañías regirse por un marco en común, para evitar que las iniciativas únicamente sean aplicadas por un grupo preocupado en proporcionar seguridad a sus usuarios.

Además. [Reeves and Maple, 2018], destacan que la IoT se está desarrollando e integrando en soluciones nuevas y existentes a un ritmo vertiginoso. En combinación con los avances en la tecnología de la comunicación, el aumento de la capacidad de almacenamiento y la potencia de cálculo, tanto a nivel local como en la nube han llevado a desarrollar algoritmos cada vez más sofisticados, así como avances en el hardware, como la miniaturización, la IoT tiene el potencial de tener un impacto significativo en las vidas de

los seres humanos. Sin embargo, dada la variedad de orígenes del desarrollo de las partes del ecosistema de la IoT y cada una con sus propias normas, directrices y procesos, de distinto grado de madurez y sofisticación.

Asimismo, los mismos autores resaltaron que la integración de la IoT, ha llevado a estas empresas privadas al estudio de normas que cubren una serie de escenarios que incluyen el diseño, instalación, operación y el mantenimiento en una variedad de eventos, incluyendo ataques cibernéticos, incendios y explosiones. Para garantizar la seguridad de los activos ciberfísicos y la capacidad de recuperación en los proyectos de infraestructuras, es recomendable que las organizaciones colaboren para garantizar la interoperabilidad.

Es importante mencionar los autores destacan finalmente, que motivado a que exite una multitud de normas a tener en cuenta en los proyectos de IoT, y que algunas de ellas pueden ser tangenciales en lugar de centrales, la alineación de las normas con los procesos de la industria y el desarrollo de bibliotecas de código abierto, podrían facilitar la adopción de mayor seguridad y protección de los datos de sus clientes.

Asimismo, [Radanliev et al., 2020a] indican que a pesar del interés por estandarizar los marcos, modelos y metodologías de ciberriesgo existentes, esto no se ha hecho hasta ahora de forma generalizada a través de un organismo encargado de regularizar este tipo de dispositivos que minimicen el impacto del riesgo cibernético de los vectores de la IoT. Sin embargo, existen iniciativas aisladas que pueden representar un inicio en esa dirección que permitan definir los procesos de estandarización de los enfoques de evaluación del impacto del ciberriesgo en el IoT, lo que contribuiría al mejoramiento de la seguridad, privacidad y ética en el empleo de estos dispositivos.

Adicionalmente, [Kandasamy et al., 2020] manifiestan que el entorno de la IoT cuenta con una gran cantidad de dispositivos heterogéneos, y estos pueden ser vulnerables a los ciberataques. Los nodos de sensores, los dispositivos inteligentes y vestibles que se utilizan en el ámbito del IoT son dispositivos con recursos limitados que pueden ser afectados de diversas maneras, sino se emplean mecanismos de protección adecuados. Entre los marcos de riesgo se pueden destacar los siguientes; NIST, OCTAVE, TARA e ISO en cada uno de ellos exponen consideraciones sobre el riesgo de IoT. Por lo tanto, representa una herramienta útil para el desarrollo más seguro y adaptados a los desafíos del IoT y la seguridad.

Asimismo, [Ferrara et al., 2020] comentan que el desarrollo del IoT se ha extendido ampliamente en todos los sectores, tanto empresariales como en el hogar, y los consumidores están creando conciencia de los problemas relacionados con los posibles ataques que afectan la seguridad de quienes emplean estos dispositivos, por lo tanto han surgido iniciativas en este sentido para prevenir las vulnerabilidades de seguridad en los sistemas IoT.

Cabe destacar que, los mismos autores describen que herramientas como la Top 10 de OWASP IoT que proporciona una clasificación genérica de vulnerabilidades al diseñar un listado de problemas críticos relevantes tanto para los fabricantes, empresas y los consumidores en general, contribuyendo en gran medida a los esfuerzos por mejorar el empleo de esta tecnología que sigue creciendo cada día para proporcionar herramientas efectivas y seguras para todos los sectores que la utilizan.

Además, [Anand and Sharma, 2020] destacan que el IoT ha alcanzado gran popularidad, ya que una gran cantidad de aparatos y aplicaciones se conectan con éxito a sensores e internet, ofreciendo así nuevas formas de comunicación e interacción. Es por ello que, se han dado lugar a varios problemas de privacidad y protección que dificultan la seguridad. Como el IoT se usa comercialmente, ha abierto las puertas a los hackers y atacantes para que invadan la privacidad del público en general junto con el crimen organizado y los ciberataques.

En este contexto, los autores mencionaron que los avances en el IoT han ofrecido muchos más beneficios de los que es posible imaginar, pero, como cualquier tecnología en constante evolución, también tiene varios retos, como en términos de gestión, privacidad, identificación, eficacia energética y seguridad. En este sentido, la tarea de proporcionar la máxima seguridad es la más importante y es un tema crítico. Resumidamente, todo el concepto de IoT se basa en la idea de conectarse a internet para ejecutar las operaciones a medida que el IoT gana popularidad, el número de dispositivos asociados y las aplicaciones también crecen. Por lo tanto, es necesario definir y trabajar en un ecosistema de confianza e interoperable de la IoT en el que todas las necesidades de las entidades heterogéneas implicadas puedan satisfacerse cuidadosamente, garantizando la máxima seguridad.

Asimismo, [Petar et al., 2019] manifiestan que el diseño de un modelo holístico para la evaluación y gestión de riesgos de la IoT sigue siendo un reto y para diseñar dicho modelo, las investigaciones deberían centrarse en; el impacto económico, la ética de las máquinas, las redes de sensores, la seguridad y los equipos de IoT combinados, ya que los riesgos más generales tienen que ver con la vulnerabilidad que tienen actualmente las soluciones de IoT en relación con los ciberataques y la capacidad de dichas soluciones para establecer y mantener el derecho a la privacidad.

En este sentido, los mismos autores señalaron que, los ataques DDoS relativamente recientes que vulneraron dispositivos de IoT de funcionalidad sencilla, pero mal protegidos, como monitores de bebés con contraseñas predeterminadas que no se pueden personalizar, demuestran que, por un lado, el modelo de soluciones de IoT de bajo coste y baja seguridad no es sostenible, y que, por otro lado, las organizaciones y los individuos deben protegerse mediante colaboraciones, mayor transparencia, rediseño de los actuales dominios de responsabilidad y rendición de cuentas, entre otros elementos.

Es así como, [Cardenas and Hahn, 2019] mencionan que las empresas de servicios públicos deben comprender y abordar los nuevos riesgos que surgen tanto en la infraestructura interna como en la externa, incluidos los dispositivos de IoT que están conectados a su infraestructura. Las empresas de servicios públicos también deben reconocer que no tienen control sobre los dispositivos ubicados fuera de sus instalaciones, pero deben ser capaces de soportar el impacto de un gran centro de IoT que se comporte mal.

De igual manera, los autores destacaron que las empresas de servicios públicos también pueden colaborar con las entidades gubernamentales solicitando políticas que 1) promuevan la diversidad del mercado, 2) limiten el número de dispositivos controlados por una sola entidad, 3) establezcan marcos de análisis de riesgos que incluyan procedimientos de contingencia y mitigación. En este contexto, los estados deben establecer directrices estratégicas para abordar la ciberseguridad de la infraestructura del IoT que permitan proteger a los consumidores en el empleo de estas tecnologías.

En este mismo contexto, [Ali and El-Medany, 2019] indican que la privacidad es muy importante y con más dispositivos que capturan datos en todos los aspectos de la vida cotidiana, entonces los Gobiernos tienen que incluir nuevas leyes y los fabricantes tienen que crear nuevos mecanismos para defenderse de estos ataques o no recopilar tantos datos de los usuarios, ya que los cibercriminales siguen encontrando nuevas formas de invadir la privacidad, a través de los dispositivos IoT o utilizarlos como herramienta para lanzar ataques más avanzados. Por lo tanto, la solución propuesta por los organismos oficiales necesita ser puestas en práctica lo antes posible, motivado a la gran velocidad como esta tecnología avanza cada día.

Además, [Burgess et al., 2019] mencionan que entre las perspectivas de la industria sobre el consumidor muestran una disparidad de información entre la industria y los consumidores en torno a los riesgos y beneficios de los datos personales en la IoT, que se manifiesta como disparidades percibidas en la comprensión de cuestiones clave como la recopilación y el uso de datos personales, los derechos de los consumidores y las responsabilidades de la industria.

En este sentido, los autores destacaron la necesidad de educar a los consumidores y de aumentar la transparencia en torno al uso de los datos personales en la IoT y a las formas en que genera valor para las empresas, con el fin de mejorar la transparencia, la confianza y el valor empresarial. Por lo tanto, es importante el compromiso de las partes interesadas para garantizar la equidad, el valor y la responsabilidad de los consumidores, así como un futuro ético, innovador y competitivo para las empresas de IoT.

Al respecto, [Makhdoom et al., 2019] indican que las amenazas van desde la simple interceptación de mensajes hasta sofisticados ataques de malware, por lo que la implementación de directrices de seguridad basadas en las mejores prácticas de la industria que pueden ayudar a los organismos de estandarización de IoT a diseñar estándares mínimos de seguridad basados en los tipos de aplicaciones y dispositivos de IoT.

De esta manera, los autores señalaron que, en la actualidad, la seguridad inherente que ofrecen los protocolos de comunicación no protege contra el malware y los ataques que comprometen los nodos. Por lo que una posible alternativa se encuentre en la Blockchain que puede resolver la mayoría de los problemas de integridad de los datos de IoT debido a su capacidad para ejecutar aplicaciones distribuidas en forma de contratos inteligentes y almacenar datos en múltiples nodos.

Igualmente, [Nurse et al., 2017] manifiestan que la dinámica de los sistemas de la IoT hará que la evaluación de riesgos, mediante las prácticas actuales, sea un reto motivado a los contantes, nuevos desarrollos en este campo y los cambios en los procesos de negocio, o la inteligencia de amenazas que proporciona una visión de los nuevos ataques experimentados. Sin embargo, es probable que las evaluaciones pasen por alto riesgos que se materialicen más tarde. Por tanto, la razón por la que los enfoques de evaluación de riesgos pueden ser inadecuados para el IoT debido a la dinámica del IoT.

Otro aspecto relevante a destacar por los autores, es que al existir la variabilidad en la escala de los sistemas del IoT significa que la probabilidad de que surja un nuevo sistema entre las evaluaciones periódicas será alta. Para ser eficaz, la evaluación de riesgos tendría que ser capaz de predecir y considerar los posibles sistemas que podrían surgir

antes de la siguiente evaluación. Esto es extremadamente difícil, y los enfoques actuales no suelen exigirlo. Por lo tanto, podríamos argumentar que una extensión necesaria de la práctica actual para la IoT sería tener un elemento de evaluación para el potencial dada la dinámica de los dispositivos actualmente en uso y los que podrían conectarse.

Por otra parte, [Augusto-Gonzalez et al., 2019] manifiestan que existen nuevos enfoques en la ciberseguridad de IoT en vista de los constantes desarrollos y donde han surgido proyectos de investigación como el europeo GHOST, el cual tiene como objetivo la adopción de contramedidas eficaces para defender los ciberataques contra las pasarelas ligeras de los hogares inteligentes.

En este sentido, los autores destacaron que, el estudio se derivó de un análisis exhaustivo de las infraestructuras del IoT y de las particularidades de los entornos de los hogares inteligentes, además de las necesidades específicas de los usuarios finales que emplean estos dispositivos, por lo que este tipo de iniciativas están ayudando a mejorar los diseños y aplicaciones que garanticen la seguridad, privacidad y confiabilidad en la utilización de la tecnología de IoT.

Es así como, [Ho-Sam-Sooi et al., 2021] indican que la seguridad influye en el uso de estos dispositivos de IoT, siempre que la información relacionada con la seguridad o la privacidad se presente a los consumidores y se comunique de forma sencilla y comprensible. Además, para algunas personas la seguridad de sus datos puede ser una preocupación que sin la protección de organismos que apliquen medidas y dictaminen estándares de seguridad para la fabricación y comercialización de estos dispositivos.

En este sentido, describen los autores que es difícil hacer que algunas empresas cumplan con criterios de seguridad y mucho menos garanticen que el empleo de sus dispositivos ofrece seguridad a sus clientes, por lo que es importante que existan organismos encargados de velar por la seguridad y privacidad de los datos que se manejan en los dispositivos del IoT.

Por otro lado, [Babun et al., 2021] mencionan en su estudio realizado sobre el efecto de la seguridad y la privacidad en la decisión de utilizar dispositivos IoT y estos indicaron que la seguridad tiene un efecto notablemente fuerte en la decisión de uso de estos dispositivos. Por otra parte, la seguridad y la privacidad no es muy relevante como motivación para la utilización o no, por ejemplo, de un termostato inteligente. Sin embargo, los consumidores que son más conscientes de los riesgos de privacidad y seguridad de los servicios IoT, tienen más en cuenta la seguridad a la hora de utilizar estos dispositivos.

En este sentido, los autores destacaron la importancia de presentar una descripción fácilmente comprensible de la seguridad, lo que permite comparar fácilmente las alternativas relativas al nivel de seguridad, pero esta alternativa no siempre está presente en la descripción de los dispositivos de IoT y la información disponible tampoco es posible encontrarla en internet.

Por lo anteriormente expuesto, se puede sugerir que los organismos gubernamentales podrían incentivar a los usuarios a utilizar dispositivos más seguros y a tener en cuenta la privacidad, garantizando que se produzca dicha comunicación, lo que permitiría comparar oportunamente los dispositivos en cuanto a seguridad y privacidad. Los organismos gubernamentales podrían trabajar en pro de este objetivo, definiendo normas o legisla-

ción que describan qué información relacionada con la seguridad y la privacidad deben proporcionarse a los consumidores y cómo debe comunicarse esta información.

En este contexto, los mismos autores señalaron que debido a la inmensa complejidad del tema de la seguridad y la privacidad de la IoT, es recomendable incluir a todos los sectores del mercado, como los diseñadores y fabricantes, en el proceso de desarrollo de dicha legislación o normas. Además, los resultados del estudio indican que los consumidores que son más conscientes de los riesgos para la privacidad y la seguridad son más propensos a tener en cuenta la seguridad y la privacidad a la hora de adquirir dispositivos IoT, porque mejoran el conocimiento de los riesgos por parte de los consumidores.

Para alcanzar este objetivo, los organismos gubernamentales podrían iniciar programas de concienciación que se centren específicamente en comunicar a los consumidores los riesgos de seguridad y privacidad de los dispositivos IoT. En algunos países, estos programas han sido puestos en marcha a través de guías que pueden ser empleadas en las campañas de sensibilización en el tema de la seguridad de IoT.

4.4. Consideraciones Finales

Es importante resaltar que del análisis obtenido, los hallazgos más predominantes de esta investigación se encuentran las iniciativas de los marcos desarrollados para mitigar los riesgos de seguridad y privacidad de los dispositivos de IoT y entre los que se destacan los siguientes: NIST, OCTAVE, TARA e ISO, donde cada uno de estos focalizan diferentes consideraciones asociadas a los riesgos, representando herramientas útiles para el diseño y desarrollos mucho más seguros y ajustados a los desafíos del IoT y la seguridad.

En este mismo sentido, otro hallazgo importante en la investigación es el proyecto europeo de ciberseguridad de IoT denominado GHOST, el cual tiene como propósito la incorporación de estrategias eficientes contra los ciberataques en dispositivos de baja seguridad del IoT, por lo que este tipo de esfuerzos contribuyen en el mejoramiento del diseño y aplicaciones que aseguren la seguridad, privacidad y confiabilidad en el empleo de la tecnología de IoT.

Capítulo 5

Conclusiones y Trabajos Futuros

En la actualidad, las soluciones de IoT forman parte de casi todos los aspectos de la vida diaria, por lo que dichos dispositivos están continuamente involucrados en el monitoreo y almacenamiento de información privada y sensible, relacionados, por ejemplo, con el estado de salud, residencia, hábitos, entre otros datos, por lo que están contantemente bajo una posible amenaza de seguridad, en este documento se han analizado diversos trabajos relacionados con este tema y por los cuales se desprenden luego de la revisión sistemática las siguientes conclusiones:

En relación con los incidentes de los riesgos asociados al IoT en la protección de los datos de los usuarios, se identificaron vulnerabilidades que pueden ser empleados para atacar estos dispositivos que presentan configuraciones inseguras por defecto, empleo de componentes obsoletos e inseguros, interfaces inseguras, servicios de red inseguros, entre otros. Lo que pudiera comprometer la información que se maneja a través de estos. Sin embargo, existen iniciativas y lineamentos privados como lo representa el proyecto GHOST o marcos de trabajo como NIST, OCTAVE, TARA, entre otros. Que han permitido mitigar los riesgos asociados al empleo de estos dispositivos y favorecer a los fabricantes a adoptar mejores prácticas de seguridad en este sentido.

Adicionalmente, a la incidencia de los riesgos asociados al IoT en la protección a la intimidad de los usuarios, se concluye que existe la posibilidad de que alguien intente invadir la privacidad, a través de la vulneración a los dispositivos de IoT a pesar de que existen varios protocolos de seguridad, pero algunos dispositivos como cámaras que pueden disponer de firmware peligrosos y anticuados, los cuales permitirían un acceso por la puerta trasera que permitiría el control desde fuera.

De igual manera, estos dispositivos pueden utilizar un nombre de usuario y una contraseña predeterminadas que facilitarían el acceso algún atacante. Por lo tanto, no existe alguna garantía frente algún ciberataque, pero si se pueden minimizar estos riesgos por medio del empleo de dispositivos de empresas reconocidas en el mercado que proporcionen equipos con mejores niveles de protección ante posibles problemas de seguridad, así como la adquisición de dispositivos que permitan el cambio de credenciales de inicio de sesión, permitiendo establecer políticas de periódicas de modificación de contraseñas y que estas sean robustas. Para esto, es conveniente evitar series lógicas de números y datos familiares.

Asimismo, en la incidencia de los riesgos asociados al IoT en la protección del espionaje informático de los usuarios, se concluye que existen una gran diversidad de dispositivos de IoT dotados de sensores que pueden registrar datos, por los cuales es posible identificar patrones de comportamiento que representan un problema de seguridad al ser vulnerados por posibles ataques en la capa de percepción o la de red, sin embargo, es importante que los usuarios estén informados sobre las vulnerabilidades.

En este sentido, se destaca la importancia de disponer de herramientas necesarias basadas en la detección de posibles ataques o el empleo de conexiones VPN seguras, prevenir accesos no autorizados a los dispositivos por medio limitaciones de accesos remotos a determinada información y con la creación de niveles jerárquicos de usuarios en los equipos con el propósito mitigarlas las posibles formas de accesar de forma fraudulenta a los equipos de IoT.

Por último, en relación con plantear mejoras que ayuden a minimizar los riesgos asociados al IoT a través del uso de tecnologías descritas en el estado del arte, se concluye que, es importante que existan legislaciones que controlen la fabricación y venta de dispositivos de IoT y que los fabricantes hagan del conocimiento a los usuarios de forma transparente de cuáles son los datos que almacenan en los dispositivos y para qué los utilizan.

Por otra parte, es fundamental que los usuarios conozcan las medidas preventivas que pueden adoptar para estar protegidos ante posibles ataques en estos dispositivos y para ello existen iniciativas como la NIST, la cual describe los riesgo asociados con estos equipos o la ISO 27032 que es un marco que proporciona recomendaciones específicas para la ciberseguridad y también como la OWASP Top 10 2018 que presenta las 10 principales vulnerabilidades de la IoT y las clasifica de una forma clara y entendible para cualquier usuario que requiera de mayor información para mejorar la seguridad de estos dispositivos.

Por consiguiente, para este tipo de vulnerabilidades es relevante el desarrollo de iniciativas que fomenten estudios para analizar las vulnerabilidades y posibles ataques a los dispositivos de IoT con la finalidad de estar actualizados ante los avances tecnológicos.

5.1. Problemas Encontrados

No se encontraron problemas durante la investigación.

5.2. Recomendaciones

Por todas las razones antes mencionadas, la seguridad de los sistemas de IoT requiere un gran esfuerzo para crear soluciones específicas de IoT a la medida. La aplicación de mecanismos de seguridad tradicionales no ha producido resultados satisfactorios en relación con la seguridad de IoT. La comunidad de seguridad cibernética se ha dado cuenta recientemente de los desafíos de seguridad en el dominio de IoT y se han realizado grandes esfuerzos para producir los mecanismos y sistemas apropiados, que permitirán que

los sistemas de IoT funcionen, sin imponer amenazas de seguridad y privacidad para los usuarios finales.

Asimismo, dado el aumento previsto del número de dispositivos IoT instalados en los próximos años, es importante continuar con estudios que aporten soluciones futuras a problemas que permitan mejorar y optimizar el tema de la seguridad en el empleo de IoT como, por ejemplo: El estándar UIT Y.4806 que presenta las amenaza relacionados con la confidencialidad, integridad y la disponibilidad de IoT y sugiere métodos para mitigarlos, así como el estándar P1451-99 que especifica estrategias para el manejo de la información y la seguridad de los dispositivos de IoT.

En consecuencia, todos estos esfuerzos reflejan la preocupación de varios sectores relacionados con los dispositivos de IoT, pero es necesario conjugar todas estas iniciativas en un marco técnico y de reglamentación globalizados donde todas las empresas involucradas en el diseño y desarrollo de estas tecnologías se puedan regir en función de mejorar la seguridad y los riesgos asociados al IoT.

5.3. Trabajos Futuros

Se propone realizar una investigación con un enfoque holístico para la evaluación de riesgos de IoT. Adicionalmente, se puede investigar más sobre la seguridad y la privacidad de IoT en temas como el hardware resistente a la manipulación y el análisis de la prevención de la fuga de información.

Bibliografía

[Albataineh and Alsmadi, 2019] Albataineh, A. and Alsmadi, I. (2019). Iot and the risk of internet exposure: Risk assessment using shodan queries. *20th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2019*.

[Alharbi et al., 2020] Alharbi, H. B., Abdulrazak Baghanim, N., and Munshi, A. (2020). Cyber risk in internet of things world. In *3rd International Conference on Computer Applications Information Security (ICCAIS 2020)*, pages 1–5.

[Ali and El-Medany, 2019] Ali, H. Y. and El-Medany, W. (2019). Iot security: A review of cybersecurity architecture and layers. *IET Conference Publications, 2019(CP758)*.

[Allodi and Massacci, 2017] Allodi, L. and Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis, 37(8),*, page 1606–1627.

[Anand and Sharma, 2020] Anand, S. and Sharma, A. (2020). Assessment of security threats on iot based applications. *Materials Today: Proceedings*.

[Antonakakis et al., 2017] Antonakakis, M., April, T., Bailey, M., Bursztein, E., Cochran, J., Durumeric, Z., Alex Halderman, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., and Zhou, Y. (2017). Understanding the mirai botnet. *USENIX Association,*.

[Arateco and Lorena, 2015] Arateco, C. and Lorena, L. (2015). Seguridad informática y seguridad de la información. *In instname:Universidad Piloto de Colombia*.

[Augusto-Gonzalez et al., 2019] Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnostopoulos, M., Spathoulas, G., Giannoutakis, K. M., Votis, K., Tzovaras, D., Genge, B., Gelenbe, E., and Nijdam, N. A. (2019). From internet of threats to internet of things: A cyber security architecture for smart homes. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019-Septe*.

[Babun et al., 2021] Babun, L., Denney, K., Celik, Z. B., McDaniel, P., and Uluagac, A. S. (2021). A survey on iot platforms: Communication, security, and privacy perspectives. *Computer Networks, 192, 108040*.

[Bunawan et al., 2019] Bunawan, S. G., Aldenny, M., Setiani, D. I., and Wang, G. (2019). Architecture internet of things based on cluster housing security system using fog computing. *nternational Journal of Advanced Trends in Computer Science and Engineering, 8(6).*, page 3087–3090.

[Burgess et al., 2019] Burgess, L. C., Skatova, A., Ma, S., McDonald, R., and Maple, C. (2019). The value of personal data in iot: Industry perspectives on consumer conceptions of value. *IET Conference Publications, 2019(CP756)*.

[Caralli et al., 2007] Caralli, R., Stevens, J., Young, L., and Wilson, W. (2007). Introducing octave allegro: Improving the information security risk assessment process. *Software Engineering Institute.*

[Cardenas and Hahn, 2019] Cardenas, D. J. S. and Hahn, A. (2019). Iot threats to the smart grid: A framework for analyzing emerging risks. *ACM International Conference Proceeding Series.*, page 1–8.

[Cardenas et al., 2020] Cardenas, J., Hahn, A., and Liu, C. (2020). Assessing cyber-physical risks of iot-based energy devices in grid operations. *IEEE Access, 8,.*, page 61161–61173.

[CMMI., 2022] CMMI. (2022). What is capability maturity model integration. *Instituto CMMI, Performance Solutions.*

[Cárdenas et al., 2020] Cárdenas, D., Ropero, E., Puerto, K., Sanchez, K., Castro, S., and Ramírez, J. (2020). Vulnerabilidad en la seguridad del internet de las cosas. *Mundo Fesc, 10(19).*, page 162–179.

[Danda and Hota, 2016] Danda, J. M. R. and Hota, C. (2016). Attack identification framework for iot devices. *Advances in Intelligent Systems and Computing, 434.*, page 505–513.

[Department of Energy, 2021] Department of Energy, U. (2021). Cybersecurity capability maturity model (c2m2).

[Derawi and Zhang, 2016] Derawi, M. and Zhang, H. (2016). Internet of things in real-life—a great understanding. *Lecture Notes in Electrical Engineering, 348.*, pages 337–350.

[FAIR., 2017] FAIR. (2017). Quantitative information risk management. *The FAIR Institute.*

[FAIR., 2022] FAIR. (2022). What is a cyber value-at-risk model?. *The FAIR Institute.*

[Faried and Fajardo, 2017] Faried, F. and Fajardo, F. (2017). Plan de contingencia ante ciberataques. *Escuela Superior PolitéCnica Del Litoral.*

[Ferrara et al., 2020] Ferrara, P., Mandal, A. K., Cortesi, A., and Spoto, F. (2020). Static analysis for discovering iot vulnerabilities. *International Journal on Software Tools for Technology Transfer 2020 23:1, 23(1)*, page 71–88.

[Finkle and Seetharaman, 2014] Finkle, J. and Seetharaman, D. (2014). Cyber thieves took data on 145 million ebay customers by hacking 3 corporate employees. *Business Insider India.*

[Ghost., 2022] Ghost. (2022). Ghost | the project.

[Granjal et al., 2015] Granjal, J., Monteiro, E., and Sa Silva, J. (2015). Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys and Tutorials, 17(3)*, page 1294–1312.

[Ho-Sam-Sooi et al., 2021] Ho-Sam-Sooi, N., Pieters, W., and Kroesen, M. (2021). Investigating the effect of security and privacy on iot device purchase behaviour. *Computers y Security*.

[ISO, 2017] ISO (2017). Iso - international organization for standardization.

[Kandasamy et al., 2020] Kandasamy, K., Srinivas, S., Achuthan, K., and Rangan, V. P. (2020). Iot cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security 2020,2020:1.*, pages 1–18.

[Karale, 2021] Karale, A. (2021). The challenges of iot addressing security, ethics, privacy, and laws. *Internet of Things, 15, 100420*.

[Kitchenham, 2007] Kitchenham, B. (2007). Guidelines for performing systematic literature reviews in software engineering. *Software Engineering GroupSchool of Computer Science and Mathematics*.

[Latifi and Zarrabi, 2017] Latifi, F. and Zarrabi, H. (2017). A cobit5 framework for iot risk management. *International Journal of Computer Applications, 170(8),*, page 975–8887.

[Makhdoom et al., 2019] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., and Ni, W. (2019). Anatomy of threats to the internet of things. *IEEE Communications Surveys and Tutorials, 21(2)*, page 1636–1675.

[Microsoft, 2021] Microsoft (2021). Introduction to the azure internet of things (iot) `https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-introduction/`.

[Miloslavskaya et al., 2019] Miloslavskaya, N., Nikiforov, A., Plaksiy, K., and Tolstoy, A. (2019). Standardization issues for the internet of things. *Advances in Intelligent Systems and Computing, 931,*, page 328–338.

[Mishra and Pandya, 2021] Mishra, N. and Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*.

[NIST., 2018] NIST. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. *Cybersecurity Framework*.

[Nurse et al., 2017] Nurse, J. R. C., Creese, S., and De Roure, D. (2017). Security risk assessment in internet of things systems. *IT Professional, 19(5)*, page 20–26.

[OWASP, 2021] OWASP (2021). The owasp internet of things `https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf/`.

[Pathak and Bhandari, 2018] Pathak, N. and Bhandari, A. (2018). Understanding the internet of things and azure iot suite. *In IoT, AI, and Blockchain for .NET*, page 25–51.

[Perekalin, 2019] Perekalin, A. (2019). Spectre and meltdown vulnerabilities in cpus. *Kaspersky Official Blog.*

[Petar et al., 2019] Petar, R., David, D. R., Carsten, M., Jason, N., R. N., and Uchenna, A. (2019). Cyber risk in iot systems. *Preprints 2019.*

[Radanliev, 2014] Radanliev, P. (2014). A conceptual framework for supply: supply chain systems architecture and integration design based on practice and theory in the north wales slate mining industry. *University of South Wales*, page 1–375.

[Radanliev et al., 2020a] Radanliev, P., De-Roure, D., Page, K., Nurse, J., Mantilla, R., Santos, O., Maddox, L., and Burnap, P. (2020a). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity, 3(1).*

[Radanliev et al., 2018] Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., and Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry, 102*, page 14–22.

[Radanliev et al., 2020b] Radanliev, P., De Roure, D. C., Nurse, J. R. C., Mantilla Montalvo, R., Cannady, S., Santos, O., Maddox, L. T., B. P., and Maple, C. (2020b). Future developments in standardisation of cyber risk in the internet of things (iot). *SN Applied Sciences, 2(2).*

[Reeves and Maple, 2018] Reeves, K. and Maple, C. (2018). Iot interoperability: Security considerations and challenges in implementation. *IET Conference Publications,2018(CP740).*

[Rekha et al., 2021] Rekha, S., Thirupathi, L., Renikunta, S., and Gangula, R. (2021). Study of security issues and solutions in internet of things (iot). *Materials Today: Proceedings.*

[RiskLens., 2022] RiskLens. (2022). Cyber risk management platform.

[Statista, 2021] Statista (Diciembre 2021). Dispositivos conectados en el mundo 2018-2030 `https://es.statista.com/estadisticas/517654/prevision-de-la-evolucion-de-los-dispositivos-conectados-para-el-internet-de-las-cosas-en-el-mundo/`.

[Wynn et al., 2011] Wynn, J., Whitmore, J., Upton, G., Spriggs, L., Mckinnon, D., Mcinnes, R., Graubart, R., Clausen, L., and Bedford, M. A. (2011). Threat assessment and remediation analysis (tara) methodology description version 1.0. *MITRE.*

[Xiao and Watson, 2017] Xiao, Y. and Watson, M. (2017). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39(1).*, pages 93–112.

[Zhou, 2016] Zhou, A. (2016). Analysis of the volkswagen scandal possible solutions for recovery school of global policy and strategy. *UC at San Diego Prepared for Professor Peter Gourevitch Course on Corporate Social Responsibility Winter 2016.*