



**UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL CARRERA DE  
INGENIERÍA DE SISTEMAS**

**DISEÑO DE UNA ARQUITECTURA PARA BRINDAR SERVICIO DE  
DATOS GENERALES EN UNA EMPRESA PÚBLICA DEL ECUADOR BASADO EN  
IOT**

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

AUTOR: CARLOS ANDRÉS GARCÍA VALDIVIEZO

TUTOR: MAXIMO GIOVANI TANDAZO ESPINOZA

Guayaquil – Ecuador

2022

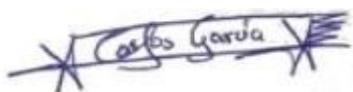
## CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Carlos Andrés García Valdiviezo con documento de identificación N° 0201563822 manifiesto que:

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

Guayaquil, 3 de agosto del año 2022

Atentamente,



---

Carlos Andrés García Valdiviezo

0201563822

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

Yo, Carlos Andrés García Valdiviezo con documento de identificación N° 0201563822, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: “Diseño de una arquitectura para brindar servicio de datos generales en una empresa pública del Ecuador basado en IoT”, el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

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

Guayaquil, 3 de agosto del año 2022

Atentamente,

A handwritten signature in blue ink that reads "Carlos García". The signature is written in a cursive style and is enclosed within a horizontal line that has asterisks at both ends.

---

Carlos Andrés García Valdiviezo  
0201563822

## CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Máximo Giovanni Tandazo Espinoza con documento de identificación N° 0916028921, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DISEÑO DE UNA ARQUITECTURA PARA BRINDAR SERVICIO DE DATOS GENERALES EN UNA EMPRESA PÚBLICA DEL ECUADOR BASADO EN IOT, realizado por Carlos Andrés García Valdiviezo con documento de identificación N° 0201563822, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 3 de agosto del año 2022

Atentamente,



---

Máximo Giovanni Tandazo Espinoza

0916028921

## **DEDICATORIA**

Dedico este trabajo a Dios debido que gracias a él, he podido culminar mi carrera Universitaria, a mi hermosa familia, mi esposa y mi hija que me han acompañado a lo largo de mi carrera y siempre me han motivado en todo lo que he emprendido.

A mis padres quienes siempre han estado a mi lado en las buenas y malas, con sus palabras de aliento y consejos me han apoyado para convertirme en el ser humano que soy.

A mi abuelo Carlos quien desde el cielo he sentido su presencia en mi vida, me cuida y me guía para que todo salga bien.

Finalmente a todas aquellas personas, amigos, compañeros, docentes y demás familiares que han puesto su confianza en mí y que de una u otra manera han contribuido en mi vida de estudiante con el fin que se vea cumplido mi sueño de culminar mi carrera Universitaria.

## **AGRADECIMIENTO**

En primer lugar y como debe de ser siempre de una manera muy especial quiero agradecer a Dios por darme la fortaleza y el conocimiento por haberme permitido superar cada una de las dificultades de mi vida universitaria, así mismo por la salud que me brindo lo cual me permitió ver culminada esta etapa tan importante de mi vida.

A mi querida familia, mi esposa Adela y mi hija Marthina quienes siempre serán mi mejor inspiración para ser cada día mejor.

A mis padres Mariana y Ubaldo por su apoyo constante sin dejarme solo en ningún momento y a todos aquellos que siempre me ofrecieron una mano amiga con amor, les ofrezco una humilde y eterna gratitud.

Para culminar me gustaría agradecer a todos mis docentes por la orientación prestada, por todo el conocimiento impartido, por el aliento a seguir adelante lo cual me permitió ver este anhelo hecho realidad, a todos aquellos que fueron parte de esta carrera universitaria les doy las gracias con todo mi corazón.

## **RESUMEN**

Se recolectó información sobre ecosistema IoT, el uso de IoT en empresas públicas a nivel global, arquitecturas y sus componentes en esta clase de sistemas distribuidos. El objetivo general es proponer un diseño de una arquitectura para brindar servicios de datos en una empresa pública del Ecuador basado en Internet de las Cosas. Se utiliza la investigación

empírico-analítico, la técnica de la observación, el enfoque cualitativo y se utiliza la revisión sistemática de la literatura sobre arquitecturas IoT. Los resultados son: Identificación de diferentes arquitecturas para conocer componentes que utilizan tecnología IoT, Diseño de una arquitectura para brindar servicio de datos en una empresa pública del Ecuador, y Elaboración de un caso de estudio. Se concluye que el diseño de arquitecturas IoT adecuadas son un excelente apoyo y generan beneficios desde el punto de vista tecnológico y pueden ser parte de las estrategias de información pública, además pueden mantener la interoperabilidad entre las empresas públicas.

**Palabras claves:** Organización pública, Internet de las cosas, Sistemas distribuidos, Arquitecturas distribuidas.

#### **ABSTRACT**

Information was collected on IoT ecosystem, the use of IoT in public companies globally, architectures and their components in this class of distributed systems. The general objective is to propose a design of an architecture to provide data services in a public company in Ecuador based on the Internet of Things. Empirical-analytical research, observation technique, qualitative approach are used and the systematic review of the literature on IoT architectures is used. The results are: Identification of different architectures to know components that use IoT technology, Design of an architecture to provide data service in a public company in Ecuador, and Elaboration of a case study. It is concluded that the design of appropriate IoT architectures are an excellent support and generate benefits from the technological point of view and public information strategies can be part, in addition they can maintain interoperability between public companies.

**Key words:** Public organization, Internet of Things, Distributed systems, Distributed architectures.

## ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN .....	8
2. REVISIÓN DE LITERATURA.....	11
2.1. Internet of Things (IoT).....	11
2.2. IoT en empresas públicas a nivel global .....	11
2.3. Seguridad de información en IoT .....	12
3. METODOLOGÍA .....	14
4. RESULTADOS	
4.1. Identificación de diferentes arquitecturas para conocer componentes que utilizan .....	18
tecnología IoT mediante una revisión sistemática .....	18
4.2. Diseño de una arquitectura para brindar servicio de datos en una empresa pública del Ecuador basado en Internet de las Cosas .....	21
4.3. Elaboración de un caso de estudio para determinar los recursos mínimos en su posible implementación mediante la descripción.....	24
5. DISCUSIÓN.....	27
6. CONCLUSIÓN .....	27
REFERENCIAS.....	28

### 1. INTRODUCCIÓN

Internet of Things (**IoT**) es un componente en la gestión y gobernanza de Gobierno Inteligente para cumplir con la optimización de servicios, cooperación social y gobernanza en la innovación de las relaciones mediante las Tecnologías de Información (Branco et al., 2020). IoT permite el seguimiento y control de objetos conectados a la red de una infraestructura gestionados por medio de un sistema integrado, por esto muchas actividades son más eficientes por la gestión de datos, servicios y operaciones en corto tiempo (Hakim & Putriandita, 2018).

Por el crecimiento de la tecnología IoT se estima que para el año 2025 existan 74 mil millones de dispositivos IoT conectados a nivel mundial con un valor aproximado de 1,6 trillones de dólares (Tomicic & Grd, 2020). Existe un aumento exponencial de dispositivos como sensores,

teléfonos inteligentes, actuadores y hardware inteligente que forman parte de Internet de las cosas (IoT) mediante interconexión y comunicación en Internet; hoy es sencillo adaptar y conectar cosas a una red y generar datos valiosos de acuerdo a los requisitos de una organización o empresa (Kolur & Reshmi, 2020).

IoT es utilizado en escenarios como: salud, ciudades, hogares, transporte, cadena de suministro, logística, monitoreo (Bharat Kumar, 2018), campus universitario (Webb & Hume, 2018), vigilancia, centros comerciales, fábricas, bancos, industrias, redes de empresa (Kolur & Reshmi, 2020), agua, basura, centro de control, edificios (Al Sultan & Suleiman, 2021), electricidad (Branco et al., 2020) y en mitigación contra COVID-19 (Upadhyay et al., 2020). El 77% de las organizaciones creen que las conexiones de dispositivos generan nuevos desafíos de seguridad y el 23% no lo considera; otro 82% de organizaciones cree en dificultades de los dispositivos conectados y el 18% no lo considera; cada vez crece la demanda en sensores o dispositivos informáticos en redes dentro de una “estructura de gobierno formal” para proteger los servicios y certificar el buen uso de los dispositivos y redes (Webb & Hume, 2018).

En tecnología, “Valor público” es un concepto en tendencia, esto significa el valor de los ciudadanos, calidad de datos y servicios que brinda un gobierno mediante Tecnologías de la Información, es decir servicios del gobierno electrónico, aquí se involucra IoT que utiliza un gobierno para optimizar sus servicios y entregar estos servicios e información de buena calidad para los ciudadanos (Chohan & Hu, 2020).

La utilización de IoT en el sector público genera servicios eficientes debido a las prácticas de transparencia, un gobierno tiene a la vista la buena oportunidad en la optimización de servicios mediante la retroalimentación de datos generados por tecnología IoT y toma de decisiones en mejor tiempo; algunos usos en gobierno son: iluminación, calefacción y enfriamiento, reducción de costos operativos, mejorar las respuestas, aumentar la eficiencia, procesamiento de datos, datos abiertos y bienestar de los ciudadanos, interconexión de instituciones o estados, plantear nuevas tácticas para la administración (Alonaizi & Manuel, 2021).

Los dominios IoT demandan infraestructuras cada vez más confiables y escalables para instituciones o ciudades, esto acelera la propuesta de proyectos en muchos escenarios a nivel global y genera buenas oportunidades en diseño e implementación.

¿Puede una organización pública gestionar eficazmente la información y las conexiones de dispositivos IoT?

Es factible la implementación de sistemas IoT diseñados de manera correcta y sustentado en la investigación científica para la mejora en los productos, servicios y consumos en el sector público, además es posible identificar comportamientos de las personas basados en los datos obtenidos de un ecosistema. IoT mejora la entrega de servicios gubernamentales a los ciudadanos y empresas, aumenta la capacidad de los ciudadanos para acceder a información, optimiza la gestión gubernamental, aumenta la transparencia y disminuye costos (Branco et al., 2020). Un gobierno puede utilizar dispositivos IoT en dos dimensiones: a) recopilar datos sobre la práctica de los servidores públicos/procedimientos/políticas y b) entregar mejores servicios en tiempo real de acuerdo a las condiciones de cada institución (Alonaizi & Manuel, 2021).

Se propone utilizar IoT para conectar varios dispositivos heterogéneos preservados por una arquitectura en niveles adaptables para que los dispositivos, los ciudadanos y los servicios en la nube se combinen para gestión de servicios gubernamentales en una aplicación informática, además que sea flexible y escalable para una organización de carácter público porque los dispositivos y servicios se pueden actualizar, adicionar o eliminar.

El sustento legal para esta propuesta es la Política de Ecuador Digital del año 2019 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019) que en sus artículos especifica el avance hacia una economía basada en tecnologías, con el uso de datos abiertos dentro de una economía digital y transformación digital apalancados en IoT, Big Data, Cloud, IA, entre otros, la cartera de estado encargado de este proceso es el Ministerio de Telecomunicaciones.

El objetivo general es proponer un diseño de una arquitectura para brindar servicios de datos en una empresa pública del Ecuador basado en Internet de las Cosas.

## 2. REVISIÓN DE LITERATURA

### 2.1. Internet of Things (IoT)

IoT es una tecnología que permite la captura, procesamiento e intercambio de datos a través de dispositivos electrónicos conectados a Internet, en IoT los dispositivos inteligentes tienen asignada una dirección IP y algunos tienen control y gestión propia (Al Sultan & Suleiman, 2021). IoT contiene sensores distribuidos en la red para adquisición y captura de datos conectados con un sistema operativo integrado (Webb & Hume, 2018). IoT es un área con datos heterogéneos con variedad de dispositivos en red y dirección única que interactúan con personas u otros dispositivos para alcanzar objetivos comunes (Tomicic & Grd, 2020).

Los dispositivos IoT se clasifican en: sensores, actuadores y puertas de enlace. Los sensores capturan datos específicos de un ambiente como temperatura y humedad. Los actuadores ejecutan actividades en el ambiente como abrir cerraduras o encender/apagar un foco. Una puerta de enlace es un mediador en las comunicaciones de dispositivos a través de protocolos (Lins & Vieira, 2021).

Se considera que Cloud Computing e IoT deben ser propuestas consolidadas en todo proyecto, aunque son tecnologías autónomas son buenos complementos en el registro de datos, estructuración de datos, uso de aplicaciones informáticas y procesamiento distribuido, la Nube es un área o capa entre los dispositivos y las aplicaciones informáticas (Bharat Kumar, 2018).

### 2.2. IoT en empresas públicas a nivel global

La Universidad West Texas USA diseñó e implementó una IoT para gestión de datos obtenidos en parqueo de vehículos, agricultura y clima, la gestión se realiza por dispositivos móviles y comunicación inalámbrica, además aplicaron un estándar de seguridad llamado NIST (Webb & Hume, 2018).

En una empresa pública de EL SALVADOR se aplica IoT para disminuir el costo general de electricidad y aumentar la eficiencia; la arquitectura utiliza sensores para el consumo de energía y actuadores para control de equipos, los datos se almacenan en la nube para su seguimiento por medio de una aplicación informática; además la red IoT protege los equipos, controla el consumo y determina comportamientos de funcionarios (Branco et al., 2020).

Un proyecto de EEUU y JAPON realiza estudios de plataformas IoT para gobiernos y ciudades inteligentes, aquí se considera que en las organizaciones del gobierno deben participar los departamentos de planeación, tecnologías de información y operaciones, el caso de estudio fue aplicado a Tokio que integra a las empresa con tecnologías (Yamakami, 2017).

El gobierno de MALASIA a través de un ministerio tiene una hoja de ruta en planificación de IoT en áreas como economía, social y gobernanza para entregar beneficios a su población, además la privacidad y seguridad son temas importantes para los usuarios (Riniy et al., 2020).

en INDONESIA aplicaron IoT para la logística de materiales y entrega hacia las oficinas, la red se diseña para entregas estratégicas y distribución a tiempo basado en un plan de implementación (Hakim & Putriandita, 2018).

Investigadores de IRAN determinaron otros usos de IoT en gobernanza pública como: servicios en línea, seguimiento, recolección de datos, colaboración pública y optimización de la cooperación; en los procesos gubernamentales se debe considerar aspectos sociales, económicos, culturales, ambientales, facilitar el acceso a ciudadanos y aumento de la capacidad (Suleimany, 2021).

En INDIA, una empresa gubernamental utilizó IoT para la demanda y distribución de alimentos para los ciudadanos, la arquitectura tiene un dispositivo inalámbrico que emite un ticket a las autoridades, y además aprovecha la infraestructura de red y nube para avisar a las autoridades la ubicación geográfica del ciudadano, posible alerta y estado (Upadhyay et al., 2020).

Para realizar el seguimiento de la contaminación del aire en edificios adjuntos a oficinas administrativas en la INDIA, se instalaron sensores inalámbricos con protocolos para captura, envío y almacenamiento de datos en la nube, el almacén centralizado ayuda a reducir la contaminación en los edificios administrativos (Saha et al., 2017).

Se implementó una red IoT para vigilancia física que minimiza el trabajo humano en revisión activa de monitores para prevenir robos o evitar malos eventos, la red contiene micrófonos, cámaras, sensores, posicionamiento y conexión inalámbrica (Kolur & Reshmi, 2020).

### 2.3. Seguridad de información en IoT

El enfoque de la seguridad es un aspecto importante en IoT, es necesario adoptar alguna medida o técnica de seguridad en un entorno IoT, algunos aspectos que se consideran son seguridad

sobre el hardware, el software, el sistema operativo e interfaces de IoT; algunos requerimientos de seguridad son cifrado, autenticación, almacenamiento, prevención de ataques, alertas, detectar anomalías, actualización, puertos seguros, accesos autenticados y detectar actividades maliciosas (Lins & Vieira, 2021). La seguridad de información también es importante por la interacción con las personas y dispositivos de cualquier clase, los dispositivos IoT tienen limitaciones en procesamiento, conectividad y poder eléctrico (Tomicic & Grd, 2020).

### 3. METODOLOGÍA

Se utiliza la investigación empírico-analítico para analizar la factibilidad sobre el diseño de una arquitectura basado en IoT mediante evidencias empíricas. Se utiliza la técnica de la Observación para identificar diferentes arquitecturas y ayuda a conocer los componentes que utilizan tecnologías IoT. Se utiliza el enfoque cualitativo que ayuda en la investigación exploratoria y estudio de procesos en las arquitecturas IoT.

Se utiliza la revisión sistemática de la literatura (Beltran et al., 2017) para determinar y obtener artículos científicos sobre arquitecturas IoT, la revisión sistemática tiene 3 fases: a) Planificación, b) Conducción y c) Informes, ver Fig. 1.



*Figura 1. Fases de la revisión sistemática*

La fase **planificación** tiene 5 pasos: 1) Establecer las pregunta de investigación, 2) Definir la estrategia de búsqueda, 3) Seleccionar los estudios primarios, 4) Definición de la estrategia de extracción de datos, 5) Selección de métodos de síntesis

#### 1) Establecer las pregunta de investigación

Las preguntas de investigación son las siguientes:

¿Cuáles son los componentes generales de una arquitectura IoT?

¿Qué otras tecnologías se utilizan con IoT?

¿Cuáles son las medidas de seguridad que se utilizan en arquitecturas IoT?

#### 2) Definir la estrategia de búsqueda

La estrategia de búsqueda se aplica en las siguientes librerías virtuales: a) IEEE Xplore Digital Library, b) Springer Link, c) Science Direct y d) ACM

La cadena de búsqueda es: (IoT government) OR (architectures IoT) OR (IoT)

Los criterios de inclusión y exclusión son:

**Tabla 1.** Criterios de inclusión y exclusión.

Inclusión	Exclusión
Tema principal sobre IoT	Artículos resumen o cortos
Artículos desde año 2018	Artículos sobre encuestas
Sólo en idioma inglés	Artículos duplicados
Enfocados a la gestión gubernamental Acceso abierto	Pagar por artículo

Fuente: Elaboración propia.

### 3) Seleccionar los estudios primarios

La búsqueda se realiza con las cadenas de búsqueda en los datos que suministra cada librería virtual mencionada anteriormente, las cadenas de búsqueda se verifican en cada biblioteca para realizar una exploración consistente. Los resultados automáticos o manuales que son obtenidos en cada librería es revisada por el autor para verificar el título, en una siguiente revisión se verifica el resumen.

Para certificar el filtrado de cada documento científico, se realiza una revisión exploratoria del contenido para establecer la aprobación, la puntualidad y oposición de criterios, luego de la aprobación del documento se procede a la lectura completa.

Se incluyen los documentos que cumplen uno o más criterios de inclusión, y se excluyen los documentos que cumplen uno o más criterios de exclusión.

El resultado de aplicar los criterios de inclusión y exclusión en los artículos científicos, se plasma en la búsqueda de las librerías digitales en la Tabla 2.

**Tabla 2.** Resultados de la búsqueda.

Librería	Total	Excluidos	Duplicados	Filtrados	Artículos finales
IEEE Xplore	1583	1403	96	84	(Webb & Hume, 2018), (Bharat Kumar, 2018), (Kolur & Reshmi, 2020), (Branco et al., 2020), (Saha et al., 2017), (Upadhyay et al., 2020), (Suleimany, 2021), (Alonaizi & Manuel, 2021), (Chohan & Hu, 2020), (Riniy et al., 2020), (Yamakami, 2017), (Lins & Vieira, 2021), (Al Sultan & Suleiman, 2021), (Tomicic & Grd, 2020)
Springer Link	3756	3689	26	41	(Silva et al., 2022), (Satpathy et al., 2020), (Sitharthan & Rajesh, 2021), (Köksal & Tekinerdogan, 2019), (S. Sharma et al., 2019), (Memon et al., 2020), (Manimuthu et al., 2021), (Fersi, 2021), (Sarker et al., 2022), (Yu et al., 2016), (Adi et al., 2020), (Kim et al., 2017), (Kulkarni et al., 2021)

Science Direct	5842	5792	11	39	(Chatfield & Reddick, 2019), (Li et al., 2021), (Wirtz et al., 2019), (Hu et al., 2021), (da Silva Rodrigues, 2021), (Luo et al., 2019), (Tanasiev et al., 2021), (Popli et al., 2021), (A. Sharma et al., 2021), (Kumar et al., 2021), (Abdelouahid et al., 2021), (Daissaoui et al., 2020), (Traboulsi & Knauth, 2020), (Samaila et al., 2021), (Le et al., 2019), (Smith et al., 2021)
ACM 558 519 8 31					(Wei et al., 2018), (Wang et al., 2018), (Grammatopoulou et al., 2018), (Krintz et al., 2018), (Thurston & de Leon, 2018), (Aneiba et al., 2019), (Luckner et al., 2020), (Bideh et al., 2020), (Barakat et al., 2021), (Muccini et al., 2021), (Blower & Kotonya, 2021), (de Almeida Souza et al., 2021), (John et al., 2021)
Total 56 Artículos					

---

Fuente: Elaboración propia.

#### 4) Definición de la estrategia de extracción de datos

Se basa en generar el conjunto de datos para las respuestas de investigación realizadas en el primer paso, esto asegura la atención en los criterios de extracción a todos artículos seleccionados, para esto se utiliza una hoja electrónica con los siguientes datos en las columnas:

En un primer grupo llamado Documento está: Nombre del artículo, Sector aplicado, Año, Librería virtual, País e Implementado. En un segundo grupo llamado Componentes de arquitectura IoT está: Sensores, Drones, Cámaras, RFID, Micrófono, Laser-Infrarojo, Controladores y Arduino. En un tercer grupo llamado Otras Tecnologías está: Big Data, Cloud Computing, IA y Blockchain. En un cuarto grupo llamado Medidas de Seguridad está: Framework NIST, IEEE 802, Otro, N/A y Protocolos.

#### 5) Selección de métodos de síntesis

Como métodos de síntesis se aplica el método cuantitativo.

La síntesis cuantitativa informa las cantidades de artículos científicos que respondan las preguntas de investigación, utilizar diagramas de barras para informar los componentes en las arquitecturas IoT, otras tecnologías y las medidas de seguridad; utilizar diagramas de pastel para informar la proporción de protocolos utilizados en las medidas de seguridad. Además se genera una visión general en este campo de investigación y ver la cantidad de artículos encontrados en las librerías digitales.

**La fase de conducción:** Al aplicar el protocolo de revisión por medio de la revisión sistemática se obtuvo los resultados de acuerdo con los criterios de inclusión y exclusión; existen artículos científicos publicados en una o más revistas y se selecciona la primera versión; otros casos encontrados son artículos de solo resumen máximo una página, contenido del artículo diferente al idioma inglés, artículos de sólo texto sin gráficos que expliquen el modelo.

**La fase de informes:** Se detalla en la fase Resultados de este documento, se responde las preguntas de investigación y se representa una arquitectura con componentes adoptados de acuerdo a los resultados de las preguntas de investigación.

#### 4. RESULTADOS 4.1. Identificación de diferentes arquitecturas para conocer componentes que utilizan

tecnología IoT mediante una revisión sistemática.

Aquí se responden las preguntas de investigación para satisfacer este primer resultado.

##### ¿Cuáles son los componentes generales de una arquitectura IoT?

De acuerdo a los 56 artículos científicos obtenidos de la revisión sistemática, los componentes más nombrados en las arquitecturas o modelos IoT son sensores utilizados en 56 artículos, drones utilizados en 1 artículo, cámaras utilizados en 11 artículos, radio frecuencia utilizada en 8 artículos, micrófono utilizado en 1 artículo, laser utilizado o infrarrojo utilizado en 3 artículos, controladores utilizados en 20 artículos, y dispositivos arduino utilizado en 10 artículos. Esto quiere decir que, el 100% de los artículos utilizan sensores en sus propuestas, luego utilizan los controladores o actuadores para reaccionar de acuerdo a los datos capturados por los sensores como prender motores, aires acondicionados, riego de agua u otros, ver Fig. 2.

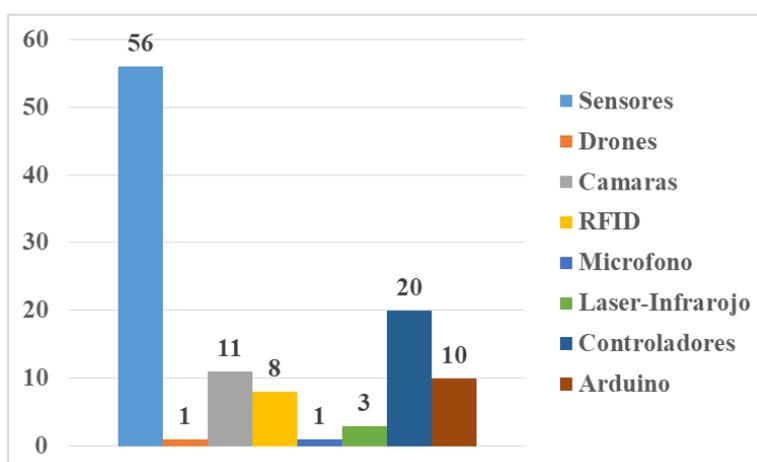
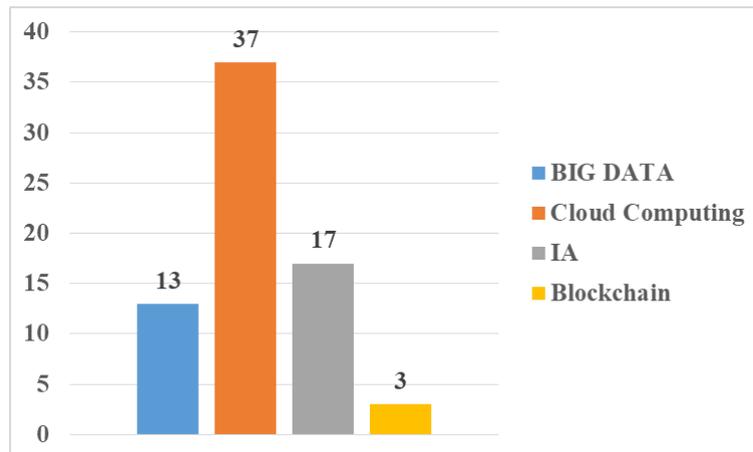


Figura 2. Componentes generales de una arquitectura IoT.

##### ¿Qué otras tecnologías se utilizan con IoT?

De acuerdo a los 56 artículos científicos obtenidos de la revisión sistemática, las tecnologías utilizadas en conjunto con IoT son: Big Data utilizada en 13 artículos con el objetivo de recolectar todos los datos que se generan, Cloud Computing utilizada en 37 artículos con el objetivo de brindar servicios, Inteligencia Artificial utilizada en 17 artículos con el objetivo de realizar predicciones o análisis, y Blockchain utilizada en 3 artículos con el objetivo de perpetuar la información resumida; esto confirma que IoT y Cloud Computing están adheridas

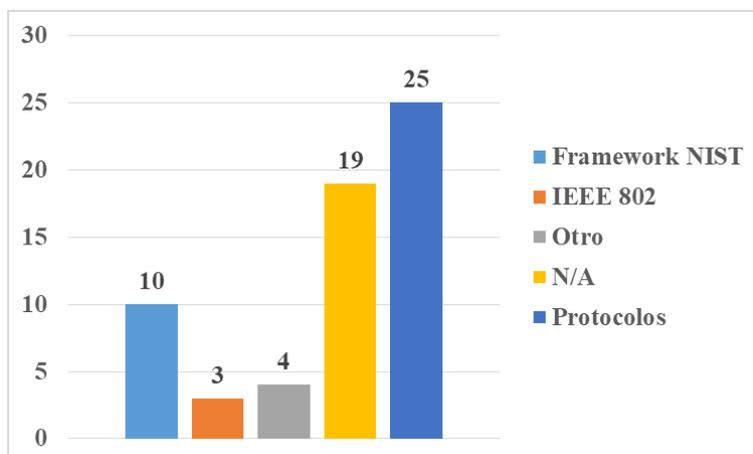
en concepto e implementación en 66% de los proyectos, el otro 34% no nombra la nube o son proyectos de alcance local como casas, fincas o edificios, ver Fig. 3.



*Figura 3. Tecnologías utilizadas con IoT.*

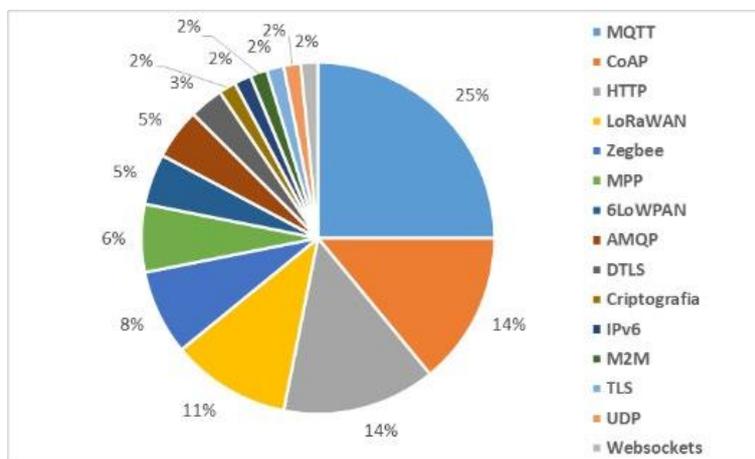
### ¿Cuáles son las medidas de seguridad que se utilizan en arquitecturas IoT?

De acuerdo a los 56 artículos científicos obtenidos de la revisión sistemática, las medidas de seguridad utilizadas en los artículos científicos son: framework NIST utilizado en 10 artículos y es un estándar internacional en seguridad utilizado en redes, el estándar IEEE utilizado en 3 artículos, otro grupo de 4 artículos nombra herramientas poco comunes, otro grupo de 19 artículos no nombra ninguna medida de seguridad en sus propuestas, y 25 artículos utilizan protocolos varios en la seguridad. Esto quiere decir que el 45% de las propuestas utilizan algún protocolo como protección, ver Fig. 4.



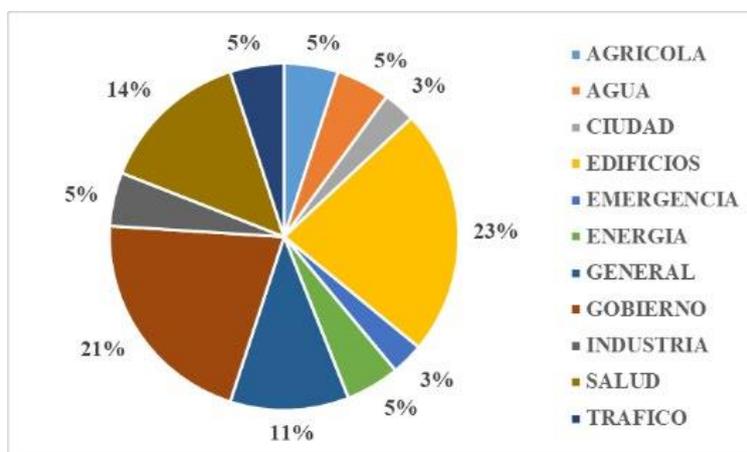
*Figura 4. Medidas de seguridad en arquitectura IoT.*

Entre los protocolos utilizados están: MQTT utilizado en 25%, CoAP utilizado en 14%, HTTP utilizado en 14%, LoRaWAN utilizado en 11%, Zegbee utilizado en 8%, MPP utilizado en 6%, 6LoWPAN utilizado en 5%, AMQP utilizado en 5%, DTLS utilizado en 3%, y Criptografía, IPv6, M2M, TLS, UDP, Websockets utilizadas en 2% cada uno. Esto quiere decir que, entre los 25 artículos que utilizan protocolos, 16 de ellos nombran el protocolo MQTT como medida de seguridad, luego el más utilizado es CoAP y HTTP, ver Fig. 5.



*Figura 5. Componentes generales de una arquitectura IoT*

Además, los 56 artículos científicos se clasificaron en sectores de aplicación, el mayor sector es Edificios con 23%, luego Gobierno con 21%, luego Salud con 14%, Área general con 11%, Agrícola con 5%, Agua con 5%, Ciudad con 3%, Emergencia con 3%, Energía con 5%, Industria con 5% y Tráfico con 5%. Esto quiere decir que la utilización de IoT en sector Gobierno es importante, ver Fig. 6.

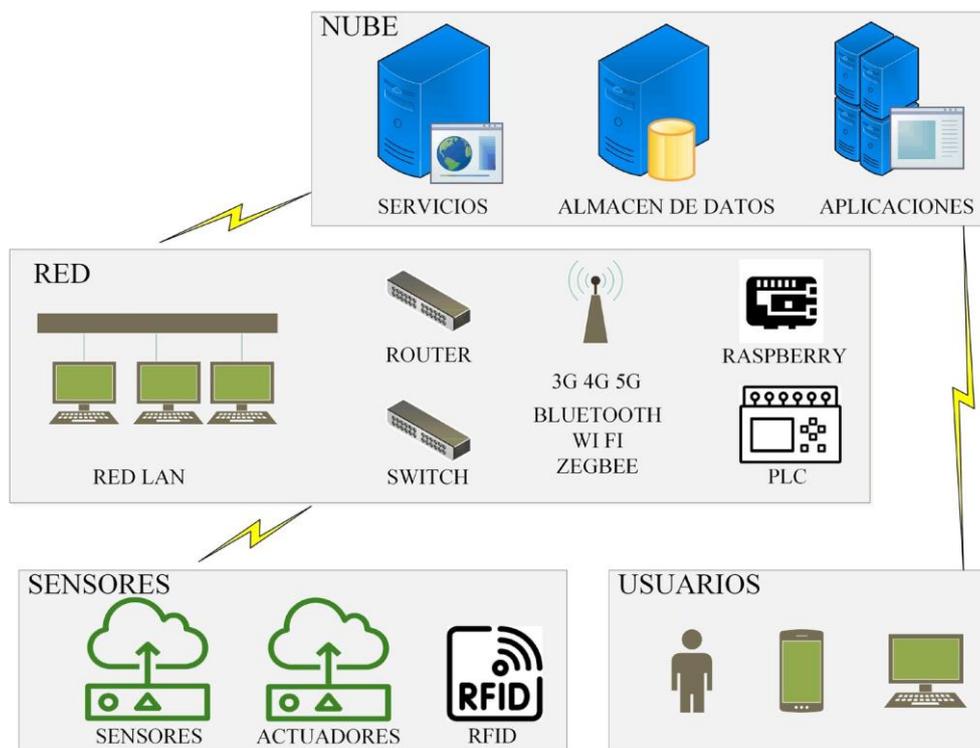


*Figura 6. Componentes generales de una arquitectura IoT*

Entre los 56 artículos científicos, el 41% si está implementado y 59% no está implementado. Entre los artículos que aplicaron al sector Gobierno sólo 2 fueron implementados. Además, los artículos científicos fueron realizados por investigadores de 33 países, aquí India tiene la mayor producción de 10 artículos, China tiene producción de 6 artículos, Reino Unido tiene producción de 5 artículos, USA tiene producción de 5 artículos, Brasil tiene producción de 4 artículos, Korea tiene producción de 4 artículos, otro grupo de 7 países tiene producción de 2 artículos cada uno, y otro grupo de 20 países tiene producción de 1 artículo cada uno.

#### 4.2. Diseño de una arquitectura para brindar servicio de datos en una empresa pública del Ecuador basado en Internet de las Cosas.

Se propone utilizar IoT para recolectar los datos de los sensores que se implementen en un empresa de carácter público y estos datos sirvan para entregar un servicio de información para la misma empresa o para los ciudadanos; se utiliza un protocolo de red para IoT, los datos se envían para guardarse en la nube, la nube apoya la gestión de los datos y los convierte en información; esta información es analizada por los ciudadanos o aplicaciones; el análisis continuo de la información es útil para minimizar esfuerzos adicionales y maximizar ventajas de una empresa pública, ver Fig. 7.



*Figura 7. Arquitectura IoT de servicio de datos.*

La arquitectura se propone de cuatro capas descritas a continuación:

**Capa de Sensores/Actuadores:** Esta capa se compone de sensores, actuadores, microcontroladores, radio frecuencia, cámaras, dispositivos bluetooth, módulo de conectividad, fuente de energía, otros dispositivos que pueden estar en esta capa son los dispositivos personales para salud y dispositivos de detección. Los dispositivos deberían consumir baja energía y tener batería de duración extendida. Los sensores capturan los aspectos o datos del mundo físico. Los sensores IoT apoyan el control de estado del ambiente físico sea en un edificio, oficina, calle u otro espacio, los datos recolectados son valiosos para rastrear o medir un ambiente o infraestructura.

Se utiliza Raspberry Pi que es una mini computadora de placa, tiene buenas capacidades informáticas y disponibilidad en los mercados, además posee un sistema operativo ligero, conveniente y compatible con cualquier dispositivo. Controlador programable (PLC) se utiliza para recolectar datos desde sensores análogos y convertir esos datos en digitales, por lo general los sensores cableados se conectan a un PLC que gestiona los datos en formato MQTT (Tanasiev et al., 2021).

**Capa Red:** Esta capa se centra en transferir los datos de la capa de sensores hacia la capa nube, existen diferentes clases de infraestructura de red como: inalámbrica, cableado o malla, entre las tecnologías de comunicación se utilizan 3G-4G-5G, Bluetooth, Wi-Fi, y ZigBee.

**Capa Nube:** IoT y Cloud Computing progresan de manera autónoma (Bharat Kumar, 2018), IoT se beneficia de las características y ventajas de la nube para equilibrar los requisitos de IoT como penetración, acceso al mundo real, computación limitada, almacenamiento limitado y datos fuentes para Big Data; la nube equilibra aquellos requisitos con representación global, recursos virtuales, computación ilimitada, almacenamiento ilimitado y gestión de Big Data. La nube con la computación ilimitada-paralela-distribuida junto a IoT componen una excelente perspectiva para muchas áreas o sectores de empresas públicas como salud, educación, energía, turismo, transporte, alcaldías, prefecturas, ministerios, secretarías, entre otras.

Se propone que la nube contenga Aplicaciones informáticas, Micro Servicios y Bases de Datos para realizar las funcionalidades de acuerdo al tipo de organización o empresa pública. A continuación se describen.

*Aplicaciones informáticas:*

Aplicaciones de prestación de servicios: Este tipo de programa realiza la prestación de servicios, además reduce costo, acelera los procesos burocráticos, minimiza las distancias geográficas y maximiza la entrega de servicios; con las aplicaciones informáticas los dispositivos de los ciudadanos se convierten en plataformas de entrega-recepción de servicios (Suleimany, 2021),

Aplicaciones de monitoreo: Este tipo de programa realiza el monitoreo de servicios e infraestructuras físicas, el monitoreo permite a los administradores analizar los sistemas y procesar eventos-alertas, monitoreo de crisis, aviso de peligros (incendios, terremotos, inundaciones, epidemias); esto se basa en los datos IoT recolectados, análisis y entrega de los datos a las aplicaciones web o móviles.

Aplicación recolector de datos: Este tipo de programa es costoso y complejo en ambientes IoT por que los dispositivos son variados y los datos son de diferentes tipos, como ejemplo clima, tráfico, edificios, entre otros; el programa debe ser modulado y actualizado de acuerdo a los dispositivos que recolectan datos, se transforman en una estructura general y se envía a la base de datos; un subprograma recolecta los datos generados por personas y otro subprograma recolecta los datos generados por el medio ambiente.

*Micro servicios*: Como recomendación se propone servicios de parqueo, reservas, clima, tiempo, generación de códigos QR, contador de personas y segmentación de cámaras.

*Almacén de datos*: Se propone utilizar una base de datos NoSQL MongoDB que es escalable y disponible, es utilizada en sector gubernamental (Branco et al., 2020), esta clase de base de datos se utiliza para almacenar los datos que son recolectados por los sensores, el aumento en la cantidad de sensores provoca el aumento en el almacenamiento de datos, está diseñada para hardware sencillo.

Se utilizan los siguientes criterios para la nube (Barakat et al., 2021):

- a) Que permita utilizar aplicaciones como: administración de dispositivos, visibilizar, almacenamiento, integración externa y adoptar protocolos de recolección de datos.
- b) Que permita continua actualización de la plataforma IoT, es decir mantenimiento por los administradores.

Para la comunicación y seguridad en el transporte de datos se adopta Message Queue Telemetry Transport (MQTT) que es un protocolo de traspaso de datos estándar para redes IoT, es ligero, realiza las actividades de publicación/inscripción de dispositivos remotos, tiene un código pequeño, y utiliza una pequeña parte del ancho de banda.

De acuerdo a (Sarjerao & Prakasarao, 2020), MQTT es más conveniente que HTTP para la comunicación entre dispositivos IoT y entre plataformas de IoT por su ligereza, de acuerdo a (Bansal & Priya, 2021) MQTT es más confiable que CoAP.

**Capa Usuarios:** Aplicaciones móviles: Se propone una aplicación móvil generalizada en la entrega de turnos para ciudadanos y entrega de información básica de la empresa pública, aunque se debe considerar otra información de acuerdo a los objetivos de la organización pública, por ejemplo el ministerio de salud entrega atención médica y medicina, un municipio entrega información sobre predios urbanos. Esta aplicación móvil debe validar los datos del ciudadano como cedula de identidad, número de teléfono celular y código de huella dactilar, esta validación es rápida y descentralizada por las características de la nube.

Aplicación web o redes sociales: El uso de una aplicación web y redes sociales se realiza para entrega de datos a los ciudadanos, la aplicación web que es más amplia para entrega o recolección de más datos y guardado en la base de datos, la red social debe conectarse a un micro servicio que obtenga los datos del sistema y entregue al ciudadano, y además obtenga los datos del ciudadano y entregue al sistema.

#### 4.3. Elaboración de un caso de estudio para determinar los recursos mínimos en su posible implementación mediante la descripción.

Se propone un caso de estudio en un área específica de la Corporación Nacional de Telecomunicaciones Empresa Pública (CNT-EP), el área de caso es un centro de integrado de servicio (CIS), los CIS atienden a los clientes de la empresa a través de 55 centros en Ecuador, cada centro tiene un espacio físico con ventanillas de atención, sala de espera, posibles parqueos, aire acondicionado, ventilación e iluminación.

El CIS seleccionado está ubicado en un centro comercial al sur de la ciudad de Guayaquil, se elabora el caso de estudio por cada capa.

**Capa de Sensores/Actuadores:** Esta en esta capa se consideran los siguientes dispositivos IoT: un contador de personas, un contador de turnos, veinte sensores de parqueo, ocho sensores de ventanillas, veinte sensores de sillas, un sensor de temperatura, un sensor de iluminación, un controlador de aire acondicionado, un controlador de iluminación, un raspberry para el contador de personas, control de temperatura para personas. El switch inalámbrico es para conectar los dispositivos IoT inalámbricos. El switch alámbrico es para conectar otros dispositivos IoT por cable.

**Capa Red:** En esta capa se aprovecha la misma red cableada e inalámbrica que tiene la empresa en cada CIS, los raspberry se conectan a la red wifi, los controladores se conectan a la red cableada. El centro de atención seleccionado tiene conexión a internet por fibra óptica y además CNT-EP es proveedor de internet en el centro comercial donde funciona el CIS.

**Capa Nube:** La infraestructura para computación en la nube se adopta de Amazon como plataforma de servicio PaaS AWS-EC2 de Amazon (Amazon, 2022). Se utiliza Amazon porque adapta un sistema regionalizado de acuerdo a la ubicación la red IoT accede al servidor que se encuentre cerca; existe disponibilidad de almacenamiento de datos con servidores de respaldo, la nube se encarga de la ubicación geográfica y direccionamiento apropiado al centro de datos. La base de datos es MONGODB para el almacenamiento de los datos generados por los sensores. Las aplicaciones existentes en la nube son: almacenamiento de datos, procesamiento de los datos obtenidos de los sensores, consulta de los indicadores, validaciones de usuarios y validación de los dispositivos.

**Capa Usuarios:** En esta capa están los clientes de CNT-EP que pueden ser atendidos en el CIS y personal administrativo. La aplicación móvil informa a los clientes lo siguiente: cantidad de personas que se encuentren en el CIS, el turno atendido, el ultimo turnos entregado, parqueos disponibles, ventanillas disponibles, sillas disponibles, la temperatura ambiente del CIS y tipo de iluminación. La aplicación móvil informa a los administradores sobre mantenimiento que debe realizar la central de aire acondicionado e iluminación.

Aplicación web y redes sociales informan a los clientes los mismos datos que la aplicación móvil. La aplicación web también es para reservación de turnos.

La tabla 3 presenta los costos promedios del mercado para los dispositivos IoT y otros dispositivos necesarios para la red IoT. Este costo es una sola vez por inicio de los servicios a los ciudadanos.

*Tabla 3. Hardware.*

<u>Dispositivo IoT</u>	<u>Cantidad</u>	<u>Valor</u>	<u>Subtotal</u>
Contador de personas	1	324.00	324.00
Contador de turnos	1	210.00	210.00
Sensores de espacio para parqueo	20	12.00	240.00
Sensores de ventanillas	8	12.99	103.92
Sensor de infrarrojo de temperatura	1	11.75	11.75
Sensor de movimiento para iluminación	1	11.81	11.81
Sensor de temperatura y humedad	1	2.50	2.50
Sensor de temperatura corporal	1	14.99	14.99
Controlador de aire acondicionado	1	85.00	85.00
Controlador de iluminación	1	160.00	160.00
Raspberry para el contador de persona	1	75.00	75.00
Raspberry para infrarrojo de temperatura	1	75.00	75.00
Raspberry para sensor de temperatura	1	75.00	75.00
Raspberry para sensor de temperatura corporal	1	75.00	75.00
Switch de 42 puertos	1	139.00	139.00
Switch inalámbrico	1	35.00	35.00
Rollo de cable UTP categoría 5	1	36.00	36.00
<u>Mano de obra de instalación</u>	<u>1</u>	<u>400.00</u>	<u>400.00</u>
<u>Subtotal</u>			<u>\$1998.97</u>

Fuente: Elaboración propia.

La tabla 4 presenta el costo anual por servicios contratados de la nube, en este caso el proveedor es AWS C2.

*Tabla 4. Software.*

<u>Servicio Nube</u>	<u>Cantidad</u>	<u>Valor</u>	<u>Subtotal</u>
Sistema operativo Linux, plataforma Java, base de datos MongoDB			
Tarifa por hora bajo demanda			
8 horas diarias * 50 semanas	4000 horas	\$0.052	\$208.00

Fuente: Elaboración propia.

Estos costos no incluyen impuestos, por ser empresa pública se puede aprovechar el régimen especial.

## 5. DISCUSIÓN

Existe desigualdad en acceso a internet, pago de internet, edades, los jóvenes tienen más agilidad en software e internet, los adultos tienen menor agilidad en software web, se debe considerar el uso correcto de IoT, internet y servicios públicos digitales en los ciudadanos y grupos sociales.

Para optimizar la recolección de datos, entrega de servicios y monitoreo, es útil que el sector privado y el sector público utilicen la misma IoT para interacción entre ambos sectores y ciudadanos. En caso que los ciudadanos proporcionen datos a IoT se debe informar el uso de protocolos de privacidad para mantener sus datos críticos y entorno privado en total seguridad.

Una consecuencia teórica de esta propuesta es que los datos almacenados en la base de datos NoSQL sirven en plataformas de análisis Big Data para un nuevo monitoreo, caracterización de comportamientos, indicadores de gestión, indicadores de servicios públicos, mejorar procesos operativos y procesos predictivos. Otra consecuencia teórica es mejorar la interoperabilidad entre las empresas públicas porque la arquitectura es escalable y con las ventajas de la nube no se degrada el rendimiento al aumentar los dispositivos o empresas.

Esta propuesta, no considera recurso humano ni cronograma de implementación solo los costos mínimos de dispositivos IoT y costo anual de servicios en la nube.

Esta propuesta se encamina a ser parte en la formación de gobierno electrónico y otros entornos públicos para disminuir el posible mal uso y aumentar la comodidad de los ciudadanos. El caso de estudio se elaboró sobre un área específica de una empresa pública, no es posible abarcar toda la empresa pública porque el despliegue es a nivel nacional con múltiples actividades y/o servicios en este tipo de empresa.

## 6. CONCLUSIÓN

La revisión sistemática de la literatura nos muestra las arquitecturas teóricas o aplicadas a diferentes tipos de áreas, se conoció los componentes, tecnologías y medidas de seguridad más utilizados, este resultado es útil para la adopción de IoT para un mejor nivel de ajuste a nuestra realidad ecuatoriana.

La propuesta de arquitectura IoT de manera general, brinda servicio de datos transparentes, aumenta el nivel de información, ofrece seguimiento de los servicios, entrega información a los ciudadanos, es una arquitectura estándar para una empresa pública y puede ser adoptada por empresas privadas.

El caso de estudio se muestra con poca inversión porque las empresas públicas cuentan con redes y conexión a internet, se espera que los dispositivos IoT mejoren en precio, eficiencia y retorno de la inversión, el diseño e implementación de las redes IoT depende de las infraestructuras de las empresas.

## REFERENCIAS

- Abdelouahid, R. A., Debauche, O., & Marzak, A. (2021). Internet of Things: A new Interoperable IoT Platform. Application to a Smart Building. *Procedia Computer Science*, 191(2019), 511–517. <https://doi.org/10.1016/j.procs.2021.07.066>
- Adi, E., Anwar, A., Baig, Z., & Zeadally, S. (2020). Machine learning and data analytics for the IoT. *Neural Computing and Applications*, 32(20), 16205–16233. <https://doi.org/10.1007/s00521-02004874-y>
- Al Sultan, O. K. T., & Suleiman, A. R. (2021). Simulation of IoT Web-based Standard Smart Building Using Packet Tracer. *Proceedings of the 7th International Engineering Conference “Research and Innovation Amid Global Pandemic”, IEC 2021*, 48–53. <https://doi.org/10.1109/IEC52205.2021.9476125>
- Alonaizi, S. Y., & Manuel, P. (2021). IoT-based smart government enablers: An exploration of governments’ experiments. *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, 58–64. <https://doi.org/10.1109/WorldS451998.2021.9514061>
- Amazon. (2022). *Amazon EC2*. [https://aws.amazon.com/es/ec2/?did=ft\\_card&trk=ft\\_card](https://aws.amazon.com/es/ec2/?did=ft_card&trk=ft_card)
- Aneiba, A., Hayes, J., Nangle, B., & Albaarini, M. (2019). Real-time IoT urban road traffic data monitoring using LoRaWAN. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3365871.3365891>
- Bansal, M., & Priya. (2021). *Performance Comparison of MQTT and CoAP Protocols in Different Simulation Environments*. 549–560. [https://doi.org/10.1007/978-981-15-7345-3\\_47](https://doi.org/10.1007/978-981-15-7345-3_47)
- Barakat, A. N., Ambark, T. M., & Bozed, K. A. (2021). Remote Healthcare Monitoring System using IoT platform. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3492547.3492628>
- Beltran, P., Rodriguez-Ch, P., & Cedillo, P. (2017). A Systematic Literature Review for Development, Implementation and Deployment of MOOCs Focused on Older People. *2017 International Conference on Information Systems and Computer Science (INCISCOS), 2017-Novem*, 287–294. <https://doi.org/10.1109/INCISCOS.2017.60>
- Bharat Kumar, G. J. (2018). Internet of things (IOT) and cloud computing in hybrid organisations using monitoring systems. *Proceedings of the 3rd International Conference on Contemporary Computing and Informatics, IC3I 2018*, 348–351. <https://doi.org/10.1109/IC3I44769.2018.9007302>

- Bideh, P. N., Sönnerup, J., & Hell, M. (2020). Energy consumption for securing lightweight IoT protocols. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3410992.3411008>
- Blower, A., & Kotonya, G. (2021). A Predictive Authorization Approach for IoT Environments. *11th International Conference on the Internet of Things*, 80–87. <https://doi.org/10.1145/3494322.3494333>
- Branco, T. T., Kawashita, I. M., De Sa-Soares, F., & Monteiro, C. N. (2020). An IoT application case study to optimize electricity consumption in the government sector. *ACM International Conference Proceeding Series*, 70–81. <https://doi.org/10.1145/3428502.3428511>
- Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, 36(2), 346–357. <https://doi.org/10.1016/j.giq.2018.09.007>
- Chohan, S. R., & Hu, G. (2020). Success Factors Influencing Citizens' Adoption of IoT Service Orchestration for Public Value Creation in Smart Government. *IEEE Access*, 8, 208427–208448. <https://doi.org/10.1109/ACCESS.2020.3036054>
- da Silva Rodrigues, C. K. (2021). Analyzing Blockchain integrated architectures for effective handling of IoT-ecosystem transactions. *Computer Networks*, 201(September). <https://doi.org/10.1016/j.comnet.2021.108610>
- Daissaoui, A., Boulmakoul, A., Karim, L., & Lbath, A. (2020). IoT and Big Data Analytics for Smart Buildings : A Survey. *Procedia Computer Science*, 170, 161–168. <https://doi.org/10.1016/j.procs.2020.03.021>
- de Almeida Souza, G., de Carvalho Bertoli, G., Torres Ferreira, G., Leitao Albuquerque de Farias, J. C., & A. C. Cesar, C. (2021). Safe Gate – IoT system to support sanitary measures to combat COVID-19. *11th International Conference on the Internet of Things*, 211–214. <https://doi.org/10.1145/3494322.3494699>
- Fersi, G. (2021). Fog computing and Internet of Things in one building block: a survey and an overview of interacting technologies. In *Cluster Computing* (Vol. 24, Issue 4). Springer US. <https://doi.org/10.1007/s10586-021-03286-4>
- Grammatopoulou, M., Kanellopoulos, A., & Vamvoudakis, K. G. (2018). A multi-step and resilient predictive Q-learning algorithm for IoT: A case study in water supply networks. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3277593.3277605>
- Hakim, I. M., & Putriandita, A. (2018). Designing implementation strategy for internet of things (IoT) in Indonesia. *ACM International Conference Proceeding Series*, 23–28. <https://doi.org/10.1145/3288155.3288165>
- Hu, J., Wu, J., Shu, X., Shen, S., Ni, X., Yan, J., & He, S. (2021). Analysis and prediction of fire water pressure in buildings based on IoT data. *Journal of Building Engineering*, 43(August). <https://doi.org/10.1016/j.jobe.2021.103197>
- John, R., Kureshi, R. R., Thakker, D., & Mishra, B. K. (2021). Internet of Things (IoT) and Indoor Air Quality (IAQ) Monitoring in the Health Domain. *11th International Conference on the Internet of Things*, 215–218. <https://doi.org/10.1145/3494322.3494704>
- Kim, K., Kim, I. J., & Lim, J. (2017). National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment. *Journal of Supercomputing*, 73(3), 1140–1151. <https://doi.org/10.1007/s11227-016-1855-z>
- Köksal, & Tekinerdogan, B. (2019). Architecture design approach for IoT-based farm management information systems. *Precision Agriculture*, 20(5), 926–958. <https://doi.org/10.1007/s11119-01809624-8>
- Kolur, V. K., & Reshmi, P. (2020). Io T based Security System for Organization. *Proceedings of BHTC 2020 - 1st IEEE Bangalore Humanitarian Technology Conference*, 2020–2023. <https://doi.org/10.1109/B-HTC50970.2020.9298007>

- Krintz, C., Wolski, R., Golubovic, N., & Bakir, F. (2018). Estimating outdoor temperature from CPU temperature for IoT applications in agriculture. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3277593.3277607>
- Kulkarni, M. D., Alfatmi, K., & Deshmukh, N. S. (2021). Social distancing using IoT approach. *Journal of Electrical Systems and Information Technology*, 8(1). <https://doi.org/10.1186/s43067-02100040-z>
- Kumar, A., Sharma, S., Goyal, N., Singh, A., Cheng, X., & Singh, P. (2021). Secure and energy-efficient smart building architecture with emerging technology IoT. *Computer Communications*, 176(June), 207–217. <https://doi.org/10.1016/j.comcom.2021.06.003>
- Le, D. N., Le Tuan, L., & Dang Tuan, M. N. (2019). Smart-building management system: An Internet-of-Things (IoT) application business model in Vietnam. *Technological Forecasting and Social Change*, 141(January 2018), 22–35. <https://doi.org/10.1016/j.techfore.2019.01.002>
- Li, W., Li, H., & Wang, S. (2021). An event-driven multi-agent based distributed optimal control strategy for HVAC systems in IoT-enabled smart buildings. *Automation in Construction*, 132(September). <https://doi.org/10.1016/j.autcon.2021.103919>
- Lins, F. A. A., & Vieira, M. (2021). Security Requirements and Solutions for IoT Gateways: A Comprehensive Study. *IEEE Internet of Things Journal*, 8(11), 8667–8679. <https://doi.org/10.1109/JIOT.2020.3041049>
- Luckner, M., Grzenda, M., Kunicki, R., & Legierski, J. (2020). IoT Architecture for Urban Data-Centric Services and Applications. *ACM Transactions on Internet Technology*, 20(3). <https://doi.org/10.1145/3396850>
- Luo, X. J., Oyedele, L. O., Ajayi, A. O., Monyei, C. G., Akinade, O. O., & Akanbi, L. A. (2019). Development of an IoT-based big data platform for day-ahead prediction of building heating and cooling demands. *Advanced Engineering Informatics*, 41(March). <https://doi.org/10.1016/j.aei.2019.100926>
- Manimuthu, A., Dharshini, V., Zografopoulos, I., Priyan, M. K., & Konstantinou, C. (2021). Contactless Technologies for Smart Cities: Big Data, IoT, and Cloud Infrastructures. *SN Computer Science*, 2(4), 1–24. <https://doi.org/10.1007/s42979-021-00719-0>
- Memon, R. A., Li, J. P., Ahmed, J., Nazeer, M. I., Ismail, M., & Ali, K. (2020). Cloud-based vs. blockchain-based IoT: a comparative survey and way forward. *Frontiers of Information Technology and Electronic Engineering*, 21(4), 563–586. <https://doi.org/10.1631/FITEE.1800343>
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). *MINTEL Ecuador Digital* (Issue 015). <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/05/PPTeStrategia-Ecuador-Digital.pdf>
- Muccini, H., Vaidhyanathan, K., & De Sanctis, M. (2021). A User-driven Adaptation Approach for Microservice-based IoT Applications. *Proceedings of ACM Conference (Conference'17)*, 1(1), 48–56. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>
- Popli, S., Jha, R. K., & Jain, S. (2021). Green NOMA assisted NB-IoT based urban farming in multistor. *Computer Networks*, 199(April). <https://doi.org/10.1016/j.comnet.2021.108410>
- Riniy, S., Mohd, F., Che, R., Yusoff, M., Lumpur, K., Maarop, N., Lumpur, K., Samy, G. N., Lumpur, K., Hassan, N. H., Lumpur, K., Kamaruddin, N., & Lumpur, K. (2020). *Government Agencies Considering Security Factors*. 3–8.
- Saha, D., Shinde, M., & Thadeshwar, S. (2017). IoT based air quality monitoring system using wireless sensors. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3018896.3025135>
- Samaila, M. G., Lopes, C., Aires, É., Sequeiros, J. B. F., Simões, T., Freire, M. M., & Inácio, P. R. M. (2021). Performance evaluation of the SRE and SBPG components of the IoT hardware platform security advisor framework. *Computer Networks*, 199(August). <https://doi.org/10.1016/j.comnet.2021.108496>
- Sarjerao, B. S., & Prakasarao, A. (2020). *Smart Healthcare Monitoring System Using MQTT Protocol*. 1–5.

- Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2022). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. *Mobile Networks and Applications*, 0123456789. <https://doi.org/10.1007/s11036-022-01937-3>
- Satpathy, S., Mohan, P., Das, S., & Debbarma, S. (2020). A new healthcare diagnosis system using an IoT-based fuzzy classifier with FPGA. *Journal of Supercomputing*, 76(8), 5849–5861. <https://doi.org/10.1007/s11227-019-03013-2>
- Sharma, A., Kumar, H., Mittal, K., Kauhsal, S., Kaushal, M., Gupta, D., & Narula, A. (2021). IoT and deep learning-inspired multi-model framework for monitoring Active Fire Locations in Agricultural Activities. *Computers and Electrical Engineering*, 93(October 2020). <https://doi.org/10.1016/j.compeleceng.2021.107216>
- Sharma, S., Chang, V., Tim, U. S., Wong, J., & Gadia, S. (2019). Cloud and IoT-based emerging services systems. *Cluster Computing*, 22(1), 71–91. <https://doi.org/10.1007/s10586-018-2821-8>
- Silva, D., Heideker, A., Zyrianoff, I. D., Kleinschmidt, J. H., Roffia, L., Soininen, J. P., & Kamienski, C. A. (2022). A Management Architecture for IoT Smart Solutions: Design and Implementation. *Journal of Network and Systems Management*, 30(2), 1–30. <https://doi.org/10.1007/s10922-02209648-6>
- Sitharthan, R., & Rajesh, M. (2021). Application of machine learning (ML) and internet of things (IoT) in healthcare to predict and tackle pandemic situation. *Distributed and Parallel Databases, ML*. <https://doi.org/10.1007/s10619-021-07358-7>
- Smith, K. J., Dhillon, G., & Carter, L. (2021). User values and the development of a cybersecurity public policy for the IoT. *International Journal of Information Management*, 56(October 2020). <https://doi.org/10.1016/j.ijinfomgt.2020.102123>
- Suleimany, M. (2021). Smart Urban Management and IoT. *2021 5th International Conference on Internet of Things and Applications (IoT), 2009*, 1–6. <https://doi.org/10.1109/IoT52625.2021.9469713>
- Tanasiev, V., Pătru, G. C., Rosner, D., Sava, G., Necula, H., & Badea, A. (2021). Enhancing environmental and energy monitoring of residential buildings through IoT. *Automation in Construction*, 126. <https://doi.org/10.1016/j.autcon.2021.103662>
- Thurston, K. H., & de Leon, D. C. (2018). The healthcare IoT ecosystem. *Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*, 51–56. <https://doi.org/10.1145/3278576.3278595>
- Tomicic, I., & Grd, P. (2020). Towards the open ontology for IoT ecosystem's security. *2020 43rd International Convention on Information, Communication and Electronic Technology, MIPRO 2020 - Proceedings*, 1064–1069. <https://doi.org/10.23919/MIPRO48935.2020.9245229>
- Traboulsi, S., & Knauth, S. (2020). Towards implementation of an IoT analysis system for buildings environmental data and workplace well-being with an IoT open software. *Procedia Computer Science*, 170(2019), 341–346. <https://doi.org/10.1016/j.procs.2020.03.048>
- Upadhyay, N., Chandna, H., & Singh, V. K. (2020). Internet of Things Based Flexible Architectures for Public Distribution System in Lockdown Situations. *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 190–194. <https://doi.org/10.1109/SMART50582.2020.9337104>
- Wang, J. X., Liu, Y., Lei, Z. Bin, Wu, K. H., Zhao, X. Y., Feng, C., Liu, H. W., Shuai, X. H., Tang, Z. M., Wu, L. Y., Long, S. Y., & Wu, J. R. (2018). Smart water Lora IoT system. *ACM International Conference Proceeding Series*, 48–51. <https://doi.org/10.1145/3194244.3194260>
- Webb, J., & Hume, D. (2018). Campus IoT Collaboration and Governance using the NIST Cybersecurity Framework. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018(CP740), 25 (7 pp.)–25 (7 pp.). <https://doi.org/10.1049/cp.2018.0025>
- Wei, M., Mo, L., Zhuang, Y., & Kim, K. (2018). Secure framework and key agreement mechanism for OPC-UA in industrial IoT. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3164541.3164568>

- Wirtz, B. W., Weyerer, J. C., & Schichtel, F. T. (2019). An integrative public IoT framework for smart government. *Government Information Quarterly*, 36(2), 333–345. <https://doi.org/10.1016/j.giq.2018.07.001>
- Yamakami, T. (2017). An organizational coordination model for IoT: A case study of requirement engineering of city-government in Tokyo in city platform as a service. *2017 International Conference on Information and Communication Technology Convergence (ICTC), 2017-Decem*, 259–263. <https://doi.org/10.1109/ICTC.2017.8190982>
- Yu, J., Kim, M., Bang, H. C., Bae, S. H., & Kim, S. J. (2016). IoT as a applications: cloud-based building management systems for the internet of things. *Multimedia Tools and Applications*, 75(22), 14583–14596. <https://doi.org/10.1007/s11042-015-2785-0>