

[2023]



IBERO

De:
Planeta Formación y Universidades

Modelo de seguridad para el Internet de las cosas, a través de la Inteligencia de negocios y cadenas de bloques.

Yesid Díaz Gutiérrez

Corporación Universitaria
Iberoamericana

Diana Carolina Candia Herrera

Corporación Universitaria
Iberoamericana

Arnaldo Andrés Gonzales

Corporación Unificada Nacional de
Educación Superior CUN

[Facultad de Ingeniería]
Corporación Universitaria
Iberoamericana



**Modelo de seguridad para el Internet de las cosas, a través de la
Inteligencia de negocios y cadenas de bloques.**

**Security model for the Internet of Things, through Business Intelligence
and blockchain.**

Yesid Díaz Gutiérrez

Diana Carolina Candía Herrera

Corporación Universitaria Iberoamericana

Arnaldo Andrés González

Corporación Unificada Nacional de Educación Superior CUN

Diciembre 14 de 2023

Agradecimientos

A la Dirección Nacional de Investigaciones por brindar los elementos estratégicos para el desarrollo del proceso Investigativo

A la Decanatura de la Facultad de Ingeniería en cabeza del Ingeniero Oscar Walteros Rangel, por su apoyo irrestricto al desarrollo de la investigación al interior de la facultad en temas de pertinencia y relevancia de la ingeniería

A la Dirección de programas TI, en cabeza del Ingeniero José Alejandro Neira Díaz, por su orientación en el planteamiento y desarrollo del proyecto de Investigación

Al Docente Jonny Rafael Plazas Alvarado, líder de investigación, por su constante acompañamiento en todos los procesos conexos al ejercicio investigativo en el marco del desarrollo del proyecto.

Resumen

Debido a la proliferación de delitos informáticos relacionados con la vulnerabilidad de la información que manejan personas y entidades, evidenciados en ataques de carácter financiero, comercial, personal e incluso familiar; Se ha identificado como una posible solución alternativa para esta situación las cadenas de bloques (BlockChain), que permiten que la información sea pública y se almacene en diferentes bloques, lo que facilita garantizar la integridad de la información en base a los siguientes aspectos:

- Identificación de la información atacada y/o comprometida, la cual puede marcarse como información no válida.
- Denunciar el ataque públicamente.
- Copia de seguridad de la información en otro bloque para facilitar su recuperación.

En ese orden de ideas, es importante resaltar que estas características funcionales y tecnológicas que ofrece la Blockchain, facilitan la gestión de la información y su integridad; Sin embargo, es necesario e imprescindible garantizar previamente la estructura de la información generada; pues algunos procesos de Inteligencia de negocios (BI por sus siglas en inglés - Business Intelligence), como el esquema ETL (Extracción, Transformación y Carga), serían de gran relevancia y apoyo durante el desarrollo de este procedimiento. Así, para el desarrollo de este proyecto se han diseñado prototipos funcionales dirigidos a estas iniciativas de solución, que permiten analizar los siguientes aspectos:

- Validación del proceso de Extracción, Transformación y carga de Información en el Internet de las Cosas a través de BI.
- Características de las funciones Hash.
- Estructura funcional de las aplicaciones BlockChain

Estos aspectos analizados anteriormente, permiten obtener resultados estructurados como insumo al proceso de Diseño y estructura de un modelo de seguridad para el Internet de las Cosas, a través de Blockchain y funciones hash.

Palabras Clave: Internet de las Cosas; Inteligencia de Negocio; cadena de bloques; Extracción, Transformación; Cargar; transmisión; Industrias inteligentes; Tecnologías emergentes; Tecnologías disruptivas; seguridad; referencia; inmutabilidad; Criptografía.

Abstract

Due to the proliferation of computer crimes related to the vulnerability of the information handled by people and entities, evidenced in attacks of a financial, commercial, personal and even family nature; Block chains (BlockChain) have been identified as a possible alternative solution for this situation, which allow information to be public and stored in different blocks, which makes it easier to guarantee the integrity of the information based on the following aspects:

- Identification of the attacked and/or compromised information, which can be marked as invalid information.
- Publicly denounce the attack.
- Backup of the information in another block to facilitate its recovery.

In this order of ideas, it is important to highlight that these functional and technological characteristics offered by Blockchain facilitate the management of information and its integrity; However, it is necessary and essential to previously guarantee the structure of the information generated; since some Business Intelligence (BI) processes, such as the ETL (Extraction, Transformation and Loading) scheme, will be of great relevance and support during the development of this procedure. Thus, for the development of this project, functional prototypes have been designed aimed at these solution initiatives, which allow the following aspects to be analyzed:

- Validation of the process of Extraction, Transformation and loading of Information in the Internet of Things through BI.
- Characteristics of Hash functions.
- Functional structure of BlockChain applications

These aspects analyzed above allow us to obtain structured results as input to the Design and structure process of a security model for the Internet of Things, through Blockchain and hash functions.

Key Words: Internet of Things; Business intelligence; BlockChain; Extraction, Transformation; Charge; transmission; Smart Industries; Emerging technologies; disruptive technologies; safety; referencing; immutability; Cryptography

Tabla de Contenido

Introducción.....	9
Capítulo 1 – Fundamentación conceptual y teórica	11
Capítulo 2 - Aplicación y Desarrollo.....	14
2.1 Tipo y Diseño de Investigación.....	14
2.2 Marco General de Trabajo	15
2.3 Población o entidades participantes.....	18
2.4 Definición de Variables o Categorías	19
2.5 Procedimiento e Instrumentos.....	19
2.6 Consideraciones Éticas.....	20
2.5 Alcances y limitaciones.....	21
Capítulo 3 - Resultados.....	22
Capítulo 4 - Conclusiones.....	23
4.1 Cumplimiento de objetivos del proyecto.....	23
4.2 Aportes a líneas de investigación de grupo y a los Objetivos del Desarrollo Sostenible – ODS.....	25
4.3 Impacto del proyecto de Investigación	26
4.4 Producción asociada al proyecto.....	27
4.5 Líneas de trabajo futuras.....	28
Anexos.....	29
Referencias	30

Índice de Tablas

Tabla 1. Procedimientos e instrumentos de la investigación, fuente:
elaboración propia.....20

Tabla 2. Fases metodológicas y productos, fuente: elaboración propia.23

Tabla 3. Resultados objetivo 1, fuente: elaboración propia.....24

Tabla 4. Resultados objetivo 2, fuente: elaboración propia.....24

Tabla 5. Resultados objetivo 3, fuente: elaboración propia.....25

Tabla 6. Tabla de productos obtenidos de esta investigación, fuente:
elaboración propia.....27

Índice de Ilustraciones

Ilustración 1. Marco metodológico, fuente: elaboración propia.	16
---	----

Introducción

En un entorno digital caracterizado por la omnipresencia y ubicuidad de las tecnologías emergentes, la seguridad de la información se marca como un desafío crucial. La cuarta revolución industrial y la expansión del Internet de las cosas (IoT) han traído consigo una creciente amenaza de delitos informáticos, especialmente durante la transmisión de datos. La necesidad de salvaguardar la integridad y privacidad de la información se ha vuelto imperativa. En respuesta a este escenario, esta investigación se propone diseñar un modelo de seguridad integral para abordar específicamente la fase de transmisión de datos en el IoT.

Considerando la vulnerabilidad inherente a la conexión ubicua del IoT a la red, exploramos la aplicación de cadenas de bloques (Blockchain) como una alternativa efectiva. Estas ofrecen una solución robusta al permitir la publicación de información en bloques individuales, garantizando así la integridad de los datos. El enfoque se completa con la integración de la inteligencia de negocios para estandarizar procesos, generando un modelo que abarca desde la identificación de información atacada hasta la recuperación eficiente de datos. A través de esta investigación, buscamos no solo proporcionar una respuesta efectiva a los desafíos actuales de seguridad informática, sino también contribuir a la estabilidad y confiabilidad de las tecnologías emergentes en el panorama digital contemporáneo.

Es por ello por lo que a continuación, se presentan los objetivos de esta investigación, así:

General

Desarrollar una investigación que permita diseñar un modelo de seguridad, para la fase de transmisión de la información en el Internet de las Cosas,

integrando la Inteligencia de negocios para su estandarización y el Blockchain en su almacenamiento.

Específicos

Implementar la Inteligencia de negocios y su esquema de Extracción, Transformación y Cargue, como protocolo de estandarización de la información generada en el Internet de las cosas.

Identificar las fortalezas que tiene Blockchain como estructura de almacenamiento de la información generada en el Internet de las cosas durante la fase de transmisión.

Caracterizar los componentes relacionados con la integridad de la información generada por el Internet de las cosas, a través de la referenciación, el acceso y la inmutabilidad del Blockchain.

Capítulo 1 – Fundamentación conceptual y teórica

La cuarta revolución industrial, también conocida como la era de la digitalización; ha generado cambios sustanciales en los procesos de recepción, manejo y transmisión de la información; esto teniendo en cuenta la aparición de múltiples tecnologías enmarcadas en el concepto de Tecnologías 4.0. El Blockchain, La Inteligencia de negocios, la Analítica de Datos, el Machine Learning y El Internet de las cosas; son algunos ejemplos de los nuevos elementos emergentes y disruptivos que han cobrado gran relevancia en esta era y que de una u otra forma, han condicionado y modificado el tratamiento de los datos como insumo primordial de la información.

Bajo este escenario, es muy común evidenciar ataques informáticos que buscan vulnerar la integridad y privacidad de los datos y por ende de la información, los cuales, en este contexto de la digitalización, se han venido proliferando por dos razones fundamentales. Por una parte, debido a la diversificación de nuevas tecnologías que generan gran cantidad de datos y que, por su aparición reciente, no habían sido contempladas en los modelos de seguridad existentes; y, por otra parte; debido a la importancia que para el contexto global actual tienen los datos y la información.

Precisamente, y dada la importancia de los procesos de manejo y tratamiento efectivo de la información, para garantizar el impacto práctico en los esquemas de los cuales se deriva; es fundamental posicionar al BI, como el mayor dinamizador de los datos generados por tecnologías como el IOT; esto en el marco del ejercicio de ETL, que desarrolla BI.

Al respecto de lo anterior, es importante aclarar que, aunque el BI, en su contexto Holístico tiene un alcance mucho más ambicioso; su proceso de ETL genera múltiples beneficios para control y dinamización de los datos

durante su transición a convertirse en información. En el artículo titulado “Porque la Inteligencia de negocios es la Inteligencia de los datos”, publicado en el año 2019, en el portal web itsitio. (Forti, 2019); se menciona que Hans Peter Luhn, en 1958, definió el concepto de “Inteligencia de Negocio”, como “La capacidad de comprender las interrelaciones de los hechos presentados de tal forma que consiga orientar la acción hacia una meta deseada”. De igual forma, en este mismo escrito, se indica que, basado en esta definición, Howard Dresner en 1989 describió a la Inteligencia de negocios como “Los conceptos y métodos para mejorar la toma de decisiones empresariales mediante el uso de sistemas basados en hechos de apoyo”; brindando un contexto aplicado hacia el uso e implementación del BI. Sin embargo, en ese momento solo se disponía de datos estructurados (Bases de Datos), por lo cual su impacto no superó las expectativas que se tenían al respecto.

Con la creciente relevancia del manejo de los datos en los ejercicios derivados de las tecnologías 4.0., la generación de grandes volúmenes de datos y la aparición de conceptos como el BigData y la Minería de Datos, el BI, cobra vital importancia y se convierte, como se ha manifestado anteriormente, en el principal dinamizador de los datos en su proceso de transición hacia su conversión en Información. De allí la importancia de vincularlo en el proceso de transmisión de la información del Internet de las cosas, a través de cadenas de bloques.

Es precisamente, el Internet de las Cosas y su proceso de transmisión de la información, el espectro sobre el cual se aplicará el BI, desde su esquema ETL. Al respecto de lo anterior, es fundamental indicar que el IOT, hace parte en la actualidad del día a día de un alto porcentaje de personas en todo el mundo, ya sea para el desarrollo de actividades cotidianas como el uso de electrodomésticos (televisores Inteligentes - Smart TV, relojes Inteligentes Smartwatch. Entre otros), hasta su uso y aplicación industrial. Jordi Salazar y Santiago Silvestre en su texto, “El Internet de las cosas”. (Silvestre, 2016), mencionan que “La IoT introduce un cambio radical en la calidad de vida de las personas, ofreciendo una gran cantidad de nuevas

oportunidades de acceso a datos, servicios específicos en la educación, en seguridad, asistencia sanitaria o en el transporte, entre otros campos”. Lo que brinda un palmarés claro y preciso del protagonismo del IOT en la generación de Datos. Desde esta perspectiva, se plantea para esta investigación una articulación y relación directa entre el producto (Datos) del ejercicio tecnológico del IOT en el contexto mundial y la capacidad que el BI tiene para Extraerlos, Transformarlos y Cargarlos, actuando como un protocolo inicial de protección a través de su delimitación y categorización.

En ese mismo orden de ideas y buscando generar una estructura robusta y articulada frente a la protección de los datos generados y transmitidos por el IOT; es fundamental analizar el papel que el Blockchain, juega dentro del planteamiento de esta investigación. Al respecto, Dolader, Bel y Muñoz en su artículo “La Blockchain: Fundamentos, aplicaciones y relación con otras tecnologías disruptivas”; afirman que “La información añadida a la Blockchain es pública y puede ser consultada en cualquier momento por cualquier usuario de la red. La información solo puede ser añadida a la cadena de bloques si existe un acuerdo entre la mayoría de las partes. Transcurrido un cierto tiempo, se puede asumir que la información agregada en un bloque ya no podrá ser modificada (inmutabilidad).” (Carlos Dolader, 2017). Esta afirmación permite identificar tres (3) elementos fundamentales, como conclusiones preliminares de esta primera parte de análisis:

La capacidad del Blockchain para “marcar” bloques específicos.

El acceso a cualquier bloque en cualquier momento, por parte de cualquier usuario.

La Inmutabilidad como esquema protector de la información.

Capítulo 2 - Aplicación y Desarrollo

Teniendo en cuenta la exposición que el Internet de las Cosas tiene a los ataques informáticos, sobre todo en el proceso de transmisión de la información, debido básicamente a la ausencia de protocolos o modelos de seguridad que permitan garantizar la integridad de los datos y a los grandes volúmenes de datos que de este proceso se derivan; se analiza la posibilidad de implementar el esquema ETL de la Inteligencia de negocios BI, como protocolo para delimitar y categorizar los datos extraídos, buscando que posteriormente estos datos sean transformados en información estandarizada para facilitar su almacenamiento y procesamiento.

Sin embargo, el concurso de BI no garantiza en su totalidad la integridad de la información, porque, aunque permite dar un formato a los datos, excluyendo información errada; no genera por sí misma, esquemas de protección que puedan repeler ataques informáticos. Por lo anterior y buscando satisfacer esas necesidades; se analizan también las características funcionales de Blockchain, en cuanto a referenciación (Marca de bloques específicos), acceso (Descentralización de la Información) y protección (Inmutabilidad). Dando origen a una segunda pregunta:

Lo anterior conduce a formular la pregunta de investigación:

¿De qué manera la Inteligencia de negocios y el Blockchain se pueden articular para el diseño de un modelo de seguridad en soluciones para el internet de las cosas (IoT)?

2.1 Tipo y Diseño de Investigación

El enfoque investigativo del proyecto se soporta específicamente en lo cualitativo, lo anterior debido a que se centra en la caracterización funcional de procesos tecnológicos No numéricos basados en la exploración en

profundidad de fenómenos funcionales de cada tecnología, sin prejuicios ni restricciones impuestas por la hipótesis planteada.

De acuerdo con lo anterior, se utilizaron las siguientes técnicas para recolección de información:

- Observación
- Análisis de documentos
- Revisión bibliográfica
- Estudios de casos

Es importante resaltar que, en cuanto al enfoque metodológico, este se estructuró desde un (1) marco general de trabajo, delimitado por el ciclo de Deming, más conocido como PHVA o de mejora continua. Este ciclo regula el accionar metodológico desde lo Investigativo y lo Disciplinar, entregando resultados propios, independientes (De acuerdo con los resultados que arroja cada metodología por sí misma), pero conexos (Debido a que todos los resultados se articulan en torno a la comprobación de la hipótesis formulada para la investigación).

De acuerdo con lo anterior, la metodología de trabajo tiene 3 elementos fundamentales:

Marco general de trabajo.

Metodología de Investigación.

Metodología disciplinar.

2.2 Marco General de Trabajo

El primer elemento, marco general de trabajo, permite tener una visión holística del desarrollo integral de la investigación, ya que está compuesto por dos (2), enfoques metodológicos; el Investigativo por medio del Método Científico y el disciplinar con la metodología Ágil Scrum.

Con el objetivo de ejercer un control sobre el desarrollo de cada una de estas metodologías, se decide vincular el Ciclo PHVA (Planear, hacer Verificar y Actuar), permitiendo disponer de un seguimiento permanente a la evolución de cada accionar metodológico. Para mayor claridad, a continuación, se presenta de forma gráfica el marco general de trabajo. Ver ilustración 1.

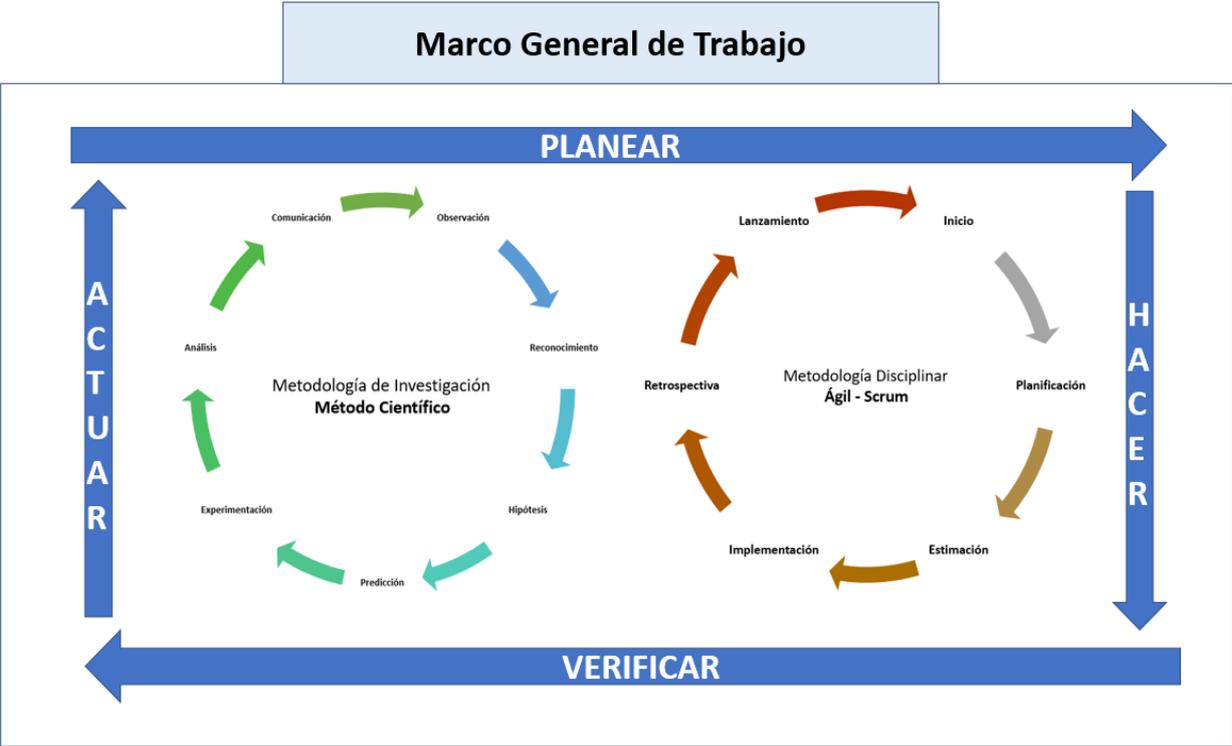


Ilustración 1. Marco metodológico, fuente: elaboración propia.

Ciclo PHVA

Planear: dentro de la planeación del proceso de desarrollo del trabajo de la investigación, se tomará como punto de partida la identificación y delimitación del estado actual del objeto de estudio, abordando como herramienta principal, el análisis de los mecanismos, protocolos y métodos de seguridad que se estaban utilizando en el momento y su pertinencia y efectividad frente a las transacciones y servicios dinamizados desde el Internet de las Cosas.

Hacer: aunque cada una de las metodologías seleccionadas (método científico y Scrum), tienen sus dinámicas particulares; desde el marco general de trabajo se realiza un control a dichas acciones por medio del ciclo PHVA. Es allí donde el “Hacer” facilita abordar los esquemas de solución por medio de pruebas desarrolladas en un entorno controlado evitando la interacción de factores externos que afecten el diseño de la solución final.

De acuerdo con lo anterior, los ejercicios de la estructura metodológica estarán delimitados a través de prototipos que permitan validar el impacto y eficiencia de los procesos disciplinares e investigativos, los cuales estarán soportados sobre la base de los pilares de la industria 4.0. que se puedan identificar como elementos de soporte tecnológico al proceso disciplinar.

Verificar: Una vez se han aplicado prototipos en el marco de pruebas preliminares o pruebas piloto, es necesario analizar detalladamente los resultados obtenidos durante el proceso de aplicación, para determinar si la proyección de la solución satisface las necesidades identificadas en el paso de planeación. Por otra parte, es necesario realizar un comparativo entre estos resultados obtenidos y los objetivos planteados.

Metodología disciplinar Ágil Scrum

Teniendo en cuenta el Marco general del trabajo en el que se definen 2 enfoques metodológicos para el desarrollo de la investigación (Investigativo y disciplinar) y habiendo desarrollado anteriormente el enfoque investigativo, a continuación, se desarrolla el contexto de aplicación de la metodología SCRUM como dinamizador disciplinar, resaltando que su aplicación se centra en lo que demanda el ejercicio de prototipado.

Desde esta perspectiva se define como marco de trabajo metodológico SCRUM bajo tres (3) componentes esenciales:

Ceremonias

- Sprint Planning
- Daily

Artefactos

- Product Backlog
- Sprint Backlog
- Incremento

Roles

- Producto Owner
- Scrum Máster
- Equipo Scrum

2.3 Población o entidades participantes

La Corporación Unificada Nacional de Educación Superior CUN, a través del programa de Ingeniería de sistemas, ha venido avanzando significativamente en investigaciones sobre la arquitectura de soluciones IOT y las características de la información que los dispositivos vinculados a la solución emiten, definiendo una estructura estándar para el formato de dicha información. Partiendo de estos avances, se ha logrado un acercamiento con ellos a fin de poder desarrollar la iniciativa de investigación planteada en esta ficha con el objetivo de aprovechar sus prototipos para realizar pruebas con la información por ellos generada.

La Universidad Santo Tomas y su programa de Ingeniería en Informática, realizó planteamientos de modelos para el refinamiento de datos a través del proceso de Extracción, Transformación y Cargue (ETL) de la inteligencia de negocios. Este modelo preliminar, podría ser ajustado en

el marco de la iniciativa de investigación que se expone en esta ficha, para adaptar el refinamiento de los datos generados por soluciones IOT, como uno de los componentes del modelo de seguridad que se plantea.

2.4 Definición de Variables o Categorías

Dentro de las definiciones para esta investigación se precisaron las siguientes variables y sus categorías, así:

Inteligencia de Negocios en los negocios: herramientas dedicadas para las métricas claves y análisis de datos, con las siguientes categorías: monitorización, predicción de datos y reportes de seguridad.

Vulnerabilidades de IoT: identificación de dispositivos IoT, estudio de protocolos de comunicación y niveles de acceso; como categorías: identificación de vulnerabilidades y análisis de amenazas.

Integridad de los datos: timestamping y algoritmos de cifrado de datos, categorías: protección de manipulación de datos.

Formación: capacitación y frecuencia de los programas de formación, agendamiento de los participantes en los eventos de divulgación tecnológica.

2.5 Procedimiento e Instrumentos

Procedimientos	Instrumentos
Revisión bibliográfica: revisión sistemática de libros, artículos y documentación científica. Análisis de los autores y estudios relacionados al Internet de las cosas IoT.	Herramientas de análisis estadísticos o de desarrollo de software: con el ánimo de analizar los procesos de datos ETL, por medio del desarrollo de un software en el lenguaje de programación de Python.
Diseño del modelo : modelado de un sistema conceptual, revisión y	Software de desarrollo: ajuste al modelo de seguridad en un entorno

validación con expertos. Desarrollo de los conceptos del modelo de seguridad.	controlado y un dataset elegido para el ejemplo de la validación de los datos.
Análisis de resultados: revisión de métricas y análisis de estos, por otra parte, se evalúa el rendimiento del modelo en cuanto a los escenarios conceptuales de ubicar un modelo.	

Tabla 1. Procedimientos e instrumentos de la investigación, fuente: elaboración propia.

2.6 Consideraciones Éticas

Teniendo el artículo 11 de la Resolución 008430 de 1993 del Ministerio de Salud, la clasificación de la investigación según las categorías allí establecidas es Investigación sin riesgo. Lo anterior teniendo en cuenta que los procesos de caracterización, análisis y validación están orientados a dispositivos tecnológicos y la información derivada de estos ejercicios no impacta poblaciones en particular, toda vez que todo el enfoque metodológico y funcional de la investigación se centra en el dato y su transformación hacia información.

Por otra parte, a continuación, se expone la articulación de las consideraciones éticas en los tres contextos solicitados:

A. Declaración de Singapur sobre la integridad en la investigación.

Honestidad en todos los aspectos de la Investigación.

Responsabilidad en la ejecución de la Investigación.

Cortesía profesional e imparcialidad en todas las relaciones laborales.

Buena gestión de la investigación en nombre de otros.

B. Ley 1581 de 2012 – Protección de Datos personales.

La investigación no manipulará datos personales.

C. CONPES 3920 – Política Nacional de Explotación de datos.

Teniendo en cuenta que no se manipulará información de personas y que todos los datos e información tratados al interior de la investigación se derivan de procesos funcionales de tres (3) prototipos; el CONPES 3920 no estará dinamizado en el desarrollo del proyecto.

2.5 Alcances y limitaciones

Alcances:

Desarrollo del Modelo de Seguridad: el proyecto se enfocará en diseñar, implementar y evaluar un modelo de seguridad.

Validación con Expertos: se buscará la validación externa del modelo mediante la retroalimentación de expertos en ciberseguridad, tecnologías emergentes y campos relacionados.

Aplicación Práctica: el modelo se implementará y evaluará en un entorno controlado para simular condiciones de uso realistas.

Limitaciones:

Recursos Limitados: las limitaciones de tiempo y recursos pueden afectar la profundidad y alcance de la investigación, así como la cantidad de escenarios de simulación de amenazas.

Dependencia de Datos Simulados: la evaluación del modelo se basará en datos simulados en lugar de datos reales, lo que puede influir en la exactitud de los resultados.

Capítulo 3 - Resultados

El desarrollo del proyecto evidenció una estrecha alineación entre los resultados obtenidos y el accionar metodológico empleado durante su ejecución. La confluencia entre la planificación estratégica y la acción práctica se convirtió en un eje fundamental para asegurar la coherencia entre los objetivos propuestos y los logros alcanzados. En este sentido, el seguimiento riguroso del marco metodológico estuvo adaptado a las necesidades del proyecto, permitiendo validar la congruencia entre las etapas planteadas y los resultados obtenidos.

La construcción y validación de los prototipos funcionales emergió como una piedra angular en la ejecución, ya que la materialización de estos prototipos no solo validó la viabilidad técnica de las soluciones planteadas, sino que también ofreció una oportunidad para ajustar y mejorar iterativamente el desarrollo del proyecto. Además de los prototipos funcionales, los productos escritos, como artículos científicos, representan un medio crucial para comunicar y validar los hallazgos y avances logrados durante la ejecución del proyecto. Estos documentos no solo consolidan los resultados obtenidos, sino que también permiten compartir las lecciones aprendidas, metodologías utilizadas y el impacto potencial de los desarrollos tecnológicos.

A continuación, se presentan los resultados obtenidos articulados con las fases metodológicas:

Fase Metodológica	Descripción	Producto
Análisis de Contexto y Diagnóstico Tecnológico	Estado del arte de modelos de arquitectura IOT	Artículo – Protocolos de seguridad y transmisión, en la construcción de una arquitectura IOT.
	Validación de la arquitectura y conectividad de las soluciones IOT	Prototipo Funcional IOT para medición de temperatura en cultivos

Caracterización funcional del soporte tecnológico	Validación del proceso de estandarización y refinamiento de datos	Prototipo Funcional del proceso ETL en Pentaho Data Integration.
	Validación del proceso de conversión salida de Datos BD – Estructura Python	Prototipo funcional aplicativo software transición MySQL – Python
	Validación del proceso de transmisión de Datos, ETL y Python	Prototipo Funcional Modulo de autenticación biométrica de usuarios
Estructuración de una solución de seguridad	Diseño del modelo de seguridad para el Internet de las cosas a través de cadenas de bloques (Blockchain)	Artículo- Modelo de seguridad para el Internet de las cosas a través de Blockchain
Socialización resultados de investigación	Ponencia internacional	Certificación de la ponencia internacional Universidad evangélica el Salvador

Tabla 2. Fases metodológicas y productos, fuente: elaboración propia.

Capítulo 4 - Conclusiones

Las conclusiones del proyecto reflejan el éxito en la consecución de sus objetivos preestablecidos. La meticulosa ejecución del plan estratégico y la alineación constante con la metodología seleccionada fueron pilares fundamentales que propiciaron el logro de cada hito propuesto. La culminación exitosa de este proyecto no solo valida la viabilidad técnica de las soluciones implementadas, sino que también destaca la importancia de la colaboración interdisciplinaria y la dedicación a lo largo del proceso. Este éxito no solo consolida los resultados obtenidos, sino que abre nuevas puertas hacia la innovación y el avance en el campo de las tecnologías de la información.

4.1 Cumplimiento de objetivos del proyecto

Teniendo en cuenta el diseño de la investigación desde la proyección de los objetivos; a continuación, se relacionan los porcentajes de cumplimiento de cada uno de ellos:

Objetivo 1

Implementar la Inteligencia de negocios y su esquema de Extracción, Transformación y Cargue, como protocolo de estandarización de la información generada en el Internet de las cosas:

Actividades	Cumplimiento
Evaluación de Prototipos	100%
Evaluaciones características de Arquitecturas IOT	100%
Evaluación de modelos ETL en soluciones IOT	100%
Definición Marco Metodológico	100%
Estructuración Arquitectura de la solución Versión 1.0.	100%
Salidas de Datos de tipo BD con Herramientas BI	100%
Caracterización Modelos de seguridad para IOT	100%

Tabla 3. Resultados objetivo 1, fuente: elaboración propia.

Objetivo 2

Identificar las fortalezas que tiene Blockchain como estructura de almacenamiento de la información generada en el Internet de las cosas durante la fase de transmisión.

Actividades	Cumplimiento
Apropiación Herramientas de construcción de BlockChain	100%
Desarrollo general para importación de BD a Blockchain	100%
Desarrollo específico para construcción de BlockChain	100%
Pruebas y Documentación de resultados parciales	100%
Estructuración Arquitectura de la solución Versión 2.0.	100%

Tabla 4. Resultados objetivo 2, fuente: elaboración propia.

Objetivo 3

Caracterizar los componentes relacionados con la integridad de la información generada por el Internet de las cosas, a través de la referenciación, el acceso y la inmutabilidad del Blockchain.

Actividades	Cumplimiento
Definición de componentes tecnológicos de la solución	100%
Definición de interacciones sobre la información	100%
Arquitectura de la solución versión final	100%
Documentación de resultados Finales	100%

Tabla 5. Resultados objetivo 3, fuente: elaboración propia.

4.2 Aportes a líneas de investigación de grupo y a los Objetivos del Desarrollo Sostenible – ODS

En cuanto a los aportes del proyecto a la línea de investigación de **Sistemas emergentes y nuevas tecnologías de redes y software**, es posible identificar los siguientes:

Caracterización de componentes tecnológicos relacionados con soluciones del Internet de las cosas.

Estructuración funcional del proceso de Extracción, transformación y Cargue a través de herramientas de software (Pentaho Data Integration)

Validación de esquemas de seguridad de tecnologías emergentes (IOT).

Desarrollo de soluciones de software para el proceso de transición de salidas de datos a cadenas de bloques.

Modelamiento de soluciones orientadas a seguridad en tecnologías emergentes.

En cuanto a los aportes del proyecto al Objetivo de Desarrollo Sostenible **Número 9 – Industria, innovación e infraestructura**, es posible identificar los siguientes:

- Delimitación tecnológica y funcional de una solución del Internet de las cosas como parte de una infraestructura tecnológica.
- Estructuración de un esquema de transición de Base de Datos a cadenas de bloques como factor de innovación.

- Concepción de un esquema de seguridad general a través de un modelo dinamizado por la inteligencia de negocios y las cadenas de bloques.

4.3 Impacto del proyecto de Investigación

La convergencia de Internet de las Cosas (IoT), Blockchain, inteligencia de negocios y el poderoso lenguaje de programación Python ha desencadenado un proyecto innovador con impactos multifacéticos y significativos en el mundo empresarial y tecnológico. Este proyecto no solo representa una sinergia entre tecnologías de punta, sino que también establece un nuevo estándar en la optimización operativa, la seguridad de datos, la toma de decisiones basada en datos y la agilidad en el desarrollo de soluciones.

A continuación, se exploran los impactos de esta amalgama tecnológica que no solo revela la magnitud de su potencial transformador, sino que también destaca la importancia y el alcance de la interconexión estratégica entre estas herramientas disruptivas en el panorama actual de la innovación tecnológica:

Eficiencia Operativa Mejorada:

La integración de IoT permite la recopilación de datos en tiempo real de dispositivos conectados, optimizando procesos y permitiendo la toma de decisiones basada en datos.

Seguridad Reforzada:

La implementación de Blockchain en la gestión de datos garantiza la seguridad y la integridad de la información, lo que es crucial en entornos empresariales y de IoT, donde la confiabilidad de los datos es esencial.

Toma de Decisiones Basada en Datos:

La inteligencia de negocios, al procesar los datos recopilados por IoT, a través del proceso ETL, ofrece análisis avanzados y visualizaciones que permiten a las empresas tomar decisiones estratégicas fundamentadas.

Desarrollo Ágil con Python:

Python, al ser un lenguaje flexible y potente, facilita el desarrollo rápido y la implementación de la solución que permite generar transición en Bases de Datos y Blockchain, concebidas desde la adquisición de datos hasta la creación de algoritmos para el desarrollo.

4.4 Producción asociada al proyecto

El proyecto ha culminado con la creación de una gama diversa y potente de productos que encapsulan la esencia de la convergencia tecnológica entre Internet de las Cosas (IOT), Blockchain, inteligencia de negocios y el versátil lenguaje de programación Python.

Estos productos representan el resultado tangible y aplicable de la sinergia entre estas tecnologías líderes, ofreciendo soluciones innovadoras que trascienden las fronteras convencionales. Cada producto es un testimonio tangible del poder transformador y la versatilidad que resulta de la unión estratégica de estas tecnologías disruptivas.

Producto	Descripción
Artículo – Protocolos de seguridad y transmisión, en la construcción de una arquitectura IOT.	Estado del arte de modelos de arquitectura IOT
Prototipo Funcional IOT para medición de temperatura en cultivos	Validación de la arquitectura y conectividad de las soluciones IOT
Prototipo Funcional del proceso ETL en Pentaho Data Integration.	Validación del proceso de estandarización y refinamiento de datos
Prototipo funcional aplicativo software transición MySQL – Python	Validación del proceso de conversión salida de Datos BD – Estructura Python
Prototipo Funcional Modulo de autenticación biométrica de usuarios	Validación del proceso de transmisión de Datos, ETL y Python
Artículo- Modelo de seguridad para el Internet de las cosas a través de Blockchain	Diseño del modelo de seguridad para el Internet de las cosas a través de cadenas de bloques (Blockchain)

Tabla 6. Tabla de productos obtenidos de esta investigación, fuente: elaboración propia.

4.5 Líneas de trabajo futuras

Con base en los resultados obtenidos en el desarrollo del proyecto, se ha planteado un trabajo futuro estructurado y soportado en la línea de la inteligencia artificial específicamente en sistemas expertos.

En ese orden de ideas, se explora la posibilidad de validar el desarrollo de un modelo de integración tecnológica entre soluciones de IoT y ecosistemas tecnológicos organizacionales, mediante la implementación de un sistema experto para el apoyo a la toma de decisiones.

Desde el trabajo exploratorio, preliminar y proyectivo, se busca en primer lugar que la implementación de este modelo puede ofrecer una optimización radical de los procesos operativos al permitir la interconexión fluida entre dispositivos IoT y los sistemas existentes en las organizaciones. Esta sinergia podría potenciar la eficiencia al recopilar datos en tiempo real desde diversos puntos, facilitando la toma de decisiones informadas y ágiles.

Además, la implementación de un sistema experto para apoyar la toma de decisiones potenciaría la capacidad de análisis y la precisión en la interpretación de datos provenientes del entorno IoT. Esto se traduce en una mejora sustancial en la toma de decisiones estratégicas y tácticas dentro de la organización, lo que puede tener un impacto directo en la productividad, la reducción de costos operativos y la identificación proactiva de oportunidades de mejora.

Asimismo, esta iniciativa abriría la puerta a una mayor seguridad y gestión eficaz de la información. La implementación de este modelo no solo facilitaría el intercambio seguro de datos entre dispositivos IoT y los sistemas empresariales, sino que también integra la robusta seguridad de los sistemas expertos, asegurando la integridad y confidencialidad de la información crítica.

Anexos

[Enlace al Drive prototipos funcionales y documentación Técnica](#)

- Artículo – Protocolos de seguridad y transmisión, en la construcción de una arquitectura IOT.
- Artículo- Modelo de seguridad para el Internet de las cosas a través de Blockchain
- Modelo gráfico del prototipo Funcional IOT para medición de temperatura en cultivos
- Manual de usuario del prototipo funcional aplicativo software transición MySQL – Python
- Evidencias fotográficas del Prototipo Funcional Modulo de autenticación biométrica de usuarios.
- Modelo Gráfico de seguridad para el Internet de las Cosas a través de cadenas de Bloques.

Referencias

Zhang, Y. (s.f.). Technology Framework of the Internet of Things and Its Application, in Electrical and Control Engineering (ICECE).

Alessio Botta, W. d. (2016). Integración de computación en la nube e Internet de las cosas: una encuesta (Vol. 56). (Elsevier, Ed.) Napoli, Italia

Sánchez-Torres, F., González, I., & Dobrescu, C. C. (2022). Machine Learning in Business Intelligence 4.0: Cost Control in a Destination Hotel.

Lovelle, J. M. C., Molano, J. I. R., & Marin, C. E. M. (2015). Introducción al Internet de las Cosas. *Redes de Ingeniería*, 6.

Retamal, C. D., Roig, J. B., & Tapia, J. (2017). La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía industrial*, 405, 33-40

Colorado, F. (2009). El ciclo PHVA de Deming y el proceso administrativo de Fayol. Academia. Recuperado de <http://www.academia.edu>

Llorián, D. M., & Lovelle, J. M. C. (2020). Socialización de Objetos Inteligentes aplicando Ingeniería Dirigida por Modelos en el marco de Internet de las Cosas (Doctoral dissertation, Universidad de Oviedo).

Douceur, J. R. (2002). The sybil attack. In *Peer-to-Peer Systems: First International Workshop, IPTPS 2002 Cambridge, MA, USA, March 7–8, 2002 Revised Papers 1* (pp. 251-260). Springer Berlin Heidelberg.

N. Ekedebe, W. Y. (2015). Securing transportation cyber-physical systems. *Securing Cyber-Physical Systems*, CRC Press, Boca Ratón.

Faludi, R. (2010). Building wireless sensor networks: with ZigBee, XBee, arduino, and processing. " O'Reilly Media, Inc."

Álvarez, M., Jiménez, J. J., González-Guerrero, M., Hernando, C., & Guerrero, H. (2012, July). Total Ionizing Dose radiation test on the temperature sensor TMP36 from Analog Devices. In 2012 IEEE Radiation Effects Data Workshop (pp. 1-7). IEEE.

González, A., Díaz, Y., & Flórez, W. (2020). Design and prototyping of an electronic cane for an indoor guide system for the blind. *Ingeniería (0121-750X)*, 25(3).

Zhang, G., Chen, X., Zhang, L., Feng, B., Guo, X., Liang, J., & Zhang, Y. (2022). STAIBT: Secure and reliable agricultural IoT Blockchain Terminal empowered by Blockchain and CP-ABE. *International Journal of Interactive Multimedia and Artificial Intelligence*, 7(Special Issue on Multimedia Transmission and Processing in IoT with Edge Intelligence)

Ruíz-Martínez, W., Díaz-Gutiérrez, Y., Ferro-Escobar, R., & Pallares, L. (2019). Application of the Internet of Things through a Network of Wireless Sensors in a Coffee Crop for Monitoring and Control its Environmental Variables. *Tecnológicas*, 22(46), 101-116.

Martínez, A. B., Lista, E. A. G., & Flórez, L. C. G. (2013). Técnicas de modelado de procesos de ETL: una revisión de alternativas y su aplicación en un proyecto de desarrollo de una solución de BI. *Scientia et Technica*, 18(1), 185-191.

Casters, M., Bouman, R., & Van Dongen, J. (2010). *Pentaho Kettle solutions: building open source ETL solutions with Pentaho Data Integration*. John Wiley & Sons.

Williams, H. E., & Lane, D. (2004). *Web Database Applications with PHP and MySQL: Building Effective Database-Driven Web Sites*. " O'Reilly Media, Inc."

Ipswich, D. (2011). Setting up a WAMP server on your windows desktop. Technology Now at Smashwords.

Arias Maestro, A., Sanjuán Martínez, Ó., Teredesai, A. M., & García-Díaz, V. (2023). Blockchain Based Cloud Management Architecture for Maximum Availability.

Gutiérrez, Y. D., & Lovelle, J. M. C. (2018). Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos. *Redes de Ingeniería*, 9(2), 82-87.

Carneiro, L. B., Silva, A. C. C., & Alencar, L. H. (2018, December). Scrum agile project management methodology application for workflow management: a case study. In 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (pp. 938-942). IEEE.

Arias Maestro, A., Sanjuan-Martinez, O., Teredesai, A. M., & García-Díaz, V. (2023). Arquitectura de gestión de la nube basada en Blockchain para máxima disponibilidad. *Revista Internacional de Multimedia Interactiva e Inteligencia Artificial*, 8(Número especial sobre algoritmos y aplicaciones impulsados por IA en entornos dinámicos y en evolución)