

Artículo de Investigación

Desarrollo de aplicaciones IoT: metodologías y estrategias

IoT Application Development: Methodologies and Strategies

Luis Carlos Luis-García¹: Corporación Universitaria Minuto de Dios, Colombia.

luis.luis@uniminuto.edu

Andrés Rodolfo Torres Gómez: Corporación Universitaria Minuto de Dios, Colombia.

andres.torres.go@uniminuto.edu

Fecha de Recepción: 05/06/2024

Fecha de Aceptación: 04/09/2024

Fecha de Publicación: 18/09/2024

Cómo citar el artículo:

Luis-García, L. C. y Torres-Gómez, L. A. (2024). Desarrollo de Aplicaciones IoT: Metodologías y Estrategias [IoT Application Development: Methodologies and Strategies]. *European Public & Social Innovation Review*, 9, 1-18. <https://doi.org/10.31637/epsir-2024-1375>

Resumen:

Introducción: Este artículo abordará los conceptos fundamentales del IoT, describiendo las metodologías clave para el desarrollo de aplicaciones, así como las estrategias de implementación más efectivas. Se explorarán además las plataformas y tecnologías que están dando forma al futuro del IoT, los requerimientos técnicos necesarios para un despliegue exitoso. **Metodología:** Para este proceso se realizó una revisión bibliográfica de los principales elementos del Internet de las Cosas, las metodologías de desarrollo más utilizadas para lograr plantear una metodología general que englobe y desarrolle todos estos componentes. **Resultados:** El resultado obtenido fue una metodología de cuatro fases que permite desde la idea inicial llegar a la solución final de la aplicación en el entorno de IoT. **Discusión:** En esta apartado se logró una síntesis de la información de las secciones anteriores para resaltar los hallazgos más relevantes y que permiten lograr un despliegue con las condiciones de calidad necesarios para una aplicación de IoT. **Conclusiones:** El desarrollo exitoso de aplicaciones IoT requiere un enfoque integral que considere aspectos metodológicos, estratégicos y tecnológicos. Esto incluye garantizar la seguridad y privacidad desde el inicio, asegurar la integración con sistemas existentes, gestionar el ciclo de vida de los componentes y aprovechar los datos para tomar decisiones informadas.

Palabras clave: Internet de las Cosas; Metodologías de desarrollo; Internet; Protocolos de

¹ Autor Correspondiente: Luis Carlos Luis García. Corporación Universitaria Minuto de Dios (Colombia).

comunicación; Plataformas; Computación en la nube; Sistemas embebidos; Redes de sensores.

Abstract:

Introduction: This article will address the fundamental concepts of IoT, describing the key methodologies for application development, as well as the most effective implementation strategies. The platforms and technologies that are shaping the future of IoT, as well as the technical requirements necessary for a successful deployment, will also be explored.

Methodology: For this process, a bibliographic review of the main elements of the Internet of Things, the most used development methodologies, is carried out to propose a general methodology that encompasses and develops all these components. **Results:** The result obtained was a four-phase methodology that allows from the initial idea to reach the final solution of the application in the IoT environment. **Discussion:** In this section, a synthesis of the information from the previous sections is achieved to highlight the most relevant findings that allow achieving a deployment with the quality conditions necessary for an IoT application. **Conclusions:** The successful development of IoT applications requires a comprehensive approach that considers methodological, strategic and technological aspects. This includes ensuring security and privacy from the start, ensuring integration with existing systems, managing the lifecycle of components, and leveraging data to make informed decisions.

Keywords: Internet of Things; Development methodologies; Internet; Communication protocols; Platforms; Cloud Computing; Embedded systems; Sensor networks.

1. Introducción

En un mundo cada vez más conectado, el Internet de las Cosas (IoT, por sus siglas en inglés) ha emergido como una pieza fundamental en la transformación digital, integrando objetos cotidianos a la red global para recopilación y análisis de datos en tiempo real, mejorando así la eficiencia y la toma de decisiones en diversas industrias. Dada su importancia creciente, el desarrollo de aplicaciones IoT se convierte en un campo crítico para investigadores, desarrolladores y empresas que buscan aprovechar estas tecnologías para impulsar la innovación. La correcta implementación de aplicaciones IoT puede transformar radicalmente operaciones empresariales, mejorar la experiencia del usuario y abrir nuevas oportunidades de negocio, a la vez que presenta desafíos técnicos y estratégicos únicos.

Las aplicaciones IoT se caracterizan por incorporar diversas tecnologías en un sistema integrado, incluyendo sensores, sistemas embebidos, redes inalámbricas, análisis de datos y sistemas de control (Chuah, 2014). Esto permite la recolección y procesamiento de datos en tiempo real, facilitando la toma de decisiones autónoma y la reducción de la intervención humana (Yang y Alouini, 2018). Algunas de las aplicaciones industriales que se han visto beneficiadas incluyen logística, producción, infraestructura inteligente y energía, lo que ha llevado a un creciente interés por parte de organizaciones en aprovechar estas innovaciones. (Aydın y Erhan, 2021)

Este artículo abordará los conceptos fundamentales del IoT, describiendo las metodologías clave para el desarrollo de aplicaciones en este ámbito, así como las estrategias de implementación más efectivas. Se explorarán además las plataformas y tecnologías que están dando forma al futuro del IoT, los requerimientos técnicos necesarios para un despliegue exitoso y un caso de estudio práctico sobre la implementación IoT, ofreciendo una perspectiva integral sobre los retos comunes y cómo superarlos. Con este enfoque, los lectores podrán obtener una comprensión profunda sobre el ecosistema del IoT desde la fase de investigación y desarrollo de aplicaciones hasta la implementación y la analítica de datos resultante,

preparándolos para contribuir a esta revolución tecnológica.

1.1. Conceptos fundamentales del Internet de las Cosas

El Internet de las Cosas se puede definir como:

Una gran red de información, basada en elementos electrónicos con reconocimiento de su entorno, e inteligencia propia, para facilitar desde tareas cotidianas hasta procesos industriales complejos, generando bienestar en primera instancia al usuario y a nivel macro a comunidades enteras (Garcia, 2015).

1.1.1. Impacto de IoT en la tecnología

El desarrollo de aplicaciones IoT ha impulsado innovaciones significativas en diversas áreas tecnológicas, tales como: (Chuah, 2014)

- Circuitos integrados de bajo consumo de energía: Permitiendo a los dispositivos IoT operar con baterías durante largos periodos.
- Sistemas embebidos: Facilitando la integración de sensores, procesadores y comunicaciones en dispositivos compactos.
- Protocolos de red inalámbrica: Posibilitando la conectividad entre los objetos y la nube, incluyendo tecnologías como Wi-Fi, Bluetooth y 5G.
- Analítica de datos y aprendizaje automático: Permitiendo la toma de decisiones inteligentes a partir de los datos recolectados por los dispositivos IoT.
- Inteligencia artificial: Favoreciendo la automatización de procesos y la interacción autónoma entre "cosas".

Estos avances tecnológicos han allanado el camino para la implementación exitosa de aplicaciones IoT en diversas industrias, impulsando una nueva era de innovación y eficiencia operativa.

2. Metodología

Para este estudio se realizó un análisis bibliométrico, para identificar la información más relevante con respecto a las metodologías de desarrollo en el entorno de IoT y luego se analizaron aplicaciones reales y se implementaron soluciones que permitieron evidenciar un mejor proceso metodológico en las diferentes fases de desarrollo de aplicaciones, a continuación se muestran los aspectos más relevantes encontrados y en la sección de resultados se mostrará la metodología planteada y adaptada de acuerdo a lo encontrado en la investigación junto con las pruebas en un desarrollo real.

2.1. Metodologías para el Desarrollo de Aplicaciones IoT

Dado el carácter multidisciplinario del IoT, que abarca hardware, software, redes y aplicaciones, su desarrollo requiere de enfoques metodológicos específicos que permitan gestionar adecuadamente la complejidad y garantizar la integración de todos los componentes.

Algunas de las metodologías más utilizadas en el desarrollo de aplicaciones IoT incluyen:

Diseño centrado en el usuario: Priorizando las necesidades y experiencia del usuario final para diseñar soluciones IoT que generen valor.

Diseño modular: Dividiendo el sistema en componentes independientes que puedan ser desarrollados, probados y actualizados por separado.

Enfoque basado en modelos: Creando representaciones abstractas del sistema que permitan su descripción a diferentes niveles de detalle, acelerando el diseño y la implementación (Agudelo-Sanabria y Jindal, 2021).

Metodologías ágiles: Utilizando ciclos de desarrollo iterativos y adaptables, para responder rápidamente a los cambios y requisitos cambiantes (Agudelo-Sanabria y Jindal, 2021).

Arquitecturas orientadas a servicios: Desarrollando componentes de software reutilizables que puedan integrarse fácilmente en la solución IoT (Jurcut *et al.*, 2020).

Estos enfoques metodológicos han demostrado ser efectivos para abordar los desafíos inherentes al desarrollo de aplicaciones IoT, tales como la diversidad de tecnologías, la necesidad de fiabilidad y consistencia operativa, y la integración con múltiples sistemas, en este caso se profundizará en los modelos de desarrollo ágil y en cascada que son los que integrando los otros tipos permiten un desarrollo más eficiente de aplicaciones en el entorno IoT.

2.1.1. Modelos de Desarrollo Ágil en IoT

Los métodos ágiles, como Scrum o Kanban, se han vuelto cada vez más populares en el desarrollo de aplicaciones IoT (Ahmad *et al.*, 2021). Estos enfoques se caracterizan por:

- Ciclos de desarrollo iterativos y adaptables, que permiten incorporar cambios y retroalimentación del usuario de manera rápida.
- Colaboración estrecha entre los equipos multidisciplinarios, incluyendo expertos en hardware, software, redes y aplicaciones.
- Entrega frecuente de versiones funcionales, lo que permite validar el producto en etapas tempranas.
- Enfoque en la automatización de pruebas y despliegue continuo, para agilizar el proceso de implementación (Jurcut *et al.*, 2020).

Estas características se adaptan bien a los requisitos cambiantes y la naturaleza evolutiva de las aplicaciones IoT, donde la flexibilidad y la velocidad de respuesta son cruciales.

2.1.2. Modelo de Desarrollo en Cascada para IoT

El modelo de desarrollo en cascada, a pesar de ser más tradicional, también se ha aplicado con éxito en el desarrollo de soluciones IoT (Jurcut *et al.*, 2020). Este enfoque se caracteriza por:

- Etapas secuenciales bien definidas, desde el análisis de requisitos hasta la implementación y mantenimiento.
- Énfasis en una planificación exhaustiva y la documentación detallada de cada fase.
- Validación y verificación rigurosas de los componentes en cada etapa antes de avanzar.
- Adecuado para sistemas IoT con requisitos más estables y arquitecturas bien establecidas.

Este modelo puede ser beneficioso cuando se requiere un enfoque más estructurado y riguroso, como en el caso de aplicaciones IoT que deben cumplir con estrictos requisitos de seguridad, o en proyectos con un alcance bien definido y una planificación detallada.

En resumen, tanto los enfoques ágiles como el modelo en cascada han demostrado ser efectivos en el desarrollo de aplicaciones IoT, dependiendo de las características y requisitos específicos de cada proyecto.

2.2. Estrategias de Implementación IoT

Una vez definido el enfoque metodológico, es crucial considerar diversas estrategias de implementación para garantizar el éxito de las aplicaciones IoT (Ahmad *et al.*, 2021).

Algunas de las estrategias clave incluyen:

- Adopción gradual: Comenzar con proyectos piloto a pequeña escala para evaluar el impacto y la viabilidad de la solución IoT, antes de escalar a implementaciones a gran escala.
- Arquitectura modular y escalable: Diseñar la solución IoT de manera que pueda crecer y adaptarse a nuevos requisitos y tecnologías a lo largo del tiempo.
- Seguridad y privacidad como prioridad: Incorporar medidas de seguridad y protección de datos desde las etapas iniciales del desarrollo, garantizando la confianza y el cumplimiento normativo (Jurcut *et al.*, 2020).
- Integración con sistemas existentes: Asegurar la compatibilidad e interoperabilidad de la solución IoT con los sistemas y procesos empresariales ya implementados.
- Gestión del ciclo de vida: Implementar estrategias para el mantenimiento, actualización y eventual reemplazo de los componentes IoT a lo largo de su vida útil.
- Monitorización y analítica de datos: Aprovechar los datos generados por los dispositivos IoT para generar información valiosa y tomar decisiones más informadas.

La adopción de estas estrategias, junto con la elección de un enfoque metodológico adecuado, ayudará a las organizaciones a implementar con éxito soluciones IoT que generen valor a lo largo del tiempo y se mantengan relevantes en el mercado, adaptándose a los cambios tecnológicos y a las necesidades cambiantes de los usuarios.

Otros elementos clave en este desarrollo son:

2.2.1. Evaluación de Necesidades y Requisitos

Es fundamental analizar cuidadosamente los requisitos y necesidades específicas de la organización o el sector en el que se implementará la solución IoT, para garantizar que el desarrollo se alinee con los objetivos estratégicos y las expectativas de los usuarios (Ullah *et al.*, 2020), esto implica un análisis exhaustivo de los procesos de negocio, las funcionalidades requeridas, los casos de uso, los datos a recopilar, los requisitos de seguridad y privacidad, y cualquier otra consideración relevante para asegurar que la solución IoT cumpla con las necesidades de la organización.

Desde esta perspectiva, algunas investigaciones respaldan la importancia de este análisis de requisitos previo al desarrollo, ya que permite definir una hoja de ruta clara y alinear el proyecto con las prioridades del negocio (Čolaković y Hadžialić, 2018; Iqbal *et al.*, 2020; Jurcut *et al.*, 2020; Lampropoulos *et al.*, 2018).

2.2.2. *Arquitectura y diseño de la solución*

Otro elemento clave en el desarrollo de aplicaciones IoT es el diseño de una arquitectura sólida y escalable que permita integrar de manera efectiva los diversos componentes de la solución, como dispositivos, sensores, redes, plataformas de datos, aplicaciones y servicios (Yang *et al.*, 2015).

Según lo expuesto por Agudelo-Sanabria y Jindal (2021), un enfoque basado en modelos puede ser beneficioso para el diseño de la arquitectura IoT, ya que permite una descripción detallada de la aplicación en diferentes niveles de abstracción, sin estar limitado a una plataforma específica.

Además, es importante considerar aspectos como la interoperabilidad, la seguridad, la escalabilidad y la flexibilidad en el diseño de la arquitectura, para garantizar que la solución IoT pueda adaptarse a los cambios futuros y satisfacer las necesidades a largo plazo.

2.2.3. *Implementación y pruebas*

La fase de implementación y pruebas es fundamental para asegurar el correcto funcionamiento de la solución IoT y su capacidad para cumplir con los requisitos establecidos. (Jurcut *et al.*, 2020)

Aquí, los enfoques ágiles como DevOps pueden ser de gran utilidad, al permitir un desarrollo iterativo y la implementación frecuente de versiones funcionales, lo que facilita la validación y la retroalimentación temprana de los usuarios (Pereira *et al.*, 2021).

Además, es crucial implementar una estrategia integral de pruebas que incluya pruebas unitarias, de integración, de rendimiento y de seguridad, para garantizar la calidad y el cumplimiento de los estándares correspondientes.

En resumen, el desarrollo de aplicaciones IoT requiere la consideración de diversos factores metodológicos y estratégicos para asegurar su éxito a largo plazo.

2.2.4. *Plataformas y Tecnologías IoT*

Más allá de los enfoques metodológicos y las estrategias de implementación, la selección adecuada de plataformas y tecnologías IoT es fundamental para el éxito de los proyectos. (Ullah *et al.*, 2020)

Existen numerosas plataformas IoT en el mercado, cada una con diferentes capacidades y características, lo que puede dificultar la elección de la más adecuada para un proyecto en particular, sin embargo, puede encontrarse un marco teórico que identifica 21 factores clave a considerar en la evaluación de estas plataformas.

Algunos de los aspectos a tener en cuenta incluyen:

- Conectividad y comunicación entre dispositivos
- Gestión y procesamiento de datos
- Capacidades de análisis y visualización
- Seguridad y privacidad
- Escalabilidad y flexibilidad (Guth *et al.*, 2017).

Asimismo, es importante evaluar la compatibilidad de la plataforma IoT con los sistemas y tecnologías existentes en la organización, para facilitar la integración y la adopción de la solución.

Una revisión detallada de las características y diferencias entre las principales plataformas IoT, como se describe en (Alvarado *et al.*, 2018), puede ayudar a las organizaciones a seleccionar la opción más adecuada para sus necesidades específicas.

En resumen, el desarrollo de aplicaciones IoT requiere la integración de diversos enfoques metodológicos, estrategias de implementación y la selección de plataformas y tecnologías adecuadas. Este enfoque integral ayudará a las organizaciones a implementar soluciones IoT exitosas y sostenibles en el tiempo.

Algunas de las principales plataformas IoT son:

- **Google Cloud Platform:** Proporciona información comercial en tiempo real para dispositivos dispersos globalmente, tiene potentes capacidades de inteligencia artificial, soporte para inteligencia de ubicación, capacidad para acelerar los procesos de negocio y utiliza servicios en la nube para minimizar los costos (Zheng *et al.*, 2019).
- **Particle:** Ofrece soluciones de IoT para conectividad, *hardware*, *device cloud* y aplicaciones. Tiene capacidad para ofrecer una infraestructura confiable, una nube protegida por firewall, integración con Google Cloud o Microsoft Azure, capacidad para trabajar con datos y fácil integración con REST API (Zolfaghari *et al.*, 2022).
- **Salesforce IoT Cloud:** Ayuda a aumentar las ventas, los servicios de marketing y las oportunidades relacionadas con las aplicaciones. Permite probar ideas de negocio sin necesidad de programar, ofrece datos reales del uso y rendimiento del producto, y capacidad para trabajar con cualquier tipo de datos desde cualquier dispositivo (Menéndez *et al.*, 2020).
- **IBM Watson IoT:** Captura e investiga datos de máquinas, equipos y dispositivos, y los analiza para tomar mejores decisiones. Ayuda a construir, modernizar y conectar dispositivos con aplicaciones en la nube, analiza datos no estructurados, comprende patrones de datos, proporciona un dashboard para mejorar la visualización y ofrece servicios de análisis (Sheikh y Goje, 2021).
- **Amazon AWS IoT Core:** Ayuda a conectar diversos dispositivos a la nube, permitiendo la comunicación entre dispositivos y aplicaciones en la nube. Proporciona soporte para MQTT y HTTP, puede procesar una gran cantidad de mensajes, es una plataforma confiable y segura para enrutar mensajes, puede rastrear aplicaciones y comunicarse incluso sin conexión, y permite un acceso seguro para dispositivos (Villa *et al.*, 2021).

2.2.5. Protocolos de Comunicación

Los protocolos IoT son el "lenguaje" que utilizan los dispositivos IoT para comunicarse entre sí y con otras plataformas. En los entornos industriales, los datos pueden proceder de diversas fuentes, incluyendo los dispositivos del Internet de las Cosas (IoT). Desde una perspectiva técnica, los protocolos son un conjunto de normas y reglas que permiten a dos entidades entenderse e intercambiar información, facilitando la comunicación Máquina a Máquina (M2M) (Chahid *et al.*, 2017).

Los protocolos de comunicación IoT deben cumplir las siguientes funciones:

- Asegurar la conectividad e interoperabilidad entre diversos fabricantes y dispositivos.
- Permitir la comunicación entre un gran número y variedad de dispositivos simultáneamente, transportando mensajes de forma eficiente.
- Evitar el acoplamiento entre dispositivos para que no haya dependencia entre ellos.
- Facilitar la escalabilidad, permitiendo añadir o eliminar dispositivos sin afectar el despliegue general.
- Garantizar la seguridad de las comunicaciones en entornos vulnerables como el IoT industrial.
- Proporcionar un fácil acceso a los dispositivos, incluso con problemas de latencia o cortafuegos.

Algunos de los protocolos más comunes para la comunicación de dispositivos IoT con Internet son MQTT, CoAP y HTTP, ya que son flexibles y están diseñados para transmitir cualquier tipo de información (Panicker *et al.*, 2021).

En los despliegues de comunicación industrial y de IoT industrial, se utilizan protocolos más enfocados a las operaciones, como Modbus, IEC102, IEC104 para contadores eléctricos o MBUS para contadores de agua. Estos protocolos están orientados a que un dispositivo controlador (como un PLC) se comunique con otras máquinas que ejecutan órdenes (Serror *et al.*, 2021).

2.2.6. *Requerimientos Técnicos para IoT*

El *hardware* y el *software* son componentes cruciales para el desarrollo y la implementación de aplicaciones de Internet de las Cosas (IoT). A continuación, se detallan los principales requerimientos técnicos:

Hardware Necesario

El hardware de IoT es un soporte fundamental para las aplicaciones de IoT. Según IoT Analytics' El tamaño del mercado global de IoT crecerá un 19% en 2023: IoT muestra resiliencia a pesar de la recesión económica, el hardware sigue representando la mayor parte del gasto, con un 44%, o superó los 88.000 millones de dólares, superando con creces a los servicios de IoT. El gasto en hardware de IoT es mucho más alto que el soporte de servicios de IoT, lo que indica que la mayoría de los proyectos de IoT aún se encuentran en las primeras etapas de implementación preliminar (Siddalingamma, 2023).

Fabricantes de reconocido hardware IoT como Dusun IoT están capacitados para abordar y eliminar estas barreras para la adopción de IoT. Fabricantes de hardware IoT producen dispositivos inteligentes, pero también poseen una amplia gama de otras cualidades cruciales, como la experiencia con la implementación en el piso de producción y la experiencia en la industria.

Los dispositivos IoT incluyen dos partes, hardware y software. El componente de hardware lleva principalmente la operación de los programas del sistema, recopila datos y ejecuta instrucciones. Consta de varios elementos clave:

- **Módulo para comunicación uplink y downlink:** En todo el sistema IoT, la comunicación de enlace ascendente generalmente se dirige a las redes externas, y la comunicación de enlace descendente generalmente es para la conexión de dispositivos finales locales.

- **Procesadores:** Al igual que el cerebro humano, el procesador controla cómo funciona todo el sistema. Tiene muchas interfaces en el exterior y puede ejecutar una variedad de programas.
- **Comunicación interna:** La comunicación entre los componentes internos tiene dos formas: comunicación de señal analógica y comunicación de señal digital.
- **Almacenamiento:** Flash se usa para almacenar datos en dispositivos de hardware, aunque su capacidad de almacenamiento es bastante limitada, desde unos pocos KB hasta decenas de MB, y se usa principalmente para almacenar datos en caché o almacenar instrucciones de programas.
- **Sistema de alimentación:** El sistema de alimentación se refiere al sistema de transformación y rectificación cuando la alimentación externa se introduce en el hardware.
- **Componentes principales:** Un producto puede tener cientos o incluso miles de partes. Como resultado, se recomienda concentrarse en los componentes esenciales en lugar de prestar atención a la selección de todos los componentes (Patil *et al.*, 2021).

La oportunidad que ofrece el IoT es tan grande como el reto que plantea la seguridad del IoT. Esta última ya no depende solo del software que utilicemos, sino también del hardware que tengamos. Mientras que, en el caso del software, en muchos casos es responsabilidad del usuario hacer un uso correcto del mismo para mantenerlo seguro, ¿quién es el responsable de asegurar el hardware? El fabricante.

Si nos centramos en el IoT Industrial, lo primero que debemos tener en cuenta es que los dispositivos que instalaremos en nuestro despliegue están pensados para ser una inversión a largo plazo. Esto nos hará correr el riesgo de quedarnos obsoletos en términos de seguridad. Por eso debemos tomar conciencia de lo que se necesita a la hora de elegir el *hardware* para IoT y acompañarlo de medidas de software que garanticen la seguridad a lo largo de los años.

Antes de tomar la decisión de adquirir los dispositivos IoT, debemos analizar si el fabricante cumple con una serie de requisitos que son básicos para garantizar que el hardware IoT sea robusto y fiable:

- Trabaja con la seguridad por diseño. Implica fabricar el hardware con la misma filosofía con la que se desarrollaría el *software*. Esto también implica contar con personal que proviene del trabajo de *software* y *hardware* en su diseño.
- Incluye chips de seguridad de hardware, que permiten almacenar claves o certificados de forma privada y segura. Así, el sistema podrá cifrar o descifrar los datos de forma única. Son las bases para generar una Raíz de Confianza Hardware.
- Utiliza una identidad única para cada sensor. Esto permite identificar de forma inmutable, como si fuera un DNI, el dispositivo a lo largo de su ciclo de vida. Así se evitan confusiones a la hora de configurar y gestionar los dispositivos.

No hay forma de asegurar los dispositivos IoT teniendo en cuenta solo uno de estos dos aspectos. A medida que la tecnología avanza, el *hardware* puede quedar obsoleto, pero mientras tengamos un *software* actualizado en su interior, podemos mantener la seguridad (Gupta y Vanjale, 2020).

2.2.7. Software y Herramientas

El término "software IoT" se refiere a las aplicaciones informáticas y plataformas de software diseñadas específicamente para el Internet de las Cosas (IoT). Estas herramientas están destinadas a facilitar el desarrollo, la implementación y la gestión de soluciones y dispositivos IoT (Alnasser *et al.*, 2019).

Las aplicaciones IoT requieren dos tipos de análisis de datos: construcción del contexto y análisis masivo de datos. El primero es un análisis en tiempo real de la situación actual, es decir, la aproximación en tiempo real al escenario del mundo real. Mientras que el segundo es un análisis de la historia para predecir tendencias y acciones preventivas.

El reto consiste en proporcionar una computación fiable en tiempo real para la construcción del contexto y las acciones en tiempo real. La creación de un contexto y la puesta en marcha de acciones en tiempo real en el límite hacen que el sistema IoT sea más funcional incluso en los casos de pérdida prolongada de la conectividad a la Internet y la nube (Farooq *et al.*, 2020). Una de las principales necesidades clave para el software IoT es la capacidad de interoperabilidad entre los diferentes sistemas y componentes, permitiendo una comunicación fluida y el intercambio de datos.

La interfaz entre las "cosas" (objetos físicos dotados de tecnología) y la nube/internet es el eslabón más débil, ya que las cosas son los dispositivos restringidos (limitados por la potencia de procesamiento, la batería y el ancho de banda). Esto los convierte en los elementos de red menos autoprotegidos.

Una forma de resolver los problemas de seguridad en IoT es llevar la batalla a un nivel superior y ayudar a las necesidades informáticas de los dispositivos IoT en el nivel del borde (*edge*). Para asegurar la Internet de las Cosas, es necesario construirla a la primera. Esto, a su vez, requiere que se establezcan ciertas directrices, políticas y normas (Raja *et al.*, 2018).

Estas normas y directrices facilitan la creación de un ecosistema de colaboración entre los vendedores de dispositivos, los desarrolladores de software, los constructores de redes, los integradores de sistemas y los reguladores, y desempeñarían su función en la construcción de los sistemas para una IoT segura.

Las cosas generan datos continuamente, pero no todos los datos tienen sentido ni son útiles. No es prudente simplemente enrutar los datos a la nube y almacenarlos. Requiere filtrar los datos no deseados y los que pueden no ayudar para futuros análisis, y transmitir sólo los datos intermedios agregados útiles a la nube. Esto permite aumentar la eficiencia de la conectividad de retroceso. También requiere almacenar los datos localmente cuando la conectividad a la nube se rompe, y subir los datos cuando la conectividad se ha reestablecido (Alenazi *et al.*, 2022).

La interoperabilidad requiere una pasarela/puerta de enlace estandarizada con interfaces estándar para que podamos integrar los dispositivos y los servicios en la nube de forma horizontal, eligiendo los dispositivos de cualquier proveedor y obteniendo los servicios de cualquier otro proveedor. Esto no sólo nos permite construir aplicaciones IoT utilizando los mejores componentes de la raza, sino que también permite la innovación para construir nuevas aplicaciones.

Se estima que, en el año 2025, se instalarán decenas de millones de dispositivos. Este alcance requiere un gran número de personal capacitado para la instalación, configuración y puesta en marcha de los dispositivos IoT. Estos procedimientos típicamente requieren de 20 a 30 minutos para dispositivos simples hasta unas pocas horas para equipos grandes. Los esfuerzos necesarios para estos procedimientos pueden ser más costosos que el costo de los dispositivos de I/O y limitan la escalabilidad. Por lo tanto, se deben diseñar los dispositivos de I/O y las aplicaciones para la autoconfiguración y la fácil gestión del ciclo de vida de los dispositivos. Esto llevaría al desarrollo de un ecosistema en el que el despliegue de las aplicaciones de I/O sería fácil sin necesidad de conocimientos técnicos profundos para la instalación, el aprovisionamiento, la puesta en marcha y la clausura (Mikkonen *et al.*, 2021).

3. Resultados

A continuación, se presenta la metodología propuesta a partir de los diferentes análisis realizados en la sección anterior, sobre los elementos más relevantes y sus características, y las características básicas de su implementación que sus resultados más relevantes fueron presentados en otros artículos.

3.1. Metodología propuesta

De acuerdo con los elementos mencionados anteriormente se planteó una metodología genérica de desarrollo de aplicaciones de IoT que se centra en cuatro pasos y un proceso de retroalimentación que permite la mejora continua de los sistemas, en la siguiente figura se muestra la representación general de la metodología.

Figura 1.
Metodología de diseño



Fuente: Elaboración propia (2024).

3.1.1. Fases de la Metodología propuesta

Caracterización

La primera etapa es la caracterización en donde se realiza un estudio de los antecedentes y referentes de la temática que se trabaja, se evalúan las principales características del Internet de las Cosas y por último se definen los requerimientos del sistema que se va a implementar, de acuerdo con la investigación realizada esta puede ser la fase más importante, porque permite orientar el camino más lógico para todo el proceso de desarrollo, teniendo en cuenta que se pueden definir el uso de metodologías ágiles o tradicionales, de procesos iterativos (usualmente lo más conveniente) o lineales, que en todos los casos depende de tener claridad de los objetivos de desarrollo para alcanzar un buen prototipo y luego lograr una implementación que cumpla con todos los requerimiento y que permita su escalabilidad y usabilidad a futuro.

Diseño

En la segunda etapa se realiza el diseño el cual cuenta con el análisis de requerimientos establecidos en la etapa de caracterización, se realiza la selección de los protocolos, dispositivos de hardware y software, plataformas de *cloud computing* que permitan cumplir con las especificaciones establecidas para el proyecto, en esta etapa se definen claramente estándares de seguridad, tiempos de respuesta del sistema, se realiza una fase inicial de diseño industrial para mejorar el aspecto visual y de terminados del dispositivo y se identifican claramente los datos y la interacción entre las diferentes variables que se van a utilizar.

Para esta segunda etapa se desarrolló el artículo “Embedded systems for Internet of Things (IoT) applications: a review study” donde se evalúan diferentes sistemas embebidos en costo, protocolos admitidos, rendimiento, plataformas entre otros elementos, que permiten una selección rápido y eficaz de dispositivos de acuerdo con las necesidades del proyecto a desarrollar (Alvarado *et al*, 2018).

Implementación

La tercera etapa es la de implementación del prototipo en donde se deben planear tiempos para la adquisición de equipos, instalación de sistemas operativos e integración de dispositivos para la generación de las aplicaciones del Internet de las Cosas, en esta fase se deben implementar todos los requisitos de la etapa 1 a partir del diseño generado en la etapa 2 de la metodología, teniendo en cuenta los estándares de calidad y de seguridad necesarios y adaptándose a la normativa actual en el tema.

Validación

La última etapa es la validación del sistema implementado en la que se realizarán las diferentes pruebas para validar su funcionamiento tales como inducir fallas, pruebas de rendimiento, pruebas de Throughput de la red, pruebas de ciberseguridad, entre otras, revisando que se cumplan con todas las normas y regulaciones en esta materia, es importante incorporar métricas de desempeño, pero también la evaluación por parte del usuario final para identificar elementos de mejora y retroalimentar el proceso por si es necesario que se realice de forma iterativa, esto sucede en especial cuando los requerimientos no eran totalmente claros o cuando es un proceso complejo que se va desarrollando por fases.

Este es un proceso usualmente iterativo que busca garantizar que el sistema cumpla con todos los requerimientos del sistema y de calidad necesarios.

Para validar la metodología se desarrollaron 3 aplicaciones enfocadas en la conectividad a partir de diferentes plataformas, protocolos de comunicación y sistemas embebidos el más

reciente es Desarrollo De Redes De Sensores Inalámbricos En El Entorno De IoT Mediante Protocolos Wifi (Luis García *et al.*, 2023) donde se siguió la metodología planteada logrando una aplicación de IoT en todos sus aspectos, usando el protocolo de comunicación WiFi, con tarjetas de desarrollo Texas y Raspberry Pi, creando una interfaz Web pero además haciendo uso de plataformas ya establecidas evaluando las diferentes métricas mencionadas anteriormente.

4. Discusión

Aunque la adopción de IoT continúa creciendo exponencialmente, aún existen desafíos y obstáculos que las organizaciones deben superar. Entre los principales retos se encuentran los problemas de seguridad y privacidad, la falta de interoperabilidad entre dispositivos y plataformas, la complejidad de la gestión del ciclo de vida de los sistemas IoT y la dificultad para aprovechar efectivamente los datos generados.

Para abordar estos desafíos, es fundamental que las organizaciones desarrollen e implementen estrategias y metodologías sólidas para el desarrollo de aplicaciones IoT. Algunas de las estrategias clave incluyen:

- A. Definir y adoptar estándares abiertos que permitan la interoperabilidad entre dispositivos y plataformas (Čolaković y Hadžialić, 2018).
- B. Integrar enfoques de seguridad y privacidad desde el diseño inicial de las aplicaciones IoT.
- C. Desarrollar capacidades de computación en el borde que permitan a las aplicaciones IoT funcionar de manera autónoma y adaptarse a la pérdida de conectividad, asegurándose de que los datos críticos se procesen y almacenen localmente (Agudelo-Sanabria y Jindal, 2021).

Además, las organizaciones deben aprovechar las metodologías ágiles y las herramientas de automatización para acelerar el desarrollo, despliegue y gestión de aplicaciones IoT (Jurcut *et al.*, 2020).

Con la adopción de estas estrategias, las organizaciones podrán desarrollar aplicaciones IoT que sean seguras, escalables y capaces de generar valor a partir de los datos recopilados.

Además, las fases planteadas en la metodología propuesta permiten simplificar el proceso de desarrollo de una aplicación de Internet de las Cosas logrando captar los principales elementos de las metodologías generales que se usan en la actualidad y brindando una guía de como afrontar de forma inicial proyectos en Internet de las Cosas, por lo que es una herramienta didáctica que se debe seguir evaluando y fortaleciendo a partir de la ejecución de más proyectos y consolidando su validación.

5. Conclusiones

El desarrollo exitoso de aplicaciones IoT requiere un enfoque integral que considere aspectos metodológicos, estratégicos y tecnológicos. Esto incluye garantizar la seguridad y privacidad desde el inicio, asegurar la integración con sistemas existentes, gestionar el ciclo de vida de los componentes y aprovechar los datos para tomar decisiones informadas. Además, es fundamental evaluar cuidadosamente los requisitos y diseñar una arquitectura escalable. La implementación y las pruebas deben seguir enfoques ágiles para validar el cumplimiento de los requisitos. Por último, la selección adecuada de plataformas y tecnologías IoT es crucial para el éxito del proyecto.

La metodología propuesta permite una ejecución rápida de un proyecto en el entorno del Internet de las Cosas obteniendo resultados satisfactorios en soluciones específicas, es necesario validar la metodología en entornos más grandes y de mayor complejidad para lograr una generalización de los resultados obtenidos.

Al realizar un buen ejercicio de la primera etapa de conceptualización y caracterización se logran mejores resultados en las etapas posteriores teniendo en cuenta que se puede hacer una selección adecuada de todos los elementos del sistema y su posterior implementación y validación generará menos cambios y actualizaciones sobre el sistema desarrollado.

En la etapa de validación es necesario realizar varias pruebas del sistema y tratar de inducir las fallas más comunes y algunas complejas para poder realizar el proceso de retroalimentación y mejorar la confiabilidad del sistema para su puesta en marcha, sin embargo, esta es una tarea que se va afianzando en la generación de cada nuevo proyecto que presenta nuevos retos y dificultades técnicas.

6. Referencias

- Agudelo-Sanabria, S. D. y Jindal, A. (2021). The Ifs and Buts of the Development Approaches for IoT Applications. *arXiv*. <https://doi.org/10.48550/arxiv.2101.09796>
- Ahmad, A., Fahmideh, M., Altamimi, A. B., Katib, I., Albeshri, A., Alreshidi, A., Alanazi, A. y Mehmood, R. (2021). Software Engineering for IoT-Driven Data Analytics Applications. *IEEE Access*, 9, 48197-48217. <https://doi.org/10.1109/access.2021.3065528>
- Alenazi, M. M., Yosuf, B. A., Mohamed, S. H., El-Gorashi, T. E. H. y Elmighani, J. M. H. (2022). Energy Efficient Placement of ML-Based Services in IoT Networks. *2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)* <https://doi.org/10.1109/meditcom55741.2022.9928668>
- Alnasser, A., Sun, H. y Jiang, J. (2019, March 1). Cyber security challenges and solutions for V2X communications: A survey. *Computer Network*, 151, 52-67. <https://doi.org/10.1016/j.comnet.2018.12.018>
- Alvarado Moreno, J. D., Luis Garcia, L. C., Hernández, W. C. y Barrera Obando, A. M. (2018). Embedded Systems for Internet of Things (IoT) Applications: A Review Study. *2018. Congreso Internacional de Innovación y Tendencias En Ingeniería (CONIITI)*, 1-6. <https://doi.org/10.1109/CONIITI.2018.8587092>
- Aydın, Ö. y Erhan, I. I. (2021, January 1). Video or Image Transmission Security for ESP-EYE

- IoT device used in Business Processes. *YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ*.
<https://doi.org/10.48550/axiv.2107.08321>
- Carretero, J. y García, J C F. (2013, May 9). The Internet of Things: connecting the world. *Springer Science+Business Media*, 18(2), 445-447. <https://doi.org/10.1007/s00779-013-0665-z>
- Chahid, Y., Benabdellah, M. y Azizi, A. (2017, November 14). Internet of Things Protocols Comparison, Architecture, Vulnerabilities and Security. *Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems (ICCWCS'17)*
<https://doi.org/10.1145/3167486.3167554>
- J. W. Chuah. (2014). The Internet of Things: An overview and new perspectives in systems design. Paper presented at the 2014 *International Symposium on Integrated Circuits (ISIC)*, 216-219. <https://doi.org/10.1109/ISICIR.2014.7029576>
- Čolaković, A. y Hadžialić, M. (2018, October 1). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues, *Computer Networks*, 144, 17-39.
<https://doi.org/10.1016/j.comnet.2018.07.017>
- Farooq, H., Rehman, H. U., Javed, A., Shoukat, M. y Dudely, S. (2020, July 1). A Review on Smart IoT Based Farming, *Annals of Emerging Technologies in Computing (AETiC)*, 4(3), 17-28. <https://doi.org/10.33166/aetic.2020.03.003>
- Gupta, S. K. y Vanjale, S. (2020, August 31). Cyber Security Measures for Internet of Things Devices, *International Journal of Engineering Research and Technology*, 13(8), 1830-1830.
<https://doi.org/10.37624/ijert/13.8.2020.1830-1839>
- Guth, J., Breitenbücher, U., Falkenthal, M., Fremantle, P., Kopp, O., Leymann, F. y Reinfurt, L. (2017). A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences. *Internet of Everything*, 81-101. https://doi.org/10.1007/978-981-10-5861-5_4
- Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B. y Bangash, Y A. (2020, October 1). An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet of Things Journal*, 7(10), 10250-10276.
<https://doi.org/10.1109/jiot.2020.2997651>
- Jurcut, A. D., Niculcea, T., Ranaweera, P. y Le-Khac, N. (2020). Security Considerations for Internet of Things: A Survey. *SN Computer Science*, 1(4).
<https://doi.org/10.1007/s42979-020-00201-3>
- Lampropoulos, G., Siakas, K. y Anastasiadis, T. (2018, January 1). Internet of Things (IoT) in Industry: Contemporary Application Domains, Innovative Technologies and Intelligent Manufacturing. *International Journal of Advances in Scientific Research and Engineering (IJASRE)*, 4(10), 109-118. <https://doi.org/10.31695/ijasre.2018.32910>
- Luis García, L. (2015). *Estudio del impacto técnico y económico de la transición de internet al Internet de las Cosas (IoT) para el caso colombiano*. Universidad Nacional de Colombia.
<https://repositorio.unal.edu.co/handle/unal/55152>
- Luis-García, L. C., Alvarado Moreno, J. D., Pineda, J. y Bueno, D. F. L. (2023, July 26).

- Desarrollo de redes de sensores inalámbricos en el entorno de IoT mediante protocolos wifi, 2023 *IEEE Colombian Conference on Communications and Computing (COLCOM)*, 1-6. <https://doi.org/10.1109/colcom59909.2023.10334252>
- Menéndez, A R., Saura, J R. y Sanchez, P P. (2020, January 1). Identifying key performance indicators for marketing strategies in mobile applications: a systematic literature review. *International Journal of Electronic Marketing and Retailing (IJEMR)*, 11(3), 259-259. <https://doi.org/10.1504/ijemr.2020.108126>
- Mikkonen, T., Pautasso, C. y Taivalsaari, A. (2021, July 1). Isomorphic Internet of Things Architectures with Web Technologies. *IEEE Computer*, 54(7), 69-78. <https://doi.org/10.1109/mc.2021.3074258>
- Miorandi, D., Sicari, S., Pellegrini, F D. y Chlamtac, I. (2012, September 1). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497-1516. <https://doi.org/10.1016/j.adhoc.2012.02.016>
- Panicker, J., Salehi, A. y Rudolph, C. (2021, October 1). Authentication and Access Control in 5G Device-to-Device Communication. *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* <https://doi.org/10.1109/trustcom53373.2021.00229>
- Patil, S S., Agarwal, N., Choudhary, R., Dande, S. y Raj, R A. (2021, April 19). IoT based Employee Tracking and Management System. *International Journal of Computer Application*, 174(30), 5-7. <https://doi.org/10.5120/ijca2021921226>
- Pereira, I M., Carneiro, T. y Figueiredo, E. (2021, June 1). Understanding the context of IoT software systems in DevOps. *IEEE/ACM 3rd International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT)* <https://doi.org/10.1109/serp4iot52556.2021.00009>
- Raja, S. P., Rajkumar, T. D. y Raj, V. P. (2018). Internet of Things: Challenges, Issues and Applications. *Journal of Circuits, Systems and Computers*, 27(12), 1830007-1830007. <https://doi.org/10.1142/s0218126618300076>
- Serror, M., Hack, S., Henze, M., Schuba, M. y Wehrle, K. (2021, May 1). Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 17(5), 2985-2996. <https://doi.org/10.1109/tii.2020.3023507>
- Sheikh, R A. y Goje, N S. (2021, January 4). Role of Big Data Analytics in Business Transformation. *Internet of Things in Business Transformation, Developing an Engineering and Business Strategy for Industry 5.0*, 231-259. <https://doi.org/10.1002/9781119711148.ch13>
- Siddalingamma, M. (2023, June 30). Current Trends and Challenges of IOT Next 5 Years. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 11(6), 4141-4148. <https://doi.org/10.22214/ijraset.2023.54409>
- Ullah, M., Nardelli, P H J., Wolff, A. y Smolander, K. (2020, October 1). Twenty-One Key Factors to Choose an IoT Platform: Theoretical Framework and Its Applications. *IEEE Internet of Things Journal*, 7(10), 10111-10119. <https://doi.org/10.1109/jiot.2020.3000056>

- Villa, D., Song, X., Heim, M. y Li, L. (2021, January 1). Internet of Robotic Things: Current Technologies, Applications, Challenges and Future Directions. *arXiv*. <https://doi.org/10.48550/arXiv.2101.06256>
- Yang, H. y Alouini, M. (2018, January 1). Characterizing Energy Efficiency of Wireless Transmission for Green Internet of Things: A Data-Oriented Approach, *arXiv*, <https://doi.org/10.48550/arxiv.1805.11725>
- Yang, L., Chen, Y., Zuo, W., Nguyen, T., Gurumani, S., Rupnow, K. y Chen, D. (2015, November 1). System-level design solutions: Enabling the IoT explosion. *2015 IEEE 11th International Conference on ASIC (ASICON)*, 1-4. <https://doi.org/10.1109/asicon.2015.7517023>
- Zheng, T., Chen, G., Wang, X., Chen, C., Wang, X. y Luo, S. (2019, July 12). Real-time intelligent big data processing: technology, platform, and applications. *Information Sciences*, 62(8). <https://doi.org/10.1007/s11432-018-9834-8>
- Zolfaghari, B., Yazdinejad, A. y Dehghantanha, A. (2022). The Dichotomy of Cloud and IoT: Cloud-Assisted IoT From a Security Perspective. *arXiv*. <https://doi.org/10.48550/arXiv.2207>

CONTRIBUCIONES DE AUTORES/AS, FINANCIACIÓN Y AGRADECIMIENTOS

Contribuciones de los autores:

Conceptualización: Luis García, Luis Carlos; **Software:** Luis García, Luis Carlos **Validación:** Luis García, Luis Carlos **Análisis formal:** Luis García, Luis Carlos **Curación de datos:** Luis García, Luis Carlos; **Redacción-Preparación del borrador original:** Luis García, Luis Carlos **Redacción-Re- visión y Edición:** Torres Gómez, Andrés Rodolfo **Visualización:** Torres Gómez, Andrés Rodolfo **Supervisión:** Torres Gómez, Andrés Rodolfo **Administración de proyectos:** Torres Gómez, Andrés Rodolfo **Todos los/as autores/as han leído y aceptado la versión publicada del manuscrito:** Luis García, Luis Carlos; Torres Gómez, Andrés Rodolfo.

Financiación: Esta investigación no recibió financiación.

Conflicto de intereses: No Aplica

AUTORES:

Luis Carlos Luis-García

Corporación Universitaria Minuto de Dios.

Ingeniero Electrónico, magister en ingeniería – Telecomunicaciones y estudiante de Maestría en Inteligencia Artificial con interés en los campos del Internet de las Cosas, Inteligencia de Negocios y sus aplicaciones en la industria y la educación, he realizado proyectos de investigación en temas de Internet de las Cosas como parte de evaluación de bancos de pruebas para su despliegue y soluciones específicas en diferentes sectores, con habilidades en desarrollo en herramientas de hardware y software, docente investigador de la Corporación Universitaria Minuto de Dios.

luis.luis@uniminuto.edu

Índice H: 4

Orcid ID: <https://orcid.org/0000-0002-4840-0746>

Google Scholar: <https://scholar.google.com/citations?hl=es&user=VEZlZmwAAAAJ>

ResearchGate: <https://www.researchgate.net/profile/Luis-Luis-Garcia-2>

Andrés Rodolfo Torres Gómez

Corporación Universitaria Minuto de Dios.

Ingeniero Electrónico, magister en ingeniería – Telecomunicaciones, Magister en Internet de las Cosas con interés en los campos del Internet de las Cosas y sus aplicaciones en la industria y la educación, director de Posgrados de Ingeniería de la Corporación Universitaria Minuto de Dios.

andres.torres.go@uniminuto.edu

Índice H: 2

Orcid ID: <https://orcid.org/0000-0002-7424-0715>

Google Scholar: <https://scholar.google.com/citations?user=gGpPn8AAAAAJ&hl=es>

ResearchGate: <https://www.researchgate.net/profile/Andres-Rodolfo-Torres-Gomez>