

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Jurisprudencia

**Redes P2P y Hashing Criptográfico para Optimizar el
Derecho y el Acceso a la Información Pública en Ecuador**

Ismael Alexander Rodríguez Rosales

Jurisprudencia

Trabajo de fin de carrera presentado como requisito para la
obtención del título de Abogado

Quito, 19 de abril de 2024

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en la Ley Orgánica de Educación Superior del Ecuador.

Nombres y apellidos: Ismael Alexander Rodríguez Rosales

Código: 211664

Cédula de identidad: 1723890594

Lugar y Fecha: Quito, 19 de abril de 2024

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en <http://bit.ly/COPETHeses>.

UNPUBLISHED DOCUMENT

Note: The following capstone Project is available through Universidad San Francisco de Quito USFQ institutional repository. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on <http://bit.ly/COPETHeses>.

REDES P2P Y HASHING CRIPTOGRÁFICO PARA OPTIMIZAR EL DERECHO Y EL ACCESO A LA INFORMACIÓN PÚBLICA EN ECUADOR¹

P2P NETWORKS AND CRYPTOGRAPHIC HASHING TO OPTIMIZE THE RIGHT AND ACCESS TO PUBLIC INFORMATION IN ECUADOR

Ismael Alexander Rodríguez Rosales²
ismaelrodriguez2099@gmail.com

RESUMEN

Esta investigación examina el potencial de las redes Peer-to-Peer (P2P) y el hashing criptográfico para optimizar el acceso y el derecho a la información pública en Ecuador. Ante desafíos significativos como la congestión y las demoras en la obtención de documentos judiciales y públicos, este estudio explora cómo las tecnologías descentralizadas pueden agilizar el flujo de información, mejorar la transparencia y reforzar el marco legal para el acceso a la información pública. Integrando redes P2P para la gestión eficiente de documentos y hashing criptográfico para la integridad y autenticidad de los datos, la investigación destaca tanto los beneficios potenciales como los desafíos de implementación, incluidas las preocupaciones de seguridad y la brecha digital.

PALABRAS CLAVE

Redes P2P, Hashing Criptográfico, Acceso a la Información Pública, Ecuador, Brecha Digital.

ABSTRACT

This research examines the potential of Peer-to-Peer (P2P) networks and cryptographic hashing to optimize access to and the right to public information in Ecuador. Faced with significant challenges such as congestion and delays in obtaining judicial and public documents, this study explores how decentralized technologies can streamline the flow of information, improve transparency, and reinforce the legal framework for access to public information. By integrating P2P networks for efficient document management and cryptographic hashing for data integrity and authenticity, the research highlights both the potential benefits and the implementation challenges, including security concerns and the digital divide.

KEY WORDS

P2P Networks, Cryptographic Hashing, Public Information Access, Ecuador, Digital Divide.

¹ Trabajo de titulación presentado como requisito para la obtención del título de Abogado. Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Dirigido por José Sebastián Ponce Rodríguez.

² © DERECHOS DE AUTOR: Por medio del presente documento certifico que he leído la Política de Propiedad Intelectual de la Universidad San Francisco de Quito y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo de investigación quedan sujetos a lo dispuesto en la Política. Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo de investigación en el repositorio virtual, de conformidad con lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

SUMARIO

1. INTRODUCCIÓN.- 2. MARCO TEÓRICO.- 3. ESTADO DEL ARTE.- 4. MARCO NORMATIVO.- 5. CONSIDERACIONES SOBRE LAS REDES P2P Y LA INFORMACIÓN PÚBLICA.- 6. REDES P2P EN LA INFORMACIÓN PÚBLICA.- 7. PROBLEMAS DE LAS REDES P2P EN LA INFORMACIÓN PÚBLICA.- 8. SOLUCIONES A LA PROBLEMÁTICA DE LAS REDES P2P EN LA INFORMACIÓN PÚBLICA.- 9. PARÁMETROS LEGALES EN ECUADOR SOBRE LAS SOLUCIONES DE LAS REDES P2P.- 10. RECOMENDACIONES.- 11. CONCLUSIONES.-

1. INTRODUCCIÓN. —

El acceso a la información pública constituye un derecho constitucional y una garantía jurisdiccional que permite que las personas puedan acceder a la información considerada como pública³, que consiste en todo documento en cualquier formato, que se encuentre en poder de las instituciones o personas jurídicas públicas; contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado⁴.

El acceso a la información pública en el Ecuador enfrenta obstáculos significativos debido a la congestión y demora en la obtención de documentos judiciales y públicos, lo que afecta el ejercicio efectivo de los derechos civiles. Este problema no es exclusivo de Ecuador, pero su solución puede ofrecer *insights* valiosos para sistemas similares alrededor del mundo. La lentitud en los procesos públicos y la dificultad para acceder a la información actualizada⁵, necesaria para la información, defensa de derechos o el seguimiento de procedimientos judiciales subrayan la importancia de buscar soluciones que no solo sean efectivas, sino también sostenibles y seguras.

La relevancia de esta problemática se acrecienta en el contexto actual de digitalización global, donde la optimización del flujo de información pública se ha vuelto imperativa. La

³ Artículo 4, Ley Orgánica de Transparencia y Acceso a la Información Pública [LOTAIP], R.O. Suplemento 245 de 7 de febrero de 2023.

⁴ Sentencia N° 107-17 septiembre-CC: caso n° 1993-11 EP, p. 12.

⁵ N. J. Medranda-Morales, P. M. Rodríguez-Navas, y V. D. Palacios-Mieles, “Transparencia de la información pública en las páginas web de municipios de España y Ecuador,” *Journal of Iberian and Latin American Research* 27, no. 1 (2021): 1-20.

necesidad de abordar estas barreras no es únicamente una cuestión de eficiencia administrativa, sino una necesidad urgente para fortalecer el derecho a la información como un pilar de la estructura democrática y del Estado de derecho.

En este contexto, la propuesta de utilizar tecnologías de redes P2P, definida como un tipo de red informática en la que dos o más computadoras se conectan y comparten recursos sin necesidad de un servidor central; y la tecnología de hashing criptográfico, como medio de garantizar la integridad y la autenticidad de la información, se presenta como una solución innovadora que promete transformar el acceso a la información pública. Las redes P2P, por su naturaleza descentralizada, ofrecen una alternativa para el manejo y distribución de documentos públicos, reduciendo los cuellos de botella y mejorando la accesibilidad⁶. El hashing criptográfico, por otro lado, asegura la integridad y autenticidad de los documentos, dos aspectos críticos cuando se trata de información pública y judicial⁷. De este modo, el objetivo general de este trabajo es analizar cómo la implementación de redes P2P y hashing criptográfico puede optimizar el acceso y el derecho a la información pública en Ecuador.

La metodología se centra en la conceptualización de estas tecnologías, los objetivos perseguidos y los desafíos que intenta superar, proporcionando una base sólida compuesta por los principales aportes académicos y casos prácticos relevantes. Además, incorpora un análisis de las implicaciones legales de estas tecnologías en el marco normativo ecuatoriano, destacando cómo deben alinearse con los principios legales existentes y ser lo suficientemente flexibles para adaptarse a la dinámica evolución del entorno digital.

La estructura del trabajo se desarrolla con un marco teórico que examina teorías relevantes y un estado del arte que revisa literatura y casos prácticos, destacando la aplicación y desafíos de estas tecnologías. El análisis se profundiza en el marco normativo internacional y ecuatoriano, estableciendo la base legal para la implementación tecnológica propuesta. Posteriormente, se evalúan las consideraciones técnicas, legales, y prácticas sobre las redes P2P, identificando ventajas, retos, y soluciones para su aplicación en la gestión de la información pública. La investigación concluye con recomendaciones prácticas y propuestas de investigación futura, delineando un camino hacia la mejora del acceso a la información

⁶ Y. Zhang, H. Shi, X. Wang, y J. Zhang, “Collaborative Legal Information Sharing on P2P Network,” en 2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007) (2007)

⁷ Reyes Sánchez, Carlos. 2022. «Blockchain: Funcionamiento Y Pertinencia En Sectores Públicos Y Privados». Interconectando Saberes, n.º 14 (agosto):169-78.

pública mediante la integración de tecnologías avanzadas dentro del marco legal y social ecuatoriano.

Existiendo significativos obstáculos para el acceso a la información pública, este estudio propone la aplicación de redes P2P y hashing criptográfico para mejorar el derecho al acceso a la información en Ecuador.

2. MARCO TEÓRICO. —

La adaptación de tecnologías P2P y hashing criptográfico al sistema público ecuatoriano podría acelerar el acceso a la información pública y fortalecer la transparencia, reduciendo la espera por documentos y promoviendo la rendición de cuentas, reduciendo la corrupción. A su vez, fomentaría una mayor participación ciudadana en el sistema público. Sin embargo, estos avances tecnológicos también conllevan desafíos significativos, como la seguridad de la información y la necesidad de alinearlos con el cumplimiento normativo.⁸

Sin embargo, este proceso exigiría un balance entre innovación y evolución de la normativa legal y administrativa, para así proteger derechos ciudadanos y mejorar el acceso a la justicia. Estas tecnologías también plantean desafíos de seguridad y privacidad, y requieren un acoplamiento cuidadoso con la autenticidad e integridad de la información. La resistencia cultural y organizativa en instituciones conservadoras destaca la necesidad de capacitación para maximizar el potencial de estas tecnologías.⁹

Por un lado, sobre el tema tenemos una primera teoría que resulta relevante, la teoría de la sociedad de la información¹⁰, esta subraya que las tecnologías de la información y comunicación tienen el poder de alterar de sobremanera las estructuras políticas y sociales, logrando fomentar una mayor transparencia y participación de la ciudadanía. Según esta corriente, las redes P2P y el hashing criptográfico se postulan como medios que pueden acelerar y facilitar el acceso a la información pública, destruyendo barreras que impiden la participación ciudadana y el cumplimiento de derechos.¹¹ En este contexto, las redes P2P representan una infraestructura que podría democratizar y acelerar la obtención de la información al eliminar intermediarios.

⁸ Ahmad, Daelami, Ninda Lutfiani, Alfian Dimas Ahsanul Rizki Ahmad, Untung Rahardja, and Qurotul Aini. 2021. "Blockchain Technology Immutability Framework Design in E-Government". *Jurnal Administrasi Publik (Public Administration Journal)* 11 (1):32-41.

⁹ *Id.*

¹⁰ Castells, Manuel. 1996. *The Rise of the Network Society*. Oxford: Blackwell.

¹¹ Webster, Frank. 2002. *Theories of the Information Society*. London: Routledge.

En contraposición, la teoría crítica de la tecnología¹², sugiere una aproximación cautelosa al optimismo por la tecnología, puesto que las dinámicas de poder, la resistencia al cambio y la importancia de la interacción humana, enfatizando que la adopción estatal de nuevas herramientas digitales nunca es un proceso neutro, pues puede responder a estructuras de poder existentes al marginar a los que no tienen acceso a las habilidades o recursos tecnológicos y, en última instancia llevar a una situación tecnocrática, donde es la tecnología que dicta la dirección de la política y la sociedad¹³. Entonces, desde esta perspectiva, la implementación de redes P2P en el Estado debe ser considerada y su regulación responda a los factores que garanticen derechos y sirvan al bien público.

La intersección de estas dos principales teorías encuentran su relevancia en nuestro estudio al darnos luces de cómo aprovechar nuevas tecnologías, para fortalecer el derecho al acceso a la información pública, presentando a su vez los desafíos legales y sociales. La sociedad de la información provee un marco para las propuestas de un sistema más abierto y accesible, mientras que la crítica a la tecnología ofrece un enfoque prudente de los riesgos en la adopción de nuevos sistemas estatales.

La presente investigación, por lo tanto, se sitúa en una visión optimista de la tecnología, buscando demostrar cómo la integración cuidadosa de soluciones tecnológicas puede abordar desafíos y problemas jurídicos complejos, al contribuir al fortalecimiento de las instituciones públicas y sus garantías en materia de derechos. A su vez, considerando tanto los beneficios potenciales como los riesgos, equilibrando la innovación tecnológica con las regulaciones existentes para proteger los derechos de los ciudadanos.

3. ESTADO DEL ARTE. —

El siguiente apartado presenta una revisión detallada de literatura sobre la aplicación de tecnologías de redes P2P y hashing criptográfico en el acceso a la información pública, centrándose en su conceptualización, los objetivos perseguidos, y los desafíos que intenta superar. Este análisis proporcionará una base sólida compuesta por los principales aportes académicos y casos prácticos relevantes al tema, ilustrando cómo estas tecnologías pueden transformar la eficiencia, seguridad y transparencia en la gestión de los documentos públicos.

¹²Feenberg, Andrew. 1991. *Critical Theory of Technology*. New York: Oxford University Press.

¹³ Smith, Merritt Roe, and Leo Marx, eds. 1994. *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, MA: MIT Press.

Actualmente, hay varios ejemplos en la adopción de tecnologías P2P en la administración pública en cuanto el acceso a la información pública que han demostrado un potencial significativo para mejorar la eficiencia, seguridad y transparencia de los servicios gubernamentales. Iniciativas en países del Digital 5, como Estonia y el Reino Unido, han liderado la implementación de soluciones de este tipo para la gestión de registros de salud electrónicos y sistemas de votación electrónica, respectivamente. Estos ejemplos subrayan la capacidad de la tecnología basada en redes P2P para revolucionar la infraestructura de información gubernamental, facilitando un acceso seguro y confiable a la información pública y optimizando procesos administrativos.¹⁴

La adopción de tecnología blockchain en servicios de e-Gobierno, según Lykidis, Drosatos, y Rantos, ilustra la capacidad de las tecnologías distribuidas para transformar la administración pública mediante la mejora de la seguridad, eficiencia y transparencia en los servicios a ciudadanos.¹⁵ Esta evidencia respalda la viabilidad de implementar redes P2P y hashing criptográfico en el sistema ecuatoriano, destacando la importancia de la tecnología blockchain como un facilitador clave para la modernización de los servicios públicos y el acceso a la justicia.

La implementación de tecnologías como blockchain en el sector público presenta desafíos significativos, especialmente en términos de seguridad. Alketbi destaca que, aunque blockchain promete mejorar la integridad y seguridad de los datos en servicios gubernamentales, introduce nuevos retos de seguridad que deben ser abordados. Esto incluye vulnerabilidades a ataques de Denegación de Servicio y la necesidad de garantizar la privacidad y autenticidad de los datos. Este análisis subraya la importancia de investigar y mitigar estos riesgos para aprovechar plenamente el potencial de blockchain en la modernización de los servicios públicos y judiciales, resaltando la relevancia de considerar estas preocupaciones de seguridad en el contexto ecuatoriano para la implementación efectiva de redes P2P y hashing criptográfico.¹⁶

¹⁴ A. Ojo y S. Adebayo, "Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries," en *Government 3.0 – Next Generation Government Technology Infrastructure and Services*, ed. J. H. Janssen (Cham: Springer, 2017), 283–298.

¹⁵ Lykidis, Ioannis, George Drosatos, and Konstantinos Rantos. 2021. "The Use of Blockchain Technology in e-Government Services" *Computers* 10, no. 12: 168.

¹⁶ A. Alketbi, Q. Nasir, y M. A. Talib, "Blockchain for Government Services — Use Cases, Security Benefits and Challenges," en 2018 15th Learning and Technology Conference (L&T), Jeddah, Saudi Arabia, 2018, 112-119.

Según Ramos, sobre la implementación de tecnologías P2P y hashing criptográfico destaca sus ventajas, como la promoción de un acceso más inclusivo y transparente a la información, mejorando la seguridad e integridad de los datos en el contexto ecuatoriano. Sin embargo, enfrenta desafíos como la necesidad de adaptación a marcos legales locales, superar la brecha digital, y la resistencia al cambio institucional. Estas tecnologías requieren un enfoque coordinado para su implementación exitosa, incluyendo capacitación y consideración de la sostenibilidad de las soluciones tecnológicas.¹⁷

El análisis de iniciativas globales de economía colaborativa y tecnologías P2P, como las descritas por Bauwens, ofrece una perspectiva comparativa valiosa para entender el potencial de estas tecnologías en el contexto ecuatoriano. En efecto, Bauwens resalta que la contribución de las redes P2P a la justicia y sostenibilidad a nivel mundial; en Ecuador, la implementación de tecnologías similares en el acceso a la información pública refleja desafíos y oportunidades únicas. Este análisis comparativo subraya la importancia de adaptar estrategias globales a las condiciones locales, enfatizando la necesidad de considerar aspectos culturales, legales y tecnológicos específicos para maximizar los beneficios de las redes P2P y el hashing criptográfico en la promoción de un acceso más democrático y seguro a la información pública.¹⁸

Este estado del arte ha explorado el potencial y los desafíos de las tecnologías P2P y hashing criptográfico en el acceso a la información pública en Ecuador, destacando ejemplos globales y nacionales que ilustran su viabilidad y áreas de mejora. La implementación de estas tecnologías en Ecuador presenta una oportunidad única para mejorar la transparencia, seguridad y eficiencia, a pesar de los retos significativos relacionados con la seguridad, la adaptación legal y la brecha digital. La investigación futura deberá enfocarse en estrategias concretas para superar estos obstáculos, aprovechando las lecciones aprendidas a nivel internacional y adaptándolas al contexto ecuatoriano para fomentar un sistema de acceso a la información pública más inclusivo y democrático.

¹⁷ J. Ramos, M. Bauwens, y V. Kostakis, “P2P and Planetary Futures,” en *Critical Posthumanism and Planetary Futures*, ed. D. Banerji y M. R. Paranjape (Nueva Delhi: Springer, 2016), 193–214.

¹⁸ M. Bauwens y P. Jandrić, “The Seeds of The Commons: Peer-to-Peer Alternatives for Planetary Survival and Justice,” *Postdigital Science and Education* 3, no. 2 (2021): 575–591.

4. MARCO NORMATIVO. —

En el contexto internacional, el derecho al acceso a la información pública y la libertad de expresión están consagrados por instrumentos clave como la Declaración Universal de Derechos Humanos y la Convención Americana sobre Derechos Humanos. El Artículo 19 de la Declaración Universal de Derechos Humanos establece que todo individuo tiene derecho a la libertad de opinión y expresión, lo cual incluye el derecho a no ser molestado por sus opiniones y a buscar, recibir y difundir información e ideas sin consideración de fronteras y por cualquier medio de expresión.¹⁹ Asimismo, el Artículo 13 de la Convención Americana sobre Derechos Humanos afirma el derecho de toda persona a la libertad de pensamiento y expresión, que incluye la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras y por el medio de su elección.²⁰

La Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública se propone como un estándar ideal para los Estados miembros de la OEA, constituyendo un ejemplo de soft law en el ámbito de los derechos humanos. Este documento guía la implementación de políticas de transparencia, enfatizando la importancia de la accesibilidad, la rendición de cuentas y la difusión proactiva de la información. Recomienda un marco para el tratamiento de las excepciones, subrayando que deben ser limitadas y claramente definidas para no obstruir el acceso a la información.²¹ Como ley modelo, su adopción no es obligatoria, pero sirve como referencia para los países en la elaboración o reforma de sus legislaciones nacionales sobre acceso a la información, buscando equilibrar la transparencia gubernamental con la protección de otros intereses legítimos.

En la República del Ecuador, el acceso a la información pública se erige como un derecho constitucional, tutelado bajo la normativa jurídica y principios de transparencia y legalidad. En la Constitución de la República del Ecuador, el artículo 18.2 establece el acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información, excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos

¹⁹ Artículo 19, Declaración Universal de Derechos Humanos, París, 10 de diciembre de 1948, ratificada por Ecuador el 10 de diciembre de 1948.

²⁰ Convención Americana sobre Derechos Humanos, San José, 22 de noviembre de 1969, ratificada por Ecuador el 28 de diciembre de 1977.

²¹ Organización de los Estados Americanos (OEA). (2020). Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública. Washington, D.C.: OEA.

humanos, ninguna entidad pública negará la información²²; el Artículo 91 establece firmemente la acción de acceso a la información pública, permitiendo a los ciudadanos solicitar información que haya sido denegada, parcialmente concedida o cuestionable en cuanto a su veracidad, sin importar la clasificación de confidencialidad previamente atribuida a dicha información²³. Este artículo configura un pilar fundamental para garantizar la democracia y el control social sobre las instituciones y actos gubernamentales.

Dentro de este marco, la Ley Orgánica De Transparencia y Acceso a La Información Pública establece principios fundamentales como la publicidad, transparencia y rendición de cuentas, así como la gratuidad del acceso a la información pública, especificados en el Art. 5, que aboga por la máxima publicidad y el acceso libre a la información en posesión de entes obligados, sujeto a un régimen claro y preciso de excepciones definidas por ley²⁴.

Además, se define como información pública todo tipo de dato contenido en documentos en cualquier formato, bajo la responsabilidad de las instituciones públicas y sujetos definidos por la ley, asegurando su disponibilidad de manera inmediata a través de mecanismos de difusión legal o a petición de parte, mediante un proceso administrativo claro²⁵.

La LOTAIP profundiza el texto constitucional, delineando el marco legal específico para el acceso a la información, instaurando procedimientos claros para la solicitud de información²⁶ y estableciendo límites para la publicidad de la información²⁷. Además, esta ley detalla las causales y el procedimiento a seguir en caso de denegación de la información²⁸, incluyendo las sanciones pertinentes y el recurso de acceso a la información²⁹, un mecanismo de defensa que los ciudadanos pueden emplear en el escenario de un incumplimiento.

Adicionalmente, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional reafirma estos derechos y procedimientos, especialmente en su Capítulo V, Artículos 47 y 48, los cuales fortalecen los mecanismos de protección del acceso a la información y detallan la acción de acceso a la información pública. Estos artículos proveen

²² Artículo 18, Constitución de la República del Ecuador, R.O. 449, 20 de octubre de 2008.

²³ Artículo 91, CRE, 2008.

²⁴ Artículo 5, LOTAIP.

²⁵ Artículo 6, 32, 33 y 34; LOTAIP, 2023.

²⁶ Artículo 19, LOTAIP, 2023.

²⁷ Artículo 20, LOTAIP, 2023.

²⁸ Artículo 21, LOTAIP, 2023.

²⁹ Artículo 22, LOTAIP, 2023.

un marco para la acción legal cuando la información es inaccesible, ya sea por denegación directa o indirecta, o cuando la información suministrada es incompleta o alterada, incluyendo el acceso a información clasificada como secreta o reservada.³⁰

El corpus normativo ecuatoriano e internacional, por tanto, se cimienta sobre un equilibrio entre la promoción de la transparencia y el derecho de acceso a la información, frente a la necesidad de proteger ciertos datos por razones de seguridad nacional o privacidad. En el contexto de las tecnologías P2P y el hashing criptográfico, la implementación de estos sistemas debe ser cuidadosamente balanceada para cumplir con estos estándares legales, asegurando que se mantenga la integridad y confidencialidad de la información pública/judicial, mientras se potencia su accesibilidad y fiabilidad.

Este marco normativo se convierte en una guía para cualquier propuesta tecnológica que busque innovar en el acceso a la información pública; ya que no solo debe alinearse con los principios legales existentes, sino que también debe ser lo suficientemente flexible para adaptarse a la dinámica evolución del entorno digital y las expectativas de una sociedad cada vez más informada y conectada.

5. Consideraciones sobre las redes P2P y la Información pública. —

Podría en un primer momento el suponerse que es necesario un análisis detallado de toda la legislación ecuatoriana para la aplicación de las Redes P2P, no obstante, este no es el caso; dado que este tipo de redes es inherentemente transparente, de código abierto, anónimo, y de un significativo bajo coste en comparación a cualquier sistema privativo³¹, este estudio asume una aproximación más focalizada.

Comenzaremos explicando cómo las características técnicas de este sistema no comprometen información identificable de los usuarios que podrían incurrir en vulneración de derechos, y posteriormente las disposiciones legales relacionadas con el manejo de la información pública.

Así, se evalúa detenidamente cómo las redes P2P pueden alinearse y potenciar los principios del acceso a la información pública consagrada en la legislación del Ecuador,

³⁰ Artículos 47 y 48, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, R.O. Suplemento 52 de 22 de octubre de 2009.

³¹ Li, Jin. “On Peer-to-Peer (P2P) Content Delivery.” *Peer-to-Peer Networking and Applications* 1 (2008): 45–63.

buscando la conformidad legal y explorar las ventajas que tales redes ofrecen para mejorar la accesibilidad y la gestión de la información pública.

Una red peer-to-peer o P2P en su definición es un sistema de conexión entre computadoras donde todos los participantes comparten y acceden a recursos directamente, sin necesidad de un servidor central. Cada computadora en la red puede actuar como cliente y servidor al mismo tiempo, facilitando el intercambio de archivos o servicios de manera eficiente, siendo así expliquemos la definición con esta analogía³²:

Un fanático de la tecnología, siempre va a un almacén a conseguir nuevos e interesantes aparatos. Con el tiempo, las filas y la cantidad de clientes del almacén crean tiempos de espera excesivos, y servicio poco atento, por lo que ha decidido con un grupo de entusiastas, intercambiar las piezas de tecnología que necesiten, así en lugar de ir al almacén, entre los entusiastas hacen un intercambio directo y veloz.

Entendido así, el almacén representa cualquier institución pública, a menudo sobrecargada y lenta en la entrega de información. Y el grupo de entusiastas representa la red P2P, ofreciendo una forma descentralizada de intercambio eficaz, eliminando cuellos de botella. Por último, cada entusiasta, en este caso, se llama nodo, actuando simultáneamente como alguien que busca información, el cliente; y como alguien que la provee, el servidor. De esta manera, con este ejemplo, se representa cómo funciona una red básica P2P³³.

Una vez entendidas las Redes P2P, debemos entender qué tipo de información podemos intercambiar, y aunque parezca una obviedad, la información pública tiene una diversidad de alcances, y estos alcances son de menester importancia para aplicar una red P2P en Ecuador.

La LOTAIP define a la información pública como aquella que emana o que está en poder de instituciones, organismos, y entidades tanto públicas como privadas que participan del Estado o son concesionarios de este, incluyendo organizaciones de trabajadores, instituciones de educación superior que perciban rentas del Estado, y organizaciones no gubernamentales³⁴.

³² Schollmeier, R. "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications." En *Proceedings First International Conference on Peer-to-Peer Computing*, 101–102. Linköping, Sweden, 2001.

³³ *Id.*

³⁴ Artículo 4, LOTAIP, 2023

Y a su vez, la misma ley define como información no pública como la información pública personal que no está sujeta al principio de publicidad, derivada de derechos personalísimos y fundamentales. También, no se permite el acceso a información clasificada como reservada por razones de defensa nacional o establecida en otras leyes vigentes³⁵. Un último elemento es que la solicitud de acceso a la información no obliga a las entidades a crear o producir información con la que no dispongan o no tengan obligación de contar³⁶.

Además, es esencial mencionar las categorías especiales presentadas en la Ley Orgánica de Protección de Datos Personales, se consideran categorías especiales de datos personales que son sensibles, los de niños, niñas y adolescentes, datos de salud, y datos de personas con discapacidad y de sus sustitutos en relación con la discapacidad³⁷. En ese sentido, el tratamiento de datos personales que son sensibles está prohibido a menos que se presente alguna de las circunstancias especiales establecidas en la ley, como el consentimiento del titular de la información, la necesidad de cumplir obligaciones legales específicas, o para proteger intereses vitales del titular entre otros casos³⁸.

En este sentido, en el contexto de las redes P2P, este tipo de información, que no está abarcada en la definición de la LOTAIP, requiere un manejo cuidadoso para no generar una vulneración en cuanto a estos datos personales no públicos.

Y siendo así las categorías de información como las define la Ley Orgánica de Protección de Datos Personales, por su tratamiento especial y extenso, hace prudente para este estudio, delimitar el tipo de información pública de la que se dotara a las redes P2P, por lo que, se usará la definición de información pública conforme a la LOTAIP.

Con esta consideración, podemos así enmarcar el tipo de información podemos dotar a las redes P2P.

6. Redes P2P en la Información Pública. —

Ahora, entendido cómo funciona una Red P2P básica, y de qué información pública podemos dotarla para el intercambio entre los nodos. Las preguntas que salen a la luz son:

³⁵ Artículo 6 y 17, LOTAIP, 2023

³⁶ Artículo 19 y 20, LOTAIP, 2023

³⁷ Artículo 47, Ley Orgánica de Protección de Datos Personales [LOPDP], R.O. Suplemento 459 de 26 de mayo de 2021.

³⁸ Artículo 48 y 49, LOPDP, 2021

¿Realmente esto mejora el acceso a la información pública, que es el gran problema jurídico de esta tesis? Y ¿Cómo funcionaría esto en el sistema ecuatoriano?

Para responder a cabalidad a cada duda, enmarquemos casos palpables de la realidad ecuatoriana. En octubre del 2019, la Contraloría fue incendiada y dio como resultado la pérdida de varios documentos y expedientes de diferente índole³⁹. Esta catástrofe es un caso de estudio ilustrativo de las vulnerabilidades inherentes a los sistemas centralizados de almacenamiento de información. La pérdida de expedientes no solo significó un revés administrativo, sino que también puso en evidencia cómo eventos inesperados pueden desencadenar crisis de información con amplias repercusiones legales y sociales.

Esto no muestra más, que lo riesgoso que es tener documentación de forma centralizada y en archivos físicos, pues de afectarse la institución, la información podría perderse, generando una violación clara de derechos de las personas o pérdidas irreversibles para el Estado. En un caso menos extremo, no son ajenos al conocimiento público, las filas largas, pérdidas de documentos y los procesos redundantes para poder obtener algo tan simple como una copia certificada⁴⁰.

En ambos ejemplos, la aplicación de una Red P2P supera los problemas y brinda varias ventajas:

6.1. Descentralización. —

Una red P2P no se puede eliminar como una entidad centralizada y física como la Contraloría General del Estado, al menos no en el mismo sentido.

El tema de la robustez de las redes P2P, va en gran medida correlacionado a sus nodos; mientras más nodos haya, más difícil será eliminar la información que estos posean⁴¹. Volvamos a la analogía de los entusiastas de la tecnología: mientras más grande sea el grupo de entusiastas, más probable será que uno encuentre lo que esté buscando, y por ende, más

³⁹ “Jueza Ana Guerrón llama a juicio a 27 procesados por el incendio del edificio de la Contraloría.” Contraloría General del Estado. 31 de marzo de 2021. <https://www.contraloria.gob.ec/SalaDePrensa/ComunicadosDePrensa/23952>.

⁴⁰Erika Machasilla, Renato Jaramillo Paredes, y Dorian Flores Aguilera. "Estadísticas de Producción Judicial: Metodología." *Dirección Nacional de Estudios Jurimétricos y Estadística Judicial*, agosto de 2023.

⁴¹ Schleinzer, Benjamin, y Nobukazu Yoshioka. 2010. “A Security Pattern for Data Integrity in P2P Systems.” En *Proceedings of the 17th Conference on Pattern Languages of Programs (PLOP '10)*, artículo 17, 1–5. New York, NY, USA: Association for Computing Machinery.

difícil que uno no encuentre algo que necesite⁴². Entonces, si algunos miembros se van del grupo, no termina por afectar de forma significativa la facilidad de encontrar lo que uno u otro entusiasta necesite. En ese sentido, mientras más nodos haya, más información compartida hay, y así la dificultad para afectar la información aumenta.

Esta ventaja de no tener la información en un solo lado, es el más grande beneficio de la descentralización de las Redes P2P, superando por mucho la seguridad del papel y cajón de las instituciones estatales físicas.

6.2 Eficacia. —

El ámbito de la información pública que delimitamos con anterioridad, también tiene alcances en la función judicial, pues muchos documentos públicos por su condición van vinculados a una variedad de procesos judiciales, la Constitución del Ecuador establece los principios de inmediatez, celeridad, buena y economía procesal⁴³. Si bien, están poco claros los alcances de esos principios y merecerían su propio análisis individualizado, es claro que el espíritu de la ley es generar procesos lo más eficaces posible.

Entendido esto, las redes P2P representan una mejora significativa en la eficiencia y seguridad para el acceso a la información pública. A diferencia de los sistemas tradicionales, que a menudo sufren cuellos de botella y largas esperas, las redes P2P hacen posible una distribución y acceso más rápido a la información gracias a su estructura descentralizada. Recordemos la analogía de los entusiastas: cuantos más usuarios o nodos participen en la red, más eficiente será el intercambio de información. Esta eficiencia no solo disminuye el tiempo de espera innecesario, sino que a su vez brinda una resistencia superior a ataques cibernéticos⁴⁴. Los sistemas centralizados son vulnerables a interrupciones, que pueden dejar sin disponibilidad a los usuarios a información crucial por horas. En contraste, la naturaleza propia de las redes P2P asegura la accesibilidad de la información, incluso frente a intentos de comprometer o sabotear la red, protegiendo así los derechos de la ciudadanía.

⁴² Liben-Nowell, David, Hari Balakrishnan, y David Karger. 2002. "Analysis of the Evolution of Peer-to-Peer Systems." *En Proceedings of the Twenty-First Annual Symposium on Principles of Distributed Computing (PODC '02)*, 233–242. New York, NY, USA: Association for Computing Machinery.

⁴³ Artículo 75 y 169, CRE, 2008

⁴⁴ Belenkiy, Mira, Melissa Chase, C. Chris Erway, John Jannotti, Alptekin Küpçü, Anna Lysyanskaya, y Eric Rachlin. 2007. "Making P2P Accountable Without Losing Privacy." *En Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society (WPES '07)*, 31–40. New York, NY, USA: Association for Computing Machinery.

6.3 Costes. —

Aunque las dos ventajas anteriores, son los elementos de más peso en la argumentación a favor de las redes P2P, un elemento fundamental son los costes. Una red P2P en su naturaleza es open source, es decir, código libre y sin costes, lo que implica que el uso del mismo no implica una compra o algún tipo de propiedad, lo que nos evita muchos costes⁴⁵.

Ejemplifiquemos con una página web. Una página web tiene el coste del dominio y alojamiento, es decir, el nombre de la página web y la cantidad de espacio que ocupa. Y por supuesto, como se mencionó en el punto anterior, como la información está en un mismo lugar, es vulnerable a ciberataques⁴⁶, aunque estos ataques son mitigables con empresas de seguridad, esto de nuevo vuelve a tener otro coste.

En el caso de las Redes P2P, el sistema no requiere costes de dominio, o alojamiento, pues cada nodo cumple dicha función. No obstante, si el Estado quiere generar nodos en sus instituciones, en este caso es evidente que habría costes. Aun así, son varios los gobiernos que, a pesar de usar un sistema P2P, donde gran cantidad de nodos se encuentran sus instituciones, las ventajas son claras sobre los costes de sistemas privados y centralizados⁴⁷.

7. Problemas de las Redes P2P en la Información Pública. —

Si bien, la cantidad de ventajas respecto a las redes P2P es evidente en la mejora del derecho a la información, tampoco está exenta de riesgos y consideraciones, por igual, las más relevantes son:

7.1 Integridad de la Información Pública. —

El artículo 10 de la LOTAIP, menciona que debe garantizarse que la información no se altere o corrompa en el proceso de compartir archivos⁴⁸. Esto, por supuesto, implica nuevos desafíos.

⁴⁵ Aziz, Hayder, James Gao, Paul Maropoulos, y Wai M. Cheung. 2005. "Open Standard, Open Source and Peer-to-Peer Tools and Methods for Collaborative Product Development." *Computers in Industry* 56, no. 3: 260–271.

⁴⁶ Dasgupta, Rumpa, Amin Sakzad, and Carsten Rudolph. 2021. "Cyber Attacks in Transactive Energy Market-Based Microgrid Systems" *Energies* 14, no. 4: 1137

⁴⁷ Baig, Mirza Jabbar Aziz, M. Tariq Iqbal, Mohsin Jamil, and Jahangir Khan. 2022. "A Low-Cost, Open-Source Peer-to-Peer Energy Trading System for a Remote Community Using the Internet-of-Things, Blockchain, and Hypertext Transfer Protocol" *Energies* 15, no. 13: 4862.

⁴⁸ Artículo 10, LOTAIP, 2023

El primer problema son las inconsistencias de las versiones, múltiples versiones de un mismo documento modificado por los usuarios puede ser problemático⁴⁹, pues no podemos tener certeza de qué versión del documento es el documento certificado útil y verdadero, esto sumado a ser una red descentralizada dificulta llevar un rastreo de los cambios, y en su defecto, este mismo riesgo hace posible que haya modificaciones malintencionadas del archivo que se busca.

Según los artículos 7 y 13 de la LOTAIP, la información debe ser clara y accesible, lo que puede ser desafiante en redes P2P si la información se fragmenta o distribuye, de manera que dificulte la comprensión o localización por parte de los usuarios.

7.1.1 Malware y ataques cibernéticos. —

Un tipo de modificación maliciosa a la información en las redes P2P, es la de contaminar el archivo con algún tipo de programa malicioso⁵⁰, la descentralización de la red P2P, hace más accesible repartir contenido malicioso sin poder rastrearse por el inherente anonimato y descentralización de este tipo de redes.

Otro tipo de modificación, ahora, es en los nodos de la red. Las computadoras partícipes de la red pueden ser afectadas. Afectar una serie de nodos puede hacer finalmente que sea de imposible acceso⁵¹, o se corrompa en varios ámbitos la información.

7.1.2 Privacidad y Robo. —

Un elemento que merece una aclaración es la privacidad de la información, puesto que de acuerdo con el Artículo 6 de la LOTAIP, la información personal es confidencial⁵². Sin embargo, es pertinente tratarlo en este apartado, pues no implica un riesgo real.

Al tratarse de información pública, con las delimitaciones de los capítulos anteriores, no amerita ninguna preocupación que esté al acceso de propios y extraños. En ese mismo

⁴⁹ Pamies-Juarez, Lluís, Marc Sanchez-Artigas, Pedro García-López, Rubén Mondéjar, y Rahma Chaabouni. 2014. "On the Interplay between Data Redundancy and Retrieval Times in P2P Storage Systems." *Computer Networks* 59: 1–16.

⁵⁰ Damiani, Ernesto, Sabrina De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, y Fabio Violante. 2002. "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks." *En Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*, 207–216. New York, NY, USA: Association for Computing Machinery.

⁵¹ Zhang, P., Jiao, X., y Zhou, R. 2011. "Network Security Technology in P2P." En *Advanced Research on Computer Science and Information Engineering*, editado por G. Shen y X. Huang, 153–162. *Communications in Computer and Information Science*, vol. 153. Berlin, Heidelberg: Springer.

⁵² Artículo 6, LOTAIP, 2023

sentido, la idea de robo de documentación de las redes P2P, no representa un riesgo significativo, pues no tendría sentido el robo de información de índole pública.

El análisis comparativo de este apartado brindan importantes guías para lograr abordar las soluciones para adaptar estas tecnologías a las necesidades específicas del contexto ecuatoriano, maximizando así los beneficios mientras se minimizan los riesgos asociados, de este modo, resulta claro poder abordar las soluciones a las problemáticas expuestas.

8. Soluciones a la problemática de las Redes P2P en la Información Pública. —

Una vez tratados los desafíos más relevantes en la aplicación de un sistema de redes P2P, resulta necesario poder abordar las soluciones tomando en cuenta que sean más eficaces que el modelo actual ecuatoriano.

8.1 Respecto a la Integridad de la Información Pública. —

8.1.1 Centralizar las redes P2P. —

La primera solución parece desnaturalizar la inherente condición de descentralización de las Redes P2P⁵³, no obstante, en una infraestructura centralizada, un servidor principal puede implementar y hacer cumplir políticas de seguridad, realizar chequeos de integridad regulares, y autenticar los documentos antes de su distribución, evitando así, modificaciones maliciosas o virus.

Aunque esta solución es de diversa complejidad y costo variable, al aplicarse a un sistema libre, gratuito y no privativo, no resulta tan oneroso en comparación a otros sistemas privativos, debido a que los sistemas totalmente no privativos eliminan la necesidad del pago de licencias de uso costosas, permitiendo la modificación y adaptación del sistema sin restricciones financieras adicionales. Y a su vez, manteniendo el acceso de la información sin filas y horas de espera largas del modelo tradicional. No obstante, la mejor respuesta, parece cimentarse en un sistema mixto⁵⁴, es decir, un sistema centralizado que estén en varias instituciones del Estado, donde siendo el Ecuador un país con varias instituciones públicas,

⁵³ Kim, Jung-Tae, Hae-Kyeong Park, y Eui-Hyun Paik. 2005. "Security Issues in Peer-to-Peer Systems." En *The 7th International Conference on Advanced Communication Technology*, 2005, ICACT 2005, 1059–1063. Phoenix Park, Korea (South).

⁵⁴ Tsybulnik, N., K. W. Hamlen, y B. Thuraisingham. 2007. "Centralized Security Labels in Decentralized P2P Networks." En *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*, 315–324. Miami Beach, FL, USA.

esta propuesta mixta, puede evitar costes⁵⁵, o situaciones de vulneración de derechos como el caso de la Contraloría General del Estado.

8.1.2 Sistemas de Control de Versiones. —

A diferencia del punto anterior, en este caso el Estado, no es quien administra las redes P2P, manteniendo así estas últimas, sus cualidades descentralizadas; sin embargo, son sus órganos quienes ahora cumplen solo la función de revisión del control de cambios⁵⁶, pero no de administración. Esto aunque de bajo costo, la escalabilidad puede ser preocupante si la cantidad de archivos escala de sobremanera, a pesar de esto, esta solución presenta costo menor que el punto anterior, evitando los mismos riesgos.

8.1.3 Sistemas de Verificación en Documentos. —

Las opciones menos onerosas en su implementación, necesariamente mantienen la cualidad inherente de descentralización de las P2P, por su bajos requerimientos de administración, por lo que, buscar una solución de verificación de la información subida a la red P2P, resulta más viable que una administración centralizada o un sistema de verificación de versiones, es decir, es más fácil subir exclusivamente archivos verificados, que administrar o implementar un sistema de revisión de versiones en una red P2P. De este modo, se disminuye riesgos al solo dotar la red P2P con archivos que fueron previamente verificados. Hay varias opciones para hacer esto, y las iremos repasando en cada párrafo, de la más onerosa a la menos onerosa.

Blockchain⁵⁷, la tecnología de cadena de bloques, funciona como un libro contable digital público, accesible para todos, pero inmutable una vez que la información ha sido inscrita, es decir, es un tipo de red P2P. Se compone de bloques de datos encadenados cronológicamente, cada uno protegido y vinculado al anterior mediante técnicas criptográficas. Este enfoque garantiza la integridad y seguridad de la información almacenada, ya que modificar cualquier bloque requeriría alterar toda la cadena en múltiples ubicaciones simultáneamente, una tarea casi imposible dada la naturaleza distribuida de la cadena.

⁵⁵ *Ib.*

⁵⁶ Leitao, J., L. Rosa, y L. Rodrigues. 2008. "Large-Scale Peer-to-Peer Autonomic Monitoring." En *2008 IEEE Globecom Workshops*, 1–5. New Orleans, LA, USA.

⁵⁷ Laurence, T. 2023. *Blockchain for Dummies*. John Wiley & Sons.

Por ello, la cadena de bloques es ideal para registrar transacciones financieras como las de Bitcoin, o cualquier otro tipo de datos que se desee preservar de forma segura y permanente sin la posibilidad de modificaciones o eliminaciones no autorizadas. Sin embargo, su alto coste administrativo y complejidad técnica⁵⁸, al tratarse de documentación pública, resulta excesivo.

Protocolos de Comunicación Seguros⁵⁹, el uso de protocolos de comunicación seguros, como el *Secure Sockets Layer* y el *Transport Layer Security* son una práctica estándar para garantizar la seguridad en el intercambio de documentos y datos a través de Internet. Estos protocolos cifran la información durante su transmisión, lo que impide que terceros no autorizados puedan acceder o interceptar los datos enviados entre dos sistemas, esto por supuesto garantiza la seguridad y autenticidad de los archivos, pero igualmente a un costo de inversión y necesidad de mantenimiento constante⁶⁰, pero menor que el blockchain.

Firmas digitales⁶¹, las firmas digitales son una tecnología de cifrado que permite verificar la autenticidad e integridad de un mensaje, documento o archivo digital. Funcionan como la versión electrónica de una firma manuscrita o sello estampado, pero con beneficios adicionales en términos de seguridad proporcionados por la criptografía.

Si bien, esta solución es habitual en el tráfico jurídico en el Ecuador, no deja de depender de empresas privadas de terceros que tramitan el proceso de las firmas.

Finalmente, el hashing criptográfico⁶², un sistema de bajo costo y baja complejidad, es un proceso en el que se toma un documento digital y se procesa a través de un algoritmo criptográfico para producir un valor de cadena única llamado hash, es decir, se convierte un archivo en una serie de números y letras única, que se lo conoce como hash. Entonces, cualquier modificación del documento generará un hash diferente. Siendo un método

⁵⁸ Coutinho, K., Wongthongtham, P., Abu-Salih, B., Abu Saleh, M. A., y Khairwal, N. K. 2022. "Carbon Emission and Cost of Blockchain Mining in a Case of Peer-to-Peer Energy Trading." *Frontiers in Built Environment* 8: 945944.

⁵⁹ Zhang, H. 2014. *A Peer-to-Peer Security Protocol for the Internet of Things: Secure Communication for the SensibleThings Platform*. Dissertation.

⁶⁰ Zhang, H. 2014. *A Peer-to-Peer Security Protocol for the Internet of Things: Secure Communication for the SensibleThings Platform*. Dissertation.

⁶¹ Paucar, J. M. P., Flores, D. F. C., y Morillo, J. R. C. 2024. "Análisis de la regulación de firmas electrónicas en América Latina: un enfoque comparativo." *Dilemas contemporáneos: Educación, Política y Valores*.

⁶² Dionicio, P. O. G., Gil, A. J. L., y De Los Santos, A. C. M. 2023. "Principales técnicas criptográficas aplicadas a la seguridad de la información en IoT: una revisión sistemática." *Ingenio Tecnológico* 5.

sumamente simple y barato, sin necesidad de requisitos varios como las soluciones anteriores, se presenta como una excelente propuesta⁶³.

Además, no agrega peso extra al documento, a diferencia de otras técnicas como las firmas digitales que añaden más información. Y, a diferencia de la cadena de bloques, no requiere de una red complicada y costosa para funcionar. En esencia, el hashing es una forma rápida, eficiente y de bajo mantenimiento para mantener los documentos seguros y sin alteraciones⁶⁴.

9. Parámetros Legales en Ecuador sobre las Soluciones de las Redes P2P. —

En el siguiente apartado, trataremos la aplicación del sistema propuesto tomando casos de éxito, y analizándolo en el sistema ecuatoriano, junto a las especificidades del caso y la concordancia con la legislación de mismo.

9.1 Sistema P2P en Ecuador. —

El uso de tecnologías como el P2P en el Ecuador puede resultar conflictivo en muchos casos, especialmente por la curva de aprendizaje de todos los sectores para su uso, no obstante, su uso a nivel estatal y mundial muestran varios casos de éxito, resulta pertinente a este punto, antes de presentar una propuesta para el caso ecuatoriano, repasar brevemente el uso exitoso de esta tecnología a nivel estatal:

Comenzando con el caso de Estonia⁶⁵, país que es frecuentemente citada como líder en la digitalización de su gobierno. A través de su programa e-Estonia, ha implementado una serie de servicios digitales basados en la tecnología de blockchain, que es una forma de sistema P2P. Esto incluye seguridad cibernética, e-Residency, y servicios de salud digital.

Georgia implementó la tecnología blockchain en su sistema de registro de tierras. Esto permitió al gobierno aumentar la transparencia y reducir significativamente el fraude y la corrupción en el registro y transferencia de propiedades⁶⁶. La utilización de esta tecnología, que se basa en principios P2P para validar y registrar transacciones, ha sido vista como un

⁶³ Dionicio, P. O. G., Gil, A. J. L., y De Los Santos, A. C. M. 2023. “Principales técnicas criptográficas aplicadas a la seguridad de la información en IoT: una revisión sistemática.” *Ingenio Tecnológico* 5.

⁶⁴ *Id.*

⁶⁵ A. Ojo y S. Adebayo, “Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries,” en *Government 3.0 – Next Generation Government Technology Infrastructure and Services*, ed. J. H. Janssen (Cham: Springer, 2017), 283–298.

⁶⁶ Spessot, A., y Tabares, F. 2023. “Tecnología aplicada a la protección de los derechos sociales fundamentales: algunas experiencias en Argentina, Colombia, España y Georgia.” *Revista Derecho* 7: 109–131.

caso exitoso de cómo los gobiernos pueden utilizar sistemas descentralizados para mejorar la eficiencia y la confianza en los procesos administrativos.

Finalmente, el gobierno de Dubái anunció su intención de usar blockchain para hacer que todos sus documentos gubernamentales sean accesibles digitalmente para el año 2020. Aunque el proyecto está en curso, el objetivo es utilizar la tecnología para mejorar la eficiencia, reducir el papeleo y aumentar la satisfacción del ciudadano. La iniciativa incluye diversos sectores, desde la seguridad hasta los servicios de salud y educación⁶⁷.

Estos casos muestran una buena guía de las ventajas y posibilidad de la aplicación de las Redes P2P en el Ecuador, aun ejemplificando los riesgos en capítulos anteriores, se mantiene como una opción viable con ventajas varias, por ende, los siguientes apartados tratarán sobre la aplicación para el caso ecuatoriano, tomando de referencia lo analizado en los capítulos anteriores, haciendo énfasis en el marco normativo correspondiente.

9.2. Propuesta del Sistema para Ecuador. —

Una vez enmarcado los riesgos técnicos y sus soluciones, como la aplicación del sistema P2P con un sistema de hashing criptográfico, profundicemos en el estándar normativo ecuatoriano, que esbozado rápidamente en los riesgos de la privacidad de los datos en las redes P2P; hay diversos requisitos que merecen su análisis pormenorizado y detallado para la aplicación en Ecuador.

La LOTAIP en su artículo primero nos plantea que el sistema deberá garantizar el acceso libre y sin restricciones a la información pública, salvo las excepciones específicas de la ley⁶⁸. Esto implica que cualquier documento o dato compartido a través de la red debe ser accesible para el público en general, promoviendo la transparencia y el acceso a la información.

Bien, siendo claros estos requisitos, se hará el análisis bajo las propuestas del sistema que tenemos hasta ahora, es decir, ¿La red P2P con hashing criptográfico, es accesible para el público general, promueve la transparencia y el acceso a la información?

⁶⁷ Ummah, R. S., y Sofyani, H. 2024. “Testing the Intention of Employees in Local Government to Adopt Blockchain Technology in Accounting Information Systems (AIS).” *Public Accounting and Sustainability* 1 (1): 1–18.

⁶⁸ Artículo 1, LOTAIP, 2023

Cuando hablamos de accesibilidad y acceso a la información en el Ecuador en temas digitales, hablamos necesariamente de la brecha digital⁶⁹, tema que merece su propio apartado, no obstante no es ajeno el país, al uso de herramientas digitales de consulta de datos, ejemplos varios como GOB.ec, para diversidad de trámites y su aplicativo web que permite tener documentación digital como cédulas y licencias de conducción; El Sistema Informático de Trámite Judicial, que sirve para la consulta de procesos judiciales; o el Sistema Único de Pensiones Alimenticias⁷⁰, donde el usuario puede consultar deudas y pagos de pensiones alimenticias. Estos son ejemplos de sistemas digitales complejos y robustos, por lo que, una Red P2P con hashing criptográfico, siendo mucho menos complejo, para la consulta y gestión de información pública se presenta como un paso lógico y manejable dentro de este progreso tecnológico.

El siguiente elemento de la transparencia, es mucho más fácil de ilustrar, ejemplos como el E-SATJE, por su característica de sistema centralizado, dado que su funcionamiento, o su código fuente⁷¹ no están al alcance del usuario común, decisión razonable por parte del Estado, pues no resultaría prudente permitir a los posibles atacantes saber cómo funciona esta herramienta, situación distante al caso de las Redes P2P, que por su condición de difícil vulneración, logra hacer que su funcionamiento y configuración este al acceso del público general, sin implicar un riesgo significativo en su funcionamiento. Además, este mismo elemento de transparencia, logra hacer posible las auditorías privadas, logrando que cada persona natural o jurídica pueda en cualquier momento hacer rendición de cuentas al Estado⁷².

Continuando, el artículo 6 de la LOTAIP menciona que aunque la red P2P debe facilitar el acceso a la información, también debe incorporar mecanismos para proteger la información personal, asegurando que los datos sensibles no sean accesibles o identificables de manera que violen la privacidad de los individuos.

⁶⁹ Jadan, B. E. V., Vivar, S. A. M., y Rivera, D. P. P. 2023. “Explorando la brecha digital en el acceso tecnológico y su influencia en la educación: abordando las diferencias entre comunidades.” *Dilemas Contemporáneos: Educación, Política y Valores*.

⁷⁰ Yuquilema, J. C. P., Márquez, J. D. S., Nieto, L. E. B., y Romero, G. A. R. 2023. “Innovación en la gestión pública y open government.” *Polo del Conocimiento: Revista científico-profesional* 8 (9): 1219–1233.

⁷¹ Mora Bernal, Adriana Elizabeth, Sánchez Sarmiento, Marcela Paz, Cajamarca Torres, Andrea Estefanía, y Idrovo Torres, Diego Francisco. 2022. “El sistema automático de trámite judicial en Ecuador: ¿vulnera derechos fundamentales?” *Revista chilena de derecho y tecnología* 11 (1): 203–228.

⁷² Artículo 2, LOTAIP, 2023

Respecto a este punto, nuevamente la calidad de información pública, nos blindamos respecto a vulneraciones sobre la información personal, no obstante, merece la pena analizarse cómo no es posible este tipo de riesgos⁷³. Dada la condición descentralizada de las redes P2P, esto nos permite no hacer reconocible al usuario de la red, garantizando anonimato⁷⁴, que si bien logra evitar recopilar datos personales de los usuarios, en ese mismo sentido hace difícil la identificación a los usuarios malintencionados, que buscan dañar la red como se explicó en el capítulo de los riesgos. A pesar de esto, esta modalidad de total anonimato, inherente de la red como tal, y siendo un estándar muy alto en la protección de datos personales, no implica que esto pueda modificarse al gusto, pues un principio legal lógico es el de “el que puede lo más, puede lo menos⁷⁵”, y siendo así, es sensato que si el sistema puede tener un estándar tan alto de privacidad, pueda disminuirse sin mayor complicación, dando paso a un sistema de recopilación de datos mínima, como estadísticas de uso o similares.

El siguiente artículo que nos incumbe es el artículo 7 y 8 de la LOTAIP donde nos menciona que el sistema debería ser capaz de difundir una amplia gama de información pública de manera organizada y actualizada, incluyendo datos sobre la estructura organizativa, directorio de la institución, remuneraciones, servicios ofrecidos, contratos, auditorías, sobre la posibilidad de rendición de cuentas, y además la facilitación de la participación ciudadana⁷⁶.

Sobre este requisito estructural, cabe mencionarse que se refiere a la organización de la red y su interfaz, es decir, qué es lo que verá el usuario y qué tan fácil será usar el sistema para el usuario, aunque es verdad que las redes P2P pueden tener un aspecto rudimentario⁷⁷ y de difícil entendimiento, esto es fácilmente superable, pues no implica más que una cuestión técnica de presentación de la información, aun así algunos ejemplos de redes de fácil

⁷³ Kumar Sharma, P., Gosain, D., & Diaz, C. 2023. "On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies." En *The Network and Distributed System Security Symposium*. Internet Society.

⁷⁴ *Id.*

⁷⁵ Macías, A. I. 2023. "Las lagunas normativas constitucionales: su integración mediante argumentos lógicos y cuasilógicos." *Cuadernos electrónicos de filosofía del derecho no. 48*: 271-313.

⁷⁶ Artículo 7 y 8, LOTAIP, 2023

⁷⁷ Munasinghe, L. M., Gunawardhana, T., Wickramaarachchi, N. C., & Ariyawansa, R. G. 2023. "Peer-to-Peer Accommodation User Experience: Evidence From Sri Lanka." *SAGE Open 13 (4)*: 21582440231199324.

uso son los ejemplos de los Estados de Georgia⁷⁸ o Estonia⁷⁹. Entendido así, este punto no es más que un elemento estilístico técnico, por lo que, no requiere mayor análisis.

Finalmente, el último punto que nos interesa es el artículo 10, que aborda la seguridad e integridad de la información⁸⁰, riesgo crucial en nuestro análisis, como se explicó en capítulos anteriores, el hashing criptográfico ahora emerge como solución destacada frente a este desafío. El hashing criptográfico proporciona una manera eficiente de asegurar y verificar que la información permanezca inalterada, lo cual es esencial para mantener la confianza en la integridad de los datos distribuidos a través de la red⁸¹.

Dado que el hashing criptográfico funciona con cualquier tipo de archivo, y bajo un hash irrepetible, entendido por hash el resultado de un algoritmo de hashing, que es un proceso que toma una cantidad de datos de entrada como un archivo y produce una cadena de caracteres de longitud fija. Donde esta cadena, o valor del hash, actúa como una huella digital de los datos de entrada. Si los datos de entrada cambian lo más mínimo, el valor de hash resultante cambiará de manera apreciable. O en palabras sencillas, un hash es una secuencia única de letras y números irrepetibles a través de un conjunto de reglas matemáticas para transformar el archivo que se necesite, y garantizar su integridad. Siendo esto así, el requisito del artículo 10, se cumple a cabalidad en razón de poder el sistema garantizar la autenticidad de la información pública.

El análisis, a este punto, da luces de que las condiciones técnicas y legales en el Ecuador se corresponden la modelo propuesto de la implementación de Redes P2P con hashing criptográfico para el acceso y mejora del acceso a la información pública, sin embargo, en ese sentido, también es de menester importancia, hacer otras consideraciones para la aplicación del sistema en Ecuador.

9.3 Otros Instrumentos Legales. —

Una última consideración es acerca de la Ley Orgánica para la Transformación Digital y Audiovisual, esta última presenta un marco legal que impulsa la modernización y

⁷⁸ Spessot, A., y Tabares, F. 2023. "Tecnología aplicada a la protección de los derechos sociales fundamentales: algunas experiencias en Argentina, Colombia, España y Georgia." *Revista Derecho* 7: 109–131.

⁷⁹ A. Ojo y S. Adebayo, "Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries," en *Government 3.0 – Next Generation Government Technology Infrastructure and Services*, ed. J. H. Janssen (Cham: Springer, 2017), 283–298.

⁸⁰ Artículo 10, LOTAIP, 2023

⁸¹ Masood, R., Pandey, N., & Rana, Q. P. 2023. "Towards P2P dynamic-hash-table-based public auditing for cloud data privacy, security and integrity." *International Journal of Cloud Computing* 12 (1): 72-89.

digitalización de servicios, promueve la inclusión digital y la seguridad de la información, y demanda una mayor transparencia a través de la implementación de tecnologías. Mientras la LOTAIP marca las garantías del derecho del acceso a la información pública, definiendo la base legal para la transparencia y la rendición de cuentas; la Ley de Transformación Digital y Audiovisual se enfoca en cómo la tecnología y la innovación pueden potenciar y modernizar este acceso, y es apropiada la consideración de los principios fundamentales de esta última.

La Ley de Transformación Digital y Audiovisual, tiene 4 ámbitos claves a destacar. En su artículo 1⁸² establece los objetivos generales de la ley, incluida la simplificación y adopción de medios y tecnologías digitales en la prestación de servicios públicos y la mejora regulatoria, junto al artículo 21⁸³ donde se hace énfasis en la publicidad y transparencia de la administración pública y la obligación de las entidades gubernamentales de transmitir en vivo sus sesiones, estos dos artículos acerca eficacia y transparencia se corresponde a los objetivos de la propuesta de las redes P2P tratadas.

El segundo ámbito clave son los artículos 2, 17 y 18⁸⁴, donde se expande la idea de un gobierno digital, definido como la simplificación de trámites, participación ciudadana por medios electrónicos, gobierno de TIC, identidad digital, y el ecosistema compuesto por actores públicos y privados que apoyan la implementación de iniciativas digitales. Estos elementos que nos interesan, ven dada su utilidad en el sentido de la ampliación conceptual que proveen estos artículos para entender el marco en el que se inserta la transformación digital, y guiar propuestas como las redes P2P.

El tercer ámbito que nos interesa es el marco regulatorio para la transformación digital, de acuerdo a los artículos 7 y 22⁸⁵; si bien este texto académico ha hecho un análisis de las leyes vigentes, es pertinente aclarar que en el caso de implementarse los sistemas propuestos, la necesidad de un marco normativo propio, y un sistema de pruebas, *sanbox* como usa el término la Ley Orgánica para la Transformación Digital y Audiovisual, es una consideración que hay que destacar. Dicha consideración debe servir como guía conceptual

⁸² Artículo 1, Ley Orgánica para la Transformación Digital y Audiovisual [LTDA], R.O. Suplemento 245 de 7 de febrero de 2023.

⁸³ LTDA, artículo 21, 2023.

⁸⁴ LTDA, artículo 2, 17, y 18, 2023

⁸⁵ LTDA, artículo 7 y 22, 2023.

a la futura aplicación de un sistema P2P como el que ha sido propuesto, pero dado que este punto refiere a analizar elementos técnicos, y hacen referencia a la creación de marcos legales, o sistemas de pruebas futuros, resulta excesivo continuar la investigación, pues este superaría el análisis de los derechos y garantías vigentes en la legislación.

El cuarto y último ámbito que nos interesa es acerca de la inclusión digital, este punto es variopinto, y sus consideraciones van más allá del plano legal o político, a pesar de ello, repasar la normativa respecto al tema no deja de ser prudente y necesario para nuestro tema, en los artículos 2 y 34⁸⁶ se hace referencia a la cultura e inclusión social, incluyendo elementos de educación digital, es decir, establece que en el caso de crear nuevas propuestas digitales para el Estado, la necesidad de la implementación de un plan educacional debe ir a la par. Este punto en particular nos interesa de sobremanera, pues a diferencia de los anteriores elementos que nos presentan un marco de ejes rectores para posibilidades futuras, o la regulación legal para la aplicación de un sistema supuesto, la falta de inclusión digital es un riesgo palpable y actual que puede vulnerar los derechos de la ciudadanía, esta disparidad de inclusión nos es de especial importancia, dado que el éxito de las ventajas propuestas en este texto, solo son significativas si el sistema es usado en masa, por lo que, resulta necesario analizar las implicaciones de esta falta de inclusión en su propio apartado.

9.4. Brecha Tecnológica. —

La brecha tecnológica se refiere a la disparidad entre individuos, hogares, empresas o regiones geográficas en cuanto a su acceso a las tecnologías de la información y comunicación, así como en su capacidad de utilizar estas tecnologías eficazmente. Esencialmente, describe la diferencia entre quienes tienen acceso efectivo a la tecnología digital y a la información que esta proporciona, y quienes tienen un acceso limitado o nulo. Esta brecha puede ser el resultado de varios factores, incluyendo diferencias socioeconómicas, educativas, geográficas y demográficas. La brecha tecnológica también se relaciona con conceptos como la alfabetización digital y la inclusión digital, que se centran en la habilidad para usar la tecnología y en la igualdad de acceso, respectivamente⁸⁷.

⁸⁶ LTDA, artículo, 2 y 34, 2023.

⁸⁷ Reyes, José Alfredo Padilla, y Claudia Díaz Pérez. 2022. "Brechas tecnológicas entre países desarrollados y América Latina." Tesis de Maestría, Maestría en Economía, Gestión y Políticas de la Innovación, Universidad Autónoma Metropolitana, Ciudad de México, México.

Aunque hemos examinado las ventajas y riesgos propios de la tecnología P2P y su concordancia con la legislación ecuatoriana, la eficacia de cualquier sistema tecnológico depende de su accesibilidad y utilidad a la población⁸⁸. Dado que, el espíritu de este texto es presentar una solución para mejorar la eficacia y el acceso a la información pública, resulta pertinente poder ver por medio de indicadores cómo podría impactar esta tecnología.

Según datos del Instituto Nacional de Estadística y Censos⁸⁹, en el Ecuador solo el 62.2% de hogares tienen acceso a internet, es decir, 3.124.763 familias; dando como resultado un total de 1.897.443 familias que no poseen algún acceso a Internet⁹⁰; por supuesto, esto no solo muestra una brecha tecnológica, sino en materia de derechos⁹¹.

Siendo así la situación de gran parte de la población, es evidente que las instituciones tradicionales de filas y largas horas de espera, no solo toman relevancia, sino que se vuelve la única forma de la población para lograr garantizar sus derechos en cuanto a procesos, acceso a la información, justicia y demás.

Pareciera entonces, en un primer momento, que la propuesta de las redes P2P con la implementación de hashing criptográfico de este texto, cae no por sus desventajas propias, sino por su limitación en su accesibilidad, pero esta conclusión podría ser precipitada y no del todo precisa.

Aun considerando solo el 62.2% de familias con acceso a Internet, la aplicación de la propuesta descrita tendría un impacto más que significativo en la descongestión⁹² de los servicios públicos y sus respectivas instituciones. Si la población con acceso a Internet comienza a usar herramientas como las redes P2P descritas, ayudaría y mejoraría la celeridad de los procesos públicos del grupo población sin acceso a Internet.

Entonces, a pesar de la clara brecha tecnológica en el país, la solución descrita en el texto, aun así, figura como un importante aliado en la garantía y mejora, no solo del derecho

⁸⁸ *Id.*

⁸⁹ Instituto Nacional de Estadística y Censos (INEC). 2023. "Tecnologías de la Información y Comunicación." Julio 2023.

⁹⁰ Instituto Nacional de Estadística y Censos (INEC). 2023. "Tecnologías de la Información y Comunicación." Julio 2023.

⁹¹ *Nota: Se uso los indicadores de familia, debido a que no sería apropiado hablar del acceso individual, pues un mismo dispositivo electrónico es multipropósito y puede beneficiar a una pluralidad de miembros de una familia.*

⁹² Dangaiso, P., Mukucha, P., Makudza, F., Towo, T., Jonasi, K., & Jaravaza, D. C. 2024. "Examining the Interplay of Internet Banking Service Quality, E-Satisfaction, E-Word of Mouth and E-Retention: A Post Pandemic Customer Perspective." *Cogent Social Sciences* 10 (1): 2296590.

al acceso a la información pública, sino indirectamente en la gestión pública estatal de forma general, pues incluso el sector poblacional sin acceso a la misma, logra obtener el resultado de un sistema nacional menos saturado y más eficaz⁹³.

10. Recomendaciones. —

Con anterioridad se trató los posibles riesgos y soluciones de la implementación de este tipo de tecnología en su forma más sencilla, y siendo así, es necesario esbozar las posibilidades del mismo en cuanto a mejoras.

Primero, la tecnología P2P puede no solo ser útil en el campo de la información pública, puede de hecho lograr importantes avances en cualquier ámbito de la información, lograr generar copias certificadas de cualquier tipo de archivo, o documentación personal, tal como cédulas de identidad o licencias de conducir infalsificables con el uso del hashing criptográfico presenta prometedoras ventajas en el futuro.

Segundo, el uso de esta tecnología en procesos judiciales o información no pública. Se explicó en párrafos anteriores que fue necesario delimitar la información pública y de la no pública, debido a que esta última es la más vulnerable en las redes P2P, por la fácil obtención por medio de los usuarios, no obstante, existen redes P2P privadas, que permiten solo a ciertos usuarios acceder a dicha información, esta ventaja tomaría relevancia en causas penales donde el principio de publicidad por claras razones no puede aplicarse y para información no pública considera clasificada.

Tercero, el uso de redes P2P blindadas. Se mencionó como incluso el sistema más simple de una red P2P cumple con las condiciones legales conjunto a la aplicación de un sistema de hashing; sin embargo, esto es el principio, pues complementar el uso de hashing criptográfico con firmas electrónicas, o incluso con tecnología propia del blockchain, son prometedoras alternativas para mantener un sistema seguro.

Cuarto, cada nodo de la red P2P es aquel que busca información, y es también aquel que la provee, ambos partes llamadas nodos. De este modo, en la versión más simple del sistema cada nodo puede tener la información completa, o la información dividida, de este modo, lograr que cada nodo de la red tenga solo una porción fragmentada del archivo, lograría de sobremanera también descongestionar el servicio digital y por supuesto, los

⁹³ Dangaiso, P., Mukucha, P., Makudza, F., Towo, T., Jonasi, K., & Jaravaza, D. C. 2024. "Examining the Interplay of Internet Banking Service Quality, E-Satisfaction, E-Word of Mouth and E-Retention: A Post Pandemic Customer Perspective." *Cogent Social Sciences* 10 (1): 2296590.

usuarios quienes lo usan, de esta forma garantizando una disminución de recursos del sistema de manera general.

Quinto, el uso de este sistema en gobiernos locales, permitiría a la población sin acceso a Internet lograr accesibilidad sin ir a las instituciones gubernamentales principales, haciendo versátil la obtención de información y reduciendo la brecha tecnológica.

Sexto, resulta necesario considerar las mejoras para el usuario, lograr capacitar o generar una interfaz sencilla, ayudaría al cambio y promoción de este tipo de tecnologías.

Séptimo, una evaluación meticulosa del impacto ambiental de la implementación a gran escala, especialmente considerando la sostenibilidad de soluciones como blockchain o similares basadas en tecnología P2P, y a su vez como la descongestión de los sistemas tradicionales puede mejorar la sostenibilidad. La capacidad para interactuar con sistemas ya existentes es clave, asegurando una integración perfecta y una transición suave hacia plataformas más descentralizadas.

Octavo, establecer estrategias inclusivas para cerrar la brecha digital es esencial, y el diseño adaptable de estos sistemas a futuras innovaciones tecnológicas garantizará su escalabilidad, relevancia a largo plazo y garantías en materia de derechos. La formulación de un plan de acción detallado que defina objetivos claros y alianzas estratégicas con entidades académicas y del sector tecnológico contribuirá a un ecosistema más rico y colaborativo, vital para el éxito y la adopción generalizada de la tecnología P2P en la sociedad ecuatoriana.

Noveno, poder identificar las leyes existentes que regulan la protección de datos, la privacidad en línea, y demás para que el sistema P2P no solo se adhiere a estas normativas, sino que también respalda los principios de acceso a la información y transparencia. Además, cualquier propuesta legal nueva o reforma legislativa debe contemplar la dinámica cambiante de la tecnología y cómo la red P2P con hashing criptográfico se inserta en este panorama legal. De este modo, estableciendo mecanismos legales para la resolución de conflictos y la responsabilidad en el uso de las redes P2P, asegurando que los derechos de los usuarios estén debidamente protegidos y que exista un equilibrio justo entre la innovación tecnológica y la regulación.

11. CONCLUSIONES

En el transcurso de esta investigación, se demostró que las redes peer-to-peer (P2P) y el hashing criptográfico poseen un potencial significativo para mejorar el acceso y la gestión

de la información pública en Ecuador. A través del análisis y la síntesis de los principales conceptos y teorías explorados en cada capítulo, esta tesis establece una relación clara y directa entre la implementación de tecnologías descentralizadas y la optimización del derecho del acceso a la información pública.

Se evidenció que, ante los retos presentados por la congestión y demoras en la obtención de documentos públicos, las redes P2P emergen como una solución eficaz gracias a su capacidad para facilitar un intercambio de información más ágil y directo, eliminando así numerosos obstáculos administrativos. Simultáneamente, el uso de hashing criptográfico asegura la integridad y la autenticidad de los datos compartidos, abordando preocupaciones críticas sobre la seguridad y confiabilidad de la información pública disponible.

Además, esta investigación subraya las potencialidades de estas tecnologías para fomentar la transparencia y promover una cultura de rendición de cuentas dentro del sector público, alineándose con los objetivos de fortalecimiento de la estructura democrática y el Estado de derecho. Sin embargo, también se reconoció la existencia de desafíos significativos en su implementación, incluidos aspectos de seguridad, la necesidad de ajustes normativos, y la consideración de la brecha digital en el país. Esta investigación sugiere que, aunque las redes P2P y el hashing criptográfico ofrecen soluciones prometedoras, su aplicación efectiva requiere una estrategia cuidadosa y multifacética que contemple tanto sus ventajas como sus limitaciones.

A lo largo de este estudio, se ha confirmado que la integración de redes P2P y hashing criptográfico constituye una estrategia viable y potencialmente transformadora para el acceso a la información pública en Ecuador. La investigación proporciona una base que respalda la implementación de estas tecnologías, cumpliendo el marco normativo vigente y ofreciendo un camino hacia la mejora de la eficiencia, seguridad y accesibilidad de la información pública.

Finalmente, los resultados obtenidos no solo responden de manera efectiva a la pregunta de investigación planteada, sino que también abren nuevas oportunidades para futuras indagaciones y desarrollos tecnológicos en el ámbito del derecho al acceso a la información pública. Se ha demostrado que, a pesar de los desafíos existentes, la adopción cuidadosa de redes P2P y hashing criptográfico en el contexto legal y social ecuatoriano puede conducir a un acceso más democrático y seguro a la información pública,

estableciendo un precedente valioso para la integración de soluciones tecnológicas avanzadas en la gestión de la información pública.

Este estudio no solo resalta la importancia de una implementación bien considerada, sino que también enfatiza la necesidad de un enfoque inclusivo y adaptativo que maximice los beneficios de estas tecnologías para la sociedad ecuatoriana en su conjunto.