PRIVACIDAD DE DATOS EN APLICACIONES DE SISTEMAS IOT PARA SMART CITIES: UNA REVISIÓN SISTEMÁTICA

Pamela Hermosilla, *Miembro, Pontificia Universidad Católica de Valparaíso*, Ivo Cattarinich, *Miembro, Pontificia Universidad Católica de Valparaíso,* Ignacio Rojas, *Miembro, Pontificia* and Sebastián Berrios, *Miembro, Pontificia Universidad Católica de Valparaíso.*

***Abstract*- The Internet of Things (IoT) is a rapidly evolving technology that interconnects physical objects through communication networks, facilitating data collection and sharing for improved decision-making and efficiency across sectors. However, the extensive collection of personal data without consent raises privacy concerns and exposes individuals to data misuse. This systematic review aims to determine the most suitable technologies for the protection of personal data, identifying vulnerabilities in the application of IoT systems in the context of smart cities. To achieve this, existing literature on data privacy in IoT systems was analyzed, based on searches in the WoS and Scopus databases, and 15 relevant studies addressing different aspects of data privacy were selected. The review's findings revealed that data privacy in IoT systems is an active and evolving research area. Various techniques and approaches were found to protect data privacy in IoT environments, including the use of encryption algorithms, anonymization techniques, data transmission protocols, and location hiding solutions, among others. Finally, key considerations related to data privacy protection in the implementation of IoT systems were identified, such as the management of large volumes of data generated by IoT devices, system interoperability, and the reconciliation between privacy and data utility. This review can serve as a foundation for future research and the development of more effective solutions for protecting data privacy in IoT systems.**

Keywords: IoT, privacy, smart cities, data protection, data collection.

I. INTRODUCTION

La necesidad de crear un mundo conectado que ofrezca servicios y procesos más eficientes nos ha llevado a compartir un gran volumen de datos de forma poco consciente en determinadas situaciones. Los nuevos sistemas de organización del transporte público, el control del tráfico vehicular o la eficiencia energética en edificios, tienen como factor común la recopilación de datos personales. Los sensores que miden y controlan la actividad en las ciudades trabajan bajo el concepto de Internet de las Cosas (IoT), que recopilan información y la envían a un sistema centralizado en la nube donde se procesan y toman decisiones en tiempo real.

La tecnología IoT es utilizada como base fundamental del funcionamiento de las ciudades inteligentes o Smart Cities. Se considera a una ciudad como inteligente cuando ha integrado una infraestructura de tecnologías de información y comunicaciones (TIC), el análisis de datos y el control en tiempo real [1]. En una ciudad inteligente los dispositivos y sensores proporcionan datos que permiten conocer el comportamiento de una ciudad y los movimientos que se presentan en ésta. Un tratamiento adecuado de los datos permitiría adaptar y potenciar bienes y servicios requeridos para cubrir las necesidades de las personas. En el caso de Las Vegas, Estados Unidos, han trabajado en potenciar principalmente el ámbito del transporte, el uso de las energías, las obras áreas públicas y la seguridad, lo cual sustenta mediante la transmisión de datos por medios abiertos, realizando análisis de datos en tiempo real, lo que permite apoyar de manera eficiente y expedita la toma de decisiones oportuna. Este enfoque establece una alianza del sector público-privado, para resguardar tanto la seguridad de personas como de la información y su disponibilidad [2].

La ciberseguridad en IoT es una preocupación creciente, ya que los dispositivos IoT se conectan cada vez más a Internet. Estos dispositivos recopilan y comparten una gran cantidad de datos personales, que pueden ser vulnerables a ataques cibernéticos.

Los riesgos de ciberseguridad en IoT incluyen el robo de datos, los ataques DDoS, el acceso no autorizado, la manipulación de dispositivos y las vulnerabilidades de software. Estos riesgos pueden afectar a las personas de diversas maneras, desde la pérdida de privacidad hasta la seguridad física.

Para mitigar estos riesgos, es importante que las organizaciones que desarrollan y utilizan sistemas IoT implementen medidas de seguridad básicas, como el cifrado de

datos, la autenticación multifactor y las actualizaciones de software. También es importante que los usuarios estén informados de los riesgos de ciberseguridad y de las medidas de protección que pueden adoptarse.

Por lo cual sistemas IoT presentan riesgos de ciberseguridad que pueden afectar a las personas, desde la pérdida de privacidad hasta la seguridad física. Es importante que las organizaciones y los usuarios implementen medidas de seguridad para mitigar estos riesgos.

En Asia, en la ciudad de Seúl, en Corea del Sur, es posible apreciar una serie de iniciativas que han permitido ir incorporando TIC en distintos ámbitos de su quehacer, lo que la llevado a reconocerla como Smart Seoul Network (S-Net), este sistema se caracteriza por el acceso a Internet de todos sus ciudadanos, a través de la implantación de una banda ancha impartida por los municipios, potenciando las redes Wi-Fi de libre acceso. Se ha requerido de una infraestructura tecnológica adecuada para consolidar la integración a través de los dispositivos Long Rage (LoRa), tecnología ideada para conexiones a grandes distancias en redes de IoT en las que se necesiten sensores que no dispongan de corriente eléctrica de red [3]. A nivel sudamericano, la ciudad de Rio de Janeiro (Brasil) el plan de implementación reúne estratégicamente proyectos que fortalecen la integración de los ciudadanos y el gobierno, considerado servicios que se enmarcan en un centro de operaciones local, el que entrega monitoreo, inclusión digital, lo que se traduce en un indicador clave para conocer y medir la brecha y analfabetismo digital principalmente de los sectores más desprovisto de TIC [4]. A partir de los antecedentes presentados, no se ha observado un planteamiento claro para el tratamiento de datos y el resguardo de la privacidad de las personas, al integrar tecnologías en el desarrollo de ciudades inteligentes, lo que representa un espacio de contribución interesante en cuanto a la arquitectura tecnológica adecuada y un marco de trabajo estándar para el tratamiento de datos y la protección de la privacidad. Además, la complejidad de los sistemas de ciudades inteligentes y la rápida evolución de las tecnologías utilizadas, representan la necesidad de crear estándares de buenas prácticas entre los diferentes actores involucrados, en cuanto a la recopilación y procesamiento de los datos.

Las Smart Cities, ya sea construidas desde sus inicios o adaptadas a la tecnología actual, basan su funcionamiento en IoT, por lo que se hace necesario abordar en su diseño y planificación aspectos de privacidad, identificando los sensores que en definitiva captarán los datos, para definir las tecnologías requeridas para el resguardado de éstos. Por lo tanto, se ha planteado para esta revisión responder la siguiente pregunta que guiará el estudio, y que dice relación con determinar ¿Cómo resguardar la privacidad de los datos recopilados por los sistemas basados en IoT en una ciudad inteligente?

El propósito de esta revisión es determinar las tecnologías disponibles para la protección de los datos personales a partir de la identificación de puntos vulnerables en la aplicación de sistemas IoT. Se busca evaluar las medidas de seguridad existentes y determinar qué soluciones pueden ser aplicadas para salvaguardar la privacidad de los usuarios. Esta revisión permitirá establecer un marco de referencia para el desarrollo de estrategias de protección de datos en el contexto de los sistemas IoT, promoviendo así la confianza y seguridad en el uso de estas tecnologías. Esta revisión se centra en dar respuesta a la interrogante de investigación planteada a través de una revisión sistemática, para lo cual se han considerado como referencia 15 artículos publicados entre 2018 y 2023 en las plataformas WoS y Scopus bajo conceptos como privacidad de datos en Smart Cities, recolección de datos en sistemas IoT y protección de datos. La revisión tendrá un enfoque de análisis descriptivo el que permitirá indagar en el área de estudio y realizar una síntesis cualitativa de los aspectos más relevantes identificados. El estudio se ha organizado, en una primera parte describiendo la metodología con la cual se ha realizado esta revisión, la que considera desde la recolección y selección de artículos, basada en Prisma 2020 [5], para posteriormente llegar a la identificación de los aspectos más relevantes en el ámbito de las preguntas que han sido planteadas en este estudio. Como resultado, se entregan los aspectos significativos a considerar en la implantación de sistemas IoT enfocados en resguardar la privacidad de las personas, identificando enfoque en la privacidad desde el diseño, métodos de anonimización y control de los datos por parte de las personas.

II. METODOLOGÍA

La metodología de investigación establecida para esta revisión busca dar respuesta a las principales interrogantes que guían este estudio, las que se enmarcan en indagar y responder siguientes preguntas de investigación (PI):

- PI 1: ¿Qué sistemas IoT para Smart Cities recopilan datos personales?
- PI 2: ¿A qué tipos de riesgos se exponen las personas al interactuar con sistemas IoT?
- PI 3: ¿Qué tecnologías son utilizadas para resguardar la privacidad de los datos personales?

Se entenderá como datos personales los que se refieren a antecedentes propios de cada individuo, relacionado con el nombre y apellidos, dirección, número de documento de identidad, dirección de protocolo de internet (IP), número de teléfono, correo electrónico, orientación sexual, origen racial o étnico, datos genéticos o biométricos y geolocalización.

Para abordar adecuadamente las interrogantes planteadas, se han identificado dos etapas, la primera de ellas se enfoca en definir los conceptos claves que permitirán seleccionar el

conjunto de artículos que serán sometidos a revisión, mientras que la segunda etapa considera un análisis realizado por el equipo de investigación, para determinar los principales aspectos en materia de privacidad de datos para aplicaciones de sistema IoT. En la Figura 1 se puede apreciar la representación de la metodología de investigación propuesta, en la cual es posible identificar las etapas con sus herramientas, actividades y resultados. A partir de la indagación de los artículos revisados se establecen los aspectos relevantes de privacidad para la implantación de sistemas IoT y se plantean aspectos generales de los resultados, logrando establecer categorías para comparar alcances y aportes interpretando similitudes y diferencias.

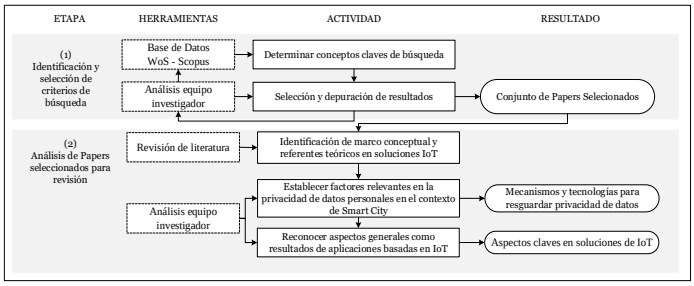

Figura 1. Metodología de Investigación

A. *Estrategia de Búsqueda*

Para la selección de los artículos científicos se utilizaron las bases de datos WoS y Scopus, realizando diversas consultas para la búsqueda de artículos que revisan los conceptos relevantes que contribuyan a responder las preguntas de investigación presentadas, y que entreguen antecedentes importantes, relacionados a la recopilación y protección de datos en sistemas IoT. Para focalizar las búsquedas a realizar, se definieron primeramente términos claves de búsquedas (TCB), los cuales se combinaron para generar las consultas de búsquedas (CB), las que finalmente guiaron la búsqueda en las bases de datos mencionadas, lo que es posible distinguir en la siguiente figura.

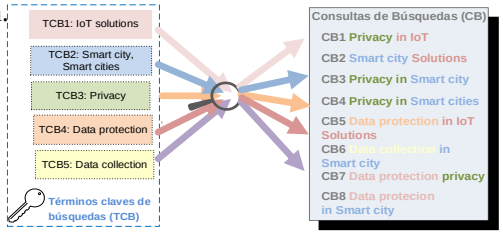

Figura 2. Términos clave de búsqueda – Consultas de búsquedas

A partir de lo anterior, para una primera iteración de búsquedas, se definieron los siguientes criterios inclusión (CI) y criterios de exclusión (CE):

CI	1	Área de conocimiento:	Computer Science Information Systems or Computer Science Artificial Intelligence or Automation Control Systems or Computer Science Hardware Architecture or Engineering Electrical Electronic or Ethics or Green Sustainable Science Technology or Information Science Library Science or Robotics or Telecommunications
CI	2	Idioma:	Inglés
CI	3	Tipo de documento:	Article, Conference papers
CE	1	Año:	<=2013 (10 años de vigencia)
CE	2	Palabras clave:	“Ethics, “law”, “laws, “legislation”

Como resultado de las primeras búsquedas, para cada uno de los sets de artículos encontrados en base de datos WoS y Scopus, se aplicó un algoritmo para eliminar los registros repetidos, no obstante, se obtuvieron cantidades de artículos superiores a las requeridas para este estudio, por lo que se aplicó un nuevo refinamiento que consideró: eliminación de artículos con utilización de encuestas, se acotó el periodo de años de 10 a 5, se excluyeron los referidos al ámbito de salud por considerarse muy específico para el objetivo de esta investigación, por otro lado se consideraron principalmente los que fueran open Access y los que contuvieran los términos security o privacy en el título.

Finalmente, aplicando estos últimos criterios de exclusión anteriormente, se ordenaron los artículos resultantes según la cantidad de citaciones de éstos, de los cuales se seleccionaron para la revisión los 15 más citados, y se dejan los primeros de 7 Scopus y los 8 primeros WoS, de tal forma de cubrir ambas fuentes de datos de forma balanceada y representativa. La Figura 2 representa el esquema general de búsqueda y selección de artículos considerados para el desarrollo de esta revisión, donde se puede apreciar el detalle de lo mencionado y las cantidades de artículos obtenidos.

B. *Categorías de Análisis*

Para llevar a cabo la revisión de los artículos seleccionados, es importante establecer las categorías de análisis que se utilizarán. Estas categorías se basarán en las preguntas que guían este estudio de investigación. El propósito de estas categorías es dirigir y estructurar el proceso de análisis, enfocándolo en la búsqueda de respuestas específicas. Esto permitirá una organización más efectiva de la información recopilada y facilitará la extracción de conclusiones relevantes.

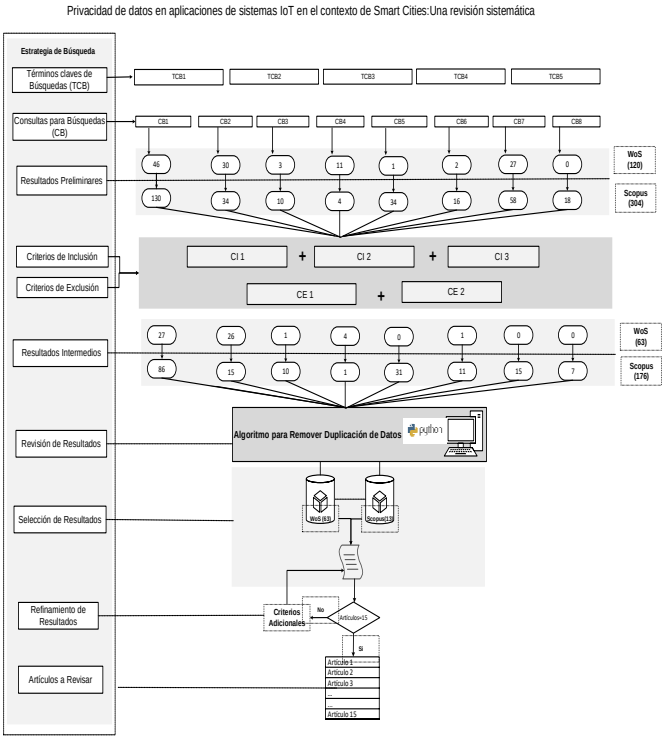

Figura 2.Estrategia de búsqueda y selección de artículos.

Se identificaron 4 categorías de análisis: aplicaciones de IoT, riesgos asociados a la recopilación de datos en sistemas IoT, tecnologías para la protección de datos y modelos de tratamiento de datos. La primera categoría busca explorar los diferentes campos de aplicación de los sistemas IoT para tener una visión general de su alcance y uso. Sin embargo, estas aplicaciones también plantean riesgos en términos de seguridad y privacidad, ya que los sistemas IoT pueden ser vulnerables a ataques cibernéticos, robo de datos personales y violaciones de la privacidad, lo cual será analizado en la segunda categoría. Por otro lado, la tercera categoría se enfoca en investigar las tecnologías disponibles para proteger los datos recopilados y transmitidos por los dispositivos IoT, como técnicas de cifrado, autenticación, control de acceso y gestión de claves. Por último, la cuarta categoría aborda la necesidad de establecer modelos de tratamiento de datos que permitan a los usuarios tener un mayor control sobre su información, garantizando un uso adecuado de los datos recopilados. Estos modelos consideran tecnologías para resguardar la privacidad de los datos en los dispositivos IoT, así como en su transmisión, almacenamiento y posterior procesamiento. Lo anterior se representa en el esquema de la siguiente figura.

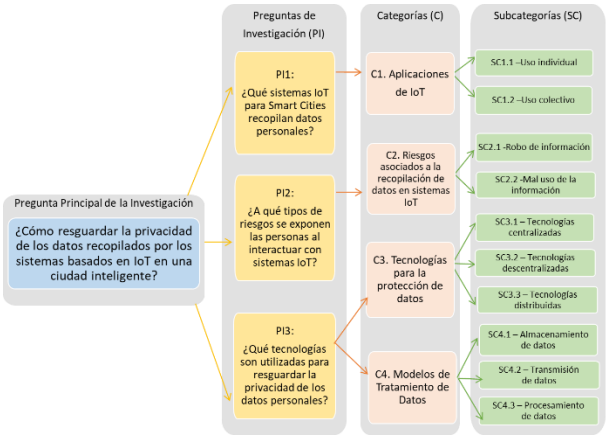

Figura 3. Esquema de categorías y subcategorías según preguntas de investigación.

III. RESULTADOS

En esta sección se presentarán inicialmente los resultados en cuanto a las características generales de los artículos revisados, de forma de tener una visión general de la cobertura demográfica y temporal de lo abordado en esta revisión. Posteriormente, se señalarán los principales hallazgos identificados a partir del análisis de las categorías mencionadas previamente, estableciendo además aspectos transversales en lo revisado, en cuanto a las subcategorías identificadas. Finalmente, se entregará una síntesis de este apartado, señalando lo más relevante de los hallazgos de esta investigación.

A. Principales características de artículos seleccionados

En este apartado se muestran los principales resultados de los 15 artículos sometidos a revisión en este estudio [6-20] **¡Error! No se encuentra el origen de la referencia.**, para lo cual se identificó inicialmente sus principales características, luego se describen los hallazgos más relevantes acorde a las categorías de análisis definidas anteriormente. Finalmente se entrega una síntesis del resultado de esta investigación.

TABLA 1: Listado de papers revisados

ID	Título	Autor	País/Año
[6]	Protecting Location Privacy in IoT Wireless Sensor Networks through Addresses Anonymity	Zhang Q., Zhang K	China/ 2022
[7]	Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments	Wu T.-Y., Meng Q., Kumari S., Zhang P.	China/ 2022
[8]	Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hash Function	Khanal Y.P., Alsadoon A., Shahzad K., Al-Khalil A.B., Prasad P.W.C., Ur Rehman S., Islam R.	Australia/ 2022
[9]	Realizing Efficient Security and Privacy in IoT Networks	Anajemba, JH; Tang, Y; Iwendi, C; Ohwoekevwo, A; Srivastava, G; Jo, O	China/ 2020
[10]	Method to implement K-NN machine learning to classify data privacy in IoT environment	OahtanMakki Shallal1, ZaidAlaa Hussien2, Alaa Ahmed Abbood3	IRAQ/ 2020
[11]	A Trust-based Security System for Data Collecting in Smart City	Weidong Fang, Ningning Cui, Wei Chen, Member, Wuxiong Zhang Yunliang Chen	China/ 2020
[12]	Searchable Encryption Scheme for Personalized Privacy in IoT-Based Big Data	Shuai Li, Miao Li, Haitao Xu * and Xianwei Zhou	China/ 2019
[13]	Authentication and Key Management in Distributed IoT using Blockchain Technology	Soumyashree S Panda, Debasish Jena, Bhabendu Kumar Mohanta, Somula Ramasubbareddy, Mahmoud Daneshmand and Amir H. Gandomi	India/ 2021
[14]	A Regulatory View on Smart City Services	Mario Weber 1, and Ivana Podnar Zarko 2	Croacia/ 2019
[15]	Security and privacy for mobile iot applications using blockchain	Carvalho K., Granjal J.	Portugal/ 2021
[16]	An efficient dummy-based location privacy-preserving scheme for internet of things services	Du Y., Cai G., Zhang X., Liu T., Jiang J.	China/ 2019
[17]	Smart City IoT Services Creation Through Large-Scale Collaboration	Cirillo, F; Gomez, D; Diez, L; Maestro, IE; Gilbert, TBJ; Akhavan, R	Italia/ 2020
[18]	A Methodological Framework for the Selection of Key Performance Indicators to Assess Smart City Solutions	Angelakoglou, K; Nikolopoulos, N; Giourka, P; Svensson, IL; Tsarchopoulos, P; Tryferidis, A; Tzovaras, D	Grecia/ 2019
[19]	Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures	Jo, JH; Sharma, PK; Sicato, JCS; Park, JH	Corea/ 2019
[20]	MicroServices Suite for Smart City Applications	Badii, C; Bellini, P; Difino, A; Nesi, P; Pantaleo, G; Paolucci, M	Italia/ 2019

Realizando un análisis preliminar de las palabras clave de los artículos identificados en la **¡Error! No se encuentra el origen de la referencia.**, se tiene el siguiente esquema de red Figura 4, realizado con la herramienta VOSviewer, el que permite identificar nodos como los elementos principales y los enlaces de cómo se relacionan entre ellos

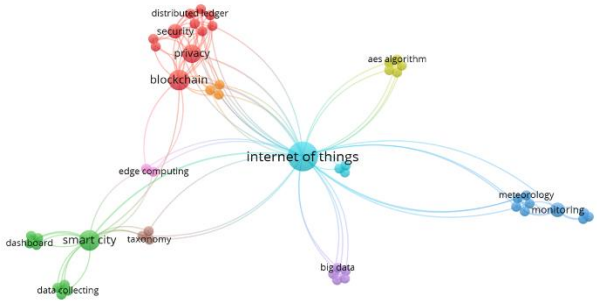

Figura 4. Esquema de red para palabras clave de los artículos seleccionados.

El esquema de red de esta investigación permite visualizar que los principales aspectos abordados por los artículos son: internet of things, smart city, blockchain y privacy, lo que se relaciona directamente con las categorías identificadas y el propósito de esta investigación. La estructura de las interacciones muestra una fuerte relación del nodo central como elemento clave del tema en estudio. Además, es posible apreciar algunos grupos enfocados en aplicaciones (nodos azules a la derecha), recolección y visualización de datos asociados a smart city (nodos en verde, lado inferior izquierdo) y aspectos de protección de datos (nodos color rojo, lado superior izquierdo)**.**

Adicionalmente, se realizó un análisis de la distribución geográfica y temporal de los artículos seleccionados, siendo China el país con mayor cantidad de investigación relacionada. Este análisis permitió examinar la procedencia de los estudios y su evolución a lo largo del tiempo.

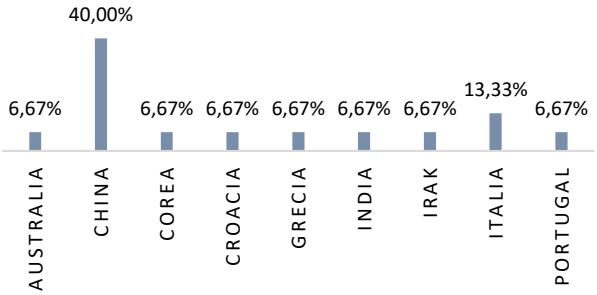

Figura 5. Gráfica distribución de los artículos según país.

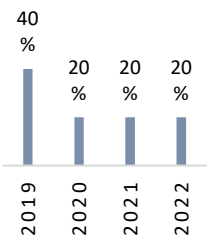

Figura 6. Gráfica distribución de los artículos según fecha de publicación.

B. Hallazgos por categorías de análisis

En esta sección se presentan los resultados y descubrimientos específicos relacionados con cada una de las categorías y subcategorías de análisis, definidas previamente. Se proporcionan los principales hallazgos relevantes, los cuales se organizan y presentan de manera estructurada para facilitar la comprensión y el análisis de los resultados.

.

B.1 Aplicaciones de IoT

✓ Aplicaciones individuales

En la revisión realizada fue posible identificar aplicaciones utilizadas en dispositivos móviles que usan los servicios de ubicación en su funcionamiento [15], las que pueden entregar información personal delicada, como la dirección particular, lugares frecuentes de visita, condiciones de salud, etc. Siguiendo el mismo concepto de aplicaciones móviles, Los autores de [9] enfocan su investigación en la protección de la transmisión de datos a través de la red celular de quinta generación (5G) y en [8] se menciona la utilización de los sistemas de geo-localización y uso de redes sociales.

Las aplicaciones de IoT (Internet de las cosas) en el contexto de las smart cities ofrecen una amplia gama de posibilidades para mejorar la eficiencia, la sostenibilidad y la calidad de vida en las ciudades [19]. Al conectar dispositivos, sensores y sistemas de información, se crea una red inteligente que permite recopilar y analizar datos en tiempo real para tomar decisiones más informadas y eficientes. Esta red de aplicaciones considera ámbitos de gobierno, transporte, servicios a la comunidad, salud, sustentabilidad con el medio ambiente, entre otras. El potencial de IoT es amplio y su implementación puede adaptarse a las necesidades específicas de cada ciudad para mejorar la calidad de vida de sus habitantes, promover la sostenibilidad y optimizar la gestión urbana.

✓ Aplicaciones colectivas

En [15] y [11] se describen algunos escenarios de aplicación específicos como es el caso de los vehículos inteligentes con capacidades de movilidad, para lo cual se implementó y evaluó experimentalmente la arquitectura y los mecanismos propuestos como una prueba de concepto. Para este caso, es necesario compartir datos relacionados con la identidad y ubicación del usuario de manera segura y privada, protegiendo la privacidad de la persona y asegurando la integridad de los datos durante la transmisión y el procesamiento.

B.2 Riesgos asociados a la recopilación de datos en sistemas IoT

✓ Robo de información

La recopilación y transmisión de datos a través de sistemas IoT en smart cities plantea riesgos significativos para la privacidad y la seguridad de los ciudadanos. A medida que los dispositivos conectados se multiplican, se recopila una gran cantidad de información personal que puede ser objeto de abuso o uso indebido [6] [7] [8] [9] [10] [11] [13] [14] [16].
Uno de los riesgos es la vulnerabilidad de los datos. La información recopilada, como la ubicación, los patrones de comportamiento y las preferencias de los ciudadanos, puede ser interceptada o accedida por personas no autorizadas. Esto podría conducir al robo de identidad, la suplantación de identidad o la exposición de información sensible. [16]
Además, los sistemas IoT en las smart cities también enfrentan riesgos de seguridad cibernética. La interconexión de dispositivos y sensores abre la puerta a posibles ataques y manipulaciones maliciosas. Los hackers pueden explotar las vulnerabilidades de seguridad para interrumpir servicios críticos, como el suministro de energía o el control del tráfico, lo que afecta la vida cotidiana de los ciudadanos. Para disminuir estos riesgos, es fundamental implementar medidas de seguridad sólidas. Esto implica adoptar prácticas de encriptación robustas para proteger los datos en tránsito y en reposo [9]. Además, se deben establecer políticas claras de privacidad que informen a los ciudadanos sobre qué datos se recopilan, cómo se utilizan y cómo pueden ejercer su derecho a la privacidad [14].

Asimismo, se requiere una colaboración estrecha entre gobiernos, empresas y expertos en ciberseguridad para identificar y abordar las vulnerabilidades en los sistemas IoT. Es esencial realizar evaluaciones periódicas de seguridad, actualizar regularmente el software y brindar educación y concienciación sobre los riesgos a los ciudadanos [18].

✓ Mal uso de la información

En los artículos analizados no se evidenció investigación asociada al mal uso de los datos personales, la mayor parte de ellos están enfocados en el robo de la información y como evitarlos, aplicando técnicas de seguridad en el almacenamiento y transmisión de los datos. Es importante considerar que para este caso el usuario del sistema IoT entrega el consentimiento de uso de la información para el objetivo en el que fue concebido, por lo tanto, se entiende por mal uso a la práctica indebida de recopilar, almacenar, procesar o divulgar información personal de los ciudadanos para fines no autorizados.

B.3 Tecnologías para la protección de datos

✓ Centralizadas

- Bloqueadores de red y mecanismos de interferencia [9]. En estos sistemas se introduce intencionalmente una señal de radiofrecuencia (RF) para distorsionar la red de transmisión, con esto, el canal de comunicación se mantiene ocupado evitando el ingreso indeseado de atacantes.
- Machine learning para métodos de encriptación según la clasificación del dato [10]. Este sistema utiliza los métodos de reconocimiento de patrones K -vecinos cercanos (K-NN, K-Nearest Neighbor) para asignar relevancia a los datos clasificándolos como de baja, media y alta sensibilidad. Este algoritmo permitirá asignar los recursos computacionales necesarios para el cifrado y descifrado de los datos haciendo el proceso más eficiente en cuanto al consumo energético.
- Edge computing, también conocido como computación en el borde, es un enfoque de procesamiento de datos y ejecución de aplicaciones en dispositivos ubicados en el borde de la red, cerca de donde se generan los datos. A diferencia del procesamiento tradicional en la nube, donde los datos se envían a centros de datos remotos para su procesamiento, el edge computing permite realizar el procesamiento y análisis de datos de manera local, lo que reduce la latencia y mejora la eficiencia en la transmisión de datos. El edge computing permite llevar la capacidad de cómputo más cerca de la fuente de datos, lo que brinda beneficios como mayor privacidad y seguridad de los datos, mayor disponibilidad de servicios y reducción de la carga en las redes de comunicación [19].

✓ Descentralizadas

- K-anonimato para aplicaciones que operan con servicios basados en la ubicación (LBS, location-based services), a través del uso de GPS integrados en distintos dispositivos de IoT. Este sistema permite asegurar que la ubicación de un usuario sea identificada con una probabilidad menor o igual a 1/k, donde k es un parámetro de anonimato. En estos esquemas, se utilizan ubicaciones ficticias o "dummy locations" que son similares a la ubicación real del usuario. Estas ubicaciones ficticias se emplean para formar conjuntos anónimos, dificultando que un atacante pueda distinguir cuál es la ubicación real del usuario dentro de dicho conjunto. Este tipo de ubicaciones presenta ventajas significativas, como no requerir complicados esquemas de cifrado y descifrado, y permitir el ahorro de recursos computacionales en dispositivos del IoT [10] [16].

- Enmascaramiento espacial es utilizada en la protección de datos y la privacidad para ocultar o anonimizar la información de ubicación geográfica, consiste en alterar o distorsionar los datos de ubicación para evitar que se pueda identificar la ubicación real de un individuo o entidad [16].

- Los algoritmos de encriptación cobran vital importancia en el tratamiento y seguridad de la transmisión de datos, como se menciona en [10] [12] es necesario cifrar los datos fuertemente para evitar ataques externos, sin embargo, el proceso de cifrado y descifrado requiere de un consumo de recursos computacionales elevados lo que conlleva a un alto consumo de energía eléctrica.

✓ Distribuidas

- Blockchain permite el anonimato de los usuarios, compartiendo información sin revelar la identidad del propietario. Un sistema de este tipo ofrece mayor resistencia a fallos individuales, donde los nodos participantes se encargan de su correcto funcionamiento y validación, lo que crea una red con propiedades de inmunidad capaces de mitigar acciones maliciosas, como la manipulación de información. Básicamente, blockchain funciona como un registro que almacena información (transacciones) en bloques interconectados de forma secuencial, formando una cadena. Esta característica permite el intercambio de activos criptográficos entre usuarios y también registra y realiza un seguimiento seguro del estado del blockchain [8] [13] [15].

- El desarrollo de una suite de microservicios para aplicaciones de Smart City utilizando Node-RED [20], que permite la creación de una amplia gama de nuevas aplicaciones IoT para ciudades inteligentes. El artículo destaca los requisitos para las aplicaciones IoT de ciudades inteligentes y presenta un conjunto de microservicios, su ámbito de aplicación y requisitos en relación con las soluciones IoT de ciudades inteligentes.

Para los aspectos mencionados anteriormente es importante tener en consideración a arquitectura de los dispositivos IoT, la cual ab abarca el diseño y la estructura de los sistemas de IoT, así como la forma en que estos sistemas interactúan entre sí y con otros servicios. Esta arquitectura se compone de diversas capas y componentes, cada uno desempeñando funciones específicas para garantizar el funcionamiento adecuado de los dispositivos IoT. Entre las principales capas de esta arquitectura se encuentran: la capa de percepción o sensor, la capa de red, la capa de middleware y la capa de aplicación [21].

- Capa de percepción o sensor

Esta capa desempeña un papel crucial al detectar, recolectar, procesar y transmitir información o datos a través de los dispositivos IoT. Estos dispositivos pueden variar en tipos, incluyendo sensores, actuadores, cámaras, micrófonos y otros. Funcionando como el puente entre el mundo físico y el digital, esta capa suministra datos que reflejan el estado y el comportamiento de objetos y su entorno [22, 23]. Además, tiene la capacidad de ejecutar ciertas funciones de procesamiento local, como el filtrado, la compresión o la agregación de datos, con el propósito de reducir la carga en la red y mejorar la eficiencia. Esta capa actúa como un enlace vital entre el mundo físico y el digital. Esta capa se encarga de la detección, recolección, procesamiento y transmisión de información a través de una variedad de dispositivos IoT, como sensores, actuadores, cámaras y micrófonos. Su función principal es proporcionar datos que reflejen el estado y comportamiento de objetos y su entorno. Además, esta capa posee la habilidad de realizar procesamiento local, incluyendo tareas como el filtrado, la compresión y la agregación de datos, lo cual es fundamental para disminuir la carga en la red y aumentar la eficiencia general del sistema. [24].

- Capa de red

Esta capa desempeña un papel fundamental al facilitar la transferencia de datos entre los dispositivos IoT y los servidores o la nube. Utiliza una variedad de medios de comunicación, ya sea a través de conexiones cableadas o inalámbricas, y se apoya en diversos protocolos de red, que pueden incluir tanto IP como otros, para establecer la conectividad y gestionar el enrutamiento de los datos [25]. Además de estas funciones esenciales, esta capa también puede realizar tareas de procesamiento intermedio, como el almacenamiento en caché, la replicación o la transformación de datos, con el objetivo de mejorar la calidad y la disponibilidad de la información [26, 27, 28].

- Capa de middleware

Esta capa, posicionada entre la capa de red y la capa de aplicación, opera como un componente de software fundamental. Su propósito es proporcionar servicios comunes y abstractos que simplifican el desarrollo e integración de las aplicaciones IoT. Dentro de su repertorio de servicios se encuentran funciones como la gestión de dispositivos, el manejo de datos, la administración de eventos, la seguridad, la identidad y el contexto, entre otros [29, 30]. Además de estas funciones esenciales, esta capa también puede llevar a cabo tareas de procesamiento avanzado, como el análisis, la minería de datos o el aprendizaje de datos, para extraer información y conocimiento valioso a partir de los datos.

- Capa de middleware

Esta capa tiene la responsabilidad de ofrecer las funcionalidades específicas de las aplicaciones de IoT destinadas a los usuarios finales. Entre las diversas aplicaciones que pueden formar parte de esta capa se encuentran la monitorización, el control, la optimización, la predicción y la automatización [31, 32, 33]. Además de estas funcionalidades clave, esta capa también puede desempeñar funciones de procesamiento final, como la visualización, la presentación y la ejecución de los datos [34]. Además, esta capa gestiona aspectos de seguridad y privacidad, asegurando que los datos de los usuarios estén protegidos y que se cumplan las regulaciones pertinentes.

B.4 Modelo de Tratamiento de datos

✓ Almacenamiento de datos

- El Modelo de Información adicional permite recopilar datos sobre las preferencias de privacidad de los usuarios, como las opciones de consentimiento, las restricciones de divulgación de datos, las preferencias de compartición selectiva, entre otros aspectos relacionados con la gestión de la privacidad [16]. Estos datos adicionales se agregan a la información personal básica para proporcionar un panorama más completo y contextual de las preferencias y requerimientos de privacidad de cada persona.

- El establecimiento de una comunidad técnica de ciudades inteligentes [12][17] minimiza los esfuerzos de implementación de nuevas soluciones, maximizando el intercambio de componentes, estandarizando los modelos de datos en una plataforma común. Se presentan metodologías para motivar a los desarrolladores a idear aplicaciones utilizando un enfoque modular, donde los componentes de una sola función que son reutilizables por otros servicios de la ciudad se empaquetan y publican como componentes independientes, llamados Atomic Services. Los servicios atómicos son componentes de una sola función que son reutilizables por otros servicios de la ciudad y se empaquetan y publican como componentes independientes [35, 36].

✓ Transmisión de datos

- MQTT (Message Queuing Telemetry Transport) [6], integra diversos componentes como protocolos de comunicación el cual utiliza un modelo de publicación y suscripción que almacena mensajes asíncronos y de tamaño pequeño, adecuados para aplicaciones IoT, además considera Storj [7] [37] una plataforma de almacenamiento distribuido que permite la eliminación y modificación de datos bajo demanda.

✓ Procesamiento de datos

- Big data analytics desempeña un papel fundamental al permitir el análisis de grandes volúmenes de datos generados en las ciudades. Las ciudades inteligentes generan una gran cantidad de datos a partir de sensores, dispositivos conectados, redes de transporte, sistemas de energía, redes sociales y otras fuentes. Estos datos pueden ser estructurados o no estructurados y contienen información valiosa sobre el funcionamiento de la ciudad, los patrones de comportamiento de los ciudadanos y las tendencias urbanas. Este análisis permite extraer conocimientos y patrones significativos de estos datos para obtener información que puede ser utilizada para mejorar la toma de decisiones en diferentes áreas [19].

- La medición de privacidad basado en entropía representa la incertidumbre de poder identificar la ubicación real del usuario a partir de un conjunto de ubicaciones ficticias. Cuanto mayor sea la entropía, más difícil será determinar la ubicación real del usuario en el conjunto anónimo. La entropía se calcula utilizando la probabilidad de consulta histórica para cada ubicación en el conjunto anónimo [8].

- La Preservación de Privacidad de Ubicación Basado Dummy (DLP) consiste en agregar información ficticia o "dummy" a los datos de ubicación real con el fin de ocultar la identidad y preservar la privacidad de las personas. La idea de DLP de introducir ubicaciones falsas o ficticias en los conjuntos de datos, utilizando algoritmos específicos que preservan la estructura y las características generales de los datos reales, pero sin revelar información personal identificable [16] [38].

- DLP Mejorado selecciona de manera eficiente las ubicaciones ficticias teniendo en cuenta información adicional disponible para un atacante. En la construcción del conjunto anónimo de ubicaciones ficticias tienen la probabilidad de consulta histórica más similar a la ubicación real del usuario, generando un conjunto anónimo con una entropía lo suficientemente alta utilizando algoritmos específicos que preservan la estructura y las características generales de los datos reales, pero sin revelar información personal identificable [39,40].

Para finalizar esta sección de resultados, se presenta siguiente tabla que relaciona los artículos sometidos a revisión con las correspondientes categorías definidas para esta investigación

TABLA I
Listado de papers revisados

	Artículos /Subcategorías	Uso individual	Uso Colectivo	Robo de información	Mal uso de información	Tec. centralizadas	Tec. descentralizadas	Tec. distribuidas	Almacenamiento de datos	Transmisión de datos	Procesamiento de datos
[6]	Protecting Location Privacy in IoT Wireless Sensor Networks through Addresses Anonymity			x						x	
[7]	Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments			x						x	
[8]	Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hash Function	x		x				x			x
[9]	Realizing Efficient Security and Privacy in IoT Networks			x		x					
[10]	Method to implement K-NN machine learning to classify data privacy in IoT environment			x		x	x				
[11]	A Trust-based Security System for Data Collecting in Smart City		x	x							
[12]	Searchable Encryption Scheme for Personalized Privacy in IoT-Based Big Data						x		x		
[13]	Authentication and Key Management in Distributed IoT using Blockchain Technology			x				x			
[14]	A Regulatory View on Smart City Services			x							
[15]	Security and privacy for mobile iot applications using blockchain	x	x					x			
[16]	An efficient dummy-based location privacy-preserving scheme for internet of things services			x			x		x		x
[17]	Smart City IoT Services Creation Through Large-Scale Collaboration								x		
[18]	A Methodological Framework for the Selection of Key Performance Indicators to Assess Smart City Solutions			x							
[19]	Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures	x				x					x
[20]	MicroServices Suite for Smart City Applications							x			
% de presencia en la revisión de la literatura		15%	10%	50%	0%	15%	15%	20%	20%	10%	15%

C. *Síntesis*

La presente revisión sistemática se enfocó en la seguridad y protección de datos para los sistemas IoT en smart cities. A partir de los hallazgos obtenidos, se categorizaron los resultados en cuatro segmentos: aplicaciones de IoT, riesgos asociados a la recopilación de datos en sistemas IoT, tecnologías para la protección de datos y modelos de tratamiento de datos.

De los artículos revisados, es posible señalar en primera instancia que el riesgo eminente al que se exponen los sistemas de IoT se relaciona con la posibilidad de los datos sean interceptados y utilizados para otros fines distintos a los considerados en su operación normal. La falta de supervisión, en el sentido de implementaciones tecnológicas adecuadas en los sistemas de aplicaciones IoT, puede evidenciar posibilidad de riesgos importantes para las personas y la comunidad, en la que se insertan estas soluciones

Con respecto al resguardo de la privacidad, se identificaron aportes en la mejora de la eficiencia de las ubicaciones ficticias requeridas para los esquemas de anonimato, considerando además una reducción del tiempo computacional para entregar ubicaciones irreales, lo que permite encontrar fácilmente la ubicación ficticia óptima sin recorrer todas las ubicaciones en el conjunto de candidatos, y con mayor probabilidad de dificultar algún ataque que intente distinguir la ubicación real. No obstante, esta tecnología presenta una deficiencia cuando se trate de ubicaciones que antes no han sido visitadas, pudiendo entregar lugares con probabilidad histórica de 0% como océanos o desiertos, los cuales serían ubicaciones ficticias falsas.

Adicionalmente, la propuesta de utilizar MQTT como complemento para mejorar la interoperabilidad entre dispositivos IoT y la cadena de bloques, evita la sobrecarga computacional de los dispositivos. Los datos se almacenan en un sistema de almacenamiento descentralizado, y no directamente en la cadena de bloques lo que garantiza la posibilidad de modificación y eliminación de datos. Además, proporciona control de privacidad y gestión de datos a los usuarios, incluyendo la capacidad de eliminar o modificar datos.

Respecto de las plataformas de almacenamiento permiten que los mensajes se almacenen en forma de cadena de bloques. Estos mensajes son intercambiados entre nodos autorizados utilizando algoritmos de cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. En cuanto a la seguridad y confidencialidad de los datos, los mensajes intercambiados entre nodos autorizados utilizan algoritmos de cifrado simétrico y asimétrico. El cifrado simétrico utiliza una única clave compartida para cifrar y descifrar los mensajes, mientras que el cifrado asimétrico utiliza un par de claves, una pública y una privada, para cifrar y descifrar los mensajes.

Otro punto importante es la eficiencia del proceso de encriptación y el aumento en la seguridad de los datos utilizando algoritmos más rápidos. Se han propuesto técnicas de procesamiento basadas en machine learning para la clasificación de la sensibilidad de los datos y así generar cifrados más rápidos y con correlaciones más bajas lo que se traduce en una mayor seguridad y privacidad. Al mejorar la eficiencia del proceso de encriptación y aumentar la seguridad de los datos utilizando algoritmos más rápidos y técnicas de procesamiento basadas en machine learning, se logra una mayor protección de la privacidad y la seguridad en los sistemas basados en blockchain.

En resumen, se han realizado avances en la protección de la privacidad y seguridad en aplicaciones IoT, pero aún existen desafíos a superar. La supervisión tecnológica adecuada, la generación de ubicaciones ficticias más precisas y el uso de algoritmos de cifrado eficientes son aspectos clave para garantizar la integridad y privacidad de los datos en sistemas de IoT.

IV. Discusión

Considerando los hallazgos de esta revisión en relación a otras investigaciones del área en estudio, es posible señalar preliminarmente que existen diversas técnicas para resguardar la protección de los datos, las que se basan principalmente en algoritmos que buscan mantener la seguridad de éstos y protegerlos ante eventuales vulnerabilidades. No obstante, no ha sido sencillo inferir cómo se podría operacionalizar su implementación, así como tampoco el identificar claramente en qué capa se integrarían dichas técnicas, entendiendo que la protección de los datos se debe dar tanto en los dispositivos IoT, como en la transmisión del mensaje, almacenamiento y procesamiento [41].

Para abordar de manera más exhaustiva el alcance final de esta investigación, nos referimos a las preguntas que guían este estudio. Estas preguntas proporcionan una guía clara sobre los

aspectos que se abordarán y los objetivos que se pretenden alcanzar. Al responder a estas preguntas, se espera obtener una comprensión más profunda y completa del tema en cuestión, lo que permitirá reconocer la implicancia de los hallazgos mencionados y plantear proyecciones para trabajos futuro en el área.

A. ¿Qué sistemas IoT para Smart Cities recopilan datos personales

En cuanto a la recopilación de datos personales a través de los sistemas IoT, la mayoría de los artículos revisados entregan información general del tema en estudio, resultados que se pueden extrapolar a distintas áreas en el contexto de las smart cities, no obstante, en algunos casos fue posible identificar algunos ámbitos de aplicación específica, como los son las aplicaciones móviles que pueden recopilar datos personales, como ubicación, preferencias, hábitos de consumo, información de registro y otros datos relevantes para brindar servicios personalizados a los usuarios, pero que también pueden ser considerar una invasión a privacidad si es acceso a estos datos no es debidamente informado y consensuado por el usuario. Por otro lado, en la indagación inicial de esta investigación se pudo apreciar que, en el contexto de las ciudades inteligentes, los sistemas IoT se utilizan en el sector del transporte para el monitoreo y gestión del tráfico, sistemas de estacionamiento inteligente, seguimiento de flotas y optimización de rutas. Estos sistemas mejoran la eficiencia del transporte, reducen la congestión y brindan una experiencia más fluida para los usuarios. En esta investigación se pudo complementar lo anterior con la revisión de los vehículos inteligentes, llamados también vehículos IoT, que son automóviles equipados con tecnología avanzada que les permite conectarse a Internet y comunicarse con otros dispositivos y sistemas. Estos vehículos utilizan sensores, redes de comunicación y sistemas de procesamiento de datos para recopilar información y tomar decisiones en tiempo real. En este sentido toman un papel importante los dispositivos de GPS, que proporcionan rutas optimizadas en tiempo real y actualizaciones de tráfico en tiempo real. Esto ayuda a los conductores a evitar congestionamientos y encontrar la ruta más eficiente.

Estos son solo algunos ámbitos de los diversos sectores en los que se aplican sistemas IoT. La tecnología IoT tiene un amplio potencial en varios campos y su adopción continúa creciendo, impulsando la eficiencia, la automatización y la toma de decisiones basadas en datos en diferentes industrias que se encuentran presente en el contexto de las smart cities.

B. ¿A qué tipos de riesgos se exponen las personas al interactuar con sistemas IoT?

Respecto a esta pregunta, es importante mencionar que existen varios riesgos asociados a la seguridad y privacidad de los datos en las aplicaciones de IoT. Uno de los riesgos más destacados es el robo de información. Los datos personales recopilados por los dispositivos de IoT, como la ubicación, los patrones de comportamiento y la información personal identificable, pueden ser objeto de robo por parte de actores malintencionados. Este robo de información puede tener consecuencias graves, como el uso indebido de datos personales, el fraude o el compromiso de la privacidad de las personas.

Además del robo de información, los ataques informáticos son otra preocupación importante, en la que los sistemas de IoT pueden ser vulnerables a ataques como de denegación de servicio (DDoS), inyección de código malicioso, interceptación de comunicaciones y acceso no autorizado a los dispositivos. Estos ataques pueden comprometer la integridad de los datos, la funcionalidad de los dispositivos y la privacidad de los usuarios.

Dentro de los artículos seleccionados, no fue posible identificar estudios o posibles soluciones para el mal uso de la información personal por parte de las empresas. Si bien el usuario entrega su consentimiento para el tratamiento de sus datos como parte de una funcionalidad de un sistema IoT, el reglamento de protección de datos de la unión europea [42] dicta directrices sobre el uso correcto de los datos personales. Como trabajo futuro será necesario extender la investigación a los marcos reguladores y aspectos legales para tener una comprensión clara del problema.

Los sistemas IoT presentan riesgos de ciberseguridad como el robo de datos, ataques DDoS, acceso no autorizado, manipulación de dispositivos y vulnerabilidades de software. Estos riesgos pueden afectar a las personas de diversas maneras, desde la pérdida de privacidad hasta la seguridad física.

Estos riesgos pueden afectar a las personas de diversas maneras, desde la pérdida de privacidad hasta la seguridad física. Por ejemplo, si los datos de salud de una persona son robados, los atacantes podrían utilizarlos para robar su identidad o cometer fraudes médicos. Si un dispositivo IoT que controla una infraestructura crítica, como una central eléctrica o una red de transporte, es manipulado, podría provocar daños físicos o incluso la pérdida de vidas.

Para mitigar estos riesgos, es importante que las organizaciones que desarrollan y utilizan sistemas IoT implementen medidas de seguridad básicas, como el cifrado de datos y la autenticación multifactor. También es importante que los usuarios estén informados de los riesgos de ciberseguridad

y de las medidas de protección que pueden adoptarse.[23][24][25]

De lo anterior, queda de manifiesto que es fundamental implementar medidas de seguridad adecuadas para proteger los datos personales en las aplicaciones de IoT, aspecto que se abordó en la siguiente pregunta.

C. ¿Qué tecnologías son utilizadas para resguardar la privacidad de los datos personales?

Respecto de las tecnologías para resguardar la privacidad de los datos, tanto en el análisis de los artículos sometidos a esta revisión, como en extensa literatura existente en esta área, se pueden encontrar estudios de técnicas de cifrado robustas, la autenticación y autorización de dispositivos, la monitorización constante de la red, la segmentación de la red para limitar el acceso no autorizado y la actualización regular de software y firmware para mitigar vulnerabilidades conocidas.

Se destaca la incorporación de tecnología distribuida como blockchain, que proporciona una forma segura y transparente de almacenar y verificar transacciones. Bajo este enfoque, las transacciones son agrupadas en bloques y enlazadas en una cadena secuencial. Cada bloque contiene un conjunto de transacciones verificadas y selladas criptográficamente. Una vez que un bloque es agregado a la cadena, no puede ser modificado sin alterar los bloques siguientes, lo que garantiza la integridad de los datos. La seguridad de blockchain se basa en algoritmos criptográficos, donde cada participante en la red tiene una copia del blockchain completo, lo que impide la manipulación de datos por parte de un único actor.

La indagación de esta pregunta abarcó diversos técnicas y modelos de protección de datos en aspectos tecnológicos y niveles de profundidad y complejidad algorítmica, por lo que cada una las tecnologías investigadas podrían ser en sí una investigación o considerar la opción de plantear una integración de ésta para proporcionar una solución más robusta y segura.

Integrando los aspectos mencionados en las preguntas anteriormente desarrolladas, es posible indicar que la protección de datos personales en el entorno digital es de vital importancia en la actualidad. El auge de las tecnologías como el Internet de las Cosas (IoT) y la digitalización de servicios han incrementado la recopilación de datos personales, aumentando a su vez la necesidad de fortalecer las medidas de seguridad y privacidad.

Junto con lo anterior, y en respuesta a nuestra pregunta de investigación principal, concluimos que resguardar la privacidad de los datos recopilados por los sistemas basados en IoT en una ciudad inteligente requiere una combinación de tecnologías y estrategias. Esto incluye el uso de encriptación para proteger los datos durante la transmisión y el almacenamiento, la implementación de técnicas de anonimización de datos para resguardar la identidad de los individuos y la consideración de tecnologías emergentes como el blockchain.

Además, identificamos que existen riesgos inherentes asociados con la interacción con los sistemas IoT, como la violación de datos y el uso no consentido. Por lo tanto, además de las soluciones tecnológicas, también es esencial contar con políticas sólidas de privacidad y seguridad de los datos, así como una mayor transparencia en cómo se recogen, almacenan y utilizan estos datos.

Por otro lado, para garantizar la privacidad de los datos en una ciudad inteligente, será necesaria una cooperación multidisciplinaria entre los desarrolladores de tecnologías, los responsables de la formulación de políticas públicas, los organismos reguladores y los ciudadanos para desarrollar e implementar soluciones de privacidad efectivas y sostenibles. Solo a través de estos esfuerzos combinados se puede garantizar la seguridad y privacidad de los datos personales en un mundo cada vez más conectado.

Finalmente es posible señalar, que la temática en revisión, deja en evidencia que la privacidad de los datos conlleva la interrelación de aspectos tecnológicos, y que además involucra elementos inherentes a las sociedades y a las personas que habitan, por lo tanto existen distintas perspectivas desde las cuales se puede plantear la privacidad de datos en soluciones IoT, y se deja en evidencia que se requiere una adecuada integración de los lineamientos públicos y privados, que permitan potenciar la implantación de este tipo de sistemas.

V. REFERENCIAS

[1] A. L. Samarakkody, U. Kulatunga y D. Bandara, «What differentiates a smart city? A comparison with a basic city,» de 8th World Construction Symposium, Sri Lanka, 2019.

[2] Consumer Technology Association, «Innovate Vegas " Six Pillars of smart Vegas",» 19 March 2021. [En línea]. Available: https://www.ces.tech/articles/2021/march/las-vegas-becoming-a-smart-city.aspx. [Último acceso: 15 May 2023].

[3] Ministry of Land, Infrastructure and Transport, «Smart city Korea,» 18 February 2020. [En línea]. Available: https://smartcity.go.kr/en/2020/02/18/서울시-스마트서울-네트워크s-net-자문위원회-출범/. [Último acceso: 15 May 2023].

[4] Rio Prefeitura, «City Hall signs PPP of public lighting,» 28 April 2020. [En línea]. Available: https://prefeitura.rio/cidade/crivella-assina-ppp-da-iluminacao-publica. [Último acceso: 10 April 2023].

[5] M. J. Page y J. E. McKenzie, «Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas,» Revista Española de Cardiología, vol. 74, nº 9, pp. 790-799, 2021.

[6] Z. Qiong y K. Zhang, «Protecting Location Privacy in IoT Wireless Sensoe Networks through addresses Anonymity,» Wiley Hindawi, vol. 2440313, p. 12, 2022.

[7] W. Tsu - Yang, M. Qian, S. Kumari y P. Zhang, «Rotating Behind Security: A Lightweight Authentication Protocol Based on IoT - Enabled Cloud Computing Environments,» Sensors, vol. 3858, 2022.

[8] K. Yurika Pant, A. Alsadoon, S. Khurram, A.-K. Ahmad, P. Penatiyana W.C., S. Ur Rehman y I. Rafiqui, «Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hsh Function,» Future Internet, vol. 1477, 2022.

[9] J. H. Anajemba, Y. Tang, C. Iwendi, A. Ohwoekevwo, G. Srivastava y J. Ohyun, «Realizing Efficient Security and Privacy in IoT Networks,» Sensors, vol. 2609, p. 20, 2020.

[10] S. QahtanMakki, H. Zaidalaa y A. Alaa Ahmed, «Method to implement K-NN machine Learningto Classify Privacy in IoT environment,» Indonesian Journal of Electrical Engineering and Computer Science, vol. 20, nº 2, pp. 985-990, 2020.

[11] W. Fang, N. Cui, C. Wei, Z. Wuxiong y C. Yunliang, «A Trust-based Security System for Data Collecting in Smart City,» Transactions on Industrial Informatics, vol. 101109, pp. 1551-3203, 2020.

[12] S. Li, M. LI, H. Xu y X. Zhou, «Searchable Encryption Scheme for Personalized Privacy in IoT- Based Big Data,» Sensors, vol. 1059, p. 19, 2019.

[13] P. Soumyashree, J. Debasish, M. Bhabendu Kumar, S. Ramasubbareddy, M. Daneshmand y A. Gandomi, «Authentication and Key Management in Distributed IoT using Blockchain Technology,» Things Journal, vol. 101109, 2021.

[14] M. Weber y I. Podnar Zarko, «A Regulatory View on Smart City Services,» Sensors, vol. 103390, p. 415, 2019.

[15] K. Carvalho y J. Granjal, «Security and Privacy for Mobile IoT Aplications using blockchain,» Sensors, vol. 5931, p. 21, 2021.

[16] Y. Du, G. Cai, X. Zhang, T. Liu y J. Jiang, «An efficient Dummy-Based Location Privacy-Preserving Sheme For Internet Of Things Service,» MDPI, vol. 278, p. 10, 2019.

[17] F. Cirillo, D. Gomez, L. Diez, I. Elicegui Maestro, T. B. Juel Gilbert y R. Akhavan, «Smart City IoT Service Creation Through Large Scale Collaboration,» IEEE internet of things Journal, vol. 1, pp. 43 - 48, 2020.

[18] K. Angelakoglou, N. Nikolopoulos, P. Giourka, I. L. Svensson, P. Tsarchopoulos, A. Tryferidis y D. Tzovaras, «A Methodological Framework for the selection of key Performance Indicators to Assess Smart City Solutions,» Smart Cities, vol. 2020018, pp. 269-306, 2019.

[19] J. Hoon Jo, P. Kumar Sharma, J. Sapalo Sicato y J. Hyuk Park, «Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures,» Journal or Information ProcessingSystems, vol. 15, nº 4, pp. 765-784, 2019.

[20] C. Badii, P. Bellinio, A. Difino, P. Nesi y G. Pantaleo, «Microservices Suite for Smart City Applications,» Sensors, vol. 4798, p. 19, 2019.

[21] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, doi: 10.1109/COMST.2015.2444095.

[22] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", 2020, [Online].

[23] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," in Computer Networks, vol. 76, pp. 146-164, 2015, doi: 10.1016/j.comnet.2014.11.008.

[24] M. A. Razzaque, M. Milojevic-Jevric, A. Palade and S. Clarke, "Middleware for Internet of Things: A survey," in IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70-95, Feb. 2016, doi: 10.1109/JIOT.2015.2498900.

[25] M. R. Palattella et al., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," in IEEE Journal on Selected Areas in Communications, vol. 34, no. 3, pp. 510-527, March 2016, doi: 10.1109/JSAC.2016.2525418.

[26] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," in IEEE Internet Computing, vol. 21, no. 2, pp. 34-42, March-April 2017, doi: 10.1109/MIC.2017.37.

[27] M. A. Alsheikh, S. Lin, D. Niyato and H. Tan, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996-2018, Fourth Quarter 2014, doi: 10.1109/COMST.2014.2320099.

[28] A. B. Adeel, M. A. Azam, A. Nadeem, M. H. Durad and M. A. Usman, "A Survey on Security and Privacy Issues of Internet of Things," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 2019, pp. 1971-1976, doi: 10.1109/IWCMC.2019.8766648.

[29] S. B. Mokhtar, A. Ksentini, Y. Hadjadj-Aoul, T. Taleb and D. Benferhat, "A Survey on Security in Internet of Things: Standards, Challenges and Solutions," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1506-1532, thirdquarter 2020, doi: 10.1109/COMST.2020.2984400. A.-a. AFFIA, A. NOLTE y R. MATULEVIČIUS, «IoT Security Risk

[30] S. Raza, L. Wallgren and T. Voigt, "SVELTE: Real-time intrusion detection on the Internet of Things," 2013 IEEE International Conference on Distributed Computing in Sensor Systems, Cambridge, MA, 2013, pp. 335-342, doi: 10.1109/DCOSS.2013.78.

[31] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes," in Journal of Network and Computer Applications, vol. 101, pp. 55-82, 2018, doi: 10.1016/j.jnca.2017.12.001.

[32] Aslan, Ö.; Aktu g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333. https://doi.org/10.3390/electronics12061333

[33] JP. A. Yaacoub, H. N. Noura, O. Salman, A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," in KeAi Internet od Things and Cyber-Physycal Systems, vol 3, 2023.

[34] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," in Wireless Networks, vol. 8, no. 5, pp. 521-534, Sept. 2002, doi: 10.1023/A:1016598314198.

[35] IBM, "Autenticación de nodos", [en línea]. Disponible en: https://www.ibm.com/docs/es/iad/7.2.x?topic=security-node-authentication.

[36] M. Salinas Rosales y G. Duchén Sánchez, "Protocolo de autenticación para redes inalámbricas de sensores basado en identidad", Rev. Fac. Ing. Univ. Antioquia, no. 52, pp. 203-217, abr. 2010.

[37] J. N. Al-Karaki y A. E. Kamal, "Routing techniques in wireless sensor networks: a survey", IEEE Wireless Communications, vol. 11, no. 6, pp. 6-28, 2004, doi: 10.1109/MWC.2004.1368893.

[38] 17. J. Li, X. Chen, M. Li, J. W. Li, P. Lee y W. Lou, "Secure deduplication with efficient and reliable convergent key management", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 6, pp. 1615-1625, 2014, doi: 10.1109/TPDS.2013.284.

[39] Z. Shelby, K. Hartke y C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, Junio 2014, doi: 10.17487/RFC7252.

[40] S. Khanam, I. B. Ahmedy, M, Yamani, M. Hisham y A. Qalid, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures on the Internet of Things," in IEEE Access, vol 8, Nov. 2020

[41] H. Beige, "The Advance of Internet od Things Security Threats and Possible Measures", in Highliths in Science, Engineering and Technology, vol 68, 2023.

[42] Management: A Framework and Teaching Approach,» Informatics in Education, 2023.

VI. BIOGRAFIAS

Pamela Hermosilla nacida en Valparaíso, Chile, el 8 de octubre de 1974. Graduada de Universidad Téecnica Federico Santa Naría (UTFM Ingeniero Civil en Informática (UTFSM), Diplomada en Comercio Electrónico y Logística Empresarial (UTFSM), Auditor Interno ISO 9001 (Brain & Cia Consultores), MBA of Chief Information Officer CIO (Abet Open University), Diplomada en Docencia Universitaria de la Pontificia Universidad Católica de Valparaíso (PUCV), Diplomada en Formación Virtual Universitaria (PUCV), Symposium for Entrepreneurship Educators (Luksic Scholars – Babson College). Asesorías: miembro del Consejo Público Privado de la red Fortalece Pyme, Valparaíso - Corfo, integrante del Boardd de Directores, de la incubadora Chrisalys PUCV. Desarrollo profesional en áreas de Aseguramiento de calidad en gestión de proyectos, Planificación estratégica organizacional, Rediseño curricular basado en competencias, Habilidades de Innovación y emprendimiento en estudiantes de ingeniería, Gamificación en el proceso de enseñanza y aprendizaje.

Ivo Cattarinich , nacido en Antofagasta, Chile. El 6 de abril de 1968.Estudio en colegio Salesiano de Valparaíso, Armada de Chile y Universidad Técnica Federico Santa María. Con amplia experiencia en diferentes áreas tales como Marítima, construcción, gas y petróleo. Se ha desempeñado en empresas tales como: Bureau Veritas, Constructora VINCI, Salfa, Besalco, Transmarko, Cpt marítima, Navimag, Humboldt, Transmarchilay, Armada de Chile. Actualmente en formación de Doctorado en Industria Inteligente, de la Pontificia Universidad Católica de Valparaíso.

Ignacio Rojas, nacido en Curicó, Región del Maule, Chile, el 21 de septiembre de 1986. Graduado de Universidad de Talca (Ingeniero en Mecatrónica). 18 años de experiencia en procesos industriales automatizados para la agroindustria, visión artificial, tecnologías láser, cámaras multiespectrales, robótica e inteligencia artificial. Investigación basada en inteligencia artificial aplicada a procesos industriales.

.

Dr.(c)Sebastián Berrios nacido el 7 diciembre de 1986.Actualmente candidato a doctor en Ingeniería informática en la Pontificia Universidad Católica de Valparaíso. Graduado de Ingeniería Civil en Computación e Informática en la Universidad De Las Américas. Magíster en Ciencias de la Ingeniería y Magíster en Ingeniería en Informática en la Pontificia Universidad Católica de Valparaíso. Actualmente docente del área de Ciberseguridad de la Pontificia Universidad Católica de Valparaíso.
Administrador de TI de la escuela de ingeniaría informática de la Pontificia Universidad Católica de Valparaíso.
Actualmente Cursando un Diplomado de Inclusión en Educación en la Pontificia Universidad Católica de Valparaíso, además posee un Diplomado en Seguridad de la Información de 132 horas en la Universidad de Chile y un Diplomado en Ciberseguridad de 96 horas en la misma universidad. También se obtuvo un Diplomado en Ciberseguridad de 100 horas en el Instituto Profesional IACC.