UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO 2023 - OCTUBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE LA PRIVACIDAD DE LOS DATOS DE LOS USUARIOS, EN EL CONTEXTO DEL INTERNET DE LAS COSAS.

EGRESADA:

MILDRED VICENTA COELLO MARQUEZ

TUTOR:

ECO. GERSON DAMACIO LEDESMA ÁLVAREZ. MUFI

AÑO 2023

CONTENIDO

PLANTEAMIENTO DEL PROBLEMA

A medida que la tecnología avanza, van naciendo nuevas herramientas y también se van potenciando a nuevas escalas, tal es el caso del internet. El internet en un comienzo, se limitaba a las computadoras, después a los teléfonos inteligentes, estos dos últimos son utilizados por personas, sirviendo como medio para que las personas utilicen internet, sin embargo, en la actualidad, el internet no solo se limita al uso y beneficio de las personas, ahora, también, el internet ha llegado a las cosas.

El Internet de las cosas (IoT, del inglés: Internet of Things) ha emergido como una tecnología transformadora que conecta una variedad de dispositivos y objetos cotidianos a la red, el IoT ha revolucionado la forma en que interactuamos con la tecnología y cómo esta interactúa con nosotros. Desde dispositivos y sistemas que utilizamos prácticamente a diario, desde autos, televisores, relojes hasta el refrigerador de nuestros hogares, permitiendo la recopilación, el procesamiento y el intercambio de datos de manera eficiente y en tiempo real. A medida que esta interconexión continúa expandiéndose, surge un problema crítico relacionado con la privacidad de los datos de los usuarios.

El crecimiento exponencial de dispositivos IoT ha dado lugar a una recopilación masiva de datos personales. Los dispositivos conectados recopilan información sobre nuestros hábitos, preferencias, ubicaciones y más. Estos datos pueden incluir desde datos de salud recopilados por dispositivos médicos hasta información de ubicación rastreada por sistemas de navegación en automóviles conectados. Si bien esta recopilación de datos tiene el potencial de brindar beneficios significativos en términos de comodidad y eficiencia, también plantea preguntas críticas sobre cómo se manejan y protegen los datos sensibles de los individuos.

Este planteamiento del problema se basa en la imperiosa necesidad de comprender y abordar las amenazas a la privacidad que surgen en el contexto del IoT. Con la creciente adopción de dispositivos IoT en la vida diaria de las personas, entornos domésticos, empresariales e industriales, la cantidad y la diversidad de datos recopilados sobre los usuarios se incrementa exponencialmente. Sin embargo, existe una falta de claridad en cuanto a cómo se recopilan, almacenan, procesan y comparten estos datos, así como los riesgos asociados con la exposición no autorizada o el mal uso de la información personal.

Preocupaciones tales como: ¿Qué finalidad tienen nuestros datos personales para las empresas? ¿Cómo se recopilan nuestros datos personales en el contexto IoT? ¿Cuáles son los principales riesgos y amenazas a la privacidad que enfrentan los usuarios debido al uso de dispositivos IoT? Son de suma importancia y actualidad y muy poco se esclarece sobre ellas.

Como usuarios, poco nos detenemos a pensar en la implicación de utilizar una tecnología nueva, innovadora y que ofrece comodidades, y también, estas tecnologías poco les informan a los usuarios cuál es su modus operandi, cuáles son los términos a tener en cuanta al utilizar esta tecnología, si existe un potencial riesgo al integrarlas en nuestra vida diaria, si recopila datos, que datos recopila, para que los recopila y que finalidad tienen aquellos datos recopilados.

La privacidad de los datos de los usuarios en el contexto del Internet de las cosas es un tema muy relevante e importante y muy poco popular, teniendo en cuenta que vivimos en un mundo globalizado e hiperconectado, es necesario analizar e identificar los riesgos y desafíos asociados que puedan existir con la recolección, procesamiento y

almacenamiento de datos personales que se generan mediante el uso de los dispositivos IoT.

JUSTIFICACIÓN

Con la proliferación del Internet de las cosas (IoT) en un mundo hiperconectado, y la poca relevancia que se le da al tema de la privacidad de los datos personales, es menester efectuar análisis que contribuyan a la comprensión del modo de funcionamiento de esta nueva tecnología, los riesgos y las amenazas para la privacidad que pueda representar el IoT para los usuarios.

La recopilación masiva de datos personales en el contexto IoT, hace que sea necesario abordar el tema de la privacidad de los datos, que finalidad tienen estos datos y si pueden llegar a representar un riesgo significativo para la vida del usuario, cómo se almacenan, manejan, dado que los usuarios deben comprender los riesgos y las implicaciones de privacidad asociados con el IoT.

Por lo tanto, al investigar y abordar estos problemas contribuye a la educación del usuario, para que les permita tomar decisiones informadas, fomentando una mayor conciencia sobre la importancia de la privacidad de los datos y debido a que el IoT es una tecnología disponible para tantos usuarios como sea posible y tengan acceso a internet, se espera que este estudio pueda beneficiar a tantas personas como sea posible que tengan acceso a esta información, en un mundo globalizado.

La factibilidad de este estudio radica en la necesidad de abordar las preocupaciones sobre la privacidad de los datos de los usuarios en el contexto del IoT. A medida que la tecnología IoT se integra en diversos aspectos de nuestra vida diaria, es fundamental entender los riesgos y desafíos asociados. La protección de la privacidad de los usuarios se ha convertido en un desafío crítico, teniendo en cuenta que la

exposición indebida de estos datos puede llevar a problemas como el robo de identidad, el acoso cibernético y la manipulación de información personal.

OBJETIVOS

Objetivo general

- ✓ Analizar los riesgos y la exposición de la privacidad de los datos del usuario en el contexto del Internet de las Cosas (IoT).

Objetivos específicos

- ✓ Contextualizar acerca del Internet de las cosas y temas pertinentes.
- ✓ Evaluar cómo los dispositivos IoT recopilan, almacenan, procesan y comparten datos de los usuarios.
- ✓ Determinar cómo puede afectar a los usuarios los riesgos de privacidad de los datos asociados con el Internet de las cosas (IoT).

LÍNEAS DE INVESTIGACIÓN

Para el presente estudio de caso, la investigación se contempla bajo la línea de "Sistemas de información y comunicación, emprendimiento e innovación", dado a que el tema central de la investigación comprende a el Internet de las cosas (IoT), y esta es una tecnología, un sistema de información y comunicación, el IoT tiene la capacidad de recibir y transmitir información en tanto que tenga comunicación con el usuario, aunque este último no interactúe específicamente con el dispositivo, ya que esta con esta tecnología basta con que sienta su presencia a partir de sensores integrados, además, también tiene la capacidad de comunicarse con otros sistemas y dispositivos inteligentes en tiempo real creando un hiperconexion entre ellos, siendo una tecnología relativamente nueva, se supone como una tecnología innovadora, con un potencial y proliferación sin precedentes en la historia, además que el tema Internet de las cosas, es poco explorada actualmente, sobre todo sus aspectos de privacidad para con el usuario.

Como sublínea contamos con "Redes y tecnologías inteligentes de software y hardware", el tema de esta investigación (IoT) es una nueva tecnología muy inteligente, con una capacidad sin precedentes es procesos de automatización y recolección de datos, su funcionamiento se desempeña a través de hardware, ya que son dispositivos inteligentes, cosas físicas que tienen acceso a internet, concordando con la sublínea de investigación que también comprende redes. Para acceder a la red y generar interacciones, recopilar y transmitir datos e incluso, tomar decisiones, además del hardware, también se ocupa el software, softwares muy inteligentes que integran otros softwares dentro de ellos, convirtiéndose así en una red y tecnología inteligente de software y hardware. El IoT tiene la capacidad de interactuar y conectarse con otros

distintos sistemas y otros dispositivos IoT, generando una conexión en tiempo real similar como lo haría una red de redes, y mediante esta, emitir y receptar datos.

MARCO CONCEPTUAL

La tecnología avanza a pasos nunca antes registrados en nuestra historia, su crecimiento es exponencial, en pocos años el internet, los dispositivos, las cosas inteligentes se han convertido en parte fundamental de nuestra vida, redefiniendo la forma en que interactuamos con el mundo que nos rodea. El internet pasó de ser una fastuosidad o un privilegio de pocos, a ser parte indispensable de nuestra vida y funcionamiento diario; esto ha provocado que muchas de las cosas que siempre hemos utilizado y otras nuevas que se han creado, estén constantemente usando internet, incluso que algunas solo funcionen al estar conectadas al internet.

En el epicentro de toda esta nueva revolución tecnológica se encuentra el Internet de las cosas (IoT), un paradigma que ha trascendido las fronteras de la tecnología convencional para abrir un horizonte de posibilidades ilimitadas. Sin embargo, junto con esta innovación surge una pregunta crucial que suele pasar desapercibida ¿Qué sucede con la privacidad de los datos de los usuarios en este nuevo panorama?

El IoT, que abarca una red global de dispositivos, sensores y sistemas inteligentes, ha traído consigo un cambio radical en la forma en que se recopila, procesa y utiliza los datos (y por ende información). La capacidad de interconectar diversos dispositivos en un tejido digital unificado ha resultado en la generación de vastas cantidades de datos, que no solo informan sobre el entorno circundante, sino también sobre las actividades, preferencias y comportamientos de los usuarios. A medida que

esta revolución avanza, es imperativo cuestionar cómo se manejan estos datos y cuáles son las implicaciones para la privacidad y la seguridad de los usuarios.

A continuación, para comprender de mejor manera este tema, es necesario desglosar conceptos importantes.

Internet

Entendemos por internet a una red de redes interconectadas entre sí, por el cual podemos enviar y recibir paquetes de datos a nivel global, que, en la actualidad, funciona como pilar fundamental de nuestra sociedad.

Internet "conecta e interrelaciona dispositivos electrónicos y redes de computadoras entre sí, de todo el mundo. Su nombre proviene del inglés *International Network* que significa "*Red Internacional*" y el acrónimo de esas palabras dio origen al nombre *Internet*" (Equipo editorial, 2023).

El nacimiento como tal del Internet se remonta a la década de los ochentas, en concreto a 1983, cuando *ARPANET* dejó de ser exclusivamente parte de fines militares, pasó a formar parte de la *Fundación Nacional de Ciencias*, además a la red se le agrego protocolo *TCP/IP* pasándose a llamar *Arpa Internet*.

Finalmente es en 1989 que Internet pasa a ser conocida como la conocemos hoy, y desde ahí, su crecimiento tanto útil como expansivo ha sido exponencial.

"El 12 de marzo de 1989 Tim Berners Lee describió por primera vez el protocolo de transferencias de hipertextos que daría lugar a la primera web utilizando tres nuevos recursos: HTML, HTTP y un programa llamado Web Browser" (Equipo editorial, 2023).

Con el pasar de los años, Internet ha evolucionado a estrepitosamente, siendo que, en la actualidad, la gran mayoría de industrias dependen de internet para poder funcionar, además de que se crearon nuevas industrias exclusivamente gracias a la existencia de Internet, de poner transmitir grandes cantidades de datos a gran velocidad en tiempo real, acceder a esos datos desde cualquier parte del mundo, siendo que ahora, no solo las personas podemos usarlo, ahora también las cosas.

Dispositivos inteligentes (Cosas)

El termino *cosas* en el contexto de *Internet de las cosas*, no son más que objetos físicos inteligentes conectado a la red (internet), con capacidad de receptar, intercambiar y recibir datos a través de otros dispositivos, bases de datos, sistemas; todo esto en tiempo real y de forma autónoma, sin que necesariamente exista intervención humana, osease, son dispositivos inteligentes.

"Un dispositivo inteligente es un dispositivo electrónico., generalmente conectado a otros dispositivos o redes a través de diferentes protocolos inalámbricos como Bluetooth, NFC, Wifi, 3GRAMO, LoRa, NB-IoT, Zigbee y así sucesivamente, que puede funcionar de forma algo interactiva y autónoma" (Kuan, 2017).

Para el asombro de varios, el pionero como dispositivo inteligente fue concebido en 1905, con la creación de la primera aspiradora eléctrica. Desarrollada por Walter Griffiths, un inventor británico, esta aspiradora marcó un punto de inflexión en la evolución de los dispositivos inteligentes en el ámbito doméstico. Tan solo dos años después, en 1907, llegó al mercado la primera lavadora eléctrica, seguida en 1928 por la presentación de la primera lavavajillas eléctrica (Takes, 2023).

En la actualidad, para considerar a un dispositivo inteligente, primordialmente debe contar con tres aspectos fundamentales:

- **Sensores**, como cámaras, micrófonos, sensores de geolocalización, proximidad, humedad, luz, sonido, entre otros como sensores de temperatura o presión.
- **Autonomía**, que permita automatizar una tarea o que pueda funcionar sin la necesidad de la intervención de una persona.
- **Conectividad**, debe tener la capacidad de conectarse a internet para poder comunicarse con otros dispositivos o sistemas en la nube, recibir y transmitir datos, ya que incluso, sin esta capacidad, el dispositivo no sería de utilidad.

Estos dispositivos comprenden en una amplia variedad de objetos, desde los más comunes, como teléfonos inteligentes, que cuentan con múltiples sensores y capacidades para satisfacer y recopilar datos de los usuarios, relojes inteligentes, que permiten llevar un seguimiento del ritmo cardiaco, presión arterial, actividad física, cámaras de seguridad autónomas, que funcionan al detectar la presencia de un sujeto u objeto, hasta sistemas de alumbrado autónomo, casas inteligentes, que tienen múltiples características asistidas y pueden ser controlados de manera remota, como encender las luces al detectar movimiento u obscuridad, cortinas que funcionan a partir de la temperatura ambiente, además de asistentes de voz, puertas automáticas, electrodomésticos inteligentes, como lavadoras, refrigeradoras, cocinas, freidoras de aire, con capacidad de conectividad, reconocimiento de voz, también estos dispositivos comprenden instrumentos médicos, autos que se conducen solos e incluso ropa inteligente, como trajes de baños inteligentes, que miden la temperatura corporal, medias inteligentes para bebes que monitorean el estado del bebe o ropa deportiva con capacidad de absorción de calor, recuperación muscular.

La proliferación de estos dispositivos es completamente escalable, lo que significa que se pueden ir desarrollando nuevos dispositivos a la red sin dificultad. Esto es importante en aplicaciones que requieren un crecimiento constante, como las

ciudades inteligentes; trayendo consigo una transformación en la forma en que interactuamos con el entorno y cómo funcionan las ciudades, las empresas y los hogares.

Internet de las cosas (IoT)

Internet de las cosas mejor conocido por sus siglas *IoT* del inglés *Internet Of Things*, se entiende como un compendio de dispositivos inteligentes interconectados entre sí a internet, por el cual comparten, reciben, envían datos logrando ayudar o automatizar una acción. Dichos dispositivos (cosas), como sensores, relojes, refrigeradoras, zapatos, sistemas, pueden autónomamente funcionar sin necesidad de intervención humana.

"Se trata de una nueva tecnología que *conecta casi todo lo que hacemos*. Facilita un ecosistema interconectado de dispositivos y máquinas, lo que permite a los usuarios controlar sus dispositivos desde cualquier lugar" (Carlemany, 2021).

El Internet de las cosas, mediante la interconexión de los dispositivos inteligentes, posibilita la transferencia de información entre estos elementos, facilitando la obtención de datos fundamentales acerca del empleo y el funcionamiento de los dispositivos y objetos, con el propósito de identificar pautas, proporcionar sugerencias, optimizar la eficacia y generar experiencias superiores para los usuarios.

En nuestra rutina diaria, podemos observar una gran cantidad de elementos interconectados que constituyen una parte integral del Internet de las cosas. De acuerdo con las proyecciones del Worldwide Global DataSphere IoT Devices and Data Forecast, se anticipa que para el año 2025 habrá alrededor de 41.600 millones de dispositivos conectados (Alonso, 2023).

"Cualquier cosa que se pueda imaginar podría ser conectada a internet e interaccionar sin necesidad de la intervención humana, el objetivo por tanto es una interacción de máquina a máquina, o lo que se conoce como una interacción M2M." (Gracia, 2019).

Importancia del IoT

Actualmente, casi cualquier persona cuenta con un teléfono celular o algún dispositivo inteligente conectado a internet, vivimos en un mundo hiperconectado, en el cual, la brecha entre el mundo digital y el mundo físico cada vez es más borroso.

El IoT se ha convertido prolíficamente en la tecnología más preponderante de, probablemente, toda la historia, teniendo incluso su crecimiento asegurado de cara a la siguiente década.

"El último estudio de Juniper Research concluye que la cantidad global de datos generados por las conexiones de roaming de IoT aumentará de 86 petabytes en 2022 a 1.100 para 2027" (bisite, 2022).

Casi cualquier *cosa* que se fabrica en esta época, está diseñada para grabar, recopilar, estudiar y transmitir datos en gran parte de las personas, sin que estos mismos si quiera se den cuenta, y podemos encontrar dispositivos con esas características casi en muchos de nuestros ambientes frecuentes, en las calles, parques, semáforos, oficinas e incluso hogares, que en los hogares en particular, resulta más interesante, ya que tiene que ver con nuestro comportamiento de una manera más privada, pero ahondaremos más sobre eso es siguientes capítulos.

Utilización del IoT en nuestro contexto actual

El internet de las cosas, está presente en muchas industrias, y para algunas de ellas, se está convirtiendo en algo indispensable. A continuación, mencionaremos varias de las aplicaciones/utilización del IoT en la actualidad.

Salud: La utilización de dispositivos portables o sensores conectados a los pacientes posibilita que los médicos monitoreen sus estados de salud en tiempo real incluso fuera del entorno hospitalario, mediante la recepción automática de métricas y alertas referentes a sus indicadores vitales. Otra aplicación radica en la incorporación de la tecnología IoT en las camas de hospitalización, dando origen a camas inteligentes equipadas con sensores especializados para supervisar indicadores vitales, presión arterial, niveles de oxígeno y temperatura corporal, entre otros aspectos.

Wearables: Gafas de realidad virtual, pulseras fitness para el seguimiento de consumo de calorías y ritmo cardíaco, entre otros, constituyen solamente algunos ejemplos de dispositivos portátiles que hemos estado utilizando desde hace cierto tiempo. Empresas como Google, Apple, Samsung y otras han ideado e implementado la incorporación de la Internet de las Cosas en nuestras actividades diarias más pragmáticas. Estos dispositivos son compactos y eficientes en términos energéticos, cuentan con sensores y hardware necesarios para efectuar mediciones y capturas, y se encuentran equipados con el software requerido para recolectar y estructurar los datos e información acerca de los usuarios (Toyos, 2018).

Ciudades Inteligentes: Un gran porcentaje de la utilización de IoT conlleva a las ciudades inteligentes, por el cual, mediante supervisión y vigilancia se abordan requerimientos como delincuencia, contaminación, congestión vial, servicios de trasporte (Gil, bbva, 2021).

Tráfico vehicular: Mediante el uso de sensores ubicados en dispositivos móviles, se recopilan y envían datos desde nuestros vehículos a través de apps como Google Maps. Los usuarios tienen la capacidad de aprovechar el IoT para obtener pronósticos sobre congestiones de tráfico y hallar las rutas más aconsejables para llegar a destinos específicos (sydle, 2022).

Tecnología y comunicaciones dentro del IoT

Existen varias tecnologías que se emplean en el ambiente IoT para su funcionamiento como lo son Wifi, SigFox, Bluetooth 4.0, algunas otras destacadas son:

Tabla 1
Tecnologías empleadas en el IoT.

Tecnología	Definición
LoRa	LORA emerge como una de las novedosas tecnologías inalámbricas con mayor impacto, fundamentada en sistemas de radiofrecuencia para implementar LPWAN (Redes de Área Amplia de Baja Potencia). Entre sus características sobresalientes se encuentran: - Su alta resistencia a las interferencias, - Una notable sensibilidad para la recepción de datos (-168dB), - Un consumo energético reducido (lo que posibilita una vida útil prolongada con baterías). - La capacidad de cubrir largas distancias (aproximadamente 20 kilómetros). - Un espectro de frecuencias de operación: 868 MHz para Europa, 915 MHz para América y 433 MHz para Asia (alltimeiot, 2021).
5G	El 5G representa la generación subsiguiente de redes de comunicación móvil, con mejoras notables en términos de latencia y capacidad de banda en comparación con el 4G. Estas mejoras permitirán situaciones de comunicación que involucran grandes volúmenes de datos en tiempo real. En efecto, uno de los casos de uso proyectados para las redes 5G es la interconexión de vehículos autónomos, su frecuencia oscila entre 3 a 30 GHz y su cobertura es de alrededor de 1 kilometro (Sabas, 2018).
Big data y Cloud Big Data	El internet de las cosas genera muchos datos, todo el tiempo, y la tecnología capaz de procesar esas grandes cantidades de datos, petabytes de datos, es el Big Data, además es capaz de proporcionar la infraestructura necesaria y escalable para analizar y acceder a esa gran masa de datos de forma inmediata. **“**El papel de Big Data en IoT es la capacidad de procesar grandes cantidades de datos en tiempo real. Estos datos valiosos luego se estructuran y almacenan, utilizando múltiples tecnologías” (Tapia, 2022).
Inteligencia	La Inteligencia Artificial abarca un conjunto de tecnologías destinadas a emular

Artificial	las habilidades distintivas del ser humano. Las máquinas tienen la capacidad de replicar funciones cognitivas análogas a las operaciones mentales humanas, incluyendo el aprendizaje, la toma de decisiones y la resolución de problemas, además de llevar a cabo diversas tareas, con la facultad de mejorar basándose en los datos recolectados. En compañía del Big Data, la Inteligencia Artificial resulta esencial para procesar la inmensa cantidad de elementos interconectados y conferir sentido a los datos transmitidos por estos dispositivos (Gil, bbva, 2021)**.**
Nanotecnología	Tecnologías como la nano, que permite manipular materia de muy pequeñas dimensiones, tienen su integración y acilación con el internet de las cosas. "El uso de la nanotecnología permite fabricar unas etiquetas electrónicas en miniatura para la vigilancia y el seguimiento de objetos pequeños o cambios en la información" (EvaluandoSoftware, 2022).

Estas tecnologías junto con el IoT crean un perfecto ecosistema en el cual se generan, procesan y se almacenan una cantidad impresionantes de datos los cuales posteriormente son analizados proporcionando mucha información y valioso conocimiento.

Datos

Hablar de los datos es de suma importancia ya que es como el combustible de esta época, muchas tecnologías e industrias dependen exclusivamente de los datos, y el internet de las cosas no se queda atrás. En la actualidad existe una guerra silenciosa por los datos, los datos que generamos nosotros como usuarios.

Tabla 2
Definiciones de Dato, Información y Conocimiento.

Concepto	**Definición**
Dato	Un dato o los datos, son pequeñas partes de información, tales como números, símbolos, letras, señales, que a priori, estando separados de un conjunto de datos, se vuelve irrelevante y carece de sentido, solo estando agrupados y analizados cobran sentido y pasan de ser datos a convertirse en información. "Los datos son una forma cruda de información sin el significado o la utilidad adecuados a menos que se procesen y transformen en formas significativas" (financialcrimeacademy, 2023).
Información	Tener un montón de datos no sirven de nada si no se los interpreta, los datos son el activo más importante de esta época de la humanidad, y eso se debe a que, al interpretar esos datos, se convierten en información, información valiosa. Información no es más que el procesamiento de un compendio de datos, que, al

	interpretarlos, adquieren significado e importancia. "La información es una forma procesada de datos desarrollados o formados para llegar a una decisión particular o para usar en la toma de algunas decisiones" (financialcrimeacademy, 2023).
Conocimiento	E**s** la cúspide del proceso, una vez que los datos han sido interpretados y convertidos en información, el análisis de esta información se convierte en conocimiento, y el conocimiento siempre tiene una finalidad, una acción, ejerce un poder para lograr el hacer algo o tomar decisiones. **"**La asimilación inteligente de datos y/o información produce conocimiento, en cierto sentido de 'sabiduría', que nos permitirá anticiparnos a situaciones futuras, bien sea mediante predicciones, pronósticos, estimaciones, estudio de tendencias" (Olivas, 2022).

Los datos son la nueva moneda valiosa del mundo digital porque son la base de la cual nace el conocimiento, y siempre que se tenga conocimiento se pueden ejercer acciones, es por eso que las empresas se custodian nuestros datos y nuestra atención.

Exposición de datos en el IoT

"En 2021, había más de 10.000 millones de dispositivos de IoT en el mundo, y para 2025, IDC espera que la generación de datos globales supere los 73 zettabytes –lo cual equivale a 73 billones de gigabytes–" (sap, 2023).

En nuestro contexto nacional (Ecuador), el porcentaje de uso de internet en hogares asciende al 62,2%, y el porcentaje de personas que acceden a internet es de un 72,7% (INEC, 2023).

Son millones los datos que se generan en la actualidad mediante el uso del internet, y obviamente, también el internet de las cosas. Particularmente, con el internet de la cosas son cientos de miles de millones de datos que se generan, y la gran mayoría de esos datos son sobre el comportamiento de los usuarios que utilizan el internet de las cosas, datos del comportamiento, lo cual, no deja de representar un riesgo al tratarse de información sensible y de cuidado y para el IoT, es complicado garantizar la seguridad de los datos que se generan, ya que existen muchos fabricantes, con distintos

protocolos, que sugieren una exposición a ataques y vulnerabilidad de nuestra privacidad.

Seguridad y Privacidad

Gran parte de la población actual, no es consciente de la importancia de sus datos, y muchas empresas se aprovechan de ello, y también, ciberdelincuentes. En el contexto IoT, el recolectar, almacenar y procesar cientos de datos, ha traído consigo muchas violaciones a la privacidad del usuario.

> Según la Agencia Española de Protección de Datos, los riesgos del IoT van desde la construcción de perfiles detallados, revelación de pautas de comportamiento y estilo de vida de las personas, recopilación y uso no autorizado de datos con terceros y falta de transparencia: en algunos casos, los usuarios pueden no estar al tanto de información que se están recopilando, cómo se está utilizando y con quién se están compartiendo (Comunicación, 2023).

Con el IoT se crean millones de puntos de recopilación de datos, dichos datos pueden comprender desde intereses personales, el tiempo que permanece despierto, a qué hora se despierta, a qué hora se va a dormir, su temperatura corporal, sus rutinas diarias, hora de trabajo, hora de almuerzos, ritmo cardiaco, hábitos de sueño, lugares que visita frecuentemente, su voz, su imagen, sus conversaciones, sus preferencias, sus hábitos de consumo, sus productos favoritos, entre muchas otras cosas que el usuario puede imaginar o incluso las que no pueda imaginar.

Toda esa información resulta importante, ya que tratan del comportamiento íntimo del consumidor, con lo puede lograr crear un perfil muy detallado del usuario,

revelando pautas importantes del mismo, creando una huella digital muy precisa y desconociendo con certeza los fines para con esos datos.

La **huella digital "**es un conjunto de información y datos que se genera cuando una persona usuaria navega por la red y que permite identificarla de manera única" (smowltech, 2023)**.**

La *huella digital* se genera automáticamente a medida que usamos internet, recopilando datos nuestros, ya sea que la proporcionamos de manera voluntaria, o involuntaria, esta información se recopila por cookies, aunque en si, por el uso del internet en general, ósea, de todos los dispositivos que utilizamos y que tienen acceso a internet, crean datos y con esto una huella digital única del usuario, incluyendo claramente al IoT. Lo cual también genera serios problemas a la privacidad del usuario, ya que se desconoce el fin de toda esa información recopilada, y también se desconoce si esa información solo la usa el fabricante o también se la proporcionan a otras empresas, además del robo de información que siempre va a existir al utilizar tecnología.

En el IoT existen cuatro tipos oficiales de recolección de datos.

Tabla 3
Tipos oficiales de recolección de datos.

Tipo de dato	Definición
Datos facilitados	Son los que el propio usuario acepta facilitar de forma voluntaria, al aceptar términos y condiciones, al vincular un dispositivo inteligente como un reloj o unas cortinas de ventanas inteligentes a su teléfono inteligente y facilitando datos tanto del dispositivo como del teléfono.
Datos observados	Estos son los datos que son capturados por diferentes dispositivos, sensores, alguna cámara de vigilancia, aquí también los datos pueden ser con consentimiento del usuario, como también captados sin que el usuario se dé cuenta (ampliaremos esto más adelante).
Datos derivados	Los datos derivados surgen a partir de los datos observados y facilitados, pues una vez esos datos han sido interpretados por sistemas inteligentes de análisis, dotan de inteligencia al dispositivo IoT para que pueda tomar decisiones, como que nos siguiera tiempos de descanso, nos recomiende música, series, o productos para adquirir. El usuario interviene menos en este tipo de dato derivado, no siempre es

	consciente de este apartado ni de lo que se puedan hacer con sus datos o sugerir cosas a partir de sus datos, aunque eso no significa que en algún momento no haya otorgado permisos para esos datos, pero sin conocer completamente de que se trata.
Datos inferidos	Los datos inferidos se construyen a partir de los datos recopilados y claramente de su procesamiento y análisis, estos datos son compendios de datos de un o muchos usuarios, de una o múltiples puntos de recopilación de datos, interviniendo en su análisis la Inteligencia Artificial, el Big Data e incluso generando metadatos, que son los datos de los datos.

"Estos datos se pueden utilizar para llevar a cabo diferentes análisis y estudios estadísticos y es donde entra en juego la protección de datos y las nuevas tecnologías" (Atico34, 2022).

Al utilizar tantos dispositivos que están conectados a internet, conociendo que dejamos rastro de todo al utilizarlo, mediante la huella digital, las empresas pueden crear un perfil muy detallado y preciso, conociéndonos mejor a nosotros que nosotros mismos, puesto a que recolectan mucha información desde diferentes puntos, que contiene nuestras costumbres, preferencias y estilos de vida, lo cual implica un riesgo y vulneración a nuestra privacidad.

Además de la vulneración a nuestra privacidad, una parte importante es el propósito de esos datos, todo ese compendio de datos pasa a ser analizado por inteligencias artificiales que tienen la capacidad de predecir nuestro comportamiento e incluso manipularlo, son capases de detectar patrones y tendencias sobre nuestra forma de vida, y esta información desconocemos a ciencia cierta quien se beneficia de ella y para que, desde luego conocemos que se utiliza para la publicidad y el marketing, pero también puede ser utilizada como filtro, como violación de derechos, puede ser utilizada para reducir oportunidades automáticamente a préstamos, hipotecas, empleos, pueden emplear una discriminación sistemáticas.

"Ya no solo hablamos de publicidad personalizada, sino de poder denegar un seguro de coche, por ejemplo, si a través de los datos que recoge nuestra aplicación para

el navegador del coche, se puede determinar qué tipo de conductor somos" (Atico34, 2022).

Vulneraciones en el contexto IoT

Con la proliferación del uso del internet de las cosas, se han evidenciado varias vulneraciones que han existido en cuando a la privacidad del usuario, desde vigilancia hasta robo de información, además de que existen casos en donde los dispositivos IoT, capturan datos sin que el usuario lo sepa, llegando al espionaje.

En la actualidad, han surgido incidentes en los que dispositivos conectados a redes Wifi, enviaban información de los usuarios al fabricante y a entidades no autorizadas, generando inquietudes en torno a la privacidad en el contexto del Internet de las Cosas. Por ejemplo, algunas laptops tenían la capacidad de transmitir imágenes en tiempo real desde la cámara frontal sin activar la luz indicadora, mientras que televisores inteligentes y altavoces registraban conversaciones mientras estaban a la espera de la orden de sus propietarios para reproducir una canción específica.

Durante el año 2021, un conjunto de delincuentes informáticos consiguió evadir las medidas de seguridad cibernética de la compañía Verkada, obteniendo acceso a los registros audiovisuales almacenados en las cámaras de seguridad de la empresa de renombre. De acuerdo con los informes, estos criminales cibernéticos lograron vulnerar el sistema de cámaras y obtuvieron entrada a las imágenes y videos durante un período de 48 horas (Santos, 2023).

Centrándonos y profundizando más en la privacidad de los datos de los usuarios, es considerable destacar las combinaciones de recolección de datos que se dan dentro del IoT, que pasan desapercibidos y parecen inofensivos, pero que son más importantes de lo que se cree.

Cuando estos flujos de datos individuales se combinan o correlacionan, el perfil digital resultante de las personas tiende a ser más intrusivo que el que podría deducirse de un solo flujo de datos. Por ejemplo, un cepillo de dientes con conectividad a Internet podría recopilar y transmitir detalles sobre los hábitos de cepillado de alguien, lo cual parece inofensivo. Sin embargo, si se añade el hecho de que el refrigerador del mismo usuario registra la lista de alimentos consumidos, y si además el dispositivo usado para monitorear la actividad física provee información correspondiente, la conjunción de estos flujos de datos crea una representación mucho más minuciosa y privada de la salud general de la persona. Este proceso de combinación de datos puede tener un impacto especialmente significativo en el contexto de los dispositivos de la IoT, ya que muchos generan metadatos adicionales como marcas de tiempo y datos de geolocalización, incrementando aún más la especificidad de la información del usuario (Martinez, 2022).

Son muchas las finalidades que las empresas le pueden dan a esos valiosos datos que recopilan sobre nuestro comportamiento y estilo de vida, ejemplo:

Si alguien realiza cambios constantes en el ajuste del termostato, esta información podría resultar útil para comerciantes especializados en vidrios aislantes, empresas que ofrecen prendas más cálidas e incluso publicidades dirigidas a mantas eléctricas. Además, hackers podrían acceder a datos no cifrados de un dispositivo doméstico inteligente para averiguar qué programa de televisión se estaba viendo y luego emplear esta información. Asimismo, se podría emplear para construir perfiles de hogares y usuarios, que representan datos de mercadotecnia sumamente valiosos (Parlé, 2021).

Profundizando en el espionaje, son muchos los productos que recogen información sin que el usuario siquiera lo sospeche, recogen datos íntimos y muy posiblemente, vendiéndoselo a terceros.

Muchos de nuestros dispositivos IoT, de última generación, cuentan con características muy interesantes, disponen de micrófonos, reconocimiento de vos, reconocimiento de imagen, múltiples sensores (de proximidad, luz, temperatura) que les permite, aun sin que el usuario los utilice, detectar la presencia del usuario y comenzar a recolectar datos selectivos, como las conversaciones, entre otras actividades, y transmitirlo a una nube (de la cual, pueden obtener acceso terceros), ya que siempre están conectados a internet, incluso aun estando apagados.

"Una persona podría estar en presencia de este tipo de dispositivos sin saber que sus conversaciones o actividades están siendo monitoreadas o que sus datos están siendo registrados" (Martinez, 2022).

MARCO METODOLÓGICO

En el presente trabajo de investigación: estudio de caso, para su construcción se llevó a cabo el uso de varios métodos de investigación, siendo indispensable el *método bibliográfico*, mediante este método, se permite extraer información importante para el desarrollo del tema en cuestión, esto se logró a partir de mucha exploración y lectura.

El método bibliográfico, en este estudio de caso, se integra muy bien con el *método analítico*, ya que toda la información recogida mediante el uso del anterior método, es necesaria interpretarla y analizarla para que pueda ser fructífera para esta presente investigación.

Junto con el enfoque o método analítico, también se complementó el *método inductivo*, este método nos ayuda a poder dar conclusiones generales a partes de los

datos analizados particularmente, implica el razonamiento de lo obtenido con el método analítico a partir de la información recolectada con el método bibliográfico.

Las técnicas de investigación para este presente estudio, de acuerdo con la metodología empleada y los objetivos establecidos son: *Revisión Bibliográfica*, con la cual podemos recopilar información de documentos e información ad hoc a nuestro tema de estudio, asimismo, se utilizó la técnica de *Análisis Documental*, parecida a la anterior, aquí se recoge y escoge información relevante a partir de distintos medios, escrito, visuales, audiovisuales, evocando a la técnica de *Análisis Inductivo*, donde mediante razonamiento, finalmente llegar o desarrollar conclusiones a partir de todo lo anteriormente analizado.

Como instrumento para la recolección de datos para esta presente investigación se empleó las *fichas de trabajos bibliográficos*, que sustentan la base de la investigación en la que se utilizó citas textual y paráfrasis.

RESULTADOS

Mediante las metodologías utilizadas en este presente trabajo, se pudo llevar a cabo la construcción de este caso de estudio, mediante la recopilación de información, el análisis de la información recopilada y su posterior interpretación y razonamiento.

El objetivo de este estudio fue analizar los riesgos y la exposición de la privacidad de los datos del usuario en el contexto del Internet de las Cosas. Nos planteamos tres objetivos, con el fin de desglosar el tema, para observarlo por partes y poder llegar a la comprensión general del tema y su conclusión.

Con el primer objetivo, se descubrió y describió la creación, importancia y relevancia del internet de las cosas, siendo una tecnología nueva, que se viene gestando poco a poco, a medida que la tecnología lo permitió: como la aparición del internet, la

World Wide Web, tecnologías de transmisión de datos inalámbricos, entre otras mencionadas en este estudio. La proliferación del IoT resultó ser tanta, a tal punto que para muchas industrias se está volviendo indispensable. Invariablemente, todos usamos de alguna manera el internet de las cosas, desde nuestros hogares hasta en los hospitales, proporcionando ventajas inigualables y mucha comodidad en los usuarios, sin embargo, toda esa comodidad debe tener su costo (y la palabra costos no se limita a lo monetario).

Mediante el segundo objetivo, se pudo adentrar más al funcionamiento como tal del internet de las cosas. Las cosas, como cortinas, ropas, focos, cámaras, televisores, es decir, la gran mayoría de los productos ahora están dotados de internet y con ello, de sensores, y la tendencia sólo parece ir en crecimiento, todas estas cosas capturan datos de manera autónoma, sin necesidad de que el usuario intervenga, recopilan datos y comparten estos datos, ya que estas cosas o dispositivos inteligentes, están interconectados entre sí y estos datos se van hacia una nube, en la cual, con los datos en la nube, grandes cantidades de datos, mediante tecnologías potentes como inteligencias artificiales y el big data, son analizados extrayendo e identificando patrones de conducta sobre el usuario y desde luego, dotando de inteligencia a las *cosas*, para que puedan tomar decisiones y ejecutar acciones.

El tercer objetivo nos permitió analizar más a fondo al internet de las cosas, y analizar más detalles sobre su funcionamiento y lo que implica para los usuarios, puesto a que el utilizar IoT en nuestras vidas, es una gran ventaja y es una tecnología que vino a mejorar muchas cosas, y si para funcionar tiene que recopilar datos nuestros, compartirlos, analizarlos y sacar conclusiones, hasta cierto punto, parece valer la pena, sin embargo, poco se analiza sobre la privacidad del usuario y si esto puede representar un riesgo. El IoT, puede llegar a ser muy invasivo con la privacidad del usuario, llegando a no respetarla, ya que, la información recopilada, muchas veces es compartida

a terceros, desconociendo el usuario, como aquel tercero va a utilizar aquella información delicada, además de eso, el IoT recopila más datos de los que creemos, ya que los dispositivos continúan recopilando datos aun estando apagados, ya que muchos de esos dispositivos están dotados de sensores, cámaras, micrófonos que permanentemente recogen información, llegando a la vigilancia y espionaje y con esta información, además de la publicidad, puede ser utilizada para manipular al usuario de muchas maneras, para quitarle derechos o ventajas competitivas sistemáticas al solicitar un empleo o un crédito o una admisión a una institución de educación superior, sin dejar de lado el riesgo latente de sufrir el ataque de un ciberdelincuente, que también pueda acceder a esta información, robarla y manipular el funcionamiento de aquellos dispositivos.

DISCUSIÓN DE RESULTADOS

El internet de las cosas es una tecnología relativamente nueva, que llegó para quedarse. Como se pudo observar a lo largo de la construcción de esta investigación y en los resultados de la misma, el IoT es utilizado en muchas áreas e industrias y también en nuestros hogares, siendo estos los datos más importantes para las empresas, los datos de nuestro comportamiento y vida diaria.

En un futuro no muy lejano, la tecnología que mayor cantidad de datos produzca será el internet de las cosas, actualmente tenemos más *cosas* conectadas a internet que *personas* en todo el planeta, son 10.000 millones de dispositivos conectados registrados en 2021 y en la actualidad 2023 somos 7.900 millones de personas las que habitamos este planeta, y claramente se estima que para el 2025, los dispositivos conectados

dupliquen su marca actual, lo que nos lleva a que mientras más se prolifera esta tecnología, menos personas entienden de qué va y los riesgos que conlleva para la privacidad.

Los dispositivos inteligentes conectados internet (IoT), recopilan todo tipo de datos que les es posible, la mayoría de los procesadores utilizados cuentan con su propio sistema operativo independiente como Minix o Intel ME que tienen control total del dispositivo o computador, privilegios únicos y no puede ser desactivado por el usuario, además que puede ser controlado de manera remota, claramente permanecen ocultos a ojos del usuario, asimismo con televisores, consolas de videojuegos, refrigeradoras que recopilan datos, conversaciones, entre otras cosas sin que el usuario se dé cuenta.

Minix "tiene por función hacer de un subsistema informático pequeño de muy bajo nivel y muy silencioso. Este chip posee privilegios para actuar sobre todo el hardware, incluso cuando está inactivo o antes de que inicie el sistema operativo" (Araujo, 2022).

Con toda esta masiva cantidad de datos, se crea un perfil público muy detallado y preciso del usuario, así como también aumenta la huella digital y también el ID de publicidad, todos contamos con un ID de publicidad que nos asignan ciertas empresas como Google al usar sus servicios, entonces, todos estos perfiles recogen los hábitos de conducta, preferencias, programas favoritos, hábitos de sueño, alimentación, lugares favoritos, estilo de manejo, actividad física, entre otras muchas cosas y con esto crear un arquetipo de la persona y conocer cómo hacerle llegar publicidad persuasiva al usuario, manipularlo por cierto candidato político e incluso, que empresas de seguros, créditos, salud, reclutamiento para un empleo, hagan uso de estos datos recopilados y automáticamente negarle esas oportunidades.

El Experto en Protección de Datos y Privacidad, Alfonso Querol (2021) manifiesta:

> Si se junta la información de mi frigorífico, junto con la de mi televisor, y la de mi pulsera de actividad, tendrán un perfil completo de mi día a día, sabiendo por dónde y cómo me muevo, a qué hora preparo la comida, cuándo me siento a cenar y qué serie o programa veo mientras tanto. Un suculento menú para las empresas dedicadas al análisis del big data y a la prestación de servicios publicitarios orientados.

Aún no existen regulaciones severas o leyes que atenúen la recopilación excesiva de los datos de los usuarios para beneficio de su seguridad y privacidad, puesto que la tecnología siempre prolifera más rápido que la propuesta y aprobación de leyes, además de la implicación de conocer sobre el funcionamiento de estas tecnologías y sus métodos nocivos es tardío, que incluso, poco se habla de la privacidad en el contexto del internet de las cosas.

CONCLUSIONES

Con base a los objetivos planteados en este caso de estudio, concluimos con:

En primer lugar, se contextualizó el concepto del Internet de las cosas, destacando su creciente relevancia en nuestra vida cotidiana y cómo ha transformado la interconexión de dispositivos y datos. Esto proporcionó un marco sólido para comprender la magnitud de la influencia del IoT en nuestras vidas y cómo los dispositivos conectados han llegado a ser ubicuos en diversos entornos.

Al evaluar cómo los dispositivos IoT recopilan, almacenan, procesan y comparten datos de los usuarios, se identificó un conjunto diverso de métodos y técnicas utilizados para recolectar información. La proliferación de sensores y la

capacidad de comunicación inalámbrica de estos dispositivos han ampliado significativamente su capacidad para recopilar datos en tiempo real. Se discutió cómo estos datos se almacenan en la nube y se procesan para extraer información valiosa, planteando preocupaciones sobre la seguridad, privacidad y el control de los datos.

En relación con el tercer objetivo específico, se analizó detalladamente cómo los riesgos de privacidad de los datos asociados con el IoT pueden afectar a los usuarios. Se observó que la recopilación masiva de datos puede llevar a la creación de perfiles de usuarios altamente detallados, lo que potencialmente compromete la privacidad personal. La falta de estándares de seguridad uniformes y la insuficiente educación sobre el uso seguro de los dispositivos IoT se presentaron como desafíos importantes que deben ser abordados para proteger la privacidad de los usuarios.

RECOMENDACIONES

De acuerdo con las conclusiones, se recomienda:

Fomentar la educación y conciencia para los usuarios sobre la importancia de la privacidad de los datos en el contexto del IoT. Los usuarios deben comprender cómo funcionan los dispositivos IoT, qué datos se recopilan y cómo pueden tomar medidas para proteger su privacidad. Además, la investigación sobre privacidad y seguridad en el IoT debe continuar; universidades, instituciones de investigación y la industria deben colaborar para identificar y abordar nuevas amenazas y vulnerabilidades e instar el desarrollo de estándares de seguridad y privacidad a gobiernos y autoridades.

Promover que las empresas que desarrollan dispositivos IoT sean transparentes sobre la recopilación, uso y compartición de datos de usuarios, esto debería incluir la explicación detallada de cómo se utilizarán los datos y qué beneficios (y posibles riegos) obtendrán los usuarios a cambio y que ellos elijan dar su consentimiento, además, las empresas deberían ofrecer a los usuarios herramientas fáciles de usar para administrar y controlar sus datos. Esto incluye la capacidad de revisar y eliminar datos, así como configurar preferencias de privacidad de manera sencilla.

Revisar las políticas de privacidad antes de utilizar un dispositivo IoT y considerar cuidadosamente las implicaciones de privacidad, además tratar de limitar la cantidad de información personal que comparten con dispositivos IoT y aplicaciones, sólo proporcionando los datos necesarios para su funcionamiento. Es importante que los usuarios cambien las contraseñas predeterminadas en dispositivos IoT para evitar el acceso no autorizado.

REFERENCIAS

alltimeiot. (17 de Diciembre de 2021). *alltimeiot*. Obtenido de alltimeiot.com: https://alltimeiot.com/blog4.html

Alonso, R. (13 de Febrero de 2023). *hardzone*. Obtenido de hardzone.es: https://hardzone.es/reportajes/que-es/internet-cosas-iot/

Araujo, V. (19 de Junio de 2022). *siliseed*. Obtenido de siliseed.com: https://siliseed.com/que-es-el-intel-management-engine-intel-me-conceptos-y-peligros/

Atico34, G. (23 de Junio de 2022). *protecciondatos-lopd*. Obtenido de protecciondatos-lopd.com: https://protecciondatos-lopd.com/empresas/internet-de-las-cosas/

bisite. (17 de Agosto de 2022). *bisite*. Obtenido de bisite.usal.es: https://bisite.usal.es/es/blog/formaci-n/22/08/17/aplicaci-n-e-importancia-de-la-iot-en-la-actualidad-bisite

Carlemany, U. (21 de Junio de 2021). *universitatcarlemany*. Obtenido de universitatcarlemany.com: https://www.universitatcarlemany.com/actualidad/blog/internet-de-las-cosas-definicion-y-ejemplos/

Comunicación, A. (19 de Abril de 2023). *santanderconsumer*. Obtenido de santanderconsumer.es: https://www.santanderconsumer.es/simplefinance/blog/tu-futuro/ciberseguridad/post/iot-que-es-y-como-proteger-tu-intimidad

Equipo editorial, E. (23 de Enero de 2023). *humanidades*. Obtenido de https://humanidades.com/: https://humanidades.com/internet/

EvaluandoSoftware, D. C. (18 de Mayo de 2022). *evaluandosoftware*. Obtenido de evaluandosoftware.com: https://www.evaluandosoftware.com/tecnologias-aplicaciones-utilizadas-internet-las-cosas/

financialcrimeacademy. (25 de Julio de 2023). *financialcrimeacademy*. Obtenido de financialcrimeacademy.org: https://financialcrimeacademy.org/es/que-son-los-datos-y-la-informacion-por-que-es-importante-conocer-su-diferencia/

Gil, K. G. (08 de Julio de 2021). *bbva*. Obtenido de bbva.ch: https://www.bbva.ch/noticia/que-tecnologias-hay-detras-del-internet-de-las-cosas/

Gil, K. G. (5 de Octubre de 2021). *bbva*. Obtenido de bbva.ch: https://www.bbva.ch/noticia/principales-aplicaciones-del-internet-de-las-cosas/

Gracia, M. (11 de Enero de 2019). *deloitte*. Obtenido de deloitte.com: https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

INEC. (Julio de 2023). *ecuadorencifras*. Obtenido de ecuadorencifras.gob.ec: https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

Kuan, F. (18 de Agosto de 2017). *mokosmart*. Obtenido de mokosmart.com: https://www.mokosmart.com/es/what-is-a-smart-device/

Martinez, A. (19 de Noviembre de 2022). *issuu*. Obtenido de issuu.com: https://issuu.com/anfemagos/docs/la_internet_de_las_cosas/s/17420592

Olivas, J. Á. (15 de Julio de 2022). *obsbusiness*. Obtenido de obsbusiness.school: https://www.obsbusiness.school/blog/el-uso-impreciso-de-los-terminos-datos-informacion-y-conocimiento

Parlé, E. (29 de Septiembre de 2021). *parlemag*. Obtenido de parlemag.com: https://parlemag.com/es/2018/10/internet-of-things-affect-security-privacy/

Querol, A. (20 de Julio de 2021). *impulsocooperativo*. Obtenido de impulsocooperativo.com: https://www.impulsocooperativo.com/te-espia-tu-televisor/

Sabas, A. (24 de Marzo de 2018). *sg*. Obtenido de sg.com.mx: https://sg.com.mx/revista/56/tecnologias-inalambricas-iot

Santos, J. (22 de Agosto de 2023). *deltaprotect*. Obtenido de deltaprotect.com: https://www.deltaprotect.com/blog/seguridad-iot-ciberseguridad-de-internet-de-las-cosas

sap. (7 de Agosto de 2023). *sap*. Obtenido de sap.com: https://www.sap.com/latinamerica/products/artificial-intelligence/what-is-iot.html

smowltech. (1 de Febrero de 2023). *smowl*. Obtenido de smowl.net/: https://smowl.net/es/blog/que-es-la-huella-digital-en-internet/

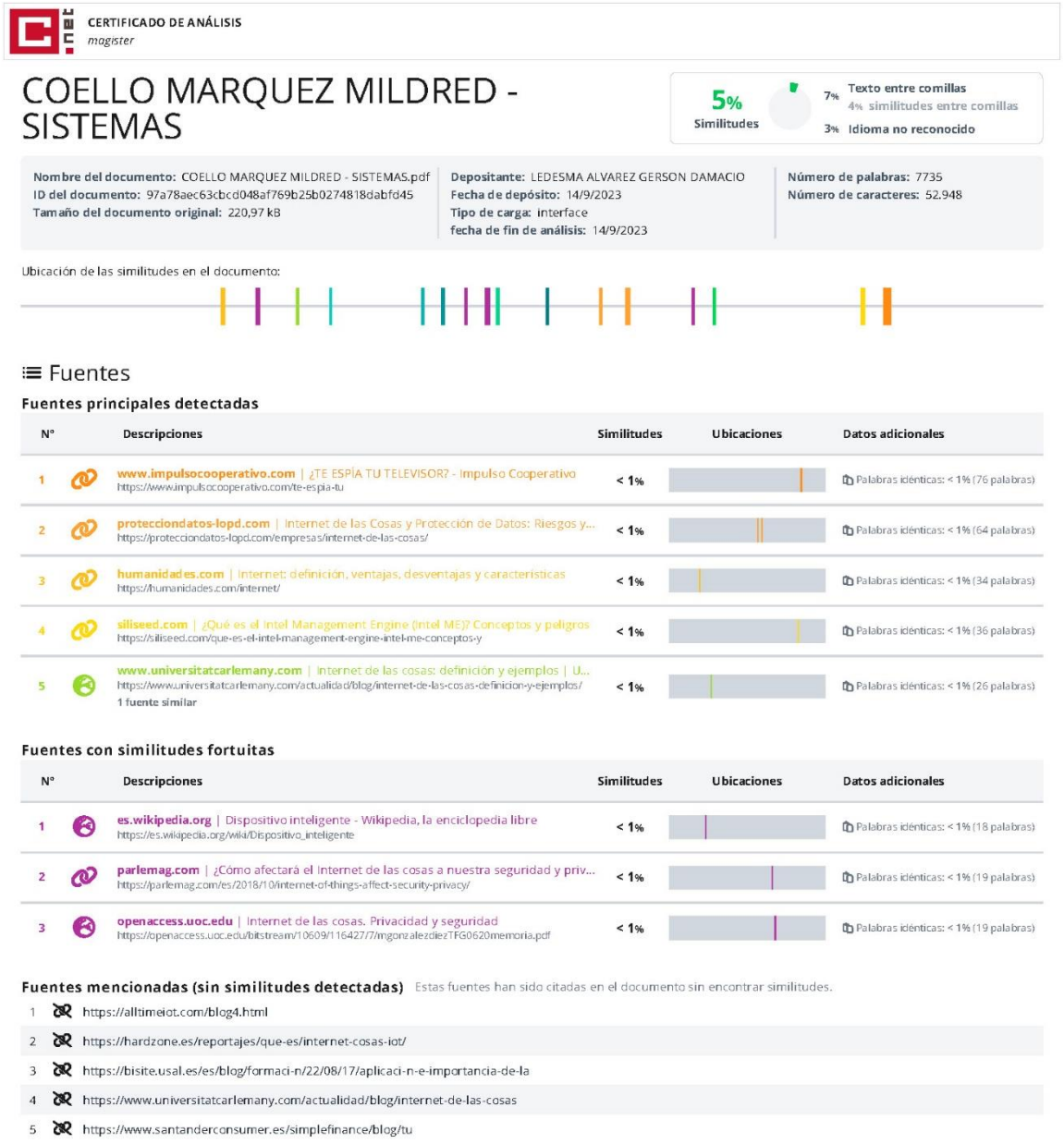
sydle. (22 de Marzo de 2022). *sydle*. Obtenido de sydle.com: https://www.sydle.com/es/blog/internet-de-las-cosas-6239c79c3bbdd676577a1e76

Takes, T. (27 de Marzo de 2023). *hp*. Obtenido de hp.com: https://www.hp.com/co-es/shop/tech-takes/dispositivos-inteligentes-smart

Tapia, I. (09 de Marzo de 2022). *wndgroup*. Obtenido de wndgroup.io: https://www.wndgroup.io/2022/03/09/internet-de-las-cosas-big-data/

Toyos, S. (10 de Octubre de 2018). *fracttal*. Obtenido de fracttal.com: https://www.fracttal.com/es/blog/9-aplicaciones-importantes-iot

ANEXOS



CERTIFICADO DE ANÁLISIS
magister

COELLO MARQUEZ MILDRED - SISTEMAS

5% Similitudes

7% Texto entre comillas
4% similitudes entre comillas
3% Idioma no reconocido

Nombre del documento: COELLO MARQUEZ MILDRED - SISTEMAS.pdf
ID del documento: 97a78aec63cbcd048af769b25b0274818dabfd45
Tamaño del documento original: 220,97 kB

Depositante: LEDESMA ALVAREZ GERSON DAMACIO
Fecha de depósito: 14/9/2023
Tipo de carga: interface
fecha de fin de análisis: 14/9/2023

Número de palabras: 7735
Número de caracteres: 52.948

Ubicación de las similitudes en el documento:

Fuentes

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.impulsocooperativo.com | ¿TE ESPÍA TU TELEVISOR? - Impulso Cooperativo https://www.impulsocooperativo.com/te-espia-tu	< 1%		Palabras idénticas: < 1% (76 palabras)
2	protecciondatos-lopd.com | Internet de las Cosas y Protección de Datos: Riesgos y... https://protecciondatos-lopd.com/empresas/internet-de-las-cosas/	< 1%		Palabras idénticas: < 1% (64 palabras)
3	humanidades.com | Internet: definición, ventajas, desventajas y características https://humanidades.com/internet/	< 1%		Palabras idénticas: < 1% (34 palabras)
4	siliseed.com | ¿Qué es el Intel Management Engine (Intel ME)? Conceptos y peligros https://siliseed.com/que-es-el-intel-management-engine-intel-me-conceptos-y	< 1%		Palabras idénticas: < 1% (36 palabras)
5	www.universitatcarlemany.com | Internet de las cosas: definición y ejemplos | U... https://www.universitatcarlemany.com/actualidad/blog/internet-de-las-cosas-definicion-y-ejemplos/ 1 fuente similar	< 1%		Palabras idénticas: < 1% (26 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	es.wikipedia.org | Dispositivo inteligente - Wikipedia, la enciclopedia libre https://es.wikipedia.org/wiki/Dispositivo_inteligente	< 1%		Palabras idénticas: < 1% (18 palabras)
2	parlemag.com | ¿Cómo afectará el Internet de las cosas a nuestra seguridad y priv... https://parlemag.com/es/2018/10/internet-of-things-affect-security-privacy/	< 1%		Palabras idénticas: < 1% (19 palabras)
3	openaccess.uoc.edu | Internet de las cosas. Privacidad y seguridad https://openaccess.uoc.edu/bitstream/10609/116427/7/mgonzalezdiezTFG0620memoria.pdf	< 1%		Palabras idénticas: < 1% (19 palabras)

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://alltimeiot.com/blog4.html
2 https://hardzone.es/reportajes/que-es/internet-cosas-iot/
3 https://bisite.usal.es/es/blog/formaci-n/22/08/17/aplicaci-n-e-importancia-de-la
4 https://www.universitatcarlemany.com/actualidad/blog/internet-de-las-cosas
5 https://www.santanderconsumer.es/simplefinance/blog/tu

Anexo 1. Informe Antiplagio

Anexo 2. Fichas Bibliográficas

Autor:

Fecha:

Titulo:

Sitio:

Consultado:

Fuente:

Anexo 3. Aplicación de la ficha bibliográfica

Autor: Cerem

Fecha: 04 de noviembre de 2022

Título: Por Qué El Internet De Las Cosas (IoT) Promete Cambiar La Vida Del Ser Humano.

Sitio: Cerem Global Business School

Consultado: 18 de agosto de 2023

Fuente: https://www.cerem.es/blog/porque-el-internet-de-las-cosas-iot-promete-cambiar-la-vida-del-ser-humano

Autor: Gracia, M.

Fecha: 11 de enero del 2019

Título: IoT - Internet Of Things

Sitio: Deloitte Touche Tohmatsu Limited

Consultado: 18 de agosto de 2023

Fuente: https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

Autor: Certus

Fecha: 27 de marzo de 2023

Título: Privacidad en la era de la inteligencia artificial y el internet de las cosas.

Sitio: Certus Legal Firm

Consultado: 18 de agosto de 2023

Fuente: https://certuslegalfirm.com/privacidad-en-la-era-de-la-inteligencia-artificial-y-el-internet-de-las-cosas/

Autor: Ayudaley

Fecha: 09 de junio de 2021

Título: Protección de datos en IoT (Internet de las Cosas)

Sitio: Ayuda Ley Protección Datos

Consultado: 21 de agosto de 2023

Fuente: https://ayudaleyprotecciondatos.es/2021/06/09/proteccion-datos-internet-de-las-cosas/

Autor: Izal, M.

Fecha: 12 de junio de 2019

Título: Seguridad y privacidad en la internet de las cosas: ¿a dónde van nuestros datos?

Sitio: The Conversation

Consultado: 22 de agosto de 2023

Fuente: https://theconversation.com/seguridad-y-privacidad-en-la-internet-de-las-cosas-a-donde-van-nuestros-datos-118414

Autor: Business Insider Intelligence

Fecha: 03 de febrero de 2022

Título: Estos son los problemas de seguridad y privacidad que vienen con el internet de las cosas.

Sitio: Business Insider México

Consultado: 22 de agosto de 2023

Fuente: https://businessinsider.mx/problemas-seguridad-privacidad-internet-de-las-cosas_tecnologia/