ESCUELA DE CIENCIAS SOCIALES Y HUMANIDADES

Tema:

USO DE LA *BLOCKCHAIN* EN EMPRESAS PRIVADAS PARA PROTEGER LOS DATOS PERSONALES CONFORME LA NORMATIVA VIGENTE

Proyecto de investigación previo a la obtención del título de Abogada

Línea de investigación:

DERECHO, PARTICIPACIÓN, GOBERNANZA, REGÍMENES POLÍTICOS E INSTITUCIONALIDAD

Autora:

Alyson Fernanda Coca Altamirano

Directora:

Mg. María Fernanda Zamora Castillo

Ambato – Ecuador

Febrero 2026

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **ALYSON FERNANDA COCA ALTAMIRANO,** con cédula de ciudadanía **1805487137**, autor del trabajo de graduación intitulado: "USO DE LA BLOCKCHAIN EN EMPRESAS PRIVADAS PARA PROTEGER LOS DATOS PERSONALES CONFORME A LA NORMATIVA VIGENTE", previo a la obtención del título profesional de **ABOGADO**, en la escuela de **CIENCIAS SOCIALES Y HUMANIDADES.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, febrero 2026

Alyson Fernanda Coca Altamirano

CC. 1805487137

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

USO DE LA BLOCKCHAIN EN EMPRESAS PRIVADAS PARA PROTEGER LOS DATOS PERSONALES CONFORME LA NORMATIVA VIGENTE

Líneas de investigación:

DERECHO, PARTICIPACIÓN, GOBERNANZA, REGÍMENES POLÍTICOS E INSTITUCIONALIDAD

Autor:

Alyson Fernanda Coca Altamirano

María Fernanda Zamora Castillo, Ab. Mg. f._____
CC. 1804079158
CALIFICADOR

Pablo Javier Silva Mejía, Ab. Mg. f._____
CALIFICADOR

Luis Fernando Suárez Proaño, Ab. Mg. f._____
CALIFICADOR

Verónica Leonor Peñaloza López, Ing. PhD. f._____
DIRECTORA ESCUELA DE CIENCIAS SOCIALES Y HUMANIDADES

Diego Gonzalo Coca Chanalata, Dr. Mg. f._____
PROSECRETARIO PUCE AMBATO

PUCE | AMBATO
PROSECRETARÍA

Ambato – Ecuador

Febrero 2026

DEDICATORIA

A Dios, por ser el guía de mi vida en los momentos más difíciles y mi refugio en tiempos de incertidumbre. Cuando el camino se tornaba oscuro y sentía que todo se iba a derrumbar, fuiste tú quien me llenó de fuerza y valor para seguir adelante y no rendirme.

A ti, papá, porque no hubo barrera lo suficientemente grande que impidiera que me ayudaras a alcanzar mis sueños, desde niña me enseñaste a ser valiente y a perseverar por mis sueños, hoy puedo decirte que todo lo que sembraste en mi ha dado sus frutos. Gracias por ser incondicional conmigo.

A ti, mamá, porque con cada abrazo me das calor de hogar, cada palabra de aliento ha sido un sostén especial que ha impedido que me desvanezca. Gracias por nunca soltar mi mano y caminar a mi lado siempre, además de darme la vida, eres mi ejemplo de vida.

A mi abuelo, Patricio, por cada consejo que me inspiró siempre a ser una buena profesional. Es profundamente satisfactorio para mí que haya podido verme crecer, y hoy, verme cumpliendo uno de mis sueños que es ser una mujer con profesión.

A mis hermanos, Gabriela, Joel y Alejandro, mis compañeros de vida, su amor constante me motivó a alcanzar mis sueños. Gracias por darme el mejor regalo que han sido mis sobrinos Mathias, Amaia y Aurora.

A mis primas hermanas, Michelle y Diana, mi apoyo incondicional. Gracias por acompañarme en este camino y por celebrar mis logros como si fueran suyos. Las quiero infinitamente.

Mi ángel en el cielo, mi abuelita Delia, su luz me sigue iluminando desde la eternidad. Gracias por haberme heredado la fortaleza, que hoy me permitió cumplir este sueño. Aunque tus manos no puedan entregarme este título, sé que tu alma

celebra conmigo, este logro es una flor que deposito en tu memoria, porque el amor es el único lazo que la muerte no puede romper.

AGRADECIMIENTO

A mi querida y anhelada universidad, Pontificia Universidad Católica del Ecuador, porque antes era un sueño, que el día de hoy se está convirtiendo en realidad. Gracias por abrirme las puertas y brindarme una de las mejores etapas de mi vida, uno de mis mejores aciertos fue escoger esta honorable institución para formarme académica y personalmente.

A mi tutoria de tesis, Mg. María Fernanda Zamora Castillo, que además de su excelencia profesional, destaca por su calidad humana. Gracias por brindarme parte de sus conocimientos académicos, por saber guiarme con paciencia y comprensión en todo este trayecto, y por recordarme que todos los sueños se pueden hacer realidad, quedo eternamente agradecida.

A Luis, mi papá, por sacrificar gran parte de su vida, para que yo pueda iniciar la mía, este proyecto de vida, no es mío, es nuestro, porque cada paso que he dado, fue gracias a tu esfuerzo y apoyo incondicional. Sin ti papá hubiera desfallecido. Gracias por desempeñar tan bien tu papel de padre, ahora es mi turno de hacerte sentir orgulloso de mi.

A mi familia, que siempre confió en mis capacidades, y me brindaron su apoyo incondicionalmente, ustedes fueron una pieza clave para culminar esta etapa de mi vida.

RESUMEN

La necesidad de esta investigación surge del requerimiento de aplicación de la ley de protección de datos por parte de las empresas privadas en el Ecuador, quienes deben resguardar los datos personales de todos los grupos de interés con los que se relacionan, tanto de ciberataques, filtraciones y el uso inadecuado de información sensible. La importancia del estudio de la blockchain en empresas privadas para proteger los datos personales, pretende garantizar la seguridad y confidencialidad de los datos, cumpliendo con lo establecido en la normativa vigente. En particular, se analiza el uso de la tecnología blockchain como un mecanismo innovador para proteger datos personales, gracias a sus características de inmutabilidad, descentralización y trazabilidad.

El objetivo general es analizar el uso de blockchain en empresas privadas para proteger los datos personales conforme la normativa vigente. Este estudio es relevante para las empresas que buscan mejorar sus prácticas de tratamiento de datos y evitar sanciones por incumplimiento de la ley de protección de datos. La metodología aplicada será de carácter cualitativo, con enfoque descriptivo y exploratorio, basada en la revisión de documentos legales, entrevistas a expertos jurídicos y en tecnología. Se espera identificar los beneficios, retos y limitaciones que implica la adopción de *blockchain* en este contexto, así como formular recomendaciones orientadas a su aplicación responsable y conforme a derecho. Los resultados permitirán a las empresas considerar nuevas estrategias para reforzar su cumplimiento normativo y generar mayor confianza en sus sistemas de gestión de datos.

Palabras clave: *blockchain*, datos personales, empresas privadas, LODPDP.(ley orgánica de protección de datos personales)

ABSTRACT

The necessity of this research arises from the requirement for private companies in Ecuador to implement the Data Protection Law. These entities must safeguard the personal data of all stakeholders from cyberattacks, leaks, and the improper use of sensitive information. The importance of studying blockchain technology within private companies to protect personal data lies in ensuring information security and confidentiality, in compliance with current regulations. Specifically, this study analyzes the use of blockchain technology as an innovative mechanism for personal data protection, leveraging its characteristics of immutability, decentralization, and traceability.

The general objective of this research is to analyze the use of blockchain in private companies for personal data protection in accordance with current legal frameworks. This study is relevant for companies seeking to improve their data processing practices and avoid sanctions resulting from non-compliance with the Data Protection Law. The methodology applied is qualitative, with a descriptive and exploratory approach, based on a review of legal documents and interviews with experts in the legal and technological fields. The aim is to identify the benefits, challenges, and limitations involved in adopting blockchain in this context, as well as to formulate recommendations oriented toward its responsible and legally compliant application. The results allow companies to consider new strategies to strengthen regulatory compliance and generate greater trust in their data management systems.

***Keywords**: blockchain, personal data, private companies, LODPDP (organic law on the protection of personal data).*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la era digital, tanto para las empresas privadas como para los usuarios de los servicios que estas ofrecen, una de las principales preocupaciones es la protección de datos personales. El crecimiento exponencial de la información digitalizada y la constante amenaza de vulneraciones a la privacidad han impulsado la búsqueda de soluciones tecnológicas innovadoras que garanticen la seguridad y el control sobre dicha información. En este contexto, la tecnología blockchain ha emergido como una herramienta disruptiva, capaz de transformar la gestión y protección de datos sensibles en el sector privado.

La *blockchain* es una herramienta digital que se asimila a un libro de cuentas, que por tratarse de tecnología se desarrolla a través de computadoras, ofrece ventajas significativas para el resguardo de datos personales, permitiendo a las empresas privadas no solo cumplir con las exigencias legales, sino también fortalecer la confianza de los usuarios y clientes en el manejo de su información, siendo imposible modificar o eliminar fácilmente los datos que ingresan. La adopción de esta tecnología puede reducir riesgos de manipulación, acceso no autorizado y pérdida de datos, al tiempo que facilita la trazabilidad y el control de los procesos de tratamiento de datos.

En los últimos años, el crecimiento la tecnología en el mundo ha sido un beneficio, pero a la vez una preocupación debido a que los datos de las personas se ven expuestos a cualquier tipo de riesgo malintencionado. Al ser un peligro de interés internacional, la tecnología blockchain se ha vuelto una solución para aquellas preocupaciones jurídicas, generando un interés doctrinario para poder fortalecer la seguridad, integridad y la lucidez en el trato de los datos personales. Finck (2018) concluye que la tecnología *blockchain* enfrenta un conflicto inherente. Aunque ofrece garantías de integridad y trazabilidad, su inmutabilidad choca con derechos fundamentales como la rectificación y el olvido. Por ende, se considera necesaria la implementación de ajustes regulatorios e interpretativos.

Como contribución complementaria, el estudio de Zyskind, Nathan y Pentland (2015) —"Decentralizing Privacy: Using Blockchain to Protect Personal Data" en IEEE Security and Privacy Workshops— proporciona una solución técnica que consiste en implementar la blockchain para que los usuarios puedan gobernar su información personal. Mediante una metodología aplicada con la validación técnica, se demostró que este modelo ofrece una gestión autónoma y acceso a los datos sin intervención de terceros. En su conclusión destaca que la tecnología blockchain, al elimina terceros, y transferir un control total a su titular, implementa el principio de autodeterminación informativa, y así genera un mecanismo de protección mejorado ante las vulnerabilidades de los modelos centralizados.

En la misma línea, Kshetri (2017) analiza en su artículo “Blockchain’s roles in meeting key supply chain management objectives" (International Journal of Information Management) cómo contribuye la tecnología blockchain para la seguridad de los datos personales en las cadenas de valor digitales. Mediante una metodología documental y teórica, que analiza casos prácticos, el autor menciona que la blockchain al ser descentralizada y transparente puede reducir los riesgos de accesos no autorizados, alteración de información y eliminación de la misma. No obstante, señala un problema importante: al ser una plataforma donde no es posible la irreversibilidad en el almacenamiento, no se respetan los principios jurídicos como la minimización, confidencialidad y supresión de datos.

Si bien las contribuciones analizadas han aportado de manera significativa a la disciplina jurídica sobre la Blockchain y la protección de datos, estas se limitan a ordenamientos específicos —europeo y estadounidense— y se enfocan en el derecho comparado o en un análisis más técnico. Esta investigación se enfoca en llenar un vacío jurídico existente en el Ecuador, analizando el uso de la Blockchain en empresas privadas como mecanismo de protección de datos bajo la Ley Orgánica de Protección de Datos Personales (2021). Así, se busca analizar las condiciones para su aplicación en conjunto con el marco jurídico local, evaluando los desafíos y la posibilidad que supone para garantizar los derechos de los titulares en el país.

En Ecuador, el tema de la Blockchain como herramienta para proteger los datos personales es emergente garantizando el derecho de las personas a decidir y controlar el uso de su información como parte de su derecho fundamental. Para cumplir estos mandatos establecidos en la normativa legal, la integración de esta herramienta tecnológica es una alternativa viable. Se establece como condición que su implementación debe realizarse en concordancia con el cumplimiento de principios como finalidad, proporcionalidad, minimización y confidencialidad, con el propósito de resguardar los datos que maneja.

Mediante un análisis crítico-normativo, Herrera, Requelme y Morales (2024), en su estudio Blockchain, privacidad y legislación ecuatoriana: una revisión crítica, plantean la necesidad de implementar una reforma legal o, a su vez, crear una guía técnica que indique los criterios que se deben considerar al momento de aplicar la Blockchain en conjunto con los principios fundamentales de la Ley Orgánica de Protección de Datos Personales. Esto se debe a que la ausencia de regulación sobre la herramienta Blockchain dificulta la asignación de responsabilidades dentro de un proceso de tratamiento y obstaculiza la tutela efectiva de los derechos de los titulares.

En la actualidad, muchos sectores productivos han sido cómplices de la transformación digital. La blockchain es una herramienta que funciona como tecnología base. Esta herramienta innovadora tiene como finalidad gestionar información de manera segura, transparente y confiable, de modo que las partes involucradas se sientan seguras con el uso, disponibilidad y resguardo de los datos que se manejan dentro del mismo. Esta base de datos demuestra que es útil para el manejo de información de manera descentralizada, inalterable y verificable de manera inmediata.

Estas peculiaridades hacen llamativa esta propuesta para los sectores empresariales privados, tomando en cuenta que, la Ley de Protección de Datos que entró en vigencia en el Ecuador en el año 2021 obliga a las empresas del sector privado a la protección de los datos personales y en caso de que se incumpla, tienen una sanción de hasta el 1% de la facturación de la empresa dependiendo de

la gravedad de la infracción, lo que obliga a las empresas el cumplimiento de la norma, so pena de sanción, por lo que, la implementación de esta herramienta ya no es solo una opción, sino una prioridad para aminorar conflictos legales y financieros.

Por otro lado, muchas de las empresas del sector privado no tienen prácticas adecuadas de manejo de datos, por ejemplo, aún archivan la información de manera física lo que puede estar expuesto a robos, reciclan hojas que contienen datos personales o se votan a la basura contratos o documentos con información personal sin ser previamente destruidos. Estas y más prácticas atentan de manera directa contra la protección de datos. En el Ecuador, el reconocimiento de la blockchain en el sistema legal es limitado, no existe una regulación jurídica integral o técnica para que se implemente la misma dentro del sector empresarial privado. La única norma que tenemos es el artículo 77 del Código del Comercio que anuncia brevemente sobre la blockchain aplicada a los actos de comercio, pero sin mayor detalle.

La inexistencia de esta normativa en la legislación ecuatoriana impide que las empresas tengan orientaciones concretas en cuanto al alcance de la blockchain, condicionamientos y limitaciones, para que se pueda implementar en sus actividades empresariales diarias, incidiendo en la eficiencia de la gestión empresarial tanto con proveedor, clientes, el Estado y demás grupos de interés con los que se relaciona. Este vacío afecta a varios principios legales que tienen relación con la protección de datos personales, como son la disponibilidad, la integridad y la confidencialidad de la información en los actos de comercio de la empresa. El no reconocimiento de la blockchain en la legislación ecuatoriana dificulta la protección de datos personales en empresas privadas.

Por ello, la presente investigación tuvo como objetivo general analizar el uso de blockchain en empresas privadas para proteger los datos personales conforme la normativa vigente, planteando las siguientes tareas investigativas, como son: Fundamentar teórica y jurídicamente el uso de blockchain en empresas privadas para proteger los datos personales conforme la normativa vigente, Caracterizar el

uso de blockchain en empresas privadas para proteger los datos personales conforme la normativa vigente y determinar los parámetros para el uso de blockchain en empresas privadas para proteger los datos personales conforme la normativa vigente.

Se plantea la idea a defender: Es necesario implementar el uso de blockchain en empresas privadas para proteger los datos personales conforme la normativa vigente. Para la ejecución del presente estudio, se aplicó una investigación de enfoque cualitativo de alcance descriptivo y exploratorio, aplicó métodos analítico sintético y exegético, basado en revisión de doctrinas, entrevistas a expertos jurídicos y en tecnología. Se espera identificar los beneficios, retos y limitaciones que implica la adopción de blockchain, determinar los parámetros orientadas a su uso y su aplicación responsable conforme a derecho. Los resultados permitirán a las empresas considerar nuevas estrategias para reforzar su cumplimiento normativo y generar confianza en sus sistemas de gestión y protección de datos.

La relevancia de esta investigación radica en su contribución al articular el desarrollo tecnológico con la protección de derechos fundamentales, particularmente el derecho constitucional a la protección de datos personales en Ecuador. La implementación de la Blockchain en el tratamiento de información podría constituir una solución prometedora para mejorar la seguridad, trazabilidad y control de los datos. Sin embargo, simultáneamente plantea desafíos que deben resolverse conforme al marco jurídico existente. El principal aporte de este estudio consistirá en definir los parámetros técnico-jurídicos que faciliten a las empresas privadas la adopción de la Blockchain en cumplimiento de las disposiciones legales sobre protección de datos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Fundamentos jurídicos y técnicos de la *Blockchain*

La blockchain es un libro digital, distribuido y descentralizado que permite el registro seguro e inmutable de transacciones o cualquier tipo de datos es la idea básica detrás de la tecnología blockchain (Tapscott y Tapscott, 2016). Tres ideas fundamentales constituyen la base de su diseño. En primer lugar, dado que cada participante de la red tiene una copia idéntica del libro mayor, la descentralización elimina la necesidad de una autoridad central fiable. La segunda es la inmutabilidad, que se consigue cuando los datos de un bloque se sellan criptográficamente y se conectan al bloque anterior, lo que impide cualquier alteración o eliminación posterior (Nakamoto, 2008). Esto es esencial para la integridad y la trazabilidad de los datos. Por último, la cadena de confianza se crea mediante criptografía, lo que garantiza que todos los bloques estén conectados cronológicamente (Buterin, 2014).

Los fundamentos de la cadena de bloques son anteriores a las criptomonedas, a pesar de que suelen asociarse con ellas. Los investigadores Stuart Haber y W. Scott Stornetta propusieron por primera vez el concepto de un sistema de bloques cronológicos en 1991 (Tapscott y Tapscott, 2016). Su investigación se centró en una forma segura de marcar la fecha y hora de los documentos digitales para que la información no pudiera modificarse. Sin embargo, el libro blanco de Satoshi Nakamoto, «Bitcoin: un sistema de efectivo electrónico peer-to-peer», publicado en 2008, marcó la materialización y la utilidad de la tecnología. Al resolver el problema del «doble gasto» sin recurrir a intermediarios financieros, Nakamoto demostró que un libro mayor descentralizado podía funcionar y creó la primera cadena de bloques transaccional (Blockchain 1.0).

Desde un registro de valores básico hasta una plataforma programable, la tecnología avanzó rápidamente. Blockchain 2.0 es el nombre que se le da a este salto evolutivo, que hace hincapié en la lógica codificada y las aplicaciones. Esta fase fue impulsada por Vitalik Buterin (2014), quien desarrolló Ethereum, una

plataforma que permitió crear aplicaciones descentralizadas y, lo que es más importante, utilizar contratos inteligentes. Los contratos inteligentes empujan a la profesión jurídica a reevaluar conceptos como el consentimiento y la validez contractual mediante la codificación de normas y acuerdos que se ejecutan automáticamente en la cadena (Filippi y Wright, 2018). Esto es esencial para el discurso jurídico. Actualmente, la tecnología avanza hacia una etapa 3.0, en la que su uso en la gobernanza y la gestión de la identidad digital, la escalabilidad y la integración de muchas cadenas y datos (Tapscott & Tapscott, 2016), un campo importante para la protección de datos personales.

Entonces la blockchain es una herramienta digital compuesta por bloques sellados con un hash criptográfico que sirve como su huella digital distintiva e irrepetible, proporcionando una forma única para identificar a cada bloque contenedores de datos o un lote de transacciones verificadas (Buterin, 2014). El hash proporciona una forma única de identificar el contenido de un bloque en un momento específico, mientras cada nuevo bloque también contiene el hash del bloque anterior, formando la cadena que da nombre a la tecnología y garantizando su inmutabilidad. Un bloque dejaría de ser válido y la cadena se rompería si se modificara un solo bit de datos dentro de él, esto daría lugar a un hash completamente diferente (Tapscott y Tapscott, 2016).

Los servidores o PC que componen la red distribuida de cadenas de bloques se conocen como nodos (Tapscott y Tapscott, 2016). El sistema está descentralizado, cada nodo mantiene una copia completa del libro mayor de la cadena, mediante el uso de técnicas de consenso, los datos almacenados en estos nodos se mantienen intactos. Antes de añadir nuevos bloques a la cadena, los nodos emplean estos mecanismos de reglas y procesos para acordar la legitimidad de las transacciones y la secuencia de los nuevos bloques (De Filippi y Wright, 2018). Así, la disposición secuencial y lineal de bloques conectados se denomina cadena. La marca de tiempo criptográfica, indica el minuto exacto en que se creó y añadió el bloque, es el componente que organiza estos bloques (Buterin, 2014).

La trazabilidad de los eventos y la defensa contra la manipulación de los registros cronológicos están garantizadas por esta secuencialidad y la marca de tiempo, de esta manera, permite documentar con precisión el momento exacto del consentimiento o la alteración, esta prueba temporal es especialmente pertinente en contextos jurídicos, como la protección de datos (Ibáñez Jiménez, 2018). En cambio, los tokens son activos digitales que pueden representar dinero, acciones o, en el contexto de esta tesis, una identidad digital o acceso a datos, aunque no formen parte directamente de la estructura física del registro (Ibáñez Jiménez, 2018), los cuales pueden ser usados y aplicados por las empresas privadas al momento de estructurar su Blockchain.

Cabe mencionar que el principio fundamental de la blockchain es la descentralización (Nakamoto, 2008). Gracias a esta característica, la red funciona sin necesidad de un único servidor, autoridad o intermediario para gestionar los datos o verificar las transacciones por medio de una red de numerosos nodos, u ordenadores, que distribuyen y replican el registro de datos, eliminando los puntos únicos de fallo y la dependencia de un tercero fiable, lo que garantiza que ninguna entidad pueda filtrar o manipular los datos.

La capacidad de todos los usuarios de la red para ver y confirmar las transacciones registradas se conoce como transparencia en la blockchain. Todos los nodos pueden ver el historial completo de transacciones, incluso si se ocultan las identidades reales de los usuarios (seudonimia) (Tapscott y Tapscott, 2016). Esta característica aumenta la confianza en los procesos al permitir una auditoría transparente y verificable del acceso y el manejo de los datos por parte de los administradores en el contexto de las empresas y la seguridad de la información. Mientras que, la transparencia y la inmutabilidad conducen directamente a la trazabilidad. El origen, el movimiento y el historial completo de cualquier activo digital o dato pueden rastrearse a lo largo de toda la cadena, cada bloque está marcado con la fecha y la hora y conectado al anterior (Tapscott y Tapscott, 2016), lo que permite a las empresas determinar con precisión quién tuvo acceso a los datos y cuándo.

La característica general que incluye las cualidades mencionadas anteriormente es la seguridad. Blockchain ofrece una alta seguridad criptográfica contra el fraude y la manipulación (Nakamoto, 2008). Debido a su arquitectura distribuida, el sistema es naturalmente inmune a los ataques, sería computacionalmente imposible en un atacante cambiar algún registro sin cambiar también los datos en la mayoría de los nodos de la red. Como resultado, el consenso y la criptografía de la red, en lugar de una autoridad centralizada, protegen la confidencialidad y la integridad de los datos.

Según Tapscott y Tapscott (2016), la tecnología blockchain no se limita a un único modelo, sino que se divide en varias categorías que difieren principalmente en su grado de acceso y derechos. Para las empresas, la selección del tipo es esencial, debido a que afecta a la seguridad, la velocidad y el cumplimiento de marcos legales como la Ley Orgánica de Protección de Datos Personales (LOPDP) y su requerimiento de protección de los datos especialmente los que se consideran sensibles.

Para entender la blockchain tenemos que entender tres elementos claves: tecnología de libro mayor distribuido, registros inalterables, contratos inteligentes. El primero elemento al que tiene acceso todos los miembros es el libro mayor y el registro de transacciones que es inmutable, las transacciones son registradas una única vez. El segundo elemento se basa en que ningún participante que ya ha sido registrado en el libro mayor compartido, puede cambiar o falsificar una transacción. Y por último el tercer elemento, este contrato inteligente existe con la finalidad de que exista una rapidez en las transacciones (IBM, 2020).

El funcionamiento esta esta herramienta inicia con una transacción, lo que sería un bloque de datos, el cual muestra los movimientos de un activo tangible o intangible. Cada uno de estos bloques se conecta con el previo y con el posterior, y así forman una cadena de datos, mostrando los movimientos en tiempo real, y se ensamblan de modo que no se puede modificar o aumentar un bloque en medio de dos ya existentes. Estos bloques que se aumentan y se enlazan entre si, forman una cadena que es irreversible, y eso da como consecuencia el blockchain, dando como

ventaja la inalterabilidad, evitando manipulaciones o modificaciones exteriores, creando así un libro mayor, en el cual todos los miembros pueden confiar (Yaga et al.,2018).

La tecnología del blockchain se da en diferentes modelos, estos varían por el nivel de acceso y los permisos, elegir un modelo es crucial para una empresa, esto regirá la seguridad, y la compatibilidad con los marcos que regula la Ley, los modelos son: público, privado, de consorcio e hibrido (Gaynor et al., 2020).

La blockchain pública, es aquella que no necesita tener autorización para su uso, está abierta al público y todos pueden aumentar una cadena de bloques, como por ejemplo el Bitcoin y Ethereum, son criptomonedas y son de códigos abiertos, todos pueden usarlas (Gandhi, 2021)

La blockchain privada es una cadena de bloques que solo una organización y sus miembros permitidos pueden tener acceso, estas cadenas están centralizadas, por aquello pueden tomar decisiones más rápido porque procesan varias transacciones por segundo. Este tipo de blockchain es la más conveniente para organizaciones, que necesiten interceptar transacciones o registros privados, fuera del alcance del público (Werbach, 2018).

La blockchain federada o también conocida como blockchain de consorcio, es una cadena de bloques autorizada, lo que significa que, diversas organizaciones que quieran tener una colaboración pueden tener acceso a esta cadena de bloques (Wegryzn & Wang, 2021). Por último, tenemos la blockchain hibrida, esta cadena de bloques es accesible para todos los usuarios como una blockchain publica y de igual manera pueden acceder y manipular los datos, pero, esta combinada con entidades privadas, algunas aplicaciones no son expuestas para cualquier usuario, de esta manera describimos una blockchain publica donde la participación es restringida y controlada por un privado (Shirmali & Patel, 2021).

En conclusión, la blockchain no es solo una base de datos, es un modelo de confianza digital que se basa en una estructura inquebrantable, que además de

resolver un problema histórico que es la intermediación obligada, nos brinda transparencia sin precedentes. El desarrollo de esta herramienta tecnológica desde su idea fundamental hasta los contratos inteligentes y sus diferentes métodos de implementación, pone de manifiesto su adaptabilidad y potencial revolucionario, lo que sienta bases para una importante reorganización de la gestión de datos, convirtiéndose en un instrumento esencial para garantizar integridad y el cumplimiento normativo, de la mano con los avances digitales.

1.2. Principios y derechos Consagrados en Tratados y Declaraciones Internacionales sobre el derecho de protección de datos personales

La protección de datos ya se reconocía como un derecho humano antes de la entrada en vigor del Ley y el RGPD en varios instrumentos supranacionales: El primer tratado internacional jurídicamente vinculante y de aplicación mundial sobre este tema es el Convenio 108 del Consejo de Europa (1981) (Ibáñez Jiménez, 2018), que estableció los principios esenciales para la protección de las personas en lo que respecta al tratamiento automatizado de datos personales, fue el primer instrumento internacional jurídicamente vinculante. Este convenio creó un marco para el flujo internacional de información al establecer los conceptos fundamentales de seguridad, calidad de los datos, finalidad específica y equidad.

La Declaración Universal de Derechos Humanos de 1948 y el Pacto Internacional de Derechos Civiles y Políticos de 1966 defienden el derecho a la intimidad y la prohibición de la injerencia arbitraria en la vida privada de las personas (García, 2007). El posterior reconocimiento por parte de la Unión Europea de la protección de datos como derecho fundamental fue posible gracias a las bases establecidas por este Convenio. En el contexto latinoamericano (Habeas Data): El Habeas Data, un mecanismo procesal que permite a los ciudadanos acceder y corregir la información almacenada en bases de datos públicas o privadas, fue la primera forma en que se expresó este reconocimiento en América Latina.

Sin embargo, con el desarrollo del procesamiento masivo de datos y la tecnología de la información en las décadas de 1960 y 1970, este derecho cambió. A la luz de

las bases de datos automatizadas, la protección de datos ha pasado de limitarse a proteger la privacidad a centrarse en la propiedad de los datos por parte del individuo. Según Hassemer (citado en Pérez-Luño, 2017), este cambio se concibió como el derecho a la autodeterminación informativa, que sostiene que el control de los datos personales es una extensión de la autonomía y la dignidad del individuo y evita que este se vea reducido a un perfil de datos.

En la era digital, el derecho a la protección de datos se considera una garantía necesaria de privacidad de la información, cualquier actividad de tratamiento de datos debe ajustarse a un conjunto de principios obligatorios establecidos por la LOPDP, así la legalidad del tratamiento y el cumplimiento de las obligaciones legales por parte de los interesados se establecen mediante los criterios de:

a) Equidad, legalidad y transparencia, así el tratamiento debe ser transparente, moral y lícito. Siempre se debe revelar al interesado quién trata sus datos y por qué.
b) Finalidad: Recopilar los datos con fines específicos, explícitos y legítimos, y no pueden utilizarse posteriormente para fines incompatibles (Asamblea Nacional del Ecuador, 2021).
c) Pertinencia y cantidad mínima (minimización): El tratamiento solo debe realizarse con los datos que sean absolutamente necesarios y pertinentes para el objetivo declarado. Retención: La información solo puede conservarse durante el tiempo estrictamente necesario para alcanzar el objetivo para el que fue recopilada. El derecho al borrado o derecho al olvido, que es el ámbito más controvertido con tecnologías como el blockchain, se ve directamente afectado por este principio (Ibáñez Jiménez, 2018). Seguridad: exige que se establezcan las garantías organizativas, técnicas y jurídicas adecuadas para garantizar la privacidad, la disponibilidad y la integridad de los datos. Este requisito previo es esencial para evaluar la fiabilidad de los sistemas tecnológicos.
d) Responsabilidad proactiva (rendición de cuentas): La LOPDP estipula que los responsables del tratamiento de datos deben poder demostrar que cumplen con la ley, al igual que el RGPD. La implementación de políticas

> internas, las evaluaciones de impacto y los registros de actividades de tratamiento forman parte de ello (Piñar Mañas, 2017).

Reconociendo indirectamente la necesidad de controlar la información personal antes de la regulación sustantiva de la protección de datos, la jurisprudencia y la teoría de autores como Óscar Puccinelli (1999) impulsaron la consagración de este recurso en las constituciones de países como Argentina, Colombia y Perú. Ecuador contribuyó de manera significativa al reconocimiento jurídico de esta prerrogativa al seguir la tendencia mundial de constitucionalizar este derecho. Promulgación en 2008: El artículo 66, párrafo 19, de la Constitución de la República de 2008 garantizaba expresamente el derecho a la protección de datos.

El acceso y el control de este tipo de información y datos se incluyen específicamente en el derecho a la protección de los datos personales, que es reconocido y garantizado por este artículo (Asamblea Nacional del Ecuador, 2008). Esta definición constitucional es extremadamente importante, esta equipara la protección de datos con otros derechos fundamentales. También sirvió de base directa para la futura Ley Orgánica de Protección de Datos Personales (LOPDP) de 2021. Por lo tanto, la Constitución ecuatoriana establece la base jurídica para la autonomía informativa del interesado sobre su ámbito personal en el mundo digital.

La LOPDP creó la Superintendencia de Protección de Datos Personales como una organización técnica, independiente y especializada para supervisar el cumplimiento de las normas y llevar a cabo tareas de inspección y sanción, entre sus funciones principales se encuentran la realización de investigaciones, la aplicación de sanciones legales por incumplimiento, la garantía del ejercicio adecuado de los derechos de los interesados (ARCOP) y el establecimiento de normas e interpretaciones reglamentarias sobre el tratamiento de datos, basado en el principio de responsabilidad y control estatal sobre la privacidad de la información, que se garantiza con la creación de este organismo.

De acuerdo con la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, todas las entidades deben adherirse a los principios de protección de

datos personales, que constituyen la base de la legalidad de cualquier tratamiento (Asamblea Nacional de Ecuador, 2021). Estas directrices, se derivan del modelo europeo (Piñar Mañas, 2017), garantizan que el tratamiento sea equitativo, abierto y respetuoso con el derecho del interesado a la autonomía informativa. Precisamente, el principal medio por el que las personas pueden ejercer su derecho a la autodeterminación informativa es a través de la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, que consagra los derechos ARCOP (Asamblea Nacional de Ecuador, 2021). No obstante, estos derechos que otorgan a los interesados la capacidad de mantener el control sobre sus datos (De Filippi y Wright, 2018), son el motivo principal de controversia con estructuras inmutables como la cadena de bloques.

Los derechos fundamentales que garantizan al interesado poder comunicarse directamente con los responsables de datos son:

a) Derecho de acceso: permite al interesado solicitar una copia de sus datos personales y confirmar con el responsable del tratamiento si estos están siendo tratados o no. Este derecho garantiza la transparencia del tratamiento.
b) Derecho de rectificación: otorga al interesado el derecho a solicitar que sus datos personales se actualicen o corrijan si son erróneos, incompletos o se tratan de forma que no se ajusta a las normas legales de exactitud y calidad.
c) El derecho de supresión: A menudo conocido como derecho al olvido, es la facultad de solicitar la eliminación permanente de datos personales cuando ya no son necesarios para los motivos de su recopilación, el interesado retira su consentimiento o el tratamiento de los datos es ilícito. Este privilegio contradice directamente la premisa de inmutabilidad de una blockchain pública (Ibáñez Jiménez, 2018).
d) El derecho de oposición: Salvo que se demuestre un interés superior o que el tratamiento sea necesario para el establecimiento o la defensa de reclamaciones legales, esto otorga al interesado el derecho a oponerse o rechazar el tratamiento de sus datos personales cuando este se base en un

interés legítimo del responsable del tratamiento. También se incluye el derecho a oponerse a ser objeto de marketing directo.

e) El derecho a la portabilidad de datos: Permite a los titulares de los datos transferirlos a otro responsable del tratamiento sin ningún obstáculo en un formato estructurado, de uso común y legible por máquina (Asamblea Nacional del Ecuador, 2021). Promover la libre competencia y la transferencia de datos personales entre servicios digitales son los objetivos de este derecho.
f) Derecho a la autodeterminación informativa: Una fuga de información es el principal peligro para la seguridad y la confidencialidad, se producen cuando se accede, se roba o se divulga ilícitamente información personal sensible, financiera o identificable, ya sea como resultado de ataques maliciosos, errores humanos o fallos técnicos (Ibáñez Jiménez, 2018).

En conclusión, la protección de datos se ha convertido en un derecho humano fundamental a nivel nacional en Ecuador, basado en principios como legalidad, transparencia y responsabilidad proactiva que busca empoderar al titular con los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales (ARCOP) y garantizar su independencia informativa, estos principios tienen como objetivo cumplir con la ley, y respetar la voluntad de los titulares de los datos, su consentimiento, hasta su portación. En resumen, son garantía de que la toma de decisiones sobre la información es únicamente responsabilidad del ciudadano y de la entidad que la trata. (que es para que nos sirven, como funcionan) El conflicto interno entre estos derechos (derecho de supresión) y la inmutabilidad que es una característica de la blockchain, pone a la LOPDP como una herramienta crucial para establecer lineamientos para la adaptación de la tecnología con esta implementación de control de datos.

1.3. Blockchain como herramienta de protección de datos

Las empresas privadas son los principales responsables y encargados del tratamiento de datos personales, éstas desempeñan un papel crucial en la protección de datos en cumplimiento de los estrictos requisitos legislativos en

Ecuador, de esta manera, Según Ibáñez Jiménez (2018), las empresas deben garantizar que el consentimiento para el tratamiento sea siempre libre, explícito, informado e inequívoco, y que pueda revocarse con la misma facilidad con la que se otorgó, garantizando que los titulares de datos puedan ejercer sus derechos de acceso, rectificación, supresión (olvido), oposición y portabilidad, so pena de la aplicación de sanciones por la violación u obstrucción de estos derechos.

La implementación de la blockchain garantizaría el cumplimiento del principio de seguridad y confidencialidad al ser una medida de seguridad organizativa y técnica adecuada para protegerse contra el acceso no autorizado, la alteración o la pérdida de datos. También facilita a la empresa cumplir con la presentación de la responsabilidad proactiva al mantener en el sistema un registro de las actividades de tratamiento (RAT) y realizar Evaluaciones de Impacto de la Protección de Datos (EIPD) en proyectos de alto riesgo, información que será de acceso del Delegado de Protección de Datos (DPD) (Piñar Mañas, 2017).

La protección de datos se ha convertido en una consideración de ética empresarial y valor reputacional, además de ser un requerimiento legal, siendo este un factor diferenciador para las empresas en el mercado digital; sin embargo, las infracciones de la privacidad dañan gravemente la reputación, la clientela y generan un riesgo financiero directo a la empresa al tener que cancelar fuertes multas por incumplimiento de la LOPDP.

La protección de la información personal es un derecho fundamental a la autodeterminación informativa, no solo un derecho a la privacidad o la confidencialidad (Pérez-Luño, 2017). Esta distinción es importante, porque la ley se centra en otorgar a los interesados el poder de seleccionar cómo se procesa y utiliza su información, y adónde va, incluso después de que haya sido divulgada (Hassemer, citado en Pérez-Luño, 2017). Obliga a las personas encargadas del tratamiento a adherirse a los valores de lealtad, finalidad y transparencia, las leyes modernas, como la implementada en Ecuador (LOPDP), pretenden garantizar que este control no sea solo formal, sino realmente efectivo (Piñar Mañas, 2017). Como resultado, la idea incluye la recopilación de directrices y protecciones legales

destinadas a proteger la seguridad, la integridad y la calidad de los datos personales frente a los riesgos asociados al tratamiento automatizado y a la economía digital.

La LOPDP clasifica a los datos en función del grado de peligro para los derechos y libertades del interesado. Para prevenir abusos contra los derechos humanos, es fundamental considerar esta clasificación de datos al implementar la tecnología blockchain. Dado que la principal característica de esta tecnología es que los datos no se pueden eliminar ni alterar, la información personal no debe almacenarse directamente en ella (Nakamoto, 2008). En consecuencia, se registra una huella digital o un código cifrado en lugar de los datos reales, lo que ayuda a confirmar su autenticidad sin revelarlos (Tapscott & Tapscott, 2016).

Los datos más sensibles, como la información genética, biométrica o de salud, deben almacenarse fuera de la blockchain en sistemas seguros; la cadena solo se utiliza para registrar quién accedió a ella, qué se modificó y cuándo (De Filippi & Wright, 2018), y así puede mitigar el fraude y el acceso ilícito a los datos, siempre que solo se documente la información esencial. Según Piñar Mañas (2017), esta clasificación establece la base jurídica para su tratamiento, así como las necesidades de seguridad. La información de identificación común es aquella que permite la identificación directa de una persona sin necesidad de investigación adicional, incluye el nombre completo, el número de identificación, la dirección postal, el número de teléfono y la dirección de correo electrónico, se clasifica así:

a) Datos de categoría especial (sensibles): esta categoría comprende los datos cuyo tratamiento o divulgación incorrectos pueden causar graves daños o discriminación al interesado. Se incluye la información sobre la orientación sexual, las ideas religiosas o filosóficas, la afiliación sindical, el origen étnico y la salud (historial médico, enfermedades) (Asamblea Nacional del Ecuador, 2021). Su tratamiento está muy regulado y, por lo general, requiere un acuerdo adicional y explícito, además de medidas de seguridad reforzadas.
b) Datos biométricos y genéticos: Estos representan un subconjunto de datos sensibles debido a su naturaleza única e inalterable. Los datos biométricos

(como las huellas dactilares, el reconocimiento facial o del iris) son datos que, mediante un tratamiento técnico específico, permiten la identificación única de una persona. Los datos genéticos son la información hereditaria de un individuo. El control de estos datos es crucial, su violación o uso indebido podría tener efectos duraderos y difíciles de reparar, lo que requiere un estudio de riesgos muy exhaustivo (Ibáñez Jiménez, 2018).

c) Datos financieros y patrimoniales: incluyen detalles sobre las cuentas bancarias, los ingresos, las deudas, los activos y el historial crediticio del propietario. Aunque pueden ser habituales en el ámbito de los servicios económicos, su tratamiento está regulado por normativas específicas, además de la LOPDP, debido al alto riesgo de fraude y al impacto económico que conlleva su filtración. La dignidad humana y el derecho a la privacidad, que en un principio se centraban en el derecho a «estar solo», están estrechamente relacionados con las raíces conceptuales de la protección de datos (Warren y Brandeis, citados en García, 2007).

La inmutabilidad de blockchain la hace incompatible con el derecho de supresión; sin embargo, en un diseño híbrido, puede ser una herramienta de cumplimiento útil para las empresas debido a la garantía de integridad y trazabilidad, por cuanto al garantizar que los datos no se han modificado desde su registro inicial, la tecnología blockchain es ideal para cumplir con los principios de precisión y seguridad (Ibáñez Jiménez, 2018). Las auditorías internas y el cumplimiento del concepto de rendición de cuentas proactiva se facilitan gracias a la trazabilidad inmutable, así el modelo híbrido (fuera de la cadena) es la mejor alternativa para que las empresas privadas o de consorcio registren los hashes criptográficos de los datos personales.

Los datos reales se conservan fuera de la cadena en sistemas externos que permiten su eliminación física, y aquí aplicamos lo que conocemos como el derecho a la supresión, que es una garantía, porque el hash en la cadena deja de funcionar cuando se eliminan los datos (De Filippi y Wright, 2018). Mediante la tecnología blockchain, se puede crear un registro inalterable de las fechas y circunstancias en las que el interesado dio o retiró su consentimiento. Esto facilita la demostración de la legalidad y la transparencia del tratamiento ante la Autoridad de Control.

La Ley Orgánica de Protección de Datos Personales (LOPDP) de 2021 impone estrictos requisitos regulatorios a las empresas privadas que operan como responsables o encargados del tratamiento de datos en Ecuador, garantizando el respeto a los derechos y principios de los titulares de los datos. Estas responsabilidades respaldan el principio de rendición de cuentas proactiva que exige la normativa, por lo que la blockchain deberá contener como parámetros mínimos la información, como, por ejemplo, quien accedió a los datos, que fecha tuvo acceso, cuál fue su motivo de ingreso, y tener una evidencia de que se le otorgo el consentimiento.

La protección de datos se eleva al rango de derecho fundamental a la autodeterminación informativa en virtud de la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador. Las empresas privadas desempeñan un papel clave en este contexto y están obligadas a adoptar medidas proactivas para garantizar la seguridad de la información y los derechos de acceso, rectificación, supresión y oposición (ARCOP). Si bien existe un conflicto entre la inmutabilidad de la tecnología blockchain y el derecho de supresión, el uso de modelos híbridos demuestra que el avance tecnológico y la ley pueden coexistir. El respeto a esta ley va más allá del mero cumplimiento o la evasión de sanciones; se ha convertido en un pilar de la ética empresarial y un elemento distintivo de la confianza digital, esencial en el mercado actual.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología de la investigación

La implementación de la tecnología blockchain en empresas privadas con el objetivo de fortalecer la protección de datos personales de acuerdo con la normativa ecuatoriana es un fenómeno jurídico y tecnológico complejo que esta investigación intenta comprender en profundidad mediante un enfoque cualitativo. Según Hernández Sampieri, Fernández y Baptista (2020), la investigación cualitativa permite examinar aspectos estructurales y prácticos que no se prestan a la medición estadística y que requieren interpretación, reflexión contextual y análisis de los discursos técnicos y normativos.

Este método fue el adecuado, debido a que el estudio aborda la aplicación de las responsabilidades corporativas descritas en la Ley Orgánica de Protección de Datos Personales (LOPDP), los principios constitucionales y los aspectos tecnológicos de la arquitectura blockchain. Las empresas privadas, los responsables del tratamiento de datos, los expertos en ciberseguridad y los interesados son algunos de los actores que interactúan con estos componentes en un marco social y jurídico. Por lo tanto, es necesario realizar un análisis interpretativo y contextualizado para comprender cómo se interpreta y se utiliza la protección de datos en situaciones prácticas (Creswell, 2013).

Desde un punto de vista interpretativo, la realidad jurídica es un proceso dinámico que adquiere significado a través de las prácticas empresariales, las normas de cumplimiento y la relación entre el derecho y la tecnología, más que una colección estática de normas. Según Schütz (citado en Creswell, 2013), las nociones jurídicas se producen socialmente y están indisolublemente ligadas a las experiencias de quienes las utilizan. Dado que el tratamiento de datos personales es una práctica que abarca los sistemas empresariales digitales y se ve inmediatamente afectada por las decisiones técnicas relativas al almacenamiento, la trazabilidad y el acceso a la información, este concepto cobra una importancia crucial para la cuestión que se examina.

El punto de vista de Morin (2006) destaca la necesidad de analizar fenómenos que integran dimensiones tecnológicas, legales, éticas y organizativas. La adopción de blockchain no solo responde a fines operativos, sino también a la búsqueda de confianza, eficiencia, seguridad jurídica y cumplimiento normativo. Estos elementos se influyen entre sí y requieren una comprensión sistémica. Por eso, su implementación implica evaluar cómo afecta al tratamiento de datos, la gobernanza y la responsabilidad de los actores, considerando además riesgos como la transparencia, la inmutabilidad y el impacto en los derechos de los titulares. En consecuencia, la blockchain debe entenderse como un sistema transformador dentro de las organizaciones, y no solo como una herramienta técnica.

En la misma línea, la integración de la cadena de bloques incorpora conceptos criptográficos, modelos de gobernanza digital, topologías de red, contratos inteligentes y opciones de diseño que tienen un impacto directo en la viabilidad de la trazabilidad del consentimiento, la responsabilidad proactiva y el derecho de supresión. Como resultado, el método cualitativo nos permite examinar cómo los responsables del tratamiento de datos comprenden sus responsabilidades legales y cómo toman decisiones que podrían ayudar o impedir el cumplimiento de la protección de datos.

Podemos determinar los principales conflictos que se producen al utilizar la tecnología blockchain para la protección de datos mediante un estudio cualitativo. Entre ellos se encuentran los conflictos entre la inmutabilidad de los registros y derechos como la autodeterminación y el borrado de la información, también los retos que se enfrentan los responsables del tratamiento de datos a la hora de cumplir con su deber proactivo. La naturaleza permanente y descentralizada de la cadena de bloques puede dificultar la restricción del uso y la conservación de los datos, lo que plantea retos para los conceptos de reducción y finalidad. En conjunto, estos componentes demuestran lo difícil que es armonizar esta tecnología con las normativas vigentes en materia de protección de datos.

Para entender estos conflictos es necesario realizar un estudio interpretativo y analítico que investigue sus causas y examine posibles soluciones, incluidos los

modelos híbridos fuera de cadena. Estos conflictos no son solo teóricos, sino que también se manifiestan en la práctica y en la dinámica organizativa. A fin de coordinar adecuadamente la tecnología blockchain con los requisitos de protección de datos personales en el contexto empresarial ecuatoriano, es necesario adoptar un enfoque cualitativo que permita captar la complejidad, la profundidad y la coherencia interna del fenómeno.

El alcance de la presente investigación fue de tipo descriptivo, (puesto que se oriente a describir, definir, analizar, el uso de la blockchain en empresas privadas como mecanismo para proteger los datos personales conforme a la normativa vigente. De este modo permitió describir los aspectos técnicos y jurídicos del tratamiento de datos personales, así como los procedimientos utilizados por las empresas para cumplir con los principios de seguridad, confidencialidad, transparencia y responsabilidad proactiva establecidos en la Ley Orgánica de Protección de Datos Personales.

Al centrarse en la búsqueda de componentes pertinentes y en la comprensión de su funcionamiento en el contexto empresarial, la investigación descriptiva permitió presentar de forma sistemática el fenómeno objeto de estudio sin intentar establecer vínculos causales. Como resultado, el estudio se centró en examinar las estrategias organizativas y tecnológicas empleadas por las empresas privadas para cumplir los requisitos normativos en materia de protección de datos personales.

En respecto a las modalidades de investigación, se empleó la modalidad bibliográfica documental, este estudio se basó en revisar y analizar fuentes normativas, doctrinarias y científicas que tengan relación con la protección de datos personales y la herramienta tecnológica blockchain. Esta modalidad permitió analizar leyes, reglamentos, libros, artículos, opiniones de especialistas, los cuales sustentaron el marco teórico y jurídico de la investigación. El análisis documental permitió una mejor comprensión del marco normativo y de aportes jurídicos que expusieron sobre la concordancia y los retos de la implementación de la blockchain en el tratamiento de datos personales (Creswell, 2013).

En la misma línea, se llevó a cabo una investigación de campo, los datos se recopilaron directamente a través de entrevistas semiestructuradas con expertos en el ámbito de la protección de datos personales y la implementación de soluciones técnicas basadas en blockchain en empresas privadas. Gracias a este enfoque, pudimos recopilar datos empíricos a partir de las experiencias de los actores, lo que complementó el estudio teórico con información real sobre cómo se aplicaban en la práctica las normas y las medidas de seguridad. Al yuxtaponer la teoría con la realidad empresarial, la investigación de campo ofreció una perspectiva contextualizada del fenómeno, lo que mejoró la validez y la profundidad del estudio (Rubin y Rubin, 2012).

2.2. Métodos y técnicas de investigación

Se emplea una metodología analítico-sintética. El primer paso consiste en analizar los aspectos organizativos, técnicos y jurídicos del uso de la tecnología blockchain para procesar datos personales. En este análisis se examinan las normas constitucionales, los principios de la LOPDP, las directrices de protección de datos, la criptografía blockchain, los modelos de red y las técnicas de almacenamiento. A continuación, se combinan estos elementos para comprender cómo funcionan juntos en un único marco tecnológico-jurídico. Este procedimiento permite identificar los riesgos, las limitaciones y las posibles soluciones relevantes para el entorno empresarial en Ecuador.

Tras la identificación de los componentes, la etapa sintética permite su integración en un marco cohesionado destinado a demostrar cómo la tecnología blockchain puede utilizarse como herramienta para reforzar la protección de los datos personales sin violar derechos fundamentales como la supresión o la modificación (De Filippi y Wright, 2018). Esto genera un conocimiento profundo que permite la creación de propuestas comerciales y normas para el cumplimiento normativo. Además, esta conexión facilita la evaluación de la viabilidad de los modelos organizativos y técnicos que hacen que la innovación cumpla con los requisitos legales existentes. En consecuencia, se interpretan los siguientes aspectos utilizando el método hermenéutico jurídico:

- La Constitución de 2008, art. 66 numeral 19
- La Ley Orgánica de Protección de Datos Personales (2021)
- El Reglamento General de Protección de Datos (RGPD europeo) como modelo comparativo
- Jurisprudencia y doctrina especializada

Gracias a la hermenéutica, podemos comprender el significado y el alcance de los derechos ARCOP, el consentimiento, la seguridad digital, el principio de responsabilidad proactiva y las ramificaciones legales de la implementación de nuevas tecnologías de procesamiento de datos. Este método permite una comprensión más profunda y contextualizada de las consecuencias prácticas de la normativa, lo que garantiza un análisis académico exhaustivo que va más allá de la simple explicación de la normativa para interpretarla y evaluarla en escenarios de aplicación técnica concretos. Esto permite identificar posibles lagunas normativas y áreas de conflicto que requieren una adaptación de la normativa. Del mismo modo, ante tecnologías como el blockchain, la hermenéutica ofrece criterios interpretativos que orientan las decisiones legales y corporativas.

Técnicas e instrumentos de recolección de datos

Se emplean dos métodos principales de acuerdo con el enfoque cualitativo. El primero es una revisión de la literatura y la documentación, que examina fuentes como las leyes ecuatorianas más recientes relativas a la protección de datos personales, regulaciones internacionales comparativas, en particular el RGPD, artículos académicos sobre blockchain y privacidad, manuales técnicos sobre el despliegue de arquitecturas blockchain privadas e híbridas, e informes de organismos reguladores y organizaciones de normalización. La organización de estas fuentes mediante matrices de análisis temático proporcionará una base sólida para comprender la relación entre la tecnología y la protección de datos en el contexto empresarial, lo que permitirá identificar puntos de convergencia, conflictos y lagunas legales (Hart, 2018).

El segundo enfoque consiste en entrevistas semiestructuradas con expertos en tecnología blockchain o ciberseguridad y abogados con experiencia en derecho digital. Esta herramienta permitirá identificar las aplicaciones prácticas de los requisitos de seguridad, trazabilidad, autorización y eliminación de datos, así como los obstáculos tecnológicos y legales que deben superar las empresas al utilizar esta tecnología. Las entrevistas se organizarán de manera que se fomente un diálogo franco que facilite el intercambio de experiencias y puntos de vista pertinentes para comprender la cuestión. Del mismo modo, se respetará la identidad profesional, el anonimato y el consentimiento informado de los participantes, de conformidad con las normas éticas de la investigación cualitativa (Hernández Sampieri, 2020).

La selección de publicaciones jurídicas y tecnológicas pertinentes es el primer paso del proceso de investigación secuencial, al que le sigue un análisis doctrinal de los principios importantes en materia de seguridad de los datos. A continuación, se elabora una guía de entrevistas especializadas basándose en la identificación de los conflictos entre el derecho al olvido y la inmutabilidad de la cadena de bloques. Con el fin de enmarcar los resultados y facilitar la integración analítica de la teoría y la práctica empresarial, la información se organiza mediante una codificación temática tras la recopilación de opiniones de expertos. Como resultado, se elaboran recomendaciones para la aplicación segura de la tecnología blockchain de conformidad con la LOPDP.

En términos de consideraciones éticas, el estudio garantiza el cumplimiento de los principios fundamentales a lo largo de todo el proceso de investigación y se basa en la defensa del derecho fundamental a la protección de los datos personales. Para lograrlo, se mantiene la confidencialidad de los nombres de los participantes, se solicita su consentimiento informado antes de realizar las entrevistas y se garantiza que la información recopilada solo se utilice con fines académicos. La integridad y la transparencia del estudio también se preservan mediante un riguroso compromiso con la honestidad en el análisis y la presentación de los resultados.

La entrevista semiestructurada se usa como un método principal para obtener información directamente de profesionales que sean especializados en las áreas de protección de datos, y en tecnología. A través de dos cuestionarios guiados, uno dirigido hacia abogados expertos en protección de datos, y el segundo direccionado a expertos en tecnología, ambos cuestionarios con preguntas abiertas (véase Tabla 1 y 2), se busca recolectar no solo los datos técnicos, sino también las experiencias, percepciones y puntos de vista de los expertos a entrevistar con respecto a la protección de los datos personales de los miembros de una empresa privada y también sobre la implementación de la blockchain. Este método de recolección de datos permite:

- Obtener información cualitativa desde la perspectiva de expertos.
- Hacer una comparación del marco teórico con casos de la vida real y la práctica profesional.
- Obtener propuestas y recomendaciones basadas en la experiencia empresarial ecuatoriana.

Tabla 1. Cuestionario para abogados

Preguntas	No. 1	No. 2	No. 3	No. 4	No. 5
1. ¿cuál considera que es el mayor desafío legal que enfrentan las empresas privadas ecuatorianas hoy para cumplir con la ley orgánica de protección de datos personales (lopdp)?					
2. Desde su experiencia, ¿cuáles son las infracciones o fallas más comunes que observa en la gestión de datos personales que generarían sanciones a las empresas?					
3. ¿mencione la normativa legal que regule el uso de la blockchain para empresas privadas en el ecuador?					
4. ¿cree que la inmutabilidad y la descentralización de la blockchain aportan al cumplimiento de los principios fundamentales de la lopdp?					
5. ¿considera que la blockchain podría ser usada por el responsable del tratamiento de datos personales como mecanismo de protección de la información? 6. ¿considera legalmente viable que una empresa utilice un sistema basado en blockchain para el almacenamiento y/o la conservación de los datos de los titulares de datos personales en ecuador? ¿por qué? 7. ¿la disponibilidad, integridad y confidencialidad de los datos personales se cumplirían con la implementación de blockchain en las empresas?					
8. ¿qué tipo de datos personales y/o datos personales sensibles considera usted que la legislación ecuatoriana permitiría gestionar mediante tecnología blockchain?					
9. ¿qué recomendaciones puntuales daría para estructurar un marco jurídico que permita el uso seguro de blockchain en la protección de datos personales?					
10. ¿cómo se obtendría los datos protegidos por la blockchain para que se considere una prueba digital?					
11. ¿cree usted que la blockchain al ser una herramienta inmutable vulnera el derecho de supresión de datos de los titulares de la información?					

Fuente: elaboración propia

Tabla 2. Cuestionario para expertos en tecnología

Preguntas	No. 1	No. 2	No. 3	No. 4
1. Desde una perspectiva tecnológica ¿Cuáles son las principales características técnicas que debe contener el diseño de la Blockchain para ser eficaz en la seguridad de datos personales frente a una base tradicional?				
2. ¿Qué tipo de Blockchain considera la más adecuada para su implementación en una empresa privada en Ecuador y por qué?				
3. Desde una perspectiva técnica, ¿cómo se puede garantizar el Derecho a la supresión (eliminación) de los datos personales en un sistema de Blockchain que es inherentemente inmutable?				
4. ¿Cuál es la diferencia técnica entre almacenar un dato personal completo on-chain (en la cadena) y almacenar un hash del dato? ¿Cuál recomienda para cumplir con la LOPDP y por qué?				
5. ¿Qué retos de integración presenta la implementación de Blockchain en los sistemas de gestión de datos (CRM/ERP) ya existentes en la mayoría de las empresas privadas? 6. ¿Qué conocimientos tecnológicos deben tener las empresas ecuatorianas para implementar y mantener un sistema de gestión de datos personales basado en Blockchain? 7. ¿Cuál es el principal riesgo de ciberseguridad que usted identifica al implementarse una blockchain como solución para la protección de datos y como puede mitigarse?				
8. ¿Puede la tecnología Blockchain ofrecer una trazabilidad y auditoría de los accesos a los datos que sea más robusta que los logs tradicionales?				
9. ¿Qué costos de infraestructura y desarrollo inicial estima usted para la adopción de una solución Blockchain de protección de datos por una PYME ecuatoriana, en comparación con una solución tradicional?				
10. Mencione uno o dos casos de uso exitoso a nivel internacional o regional donde se haya aplicado una Blockchain para la protección de datos personales.				

Fuente: elaboración propia

2.3. Población y muestra

En la investigación cualitativa, es fundamental definir con precisión la población y la muestra, sobre todo cuando el tema del estudio es extremadamente complejo desde el punto de vista técnico, jurídico y organizativo, como es el caso de la aplicación de la tecnología blockchain para la protección de datos personales en empresas privadas. La muestra es el grupo concreto de participantes seleccionados para aportar información pertinente y detallada al estudio, mientras que la población se define como el conjunto de entidades, profesionales o casos que presentan características directamente relacionadas con el fenómeno objeto de investigación (Hernández Sampieri, Fernández y Baptista, 2020).

A diferencia del enfoque cuantitativo, la investigación cualitativa prioriza la riqueza conceptual y la profundidad interpretativa por encima de la representatividad estadística. Por lo tanto, la experiencia, los conocimientos y la pericia de los actores que participan en el campo de análisis se priorizan en la selección deliberada y racional de la muestra. Este enfoque garantiza que las contribuciones recibidas representen puntos de vista que son realmente importantes para el estudio y permite obtener datos completos y útiles para comprender fenómenos complejos como la adopción de la cadena de bloques en el ámbito de la seguridad de los datos personales.

El grupo de empresas privadas que manejan datos personales en Ecuador y están sujetas a los requisitos establecidos por la Ley Orgánica de Protección de Datos Personales se denomina «población» en el contexto de la tecnología blockchain y la protección de datos personales. También se incluyen en este grupo los responsables y encargados del tratamiento de datos, los delegados de protección de datos, los asesores jurídicos corporativos especializados en privacidad, los especialistas en TI, los desarrolladores y administradores de sistemas basados en blockchain, los consultores externos y los especialistas en ciberseguridad.

Dado que la adopción de la cadena de bloques depende no solo de decisiones técnicas, sino también de interpretaciones jurídicas, políticas internas de cumplimiento normativo y estrategias corporativas de seguridad de la información, esta amplia definición nos permite abordar el fenómeno desde la intersección entre el derecho, la tecnología y la gestión organizativa. Para examinar adecuadamente las ventajas y dificultades que plantea esta tecnología, se reconoce que comprender el fenómeno requiere fusionar diversos puntos de vista.

Se utilizará un muestreo intencional, que permite seleccionar a participantes con conocimientos específicos o experiencia de primera mano en decisiones relacionadas con la protección de datos personales y la creación de soluciones basadas en cadenas de bloques, para elegir la muestra (Patton, 2015). Los profesionales que puedan ofrecer conocimientos pertinentes sobre la implementación tecnológica, los retos técnicos, el cumplimiento normativo y la

trazabilidad de los permisos serán el foco principal del proceso de selección. Con el fin de comprender los conflictos entre la inmutabilidad tecnológica y las necesidades legales de flexibilidad, también se tendrá en cuenta a los expertos que puedan explicar la gestión del derecho de supresión y el despliegue de modelos híbridos fuera de la cadena.

Del mismo modo, se puede emplear el muestreo en bola de nieve, en el que los participantes iniciales sugieren más expertos, lo que permite acceder a profesionales jurídicos y técnicos altamente cualificados que a menudo son difíciles de encontrar (Biernacki y Waldorf, 1981). Los ingenieros de cadenas de bloques, los consultores de privacidad y los auditores de seguridad son ejemplos de campos pequeños y altamente especializados en los que este enfoque resulta útil. Su uso mejora la variedad de la información obtenida y facilita la recopilación de puntos de vista complementarios sobre las oportunidades y dificultades asociadas a la implementación de cadenas de bloques en la protección de datos personales.

Tabla 3. Listado de entrevistados

Profesional	**Empleo**
Abg. Mariela Sara Camacho Vaquero	Lex Abogados
Abg. Mario Ruiz Fernandez	Abogado en AVL Abogados
Abg. Rodrigo Godoy	Libre ejercicio – Dueño de una firma Jurídica
ABG. Sofia Berenice Rueda Vargas	Abogada libre ejercicio – Dueña de un centro de rehabilitación
Abg. Katherine Sanchez	Abogada en REDCORP Servicios Profesionales
Ing. Cristian Leandro Zuñiga Quesada	Gerente General Grupo TECNOVATEL S.A.
Ing. Irma Cumanda Mena Guevara	Analista Programadora de GADBAS
Consultor Daniel Morayta	MANAGER CONSULTOR
Consultor Eduardo Martínez Fonseca	Socio, Líder de Gobernanza y de Estrategia de Datos e IA de la firma “Databris” con sedes en Barcelona, Amsterdam, Ciudad de México y Abu Dhabi.

Fuente: elaboración propia

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

El propósito de este capítulo consistió en analizar y discutir los resultados de las entrevistas semiestructuradas realizadas a expertos en derecho digital, protección de datos, ciberseguridad y tecnología *blockchain*. El objetivo fue comprender el uso de esta tecnología en empresas privadas para la protección de datos personales, de conformidad con la normativa aplicable. La evaluación de los resultados permitió comparar los marcos teóricos y legales analizados en los capítulos anteriores con la práctica profesional; de este modo, se identificaron similitudes, diferencias y criterios relevantes para la aplicación de la Ley de Protección de Datos Personales en entornos empresariales que integran nuevas tecnologías.

Un enfoque de investigación cualitativo permitió interpretar las opiniones, relatos y valoraciones de los entrevistados sobre la implementación de la tecnología *blockchain* como medida de seguridad técnica y organizacional. Asimismo, se examinó su impacto en principios como la confidencialidad, integridad, rendición de cuentas proactiva y trazabilidad. Mediante un análisis metódico de la información, se identificaron patrones comunes que permitieron una comprensión global del fenómeno; el estudio no pretendió determinar causas, sino describir y examinar el uso práctico de la tecnología en el contexto legal de Ecuador (Hernández Sampieri, Fernández y Baptista, 2020).

3.1. Presentación de resultados

Para este estudio, se realizaron nueve entrevistas semiestructuradas con expertos en protección de datos y tecnología *blockchain* en el ámbito empresarial. Con el fin de comprender el fenómeno de manera integral, se emplearon dos cuestionarios diferenciados y adaptados a los perfiles profesionales de los participantes. El primer instrumento, dirigido a abogados especializados en derecho digital, permitió obtener cinco entrevistas. Por su parte, el segundo cuestionario, diseñado para expertos en tecnología y ciberseguridad, generó cuatro entrevistas adicionales. Esta distinción metodológica facilitó el examen del objeto de estudio desde las dimensiones jurídica y técnica, lo cual favoreció la comparación de perspectivas y

la identificación de puntos de convergencia en la aplicación de la normativa y la tecnología en el sector privado.

Entrevista abogados

Tabla 4. Entrevista 1

Pregunta	Ab. Mariela Camacho
¿cuál considera que es el mayor desafío legal que enfrentan las empresas privadas ecuatorianas hoy para cumplir con la lopdp?	El mayor desafío es la adecuación de medidas jurídicas, organizativas, administrativas y técnicas según el giro del negocio, la criticidad de los datos y los recursos de cada empresa, garantizando el principio de seguridad.
Desde su experiencia, ¿cuáles son las infracciones o fallas más comunes en la gestión de datos personales?	El principal problema es el desconocimiento del alcance del consentimiento como base legitimadora, su uso incorrecto y la dificultad de garantizar que sea libre, específico, informado e inequívoco.
¿qué normativa legal regula el uso de blockchain para empresas privadas en ecuador?	No existe una normativa específica; se discute un proyecto de ley sobre inteligencia artificial. Lo ideal es un marco basado en principios generales y estándares internacionales.
¿la inmutabilidad y descentralización de la blockchain aportan al cumplimiento de la lopdp?	Sí, especialmente al principio de responsabilidad proactiva, permitiendo a cada institución definir cómo cumplir los principios según su realidad tecnológica.
¿puede la blockchain ser usada como mecanismo de protección de datos personales?	Sí, siempre que se aplique anonimización, lo que reduciría riesgos y podría excluir los datos del ámbito de aplicación de la normativa.
¿es legalmente viable usar blockchain para almacenar datos personales en ecuador? ¿por qué?	Sí, porque en el derecho privado rige el principio de que lo no prohibido está permitido, y puede ser compatible con estándares internacionales de seguridad.
¿la disponibilidad, integridad y confidencialidad se cumplirían con blockchain?	Dependerá de la herramienta utilizada; si garantiza los tres pilares de la seguridad de la información, se cumpliría el principio de seguridad.
¿qué tipo de datos personales permitiría gestionar la legislación mediante blockchain?	No se prohíbe la tecnología, pero los datos sensibles solo podrían tratarse si existe una base legitimadora conforme al artículo 26 de la lopdp.
¿qué recomendaciones daría para estructurar un marco jurídico seguro para blockchain?	Adoptar estándares internacionales como iso, nist u owasp y que la superintendencia los reconozca como guías de cumplimiento.
¿cómo se obtendrían los datos blockchain para que sean prueba digital?	Cumpliendo los requisitos de conducencia, pertinencia y utilidad establecidos en el Cogep y el Coa.
¿la inmutabilidad de la blockchain vulnera el derecho de supresión?	Depende del tratamiento; puede evitarse mediante anonimización, seudonimización o cifrado para que deje de ser dato personal.

Fuente: elaboración propia

Tabla 5. Entrevista 2

Pregunta	Abg. Mario Ruiz
¿cuál considera que es el mayor desafío legal que enfrentan las empresas privadas ecuatorianas hoy para cumplir con la lopdp?	El principal desafío es el desconocimiento de la materia y la falta de seriedad con la que las empresas han abordado la protección de datos personales, retrasando su cumplimiento hasta la inminencia de sanciones.
Desde su experiencia, ¿cuáles son las infracciones o fallas más comunes en la gestión de datos personales?	Las empresas creen que la protección de datos solo aplica a clientes, descuidando datos internos de trabajadores. Además, existe desconocimiento del rol obligatorio del delegado de protección de datos y falta de políticas mínimas exigidas por la ley.
¿qué normativa legal regula el uso de blockchain para empresas privadas en el ecuador?	No existe una normativa específica; sin embargo, hay regulación indirecta en normas como la ley de compañías, Ley Fintech y ley de comercio electrónico, que permiten usos relacionados con blockchain.
¿cree que la inmutabilidad y descentralización de la blockchain aportan al cumplimiento de la lopdp?	Sí, porque permite evitar el almacenamiento de datos en texto plano, usar cifrado criptográfico y mantener registros descentralizados, compatibles con los principios de la lopdp.
¿considera que la blockchain puede ser usada como mecanismo de protección de datos personales?	Sí, ya que permite un registro confiable, resistente a manipulaciones y accesos no autorizados, incluso internos.
¿es legalmente viable utilizar blockchain para el almacenamiento o conservación de datos personales en ecuador? ¿por qué?	Sí, es legalmente viable, ya que no existe prohibición expresa y el uso de blockchain aporta transparencia, seguridad, confidencialidad y trazabilidad.
¿la disponibilidad, integridad y confidencialidad de los datos se cumplirían con blockchain?	Sí, aunque debe gestionarse adecuadamente el acceso para garantizar el ejercicio de los derechos arco sin afectar la seguridad del sistema.
¿qué tipo de datos personales o sensibles permitiría gestionar la legislación mediante blockchain?	Incluso datos sensibles podrían gestionarse si existe consentimiento expreso del titular, siendo clave la posibilidad de revocatoria del consentimiento.
¿qué recomendaciones daría para estructurar un marco jurídico seguro para el uso de blockchain?	Evitar la sobre regulación y promover enfoques flexibles como sandboxes regulatorios y el principio de accountability, permitiendo innovación sin vulnerar derechos.
¿cómo se obtendrían los datos blockchain para que sean considerados prueba digital?	Mediante entidades certificadoras o autoridades que acrediten la existencia y depósito de la información sin revelar su contenido, preservando la confidencialidad.
¿la inmutabilidad de la blockchain vulnera el derecho de supresión de datos?	No necesariamente, ya que puede aplicarse anonimización o bloqueo criptográfico, eliminando el acceso a los datos y produciendo una supresión efectiva.

Fuente: elaboración propia

Tabla 6. Entrevista 3

Pregunta	**Abg. Rodrigo Godoy**
¿Cuál considera que es el mayor desafío legal que enfrentan las empresas privadas ecuatorianas hoy para cumplir con la ley orgánica de protección de datos personales (lopdp)?	Considera que el mayor desafío es el desconocimiento general en relación a la ley. No cree que sea falta de difusión por parte de la Superintendencia ni un obstáculo legal, sino una falta de comprensión del tema.
Desde su experiencia, ¿cuáles son las infracciones o fallas más comunes que observa en la gestión de datos personales que generarían sanciones a las empresas?	Menciona que existen infracciones leves y graves. Señala que faltas graves en la implementación de la ley pueden derivar en penas económicas de hasta el 1% del volumen del negocio.
¿Mencione la normativa legal que regule el uso de la blockchain para empresas privadas en el ecuador?	Indica que, hasta donde conoce, el blockchain no está regulado específicamente, aunque considera indispensable su relación con la normativa de protección de datos por los bloques de información que maneja.
¿Cree que la inmutabilidad y la descentralización de la blockchain aportan al cumplimiento de los principios fundamentales de la lopdp?	No está seguro y sugiere que esta pregunta debería dirigirse a un experto en tecnologías de la información (TI).
¿Considera que la blockchain podría ser usada por el responsable del tratamiento de datos personales como mecanismo de protección de la información?	Señala que para transferencias al exterior vía blockchain, la LOPDP exige analizar la normativa del país de destino y verificar las medidas de seguridad de las plataformas.
¿Considera legalmente viable que una empresa utilice un sistema basado en blockchain para el almacenamiento y/o la conservación de los datos? ¿por qué?	Reitera la necesidad de una opinión técnica de un ingeniero en TI o ciberseguridad para verificar si las medidas de seguridad del blockchain son específicas para la protección de datos.
¿La disponibilidad, integridad y confidencialidad de los datos personales se cumplirían con la implementación de blockchain en las empresas?	Posiblemente sí, pero afirma que se requiere un análisis legal y técnico previo para asegurar que se cumplan los tres pilares de la ley en Ecuador.
¿Qué tipo de datos personales y/o sensibles considera que la legislación ecuatoriana permitiría gestionar mediante tecnología blockchain?	Identifica como datos sensibles los de salud, datos masivos y datos de menores. Subraya que la viabilidad técnica debe ser validada por expertos en seguridad informática.
¿Qué recomendaciones puntuales daría para estructurar un marco jurídico que permita el uso seguro de blockchain?	Sugiere una reforma a nivel legal y resoluciones de la Superintendencia que establezcan al blockchain como una herramienta adecuada para la protección de datos.
¿Cómo se obtendría los datos protegidos por la blockchain para que se considere una prueba digital?	Explica que la prueba debe ser materializada por un notario para ser válida en juicio, conforme a las condiciones de prueba del Código Orgánico General de Procesos (COGEP).
¿Cree usted que la blockchain al ser inmutable vulnera el derecho de supresión de datos de los titulares?	Si la herramienta no permite la actualización o eliminación de datos, estaría vulnerando los derechos de los titulares, por lo que este aspecto debe regularse.

Fuente: elaboración propia

Tabla 7. Entrevista 4

Pregunta	Abg. Sofia Rueda
¿Cuál considera que es el mayor desafío legal que enfrentan las empresas privadas ecuatorianas hoy para cumplir con la LOPDP?	El mayor desafío es la adecuación operativa. No basta con avisos de privacidad; el reto es implementar medidas técnicas y organizativas que demuestren una responsabilidad proactiva.
Desde su experiencia, ¿cuáles son las infracciones o fallas más comunes que observa en la gestión de datos personales que generarían sanciones?	La falta de una base legitimadora correcta, operando con consentimientos viciados o tratando datos sensibles sin las medidas de seguridad exigidas, lo que expone a multas de hasta el 1% de su facturación.
¿Mencione la normativa legal que regule el uso de la *blockchain* para empresas privadas en el Ecuador?	No existe una ley específica. Se rigen por la LOPDP, la Ley de Comercio Electrónico para la validez de mensajes de datos y, supletoriamente, el Código Civil.
¿Cree que la inmutabilidad y la descentralización de la *blockchain* aportan al cumplimiento de los principios fundamentales de la LOPDP?	Sí, aportan significativamente a la integridad y seguridad. Al ser descentralizada, elimina puntos únicos de falla, protegiendo contra hackeos masivos o alteraciones no autorizadas.
¿Considera que la *blockchain* podría ser usada por el responsable del tratamiento de datos personales como mecanismo de protección de la información?	Absolutamente, funciona como una bitácora inalterable. Permite trazar quién accedió a qué dato y cuándo, facilitando la auditoría y la transparencia.
¿Considera legalmente viable que una empresa utilice un sistema basado en *Blockchain* para el almacenamiento y/o conservación de datos? ¿Por qué?	Es viable bajo el principio de neutralidad tecnológica. En derecho privado, lo que no está prohibido está permitido, siempre que el sistema garantice que el dato es accesible y recuperable.
¿La disponibilidad, integridad y confidencialidad de los datos personales se cumplirían con la implementación de *Blockchain* en las empresas?	La integridad es su fuerte y la disponibilidad mejora por la descentralización. La confidencialidad depende de usar capas adicionales de cifrado, ya que la cadena por sí sola es solo un registro.
¿Qué tipo de datos personales y/o datos personales sensibles considera usted que la legislación ecuatoriana permitiría gestionar mediante *blockchain*?	La ley no limita la tecnología según el dato, sino el nivel de protección. Datos sensibles (como de salud) podrían gestionarse mediante *hashes*, asegurando que el dato real esté cifrado fuera de la cadena.
¿Qué recomendaciones puntuales daría para estructurar un marco jurídico que permita el uso seguro de *Blockchain*?	Enfocarse en estándares de interoperabilidad y reconocer oficialmente las firmas criptográficas como equivalentes a firmas electrónicas certificadas para ciertos actos.
¿Cómo se obtendría los datos protegidos por la *blockchain* para que se considere una prueba digital?	Bajo las reglas del COGEP, requiriendo un peritaje informático que valide la cadena de custodia y la integridad del nodo para certificar que el registro coincide con el documento.
¿Cree usted que la *blockchain* al ser una herramienta inmutable vulnera el derecho de supresión de datos de los titulares?	No hay vulneración si se aplica la "supresión lógica". Al borrar las llaves de cifrado, el dato queda anonimizado; legalmente, un dato que no se puede asociar a una persona ya no es dato personal.

Fuente: elaboración propia

Tabla 8. Entrevista 5

Pregunta	Abg. Katherine Sanchez
¿Cuál considera que es el mayor desafío legal que enfrentan las empresas privadas ecuatorianas hoy para cumplir con la LOPDP?	El mayor desafío es la implementación efectiva del principio de responsabilidad proactiva (accountability), que implica demostrar de forma permanente el cumplimiento normativo, adecuar procesos internos, políticas, contratos y aplicar medidas reales de seguridad de la información.
Desde su experiencia, ¿cuáles son las infracciones o fallas más comunes en la gestión de datos personales?	Falta de consentimiento válido e informado, ausencia de políticas de privacidad claras, tratamiento sin base legal, medidas de seguridad insuficientes y deficiente atención de los derechos de los titulares.
¿Qué normativa legal regula el uso de blockchain para empresas privadas en el Ecuador?	No existe normativa específica; su uso se rige indirectamente por la Constitución, la LOPDP, el Código de Comercio, la Ley de Comercio Electrónico y la normativa societaria y contractual vigente.
¿Cree que la inmutabilidad y descentralización de la blockchain aportan al cumplimiento de la LOPDP?	Aportan parcialmente, especialmente a los principios de seguridad, integridad y confidencialidad, pero pueden generar tensiones con derechos como supresión, rectificación y minimización de datos.
¿Considera que la blockchain puede ser usada como mecanismo de protección de datos personales?	Sí, ya que fortalece la seguridad, trazabilidad e integridad de la información, siempre que sea compatible con los principios y derechos de la LOPDP.
¿Es legalmente viable usar blockchain para el almacenamiento o conservación de datos personales en Ecuador? ¿Por qué?	Sí, es viable siempre que se garantice una base legal para el tratamiento, medidas adecuadas de seguridad y mecanismos que respeten los derechos de los titulares.
¿La disponibilidad, integridad y confidencialidad de los datos se cumplirían con blockchain?	Sí, siempre que se complemente con controles de acceso, cifrado y una adecuada gobernanza del tratamiento conforme a la LOPDP.
¿Qué tipo de datos personales o sensibles permitiría gestionar la legislación mediante blockchain?	Principalmente datos no sensibles; los datos sensibles solo de forma excepcional, anonimizados o seudonimizados y con base legal expresa.
¿Qué recomendaciones daría para estructurar un marco jurídico seguro para el uso de blockchain?	Definir una base legal clara, priorizar anonimización o seudonimización, regular gobernanza y responsabilidades, limitar datos on-chain y garantizar los derechos del titular.
¿Cómo se obtendrían los datos blockchain para que sean considerados prueba digital?	Mediante la extracción del hash, su verificación en la cadena, peritaje informático y cadena de custodia que acrediten integridad y autenticidad.
¿La inmutabilidad de la blockchain vulnera el derecho de supresión de datos?	No necesariamente; puede gestionarse mediante almacenamiento off-chain, seudonimización o eliminación de claves de acceso conforme a la LOPDP.

Fuente: elaboración propia

Entrevistas a expertos en tecnología

Tabla 9. Entrevista 6

Pregunta	Eduardo Martinez
Desde una perspectiva tecnológica, ¿cuáles son las principales características técnicas que debe contener el diseño de la Blockchain para ser eficaz en la seguridad de datos personales frente a una base tradicional?	Debe contar con descentralización (eliminar punto único de fallo), inmutabilidad y trazabilidad (evitar manipulación de registros) y cifrado de la información mediante técnicas criptográficas.
¿Qué tipo de Blockchain considera la más adecuada para su implementación en una empresa privada en Ecuador y por qué?	Una Blockchain permisionada (privada), como Hyperledger Fabric, porque permite controlar validadores y accesos, y utiliza lenguajes y arquitecturas estándar.
Desde una perspectiva técnica, ¿cómo se puede garantizar el derecho a la supresión de datos personales en una Blockchain inmutable?	Mediante el crypto-shredding: almacenar los datos personales off-chain y solo referencias cifradas on-chain; al eliminar la llave criptográfica, el dato se vuelve inaccesible.
¿Cuál es la diferencia entre almacenar un dato personal on-chain y almacenar un hash del dato? ¿Cuál recomienda para cumplir con la LOPDP?	Almacenar on-chain expone permanentemente los datos; almacenar un hash solo prueba integridad sin revelar información. Se recomienda almacenar únicamente el hash para proteger la privacidad y cumplir la LOPDP.
¿Qué retos de integración presenta la implementación de Blockchain en sistemas CRM o ERP existentes?	Problemas de calidad y limpieza de datos, falta de interoperabilidad y necesidad de desarrollar capas intermedias como apis para conectar sistemas centralizados con Blockchain.
¿Qué conocimientos tecnológicos deben tener las empresas para implementar y mantener un sistema basado en Blockchain?	Conocimientos en desarrollo Blockchain, smart contracts, arquitectura de soluciones, devops, frameworks de desarrollo, gestión de identidad soberana y servicios cloud baas.
¿Cuál es el principal riesgo de ciberseguridad al implementar Blockchain y cómo puede mitigarse?	El manejo de llaves privadas. Puede mitigarse usando hardware HSM y esquemas de multifirma para autorizar acciones críticas.
¿Puede Blockchain ofrecer una trazabilidad y auditoría más robusta que los logs tradicionales?	Sí, porque cada acceso queda registrado de forma inmutable y no puede ser borrado ni siquiera por administradores, garantizando una auditoría forense completa.
¿Qué costos de infraestructura y desarrollo implica una solución Blockchain para una PYME en comparación con una solución tradicional?	Aunque la inversión inicial es mayor, a largo plazo los costos se equilibran e incluso pueden ser menores que soluciones tradicionales por licencias y escalabilidad.
Mencione casos de uso exitosos donde se haya aplicado Blockchain para la protección de datos personales.	Estonia (KSI Blockchain) para registros gubernamentales y Genobank.io para la protección de datos genéticos en el sector privado.

Fuente: elaboración propia

Tabla 10. Entrevista 7

Pregunta	Cristian Zuñiga
¿Cuáles son las principales características técnicas que debe contener el diseño de la Blockchain para ser eficaz en la seguridad de datos frente a una base tradicional?	La capacidad de distribuir bases de datos de forma segura en una cadena de bloques. Permite evidenciar códigos en tiempo real al integrar nuevos bloques, asegurando trazabilidad y seguridad permanente según el uso tecnológico.
¿Qué tipo de Blockchain considera la más adecuada para su implementación en una empresa privada en Ecuador y por qué?	Una cadena con base de datos distribuida orientada a la trazabilidad y ciberseguridad. Ayuda a mitigar riesgos contra la disponibilidad, confidencialidad e integridad, siendo aplicable a diversos giros de negocio.
¿Cómo se puede garantizar el Derecho a la supresión de datos en un sistema de Blockchain que es inherentemente inmutable?	Implementando procesos alineados a estándares internacionales como la norma ISO/IEC 27701. Esto requiere políticas, identificación de riesgos y medidas de mitigación específicas bajo controles ISO.
¿Cuál es la diferencia técnica entre almacenar un dato completo *on-chain* y un *hash*? ¿Cuál recomienda para cumplir con la LOPDP?	Recomienda aplicar ambas: una para salvaguardar y otra para preservar. El uso del código hash permite entregar información fidedigna y técnica ante posibles delitos informáticos.
¿Qué retos de integración presenta la implementación de Blockchain en sistemas existentes (CRM/ERP)?	Existe un alto índice de fracaso (90%) al intentar integrar Blockchain en tecnologías "Industria 3.0". Lo ideal es diseñar proyectos desde el origen con principios de protección de datos y ciberseguridad por defecto.
¿Qué conocimientos tecnológicos deben tener las empresas para mantener un sistema basado en Blockchain?	Deben basarse en estándares internacionales: ISO/IEC 27001:2022 (ciberseguridad), 27701 (privacidad), 27017 y 27018 (nube), además de normas específicas según el sector (como PCI DSS para finanzas).
¿Cuál es el principal riesgo de ciberseguridad que identifica y cómo puede mitigarse?	La principal amenaza es la afectación a la integridad de los datos. Se mitiga mediante una matriz de riesgos que identifique vulnerabilidades específicas según el giro del negocio e implementación técnica.
¿Puede la tecnología Blockchain ofrecer una trazabilidad y auditoría más robusta que los logs tradicionales?	Sí, al ser bases distribuidas, la trazabilidad es más precisa y directa sobre los niveles de acceso. Fortalece las pistas de auditoría, haciéndolas más eficaces y efectivas, especialmente en la integración entre sistemas.
¿Qué costos de infraestructura y desarrollo estima para una PYME ecuatoriana en comparación con una solución tradicional?	Una solución básica puede iniciar alrededor de los USD 10.000. Sin embargo, el costo aumenta si no hay conocimiento suficiente, ya que se requieren más horas-hombre para análisis, diseño y desarrollo.
Mencione uno o dos casos de uso exitoso a nivel internacional o regional donde se haya aplicado Blockchain para protección de datos.	Menciona al Departamento de Análisis de Datos de Inglaterra (Londres) para trazabilidad y seguridad de datos ciudadanos. También cita su uso en sistemas electorales para evitar alteraciones en bases de datos.

Fuente: elaboración propia

Tabla 11. Entrevista 8

Pregunta	Daniel Morayta
¿Cuáles son las principales características técnicas que debe contener el diseño de la Blockchain para ser eficaz en la seguridad de datos frente a una base tradicional?	El diseño debe priorizar la privacidad, la trazabilidad total, la inmutabilidad mediante criptografía y la descentralización.
¿Qué tipo de Blockchain considera la más adecuada para su implementación en una empresa privada en Ecuador y por qué?	Deben ser elementos que garanticen el cumplimiento con la LOPDP de Ecuador, la protección y privacidad de datos empresariales, y que ofrezcan eficiencia con bajos costos transaccionales.
¿Cómo se puede garantizar el Derecho a la supresión de datos en un sistema de Blockchain que es inherentemente inmutable?	A través del almacenamiento "Off-Chain" (fuera de la cadena) y la destrucción criptográfica en almacenamiento cifrado.
¿Cuál es la diferencia técnica entre almacenar un dato personal completo *on-chain* y un *hash*? ¿Cuál recomienda para cumplir con la LOPDP?	Recomienda almacenar únicamente el *hash* del dato para asegurar la integridad y el derecho a la supresión, manteniendo la información real en sistemas externos u *off-chain*.
¿Qué retos de integración presenta la implementación de Blockchain en sistemas de gestión de datos (CRM/ERP) ya existentes?	Identifica retos en la sincronización de datos y la interoperabilidad con sistemas heredados (*legacy*).
¿Qué conocimientos tecnológicos deben tener las empresas ecuatorianas para implementar y mantener este sistema?	Conocimientos en el desarrollo de contratos inteligentes, criptografía para proteger la identidad y el uso de redes descentralizadas que cumplan la normativa local.
¿Cuál es el principal riesgo de ciberseguridad que identifica y cómo puede mitigarse?	La vulnerabilidad en los contratos inteligentes (errores de programación). Se mitiga mediante auditorías de código rigurosas y pruebas constantes antes de la implementación.
¿Puede la tecnología Blockchain ofrecer una trazabilidad y auditoría de los accesos más robusta que los logs tradicionales?	Sí, porque crea un registro inmutable y distribuido donde cada acceso queda guardado criptográficamente y es imposible de modificar sin dejar rastro.
¿Qué costos de infraestructura y desarrollo inicial estima para una PYME ecuatoriana en comparación con una solución tradicional?	Aunque no precisa cifras exactas, estima que la implementación inicial es más costosa que una tradicional, pero proyecta un ahorro de costos a largo plazo.
Mencione uno o dos casos de uso exitoso a nivel internacional o regional donde se haya aplicado Blockchain para la protección de datos.	Menciona el caso de la historia clínica electrónica de Estonia, que utiliza Blockchain para registrar y proteger los datos de salud de toda su población.

Fuente: elaboración propia

Tabla 12. Entrevista 9

Pregunta	Cumandá Mena
¿Cuáles son las principales características técnicas que debe contener el diseño de la Blockchain para ser eficaz en la seguridad de datos frente a una base tradicional?	Se debe priorizar la seguridad del encriptamiento para evitar ingresos no permitidos a las bases de datos y prevenir cualquier tipo de manipulación de la información.
¿Qué tipo de Blockchain considera la más adecuada para su implementación en una empresa privada en Ecuador y por qué?	Considera que una Blockchain privada es la más adecuada, ya que ofrece un entorno más controlado y seguro para proteger los datos empresariales.
¿Cómo se puede garantizar el Derecho a la supresión de datos en un sistema de Blockchain que es inmutable?	Sugiere que, dada la naturaleza inmutable de la tecnología, la mejor opción técnica para no vulnerar este derecho sería el no registro de ciertos datos en la cadena.
¿Cuál es la diferencia técnica entre almacenar un dato completo *on-chain* y un *hash*? ¿Cuál recomienda para cumplir con la LOPDP?	Recomienda el uso de hashes. Argumenta que almacenar solo la información indispensable facilita el cumplimiento normativo y reduce las observaciones en futuras auditorías.
¿Qué retos de integración presenta la implementación de Blockchain en sistemas existentes (CRM/ERP)?	El reto principal es el costo elevado que conlleva implementar nuevas políticas y procesos de seguridad, especialmente en instituciones que requieren presupuestos aprobados para operar.
¿Qué conocimientos tecnológicos deben tener las empresas para mantener este sistema?	Se requiere personal especializado en informática y desarrollo. Es fundamental que el área de desarrollo colabore con quienes manejan el hardware para implementar medidas de seguridad robustas.
¿Cuál es el principal riesgo de ciberseguridad que identifica y cómo puede mitigarse?	Indica que, al ser la Blockchain una solución diseñada precisamente para mitigar problemas de seguridad existentes, no identifica riesgos pendientes si la implementación es correcta.
¿Puede la tecnología Blockchain ofrecer una trazabilidad y auditoría de los accesos más robusta que los logs tradicionales?	Sí, la implementación permite mayor seguridad y se apoya en auditorías constantes que refuerzan la protección y generan confianza en los procesos.
¿Qué costos de infraestructura y desarrollo inicial estima para una PYME ecuatoriana en comparación con una solución tradicional?	Estima una inversión inicial de aproximadamente USD 25.000. Señala que el mantenimiento anual será considerablemente menor una vez superada la fase de implementación.
Mencione uno o dos casos de uso exitoso a nivel internacional o regional donde se haya aplicado Blockchain para protección de datos.	Destaca la iniciativa ID2020, que articula seguridad biométrica con Blockchain para crear una identidad digital universal donde el usuario controla qué datos comparte.

Fuente: elaboración propia

3.2. Entrevistas a expertos: análisis general de los resultados obtenidos

El análisis de los resultados de las entrevistas reveló un consenso general entre los abogados de protección de datos sobre el escaso conocimiento y la limitada aplicación práctica de la Ley de Protección de Datos Personales (LOPDP) en el ámbito empresarial. Los encuestados afirmaron que, a pesar de la vigencia de la ley, muchas empresas privadas no han implementado las medidas técnicas y

organizativas necesarias para garantizar el cumplimiento de los principios de seguridad, confidencialidad y rendición de cuentas proactiva. Esta situación revela una discrepancia significativa entre la normativa aplicable y la realidad operativa de las empresas, lo que aumenta el riesgo de vulneración de los derechos de los interesados.

***Blockchain* como herramienta técnica y organizativa para la protección de datos**

Desde una perspectiva legal, los abogados entrevistados coincidieron en que la introducción de nuevas tecnologías, como blockchain, puede ser una herramienta eficaz para mejorar la protección de datos, siempre que su uso cumpla con los principios y obligaciones establecidos en la LOPDP. Se destacó que la trazabilidad e inmutabilidad de los registros de datos en esta tecnología refuerzan el principio de rendición de cuentas proactiva y facilitan la verificación de las actividades de tratamiento realizadas por las empresas privadas. Al mismo tiempo, se observó que la falta de regulaciones específicas sobre la tecnología blockchain genera inseguridad jurídica y requiere una interpretación de las regulaciones basada en el principio de neutralidad tecnológica.

Contribuciones técnicas al uso de la tecnología blockchain y su cumplimiento con la normativa de protección de datos

Los expertos en tecnología que participaron en las entrevistas aportaron perspectivas significativas al análisis legal. Señalaron que la tecnología blockchain no debe utilizarse como un sistema para almacenar directamente datos personales. Destacaron que las soluciones basadas en *blockchains* permisionadas, técnicas de hash y almacenamiento externo de datos personales son las que mejor cumplen con la normativa de protección de datos. Estas técnicas garantizan la integridad y autenticidad de la información sin vulnerar los derechos de los interesados y minimizan los riesgos asociados a la inmutabilidad de la tecnología

Conflicto entre el derecho de supresión y el principio de inmutabilidad de la *blockchain*

Un aspecto clave del análisis fue el conflicto entre el derecho de supresión de datos personales y el principio de inmutabilidad de la blockchain. Expertos legales y tecnológicos coincidieron en que este dilema podría resolverse mediante la implementación de soluciones tecnológicas que cumplan con la Ley Orgánica de Protección de Datos de Carácter Personal (LOPDP). Las entrevistas revelaron que la solución consiste en evitar el almacenamiento directo de datos personales en la blockchain y, en su lugar, utilizar referencias cifradas, huellas digitales o métodos de borrado lógico como la criptodestrucción. Esto permite proteger los derechos de los interesados sin comprometer la funcionalidad del sistema.

La importancia de la gestión de datos

Los resultados también mostraron que la simple implementación de blockchain en empresas privadas no garantiza el cumplimiento de la normativa de protección de datos. Los encuestados indicaron que es esencial complementar la tecnología con políticas internas claramente definidas, una gestión adecuada de los datos y una cultura organizacional que priorice la protección de los derechos de los interesados. La formación de los empleados, el nombramiento de responsables del tratamiento y la colaboración activa con el Delegado de Protección de Datos se han identificado como factores esenciales para una implementación responsable de la LOPDP.

A modo de conclusión de los resultados se obtuvo una valoración abrumadoramente positiva del uso de la tecnología blockchain como herramienta para mejorar la seguridad y la transparencia del tratamiento de datos personales en empresas privadas. La integración de los aspectos legales y técnicos demostró que esta tecnología cumple con la Ley de Protección de Datos Personales (LOPDP), siempre que se respeten principios como la legalidad, la minimización de datos, la seguridad y la rendición de cuentas. Estos resultados confirman la necesidad de promover directrices y buenas prácticas que guíen la implementación de nuevas tecnologías en el contexto de una protección de datos eficaz.

CONCLUSIONES

- El estudio concluyó que el uso de la tecnología blockchain en el sector privado puede ser una estrategia técnica y organizativa adecuada para mejorar la seguridad de los datos personales, siempre que se implemente de conformidad con los principios y obligaciones de la Ley Orgánica de Protección de Datos. Las entrevistas revelaron que las características de la tecnología blockchain, como la trazabilidad, la integridad y la transparencia, respaldan el principio de rendición de cuentas y facilitan a las empresas la demostración de sus actividades de tratamiento. Sin embargo, se observó que la tecnología por sí sola no garantiza el cumplimiento normativo; debe combinarse con políticas internas y controles legales adecuados.

- Respecto a la caracterización sobre el uso del blockchain en empresas privadas para la protección de datos personales, se pudo obtener que la aplicación de esta herramienta se encuentra en una etapa inicial y mayormente experimental en el mercado. Se ha analizado que tanto los abogados expertos como los expertos en tecnología están de acuerdo con que la blockchain tiene un uso para registrar operaciones que manejen datos de las personas, y no se basa tanto en almacenar información personal. Además, se nota que las empresas que acogieron y trabajaron con esta herramienta tecnológica lo hicieron a manera de tener protección con respecto a la seguridad de la información y poder cumplir con el principio de responsabilidad proactiva prevista en la LOPDP.

- La implementación de la blockchain en empresas privadas para proteger los datos personales conforme a la normativa vigente, es viable adoptando un tipo de gobernanza que sea hibrido, para equilibrar la inmutabilidad de la tecnología con las exigencias de la LOPDP, mediante la división de información sensible y la evidencia transaccional.

    - Sobre modelo permisionado: La blockchain más conveniente para este problema planteado es la blockchain permisionada, con este tipo solo podrán acceder personas que tengan autorización, garantizando

la trazabilidad del responsable del tratamiento y el control de quien puede ingresar a las operaciones, así se cumple el principio de responsabilidad proactiva.

- Sobre el almacenamiento y el derecho a la supresión: Para dar protección a los datos personales estos se deben ubicar en off-chain, es decir fuera de la cadena. En las cadenas de bloques (hash) deberían ir códigos cifrados, huellas digitales, clases de verificación, que viene siendo un elemento técnico. De este modo cualquier solicitud para aplicar el derecho de supresión, podrá eliminar el acceso o la llave de descifrado de los datos externos, así la información personal se vuelve inaccesible, sin importar que este en hash. Así se cumple la ley de eliminación efectiva y no amenazada la integridad de la cadena.
- Sobre el impacto y las consecuencias: Es necesario realizar una evaluación de impacto en la protección de datos, para determinar posibles riesgos como el tratamiento no autorizado o pérdida del control de información, para que esta herramienta tecnología se vuelva un sistema seguro conforme al marco legal.

RECOMENDACIONES

- Se recomienda que las organizaciones privadas que apliquen esta estrategia para proteger los datos derivados de este proyecto de investigación, esta enlaza el uso de la blockchain con evaluaciones de impacto, instrucciones de uso y mecanismos de control. Al implementar estos elementos ya definidos, las empresas privadas garantizaran que esta tecnología cumpla con la Ley Orgánica de Protección de Datos Personales y disminuya riesgos de sanciones administrativas por un mal manejo de esta herramienta.

- Se recomienda que las empresas tengan en cuenta esta tecnología para que puedan implementarla en su administración como un mecanismo de trazabilidad y control. Para ello debe existir una evaluación previa que analice la finalidad del tratamiento y sus riegos, garantizando que implementar esta herramienta vaya en conjunto con los principios de seguridad y confidencialidad que establece la Ley Orgánica de Protección de Datos Personales.

- Se recomienda a los legisladores reconocer en el ordenamiento jurídico la tecnología blockchain modelo permisionada, como un mecanismo para la protección de datos personales, en cumplimiento de los principios, derechos y obligaciones de la Ley Orgánica de Protección de Datos Personales, considerando los parámetros jurídicos mínimos establecidos en esta investigación, recordando que esta tecnología no es para almacenar datos directamente personales, más bien es un registro de operaciones que en lo posterior podría servir como mecanismo de prueba en conflictos judiciales.

BIBLIOGRAFÍA

Agencia Española de Protección de Datos. (2019). *Blockchain y protección de datos*. AEPD.

Arias, J., & Covinos, M. (2021). *Diseño y metodología de la investigación*. Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC).

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Sage Publications.

European Union Blockchain Observatory and Forum. (2018). *Blockchain and the GDPR*. Comisión Europea.

Finck, M. (2019). *Blockchain and the General Data Protection Regulation*. Max Planck Institute for Innovation and Competition.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Hernández Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.

Ley Orgánica de Protección de Datos Personales. (2021). Registro Oficial Suplemento No. 459. Ecuador.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos).

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin Random House.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops*, 180–184.

ANEXOS

Anexo 1. Cuestionario formulado para entrevistas direccionadas a expertos y/o especialistas Abogados

Pontificia Universidad Católica del Ecuador | Sede Ambato

ESCUELA DE DERECHO

ENTREVISTA No. _

Estimado/(a)

Con la finalidad de obtener información relevante que sustente el proyecto de investigación titulado "USO DE LA BLOCKCHAIN EN EMPRESAS PRIVADAS PARA PROTEGER LOS DATOS PERSONALES CONFORME LA NORMATIVA VIGENTE.", que se desarrolla como requisito previo a la obtención del título de Abogado de los Tribunales y Juzgados de la República del Ecuador por parte del suscrito estudiante, me permito solicitar su valiosa colaboración y, así; responder el presente cuestionario.

Agradezco de antemano su disponibilidad y contribución a este proceso académico.

La información proporcionada será tratada con absoluta confidencialidad y utilizada exclusivamente con fines investigativos.

Atentamente,

UNIVERSITARIO: Alyson Fernanda Coca Altamirano

DIRECTOR/(A) DEL PROYECTO: María Fernanda Zamora Castillo, Ab. Mg.

TEMA DE TESIS: "USO DE LA BLOCKCHAIN EN EMPRESAS PRIVADAS PARA PROTEGER LOS DATOS PERSONALES CONFORME LA NORMATIVA VIGENTE."

NOMBRE DEL ENTREVISTADO/(A):

-

PROFESIÓN:

-

LUGAR DE TRABAJO:

-

Pontificia Universidad Católica del Ecuador | Sede Ambato

CARGO EN EL CUAL SE DESEMPEÑA:

-

CUESTIONARIO:

1. **¿Cuál considera que es el mayor desafío legal que enfrentan las empresas privadas ecuatorianas hoy para cumplir con la Ley Orgánica de Protección de Datos Personales (LOPDP)?**
2. **Desde su experiencia, ¿cuáles son las infracciones o fallas más comunes que observa en la gestión de datos personales que generarían sanciones a las empresas?**
3. **¿Mencione la normativa legal que regule el uso de la blockchain para empresas privadas en el Ecuador?**
4. **¿Cree que la inmutabilidad y la descentralización de la blockchain aportan al cumplimiento de los principios fundamentales de la LOPDP?**
5. **¿Considera que la blockchain podría ser usada por el responsable del tratamiento de datos personales como mecanismo de protección de la información?**
6. **¿Considera legalmente viable que una empresa utilice un sistema basado en Blockchain para el almacenamiento y/o la conservación de los datos de los titulares de datos personales en Ecuador? ¿Por qué?**

Pontificia Universidad Católica del Ecuador | Sede Ambato

7. **¿La disponibilidad, integridad y confidencialidad de los datos personales se cumplirían con la implementación de Blockchain en las empresas?**
8. **¿Qué tipo de datos personales y/o datos personales sensibles considera usted que la legislación ecuatoriana permitiría gestionar mediante tecnología blockchain?**
9. **¿Qué recomendaciones puntuales daría para estructurar un marco jurídico que permita el uso seguro de Blockchain en la protección de datos personales?**
10. **¿Cómo se obtendría los datos protegidos por la blockchain para que se considere una prueba digital?**
11. **¿Cree usted que la blockchain al ser una herramienta inmutable vulnera el derecho de supresión de datos de los titulares de la información?**

Anexo 2. Cuestionario formulado para entrevistas direccionadas a expertos y/o especialistas en tecnología

Pontificia Universidad Católica del Ecuador | Sede Ambato

ESCUELA DE DERECHO

ENTREVISTA No. _

Estimado/(a)

Con la finalidad de obtener información relevante que sustente el proyecto de investigación titulado "USO DE LA BLOCKCHAIN EN EMPRESAS PRIVADAS PARA PROTEGER LOS DATOS PERSONALES CONFORME LA NORMATIVA VIGENTE.", que se desarrolla como requisito previo a la obtención del título de Abogado de los Tribunales y Juzgados de la República del Ecuador por parte del suscrito estudiante, me permito solicitar su valiosa colaboración y, así; responder el presente cuestionario.

Agradezco de antemano su disponibilidad y contribución a este proceso académico.

La información proporcionada será tratada con absoluta confidencialidad y utilizada exclusivamente con fines investigativos.

Atentamente,

UNIVERSITARIO: Alyson Fernanda Coca Altamirano

DIRECTOR/(A) DEL PROYECTO: María Fernanda Zamora Castillo, Ab. Mg.

TEMA DE TESIS: "USO DE LA BLOCKCHAIN EN EMPRESAS PRIVADAS PARA PROTEGER LOS DATOS PERSONALES CONFORME LA NORMATIVA VIGENTE."

NOMBRE DEL ENTREVISTADO/(A):

-

PROFESIÓN:

-

LUGAR DE TRABAJO:

-

Pontificia Universidad Católica del Ecuador | Sede Ambato

Pontificia Universidad Católica del Ecuador | Sede Ambato

CARGO EN EL CUAL SE DESEMPEÑA:

-

CUESTIONARIO:

1. **Desde una perspectiva tecnológica ¿Cuáles son las principales características técnicas que debe contener el diseño de la Blockchain para ser eficaz en la seguridad de datos personales frente a una base tradicional?**

2. **¿Qué tipo de Blockchain considera la más adecuada para su implementación en una empresa privada en Ecuador y por qué?**

3. **Desde una perspectiva técnica, ¿cómo se puede garantizar el Derecho a la supresión (eliminación) de los datos personales en un sistema de Blockchain que es inherentemente inmutable?**

4. **¿Cuál es la diferencia técnica entre almacenar un dato personal completo *on-chain* (en la cadena) y almacenar un *hash* del dato? ¿Cuál recomienda para cumplir con la LOPDP y por qué?**

5. **¿Qué retos de integración presenta la implementación de Blockchain en los sistemas de gestión de datos (CRM/ERP) ya existentes en la mayoría de las empresas privadas?**

6. **¿Qué conocimientos tecnológicos deben tener las empresas ecuatorianas para implementar y mantener un sistema de gestión de datos personales basado en Blockchain?**

Pontificia Universidad Católica del Ecuador | Sede Ambato

7. **¿Cuál es el principal riesgo de ciberseguridad que usted identifica al implementarse una blockchain como solución para la protección de datos y como puede mitigarse?**

8. **¿Puede la tecnología Blockchain ofrecer una trazabilidad y auditoría de los accesos a los datos que sea más robusta que los logs tradicionales?**

9. **¿Qué costos de infraestructura y desarrollo inicial estima usted para la adopción de una solución Blockchain de protección de datos por una PYME ecuatoriana, en comparación con una solución tradicional?**

10. **Mencione uno o dos casos de uso exitoso a nivel internacional o regional donde se haya aplicado una Blockchain para la protección de datos personales.**

Anexo 3: Evidencia fotográfica de los profesionales entrevistados