Maestría en

DERECHO DIGITAL

Trabajo de grado previa a la obtención

de título de Magister en Derecho Digital

AUTORES:

ABG. FRANCISCO XAVIER CARRIÓN TORRES

ABG. FREDDY MAURICIO JIMÉNEZ LASCANO

ABG. INÉS PATRICIA VICUÑA PERALTA

ABG. ELMER VLADIMIR ZAMBRANO TINOCO

TUTOR: ROQUE ALBUJA PONCE

Protocolo de Gestión de Riesgos Regulatorios para la protección de los derechos ARCO asociados a la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador

Quito – Ecuador

Diciembre 2023

CERTIFICACIÓN DE AUTORÍA

Nosotros, **FRANCISCO XAVIER CARRIÓN TORRES, FREDDY MAURICIO JIMÉNEZ LASCANO**, **INÉS PATRICIA VICUÑA PERALTA Y ELMER VLADIMIR ZAMBRANO TINOCO** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firmado electrónicamente por:
FRANCISCO XAVIER CARRION TORRES

…..……

FRANCISCO XAVIER CARRIÓN TORRES

Firmado electrónicamente por:
FREDDY MAURICIO JIMENEZ LASCANO

…….

FREDDY MAURICIO JIMÉNEZ LASCANO

Firmado electrónicamente por:
INES PATRICIA VICUNA PERALTA

…….

INÉS PATRICIA VICUÑA PERALTA

Firmado electrónicamente por:
ELMER VLADIMIR ZAMBRANO TINOCO

……..

ELMER VLADIMIR ZAMBRANO TINOCO

APROBACIÓN DEL TUTOR

Yo, ROQUE ALBUJA PONCE certifico que conozco a los autores del presente trabajo siendo la responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido.

_____

ROQUE ALBUJA PONCE

DIRECTOR DE TESIS

Dedicatoria

Dedicamos este trabajo a nuestras familias por su apoyo inquebrantable y amor incondicional. Cada página de este trabajo es un testimonio de sus sacrificios y creencias en nosotros. Esta conquista, más que nuestra, es también suya, un hermoso mosaico de nuestras luchas compartidas y sueños tejidos juntos.

Agradecimientos

Extendemos nuestro agradecimiento a los docentes de la Maestría en Derecho Digital, cuya guía y enseñanzas han sido fundamentales en nuestra formación académica y profesional. Agradecemos a nuestros compañeros de maestría, con quienes compartimos debates enriquecedores y momentos inolvidables, contribuyendo significativamente a nuestro aprendizaje y crecimiento personal. Finalmente, agradecemos a todas aquellas personas que, de una u otra forma, han sido parte de este viaje académico, ofreciéndonos su apoyo, sabiduría y aliento en los momentos más desafiantes de nuestras carreras. Este logro es también un reflejo de su generosidad y apoyo.

ÍNDICE

Lista de Tablas

Lista **de Figuras**

Resumen

El proyecto aborda el problema de cómo los responsables del tratamiento de datos en Ecuador pueden identificar y mitigar riesgos regulatorios relacionados con los derechos ARCO (acceso, rectificación, cancelación/eliminación y oposición), en el marco de la Ley Orgánica de Protección de Datos Personales. El objetivo es desarrollar un protocolo integral para mejorar la identificación, evaluación y mitigación de riesgos en el manejo de datos personales. La metodología de investigación combinó un análisis hermenéutico con encuestas a individuos y entidades, proporcionando una visión completa sobre la situación actual de la protección de datos en Ecuador. Los resultados evidencian una notable falta de preparación y conocimiento en la gestión de datos personales, resaltando la urgencia de implementar protocolos efectivos y programas de capacitación. La recomendación de integrar la tecnología blockchain se identificó como una solución prometedora para reforzar la seguridad, transparencia y eficiencia en la gestión de los derechos ARCO. Este enfoque innovador destaca el potencial de la blockchain para transformar la gestión de datos personales, asegurando una mayor protección y cumplimiento de los derechos individuales. El trabajo proporciona un modelo aplicable y replicable en otros contextos que enfrentan desafíos similares en la gestión de datos personales. Este proyecto subraya la necesidad de un enfoque proactivo y basado en la tecnología para la protección de datos personales, algo especialmente crítico en el actual contexto digital.

Abstract

The project addresses the problem of how data controllers in Ecuador can identify and mitigate regulatory risks related to ARCO rights (access, rectification, cancellation/deletion and opposition), within the framework of the Organic Law on the Protection of Personal Data. The objective is to develop a comprehensive protocol to improve the identification, evaluation and mitigation of risks in the management of personal data. The research methodology combined a hermeneutical analysis with surveys of people and entities, providing a complete vision of the current situation of data protection in Ecuador. The results show a significant lack of preparation and knowledge in the management of personal data, highlighting the urgency of implementing effective protocols and training programs. The recommendation to integrate blockchain technology was identified as a promising solution to improve security, transparency and efficiency in the management of ARCO rights. This innovative approach underlines the potential of blockchain to transform personal data management, ensuring greater protection and compliance with individual rights. The work provides a model that is applicable and replicable in other contexts facing similar challenges in managing personal data. This project emphasizes the need for a proactive and technology-based approach to the protection of personal data, especially critical in the current digital context.

Capítulo 1

i. Introducción

En la actualidad, caracterizada por su enfoque digital, se ha vuelto crucial salvaguardar la privacidad y protección de los datos personales. Este estudio se enfoca en la creación de un protocolo dirigido a la gestión de riesgos normativos, poniendo especial énfasis en los derechos ARCO según lo dicta la Ley Orgánica de Protección de Datos Personales en Ecuador. Este trabajo se distingue por su habilidad para proporcionar una estructura clara y efectiva en la identificación, evaluación y mitigación de riesgos regulatorios, elementos clave para proteger derechos individuales y reforzar la confianza en los entornos digitales.

El propósito principal de esta investigación radica en formular un protocolo exhaustivo para la gestión de riesgos normativos, centrado en los derechos ARCO dentro del marco de la LOPDP ecuatoriana. Proponemos la integración de la tecnología blockchain como un medio para mejorar la seguridad y transparencia, potenciando así la gestión de riesgos y la observancia efectiva de los derechos ARCO.

Este aspecto del estudio adquiere relevancia dada la creciente atención hacia el uso de blockchain para intensificar la seguridad y claridad en múltiples áreas, incluida la protección de datos personales. La exploración de esta tecnología abre camino para aplicaciones prácticas y futuros avances en la protección de datos.

El problema central que este estudio se formula ¿Cómo pueden los responsables del tratamiento de datos personales en Ecuador identificar y mitigar los riesgos regulatorios vinculados a los derechos ARCO?. La hipótesis propuesta sostiene que el protocolo diseñado será una herramienta efectiva para facilitar la implementación de la LOPDP, con especial atención a los derechos ARCO.

Este estudio se divide en cuatro secciones principales y anexos, cada sección se centra en diferentes aspectos clave del tema, contribuyendo integralmente al progreso de la investigación. El primer capítulo introduce el tema, definiendo su contexto y relevancia en el campo de gestión de riesgos regulatorios y los derechos ARCO en Ecuador. Aquí, se examina en profundidad el problema central del estudio, enfocándose en la identificación y mitigación de riesgos regulatorios por parte de las entidades encargadas, y se definen los objetivos concretos de la investigación.

El segundo capítulo aborda el método hermenéutico para interpretar las normativas relacionadas con los derechos ARCO, incluyendo un análisis detallado de literatura relevante y evaluación crítica del uso de blockchain en el marco legal existente. Además, se incluye un análisis basado en encuestas a individuos y entidades jurídicas sobre los derechos ARCO y la percepción de blockchain en la protección de datos.

En el tercer capítulo, se presentan y analizan los resultados de la investigación, determinando cómo estos apoyan o contradicen la hipótesis propuesta y se elabora el protocolo detallado, resaltando su importancia en la gestión de riesgos regulatorios y los derechos ARCO.

Finalmente, el cuarto capítulo presenta un resumen de los principales descubrimientos y aprendizajes obtenidos del estudio. Se enfatiza la importancia y aplicabilidad de estos hallazgos, subrayando su contribución al campo de la protección de datos personales. Además, se formulan recomendaciones basadas en los resultados de la investigación, destinadas tanto a futuras investigaciones académicas como a la práctica profesional en la esfera de salvaguarda de la información privada. Este capítulo cierra el trabajo de titulación, ofreciendo una perspectiva integral y orientaciones para futuros desarrollos en el campo.

ii. Problema de la Investigación

En el marco de la protección de datos, los riesgos regulatorios se refieren a la posibilidad de no cumplir con las normativas legales, especialmente en el contexto de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador. Estos riesgos son críticos en cuanto a los derechos ARCO (acceso, rectificación, cancelación/eliminación y oposición), que son clave para asegurar la independencia y el control personal sobre la propia información privada. La no observancia de estas normativas no solo puede llevar a sanciones legales para las organizaciones, sino también minar la confianza y seguridad de quienes poseen los datos..

El cumplimiento efectivo de los derechos ARCO exige una gestión proactiva y consciente de los riesgos regulatorios. Es imperativo que los responsables del tratamiento de datos personales comprendan y se adapten sus acciones administrativas y técnicas a los requisitos de la LOPDP para proteger estos derechos. La urgencia de esta situación se magnifica en un entorno digital en permanente cambio, donde la probabilidad de infracciones en la seguridad de los datos personales y las violaciones a la privacidad es considerablemente alta.

Ante este panorama, surge la necesidad de desarrollar un protocolo específico que guía a los responsables de datos personales en la identificación, evaluación y mitigación de riesgos regulatorios relacionados con los derechos ARCO. Este protocolo serviría como una herramienta para garantizar que las organizaciones no solo cumplan con la ley, sino que también promuevan una cultura de respeto y protección de los datos personales. Según autores como Kuner et al. (2020), la implementación de protocolos y directrices claras es esencial para navegar en el complejo escenario legal y ético de la protección de datos (p. 53).

La tecnología blockchain presenta una oportunidad única para reforzar el protocolo de gestión de riesgos, especialmente en lo que respeta a la transparencia y seguridad de los procesos de tratamiento de datos personales. Como argumenta Mougayar (2016), blockchain

ofrece una infraestructura descentralizada y segura que puede ser vital en la verificación y trazabilidad de las operaciones de datos, asegurando así la protección de los derechos ARCO (p. 78).

Elaborar un protocolo para la gestión de riesgos regulatorios centrado en los derechos ARCO constituye una medida esencial y adecuada frente a los retos contemporáneos en el campo de la protección de datos en Ecuador. Incorporando tecnologías de vanguardia como blockchain, este protocolo puede elevar notablemente la eficiencia y seguridad en el manejo de la información personal. Esto no solo asegura la adhesión a la LOPDP, sino que también aumenta la confianza del público en las entidades y empresas encargadas del manejo de estos datos

iii. Objetivos

Objetivo General

Elaborar un protocolo integral de gestión de riesgos regulatorios enfocado en los derechos ARCO al amparo de la Ley Orgánica de Protección de Datos Personales de Ecuador, incorporando la tecnología blockchain para fortalecer la identificación, evaluación y mitigación de riesgos en el tratamiento de datos personales.

Objetivos Específicos

- Analizar la LOPDP de Ecuador para entender disposiciones claves relacionadas con los derechos ARCO.
- Examinar los riesgos regulatorios asociados a los derechos ARCO en Ecuador.
- Crear estrategias para abordar y reducir riesgos, asegurando la protección efectiva de los derechos ARCO.
- Incorporar la tecnología blockchain en el protocolo para mejorar seguridad, transparencia y eficiencia.
- Establecer sistemas de supervisión y evaluación para el protocolo.

- Elaborar programas de capacitación sobre la importancia y manejo adecuado de los derechos ARCO y la aplicación del protocolo.

Capítulo 2

i. Metodología

Método Hermenéutico

En este estudio se adoptó el enfoque hermenéutico para una evaluación minuciosa de las leyes, regulaciones y literatura académica relevante. Este método permitió un análisis profundo sobre cómo estas normativas inciden en la gestión de riesgos regulatorios y en la protección de los derechos ARCO. También se exploró el papel y las posibles restricciones de la tecnología blockchain en el marco legal y normativo actual. Paralelamente, se realizó una comparación de las prácticas en Ecuador con las de otros países en materia de riesgos regulatorios y protección de datos, enfatizando el empleo de la tecnología blockchain.

Recopilación de Datos Prácticos

Se realizaron encuestas diseñadas para personas naturales y jurídicas que abordaron temas específicos relacionados con los derechos ARCO y la percepción sobre el uso de blockchain en la protección de datos.

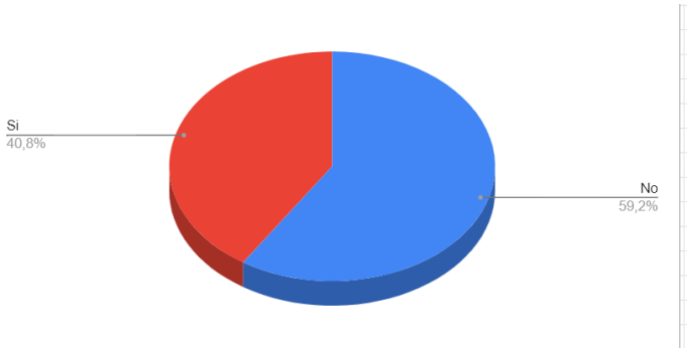
Encuesta Dirigida a personas naturales

Se realizó una encuesta anónima para recopilar datos relevantes a la gestión de riesgos regulatorios y la Ley Orgánica de Protección de Datos Personales en Ecuador. La confidencialidad de las respuestas se garantizó, asegurando su uso exclusivo para fines de investigación académica en el contexto del estudio.

Pregunta 1 ¿Está familiarizado/a con los derechos ARCO (acceso, rectificación, cancelación y oposición) en relación con sus datos personales?

Figura 1

Gráfica de la Pregunta 1 Dirigida a Personas Naturales



Pregunta 2 ¿Ha ejercido alguno de sus derechos ARCO con respecto a sus datos personales?

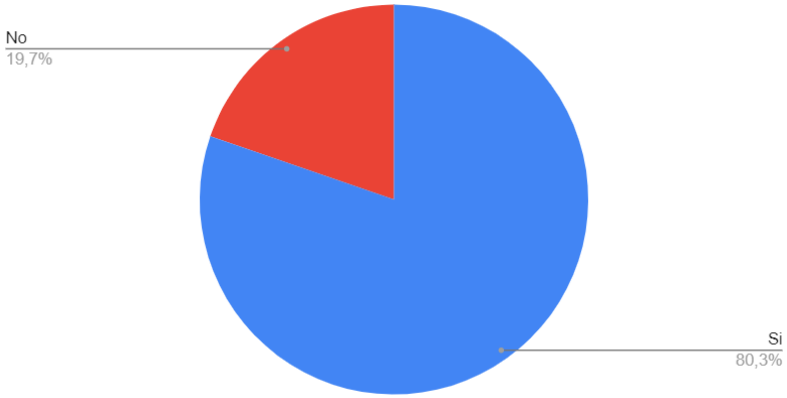
Figura 2

Gráfica de la Pregunta 2 Dirigida a Personas Naturales

Pregunta 3 ¿Considera que existe un riesgo regulatorio (legal) en la protección de sus datos personales?

Figura 3

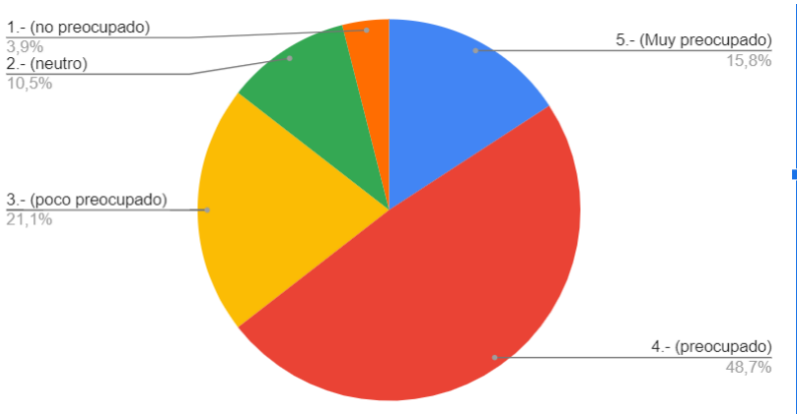
Gráfica de la Pregunta 3 Dirigida a Personas Naturales



Pregunta 4 ¿Cómo calificaría su nivel de preocupación sobre los riesgos legales en el uso y manejo de sus datos personales en el entorno digital? (1: No preocupado, 5: Muy preocupado)

Figura 4

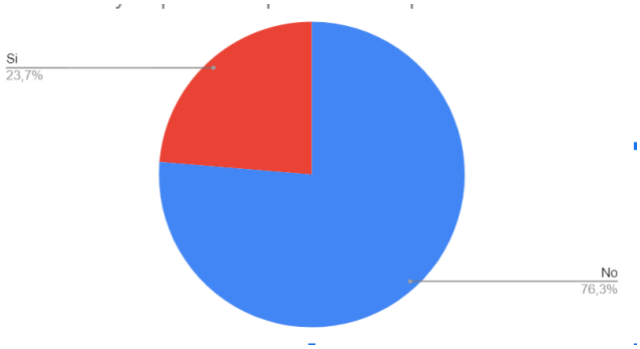
Gráfica de la Pregunta 4 Dirigida a Personas Naturales



Pregunta 5 ¿Está familiarizado con la tecnología blockchain y su potencial aplicación en la protección de datos personales?

Figura 5

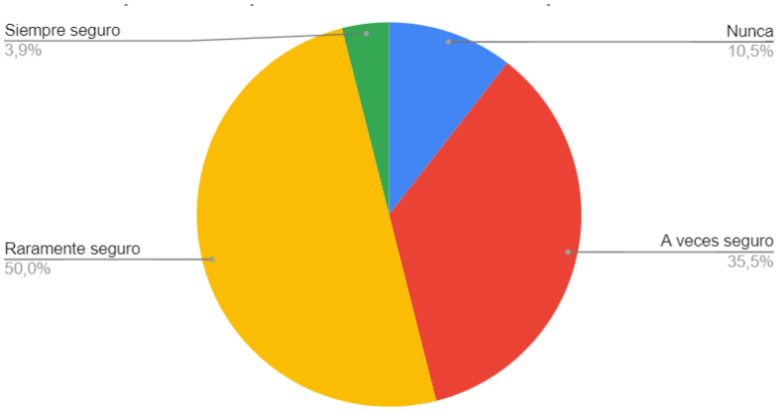
Gráfica de la Pregunta 5 Dirigida a Personas Naturales



Pregunta 6 Al navegar por internet, ¿cuán seguros se siente respecto a la protección de sus datos personales?

Figura 6

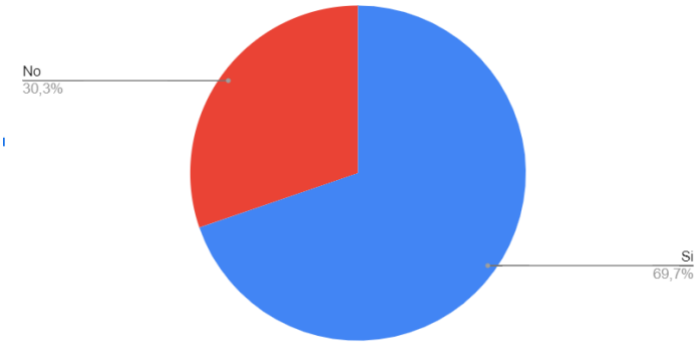
Gráfica de la Pregunta 6 Dirigida a Personas Naturales



Pregunta 7 ¿Ha experimentado alguna situación en la web donde sintió que sus datos personales estaban en riesgo legal?

Figura 7

Gráfica de la Pregunta 7 Dirigida a Personas Naturales



Encuesta Dirigida a personas jurídicas

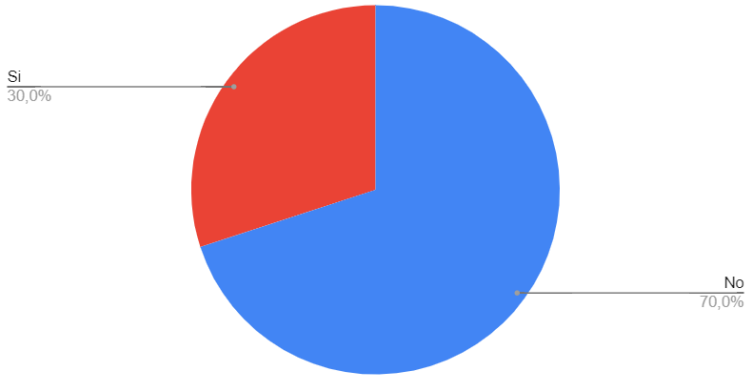
Esta encuesta fue anónima y se realizó con fines de investigación académica sobre el Protocolo de Gestión de Riesgos Regulatorios y la Ley Orgánica de Protección de Datos Personales en Ecuador Sus respuestas fueron confidenciales y el fin es exclusivo para este estudio.

Pregunta 1: ¿Su empresa tiene un protocolo para gestionar los riesgos regulatorios asociados al tratamiento de datos personales, en especial los derechos ARCO (acceso, rectificación, cancelación y oposición)?

Figura 8

Gráfica de la Pregunta 1 Dirigida a Personas Jurídicas

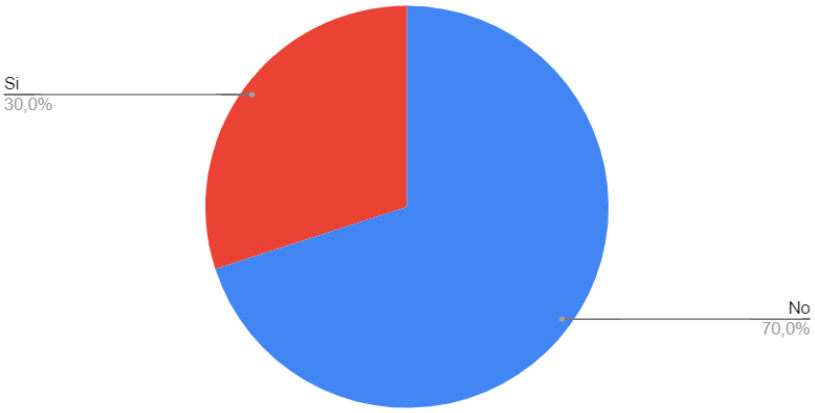
Figura 8
Gráfica de la Pregunta 1 Dirigida a Personas Jurídicas



Pregunta 2: ¿Considera que su empresa está adecuadamente preparada para identificar y mitigar los riesgos asociados al tratamiento de datos personales en el entorno digital?

Figura 9

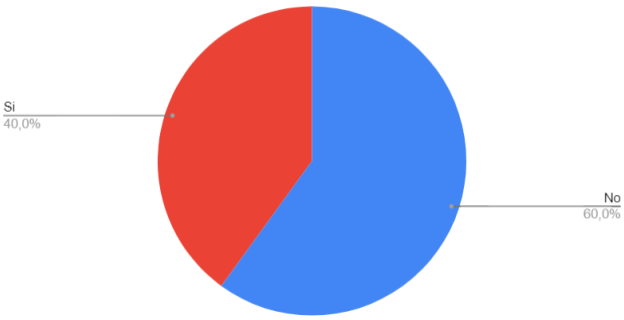
Gráfica de la Pregunta 2 Dirigida a Personas Jurídicas



Pregunta 3 ¿Su empresa utiliza o considera el uso de tecnología blockchain para fortalecer la protección de datos personales?

Figura 10

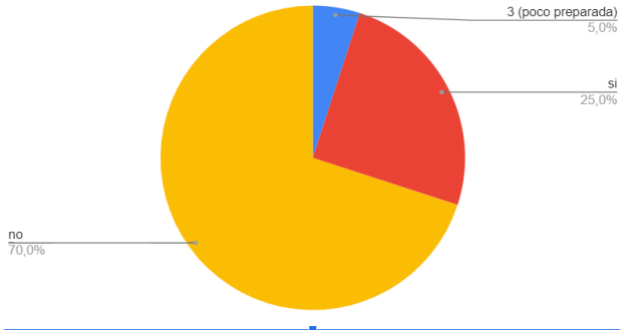
Gráfica de la Pregunta 3 Dirigida a Personas Jurídicas



Pregunta 4: ¿Ha enfrentado su empresa alguna situación donde los derechos ARCO de los titulares de datos personales han sido comprometidos?

Figura 11

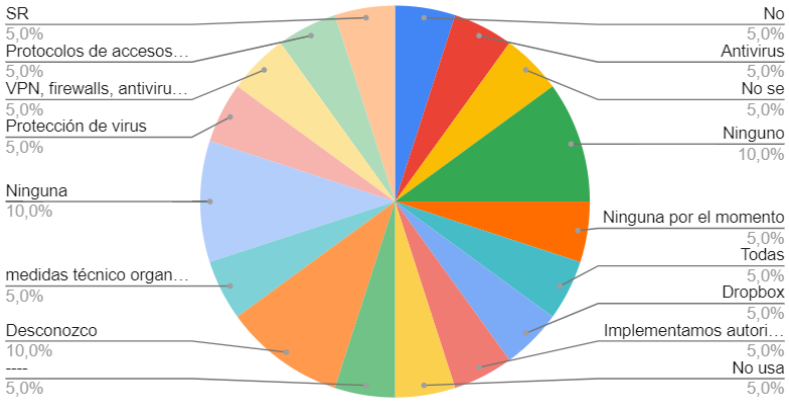
Gráfica de la Pregunta 4 Dirigida a Personas Jurídicas



Pregunta 5 ¿Qué herramientas o soluciones utiliza su empresa para proteger los datos personales en la web y gestionar los riesgos regulatorios (legales)?

Figura 12

Gráfica de la Pregunta 5 Dirigida a Personas Jurídicas



Se recolectó datos sobre el cumplimiento de los derechos ARCO, en países algunos países de Latinoamérica, como se detalla en las figuras a continuación:

México

Figura 13

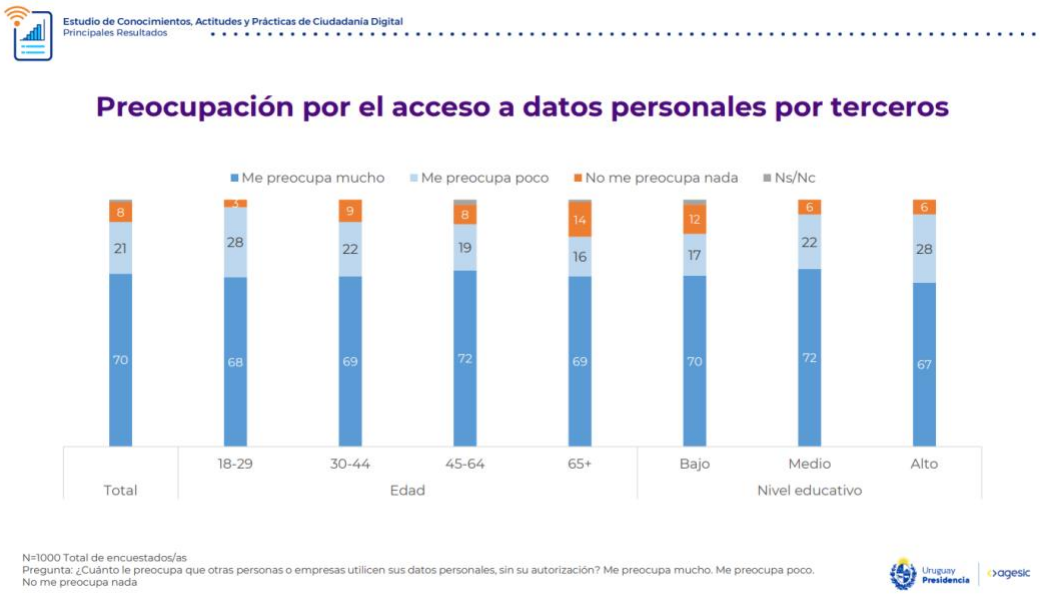
Sujetos Obligados que Cuentan con Medios y Procedimientos para Atender Solicitudes para el Ejercicio de los Derechos ARCO

Nota. Reproducida del Informe anual de resultados 2022 – 2023, Evaluación del desempeño en materia de protección de datos personales Secretaría de Protección de Datos Personales, P. 17.

Uruguay

Figura 14

Preocupación por el Acceso a Datos Personales por Terceros



Nota. Reproducida del Estudio de Conocimientos, Actitudes y Particas de la Ciudadanía Digital, Principales Resultados 2022, s.p.

Perú

Figura 15

Resoluciones de las Solicitudes de Tutela de los Derechos ARCO

Nota. Reproducida del (Transparencia, Acceso a la Información Pública y Protección de Datos Personales - Balance de Gestión 2018 – 2021, p. 14).

ii. Desarrollo

El derecho a la privacidad se remonta a la época romana, marcando un hito en la historia de la protección de datos personales. Este derecho Este derecho ha sido reconocido y protegido en numerosos tratados internacionales y constituciones a lo largo de la historia, destacando su importancia fundamental en la libertad individual

En Estados Unidos, la protección de datos personales ha seguido un enfoque sectorial, centrándose en sectores específicos a través de legislaciones como la "Privacy Act" de 1974. Esta actitud sectorial implica que no existe una legislación omnibus[1], sino una serie de leyes que regulan aspectos concretos de la privacidad y la protección de datos en diferentes áreas como la salud, educación y finanzas (Departamento de Justicia de Estados Unidos, 2015).

[1] El término de ley ómnibus se emplea en diversos países cuando se tiene la necesidad de revisar y ratificar algunas leyes en específico. Esto, por supuesto, es algo que puede suceder en cualquier momento. La definición de la ley ómnibus nos explica que regula a todas aquellas leyes que deberían de estar separadas según su contenido. Así como también puede ratificar los decretos de un mismo contenido. Esta es una ley que ha sido aplicada en diversas ocasiones en varios países del mundo (Economía 3. Santaella J. https://economia3.com/ley-omnibus-caracteristicas/)

En contraste, Europa ha adoptado un enfoque más holístico y regulador en la protección de datos. La Directiva de Protección de Datos de 1995, el primer marco legal significativo de la Unión Europea en este ámbito, se centró en el manejo y la movilidad de los datos personales. Esta Directiva fue sustituida por el Reglamento General de Protección de Datos (RGPD), efectivo desde mayo de 2016 y aplicable desde 2018, estableciendo un conjunto de normas más riguroso y detallado, con penalizaciones más severas para las infracciones en la protección de datos personales (Unión Europea, 1995

La evolución tecnológica y la digitalización han generado nuevos retos en la gestión de datos personales. La recopilación masiva de datos por parte de entidades gubernamentales y privadas ha suscitado preocupaciones significativas sobre la privacidad y la seguridad de la información personal (Parlamento Europeo y Consejo, 2016 numeral 6).

Estos desafíos se han materializado en acuerdos internacionales como el "Safe Harbor" y posteriormente el "Privacy Shield". Estos acuerdos, establecidos entre la Unión Europea y Estados Unidos, intentarán regularmente la transferencia de datos personales desde Europa a Estados Unidos. Sin embargo, el "Safe Harbor" fue invalidado en 2015 por el Tribunal de Justicia de la Unión Europea, debido a preocupaciones sobre el acceso irrestricto de las autoridades estadounidenses a los datos europeos. El "Privacy Shield" fue introducido como un reemplazo en 2016 para ofrecer mayores garantías y un mecanismo de resolución de disputas más robusto para los ciudadanos europeos (Schwartz y Peifer, 2017. ´p.116).

Estos convenios evidencian la necesidad de un balance entre la movilidad libre de los datos personales y su privacidad en un contexto internacional y digital. El abordaje a estos retos es dinámico, ajustándose constantemente a las innovaciones tecnológicas y a una sociedad cada vez más alerta sobre el valor de la protección de su información personal. La progresiva conciencia sobre la seguridad de los datos impulsa la evolución de las respuestas a estos desafíos.

Latinoamérica ha experimentado un desarrollo significativo en la regulación de datos personales, reflejando un aumento en la comprensión sobre la relevancia de la privacidad en el época digital. Ecuador es un ejemplo destacado de este progreso. Con la implementación de la LOPDP, Ecuador busca abordar desafíos específicos en la privacidad digital, tomando inspiración de modelos regulatorios avanzados como el RGPD de la Unión Europea. Esta ley representa un esfuerzo significativo por alinear las prácticas locales de protección de datos con estándares internacionales, reconociendo la importancia de la privacidad y seguridad de la información personal en un mundo cada vez más interconectado (López Carballo, 2021, p.44).

La protección de datos personales se ha convertido en un componente esencial de la economía digital[2] En este contexto, la necesidad de desarrollar protocolos específicos en Ecuador para abordar los riesgos regulatorios asociados a los derechos ARCO es evidente. Estos protocolos son vitales para asegurar que las organizaciones no solo cumplan con la LOPDP, sino que también promuevan prácticas que respeten y protejan la información personal de los ciudadanos. La adopción de tales protocolos permite adaptar la legislación y las prácticas de protección de datos a las particularidades y realidades específicas de Ecuador, garantizando así un equilibrio entre el respeto a los derechos individuales y las necesidades del entorno empresarial y gubernamental (Solange Maqueo & Viecens, 2022; Camacho Gutiérrez & Velásquez Veloza, 2022).

Los derechos ARCO en Ecuador, al igual que en otras jurisdicciones, son fundamentales para empoderar a los ciudadanos, otorgándoles control sobre sus datos

[2] Economía digital se hace referencia a una **economía basada en la tecnología digital, es decir, que toma consistencia mediante las Tecnologías de la Información y la Comunicación (TICs)** y que, con el paso del tiempo, se ha ido mezclando cada vez más con la tradicional hasta el punto de que es complicado distinguir la diferencia entre ellas. Se podría decir que la economía digital se presenta como una **forma novedosa de producción, comercialización y consumo de bienes y servicios**, un proceso complejo que requiere cambios en la organización económica, social y política de los países, pero que actúa como facilitador para su desarrollo y cuyo objetivo es cubrir las necesidades de la sociedad. (Ángela Toro, 2022. https://www.escueladenegociosydireccion.com/revista/business/economia-digital-como-afecta-negocios/)

personales. Estos derechos permiten a los individuos acceder a su información personal, solicitar correcciones, pedir la eliminación de sus datos y oponerse a su tratamiento bajo ciertas condiciones. La LOPDP establece que las empresas y entidades responsables del tratamiento de datos personales en Ecuador tienen la obligación de informar a los titulares sobre el uso que se da a sus datos, en estricto cumplimiento de los principios que consagrada dicha ley. Además, deben obtener el consentimiento necesario para ciertos tratamientos y garantizar que se implementen medidas de seguridad apropiadas para proteger la información y evitar accesos no autorizados, alteraciones o pérdidas. Estas obligaciones subrayan la responsabilidad de las entidades en el manejo de la información personal y refuerzan la necesidad de un enfoque proactivo y transparente en su tratamiento (Asamblea Nacional, 2021, LOPDP).

En América Latina, varios países han establecido organismos supervisores dedicados a garantizar el cumplimiento de las leyes de protección de datos personales, por ejemplo: México, destaca el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI); en Argentina, por su parte posee la Agencia de Acceso a la Información Pública (AAIP), Brasil cuenta con su órgano supervisor que es la Autoridad Nacional de Protección de Datos (ANPD). Estos organismos juegan un papel crucial en la supervisión y regulación del tratamiento de datos personales. En Ecuador, la LOPDP también ha previsto la creación de un organismo de control con responsabilidades similares. Una función clave de este organismo es la supervisión de la administracion de vulnerabilidades de seguridad. De acuerdo con la LOPDP, las empresas tienen la responsabilidad de informar cualquier brecha de seguridad que pueda comprometer la privacidad y seguridad de los datos personales (Asamblea Nacional, 2021, LOPDP, Art. 47). Esta disposición es crucial para preservar la confianza en la protección de los datos personales y asegurar una reacción pronta

y eficiente ante cualquier incidente. Su importancia radica en fortalecer la seguridad de la información personal y en responder adecuadamente a posibles brechas de seguridad.

La Ley Orgánica de Protección de Datos Personales de Ecuador, promulgada en mayo de 2021, junto con su Reglamento General de noviembre de 2023, representan un progreso significativo en la legislación de protección de datos personales para nuestro país. Esta nueva ley introduce derechos fundamentales para los titulares de datos, incluyendo los derechos ARCO, marcando un hito en la protección de la privacidad y la información personal en el país (Asamblea Nacional, 2021, LOPDP). La LOPDP establece principios y obligaciones alineados con los estándares internacionales, como el RGPD de la Unión Europea. Sin embargo, Ecuador enfrenta desafíos únicos en la implementación de estas normas. Estos desafíos incluyen la adaptación de las regulaciones a las realidades locales, la creación de una cultura de protección de datos y la construcción de la infraestructura necesaria para el cumplimiento efectivo de la ley. Además, la falta de una autoridad de control operativo plenamente y la necesidad de educar tanto a las entidades responsables del tratamiento de datos como al público en general son aspectos clave que deben abordarse (Kuner et al., 2020, p.259).

A pesar del avance que representan los derechos ARCO, su aplicación práctica enfrenta desafíos, especialmente en un contexto digital en constante evolución. La legislación contempla situaciones en las que el ejercicio de los derechos ARCO no es factible, como en casos de solicitudes por parte de personas no titulares de los datos o en situaciones donde la ley requiere la revelación de los mismos. Estas excepciones, señaladas en el artículo 18 de la LOPDP, subrayan la necesidad de una simetria entre la protección de datos personales y otros intereses legítimos. Por estas razones es necesario la implementación efectiva de los derechos ARCO, requiere una gestión proactiva y consciente de los riesgos regulatorios. Es fundamental que las entidades comprendan y se adapten a los lineamientos de la LOPDP, especialmente en un entorno digital con altos riesgos de violaciones de datos y abusos de privacidad. Surge así

la necesidad de desarrollar un protocolo específico que guía a los responsables en la identificación, evaluación y mitigación de estos riesgos, promoviendo una cultura de respeto y protección de los datos personales (Kuner et al., 2020, p. 53).

La integración de la tecnología blockchain en este protocolo ofrece una oportunidad única para reforzar la transparencia y seguridad en los procesos de tratamiento de datos personales. Esta tecnología, con su infraestructura descentralizada y segura, es vital para la verificación y trazabilidad de las operaciones de datos, lo que puede ser crucial para avalar la trazabilidad y la seguridad en el manejo de datos personales (Mougayar, 2016, p. 78; Swan, 2015, pág.117). En Ecuador, hay acceso a redes de blockchain públicas y privadas, y varias empresas y organizaciones están fomentando proyectos basados en esta tecnología. Estas entidades pueden facilitar el acceso a blockchain y su aplicación en el contexto de la protección de datos personales.

La incorporación de la tecnología blockchain en el protocolo de gestión de riesgos regulatorios en Ecuador presenta una oportunidad innovadora para modernizar y asegurar la protección de datos personales. Este “distributed ledger”[3] destaca por sus características de transparencia, integridad e inmutabilidad, lo que la convierte en una herramienta valiosa para la gestión de datos personales. Esta tecnología puede fortalecer la seguridad y la trazabilidad de las operaciones de datos, ofreciendo un registro inalterable y transparente de las transacciones y cambios en los datos personales (Mougayar, 2016; Swan, 2015).

La creación de un protocolo de gestión de riesgos regulatorios centrado en los derechos ARCO aborda directamente los desafíos contemporáneos en la protección de datos personales

[3] La Tecnología de Libro Mayor Distribuido, también conocida como DLT (por sus siglas en inglés, Distributed Ledger Technology), compone un conjunto de tecnologías que permiten la creación de una estructura de sistemas que opera como una base de datos no centralizada. A diferencia de las bases de datos tradicionales, donde un servidor central almacena y gestiona toda la información, los sistemas DLT distribuyen y albergan la información en múltiples nodos o participantes dentro de una red. (Bit Lab 2023, https://bitlab.world/que-es-distributed-ledger-technology-dlt/)

en Ecuador. La inclusión de tecnologías avanzadas como blockchain podría mejorar la eficacia y seguridad en el manejo de datos personales, asegurando así el cumplimiento de la LOPDP y fortaleciendo la confianza en las entidades responsables de datos personales.

El riesgo regulatorio, definido por Ángel Garcés Sanagustín (2014) como la posibilidad de cambios en las normativas legales, emerge como una dimensión crítica en la gestión empresarial y personal. La identificación, evaluación y gestión efectiva de estos riesgos son esenciales para salvar la integridad y continuidad de las operaciones. En el contexto de la LOPDP en Ecuador, estos riesgos están asociados principalmente con los derechos ARCO, lo que implica una necesidad de cumplimiento proactivo y consciente por parte de los responsables del tratamiento de datos personales.

El Reglamento General de la LOPDP enfatiza la obligatoriedad de adoptar medidas técnico-administrativas y jurídicas, basadas en el principio de responsabilidad proactiva y demostrada. Este enfoque requiere que las organizaciones no solo cumplan con las normativas, sino que también demuestren de manera activa sus esfuerzos y medidas para proteger los derechos de los titulares de datos (Asamblea Nacional, 2023, RGLOPDP, Art. 58).

La tecnología blockchain se presenta como una herramienta clave para fortalecer la protección de datos personales en Ecuador. Con sus características de transparencia, integridad e inmutabilidad, blockchain puede ser crucial para avalar la trazabilidad y la seguridad en el manejo de datos personales. Esta tecnología puede aportar una infraestructura segura y descentralizada, esencial para la verificación y trazabilidad de las operaciones de datos, alineándose con los objetivos del protocolo de gestión de riesgos regulatorios (Mougayar, 2016; Swan, 2015). El desafío central en Ecuador es cómo los responsables del tratamiento de datos personales pueden identificar y mitigar los riesgos regulatorios relacionados con los derechos ARCO para asegurar el cumplimiento de la LOPDP. La respuesta a esta pregunta es crucial para proteger eficazmente los datos personales en un

entorno digital que evoluciona constantemente, por lo que el desarrollo de un protocolo de gestión de riesgos regulatorios centrado en los derechos ARCO es un paso crucial para Ecuador en su camino hacia una protección de datos personales más efectiva y alineada con los estándares internacionales. Este protocolo no solo debe garantizar el cumplimiento de la norma, sino también incorporar tecnologías avanzadas como el blockchain para elevar la preotección y rendimineto en el manejo de datos. Esta integración es fundamental para ajustarse a un ambinete digital que cambia constantemente, proporcionando las herramientas necesarias para proteger la privacidad y los derechos de los ciudadanos en el mundo digital.

Capítulo 3

i. Análisis de resultados

Análisis Descriptivo y Exploratorio de la Encuesta a Personas Naturales

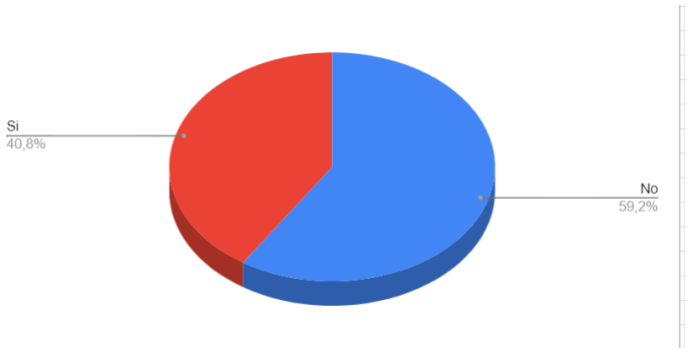
Población 74 personas naturales

País Ecuador

Pregunta 1 ¿Está familiarizado/a con los derechos ARCO (acceso, rectificación, cancelación y oposición) en relación con sus datos personales?

Figura 16

Conocimiento sobre los Derechos ARCO



Del resultado recabado por los participantes, denota que el 59,2% no están familiarizados con los derechos ARCO, podríamos aseverar que algunas personas en calidad

de titulares no estan siendo conscientes de la relevancia de salvaguardar su datos personales o pueden tener una comprensión limitada de cómo se utilizan y protegen sus datos personales. Esto podría acarrear vulneraciones sobre los derechos ARCO.

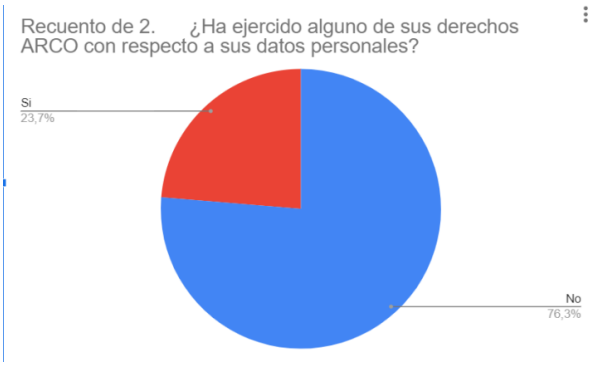
La falta de conocimiento tiene implicaciones profundas, si las personas no están al tanto de sus derechos de acceso, rectificación, Cancelación/eliminación y oposición, podrían no saber cómo acceder a sus datos personales que poseen terceros, cómo corregir información incorrecta, cómo solicitar la eliminación de sus datos o cómo oponerse a su uso para ciertas multas.

Asimismo, la falta de comprensión sobre cómo se emplean y resguardan sus datos personales puede llevar a una menor vigilancia en la protección de su información personal, resultando en una protección inadecuada contra el empleo inapropiado o la explotación de sus datos personales, aumentando el riesgo de vulnerabilidades de privacidad y otros desafíos vinculados con la seguridad de los datos.

Pregunta 2 ¿Ha ejercido alguno de sus derechos ARCO con respecto a sus datos personales?

Figura 17

Ejercicio de Derechos ARCO



Un porcentaje significativo de participantes (76,3%) no ha ejercido sus derechos ARCO, lo que estaría relacionado con el bajo nivel de conocimiento sobre estos derechos; podemos presumir que un factor principal por el cual un gran número de personas encuestadas pueden

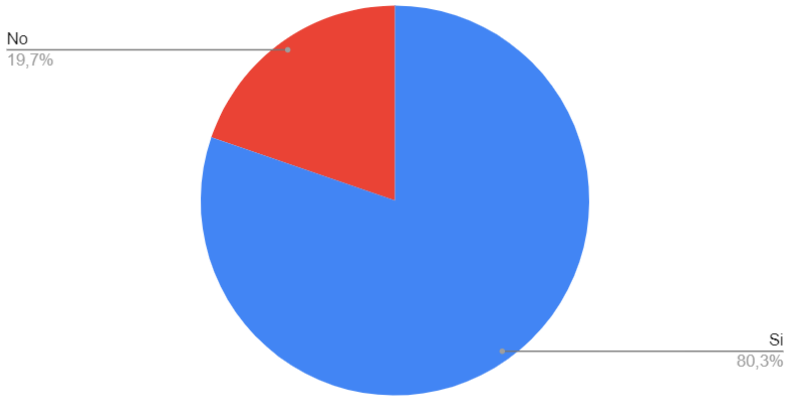
no haber ejercido algún derecho ARCO con respecto a sus datos personales, sería la falta de conocimiento de la LOPDP.

El escaso ejercicio de los derechos ARCO implica que muchas personas pueden no ser conscientes de su derecho al acceder a sus datos que entidades mantienen sobre ellas, ni de cómo pueden rectificar datos incorrectos o desactualizados; la falta de ejercicio de los derechos ARCO por un alto porcentaje de participantes parece estar directamente relacionada con un déficit en el conocimiento y la comprensión de la LOPDP, dando a denotar la necesidad de iniciativas de educación y sensibilización más robustas que puedan ayudar a las personas a comprender mejor sus garantias en relación con sus datos personales y cómo pueden ejercerlos exitosamente.

Pregunta 3 ¿Considera que existe un riesgo regulatorio (legal) en la protección de sus datos personales?

Figura 18

Percepción de Riesgo Regulatorio en la Protección de Datos



La mayor parte de los encuestados (80,3%) percibe que existe un riesgo regulatorio en la protección de sus datos personales; sin embargo, en muchos de ellos se refleja una incertidumbre sobre cuáles exactamente son las regulaciones aplicables a los datos

personales, lo cual resalta la importancia de fortalecer el marco legal y la regulación en relación a la protección de datos personales.

La percepción de riesgo regulatorio podría estar vinculada a una variedad de factores, los cuales pueden reflejar una preocupación por la insuficiencia o inadecuación de las normas existentes para proteger eficazmente los datos personales, esta preocupación podría estar alimentada por el ritmo acelerado de desarrollo tecnológico, que a menudo supera la velocidad con la que se actualizan las leyes y regulaciones.

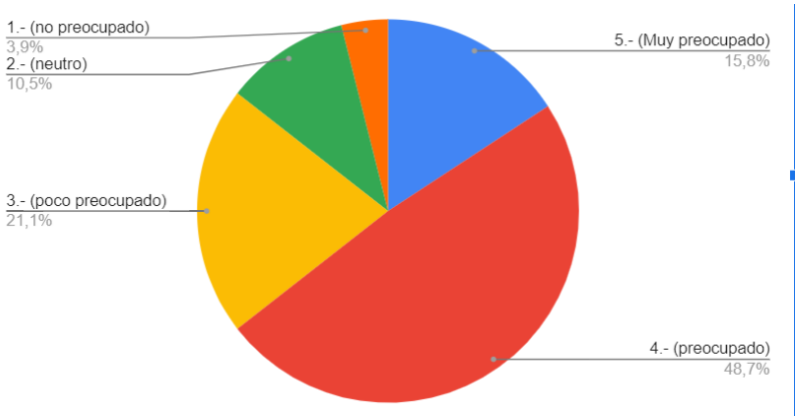
El hecho de que muchos participantes manifiesten incertidumbre sobre las regulaciones exactas aplicables a los datos personales sugiere un problema de falta de claridad y accesibilidad en la legislación existente, indicando que las leyes y regulaciones son demasiado complejas o técnicas para que el ciudadano promedio las comprenda, o que hay una falta de comunicación efectiva y educación sobre estas regulaciones.

Esta situación resalta la importancia de fortalecer el marco legal y la regulación en torno a la protección de datos personales, reforzar la normativa puede implicar no solo la revisión y modernización de las leyes existentes para abordar las nuevas realidades tecnológicas y digitales, sino también asegurarse de que estas leyes sean claras.

Pregunta 4 ¿Cómo calificaría su nivel de preocupación sobre los riesgos legales en el uso y manejo de sus datos personales en el entorno digital? (1: No preocupado, 5: Muy preocupado)

Figura 19

Nivel de Preocupación sobre Riesgos Legales



El auge de la interacción en el ámbito digital ha generado una creciente preocupación entre los participantes, solo un 48,7% de ellos manifiesta inquietud, y un 15,8% expresa una alarma más intensa en relación con los desafíos legales relacionados al manejo de sus datos personales en línea. Estas cifras reflejan una conciencia en aumento acerca de la crucial relevancia de resguardar la privacidad y seguridad de la información personal en el ambiente digital.

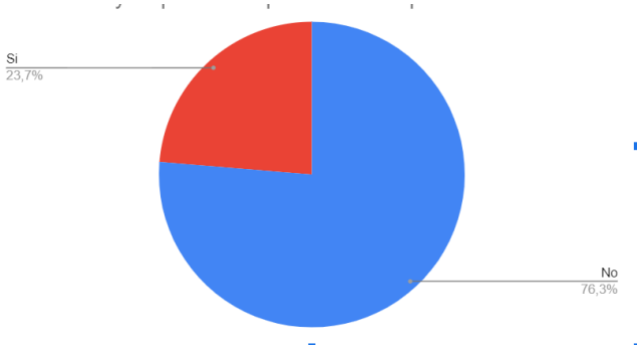
La era digital plantea retos de gran relevancia en lo que respecta a la protección de datos, como amenazas cibernéticas, posibles usos indebidos de la información y falta de control sobre el manejo de datos en línea, lo que denota la necesidad de aprender a establecer medidas normativas y efectivas que aborden estos riesgos y protejan los derechos individuales en el ciberespacio.

La preocupación de los participantes no solo refleja la percepción de vulnerabilidad en la esfera digital, sino que también impulsa la llamada a la acción para que las autoridades potencien sus esfuerzos en la promulgación y aplicación de marcos legales sólidos que salvaguarden efectivamente los datos personales. La invulnerabilidad de la privacidad en la web es esencial para garantizar la confianza y la integridad en el uso de plataformas digitales en la sociedad actual.

Pregunta 5 ¿Está familiarizado con la tecnología blockchain y su potencial aplicación en la protección de datos personales?

Figura 20

Familiaridad con Blockchain en la Protección de Datos



La considerable falta de familiaridad, evidenciada por un 76,3% de los participantes respecto a la tecnología blockchain y su aplicación en la protección de datos personales, resalta la necesidad de aprender iniciativas educativas integrales, este revelador hallazgo subraya una oportunidad estratégica para brindar información y concienciación acerca de las nuevas tecnologías y su potencial transformación en el entorno de la seguridad de datos personales.

Ante el mencionado escenario la tecnología blockchain, conocida por su carácter descentralizado y su capacidad de asegurar la integridad y seguridad de la información, posee un potencial sustancial en el ámbito de la protección de datos personales, el presente análisis apunta hacia la urgencia de abordar la brecha de conocimiento existente, ya que el discernimiento de la tecnología blockchain puede catalizar una percepción significativa y la aplicación de estrategias para la salvaguarda de datos personales sensibles.

El diseño de programas educativos que abordan específicamente la asociación entre la tecnología blockchain y la protección de datos personales podría tener un papel fundamental en capacitar a los involucrados a fin de decidir de manera informada y proactiva en el entorno digital que está en constate evolución, este enfoque no solo es beneficioso para los individuos, sino también contribuye al desarrollo de una sociedad digital más segura y consciente.

Un caso que ilustra la preocupación sobre la seguridad de nuestros datos personales en línea es el incidente de Facebook y Cambridge Analytica en el año 2018.

La empresa de análisis de datos que trabajó con el equipo electoral de Donald Trump y la campaña ganadora del Brexit recopiló millones de perfiles de Facebook de votantes estadounidenses, en una de las mayores filtraciones de datos jamás realizadas por el gigante tecnológico, y los utilizó para crear un potente programa de software para predecir e influir en las elecciones. en las urnas. (Cadwalladr, C., 2018, s.p.)

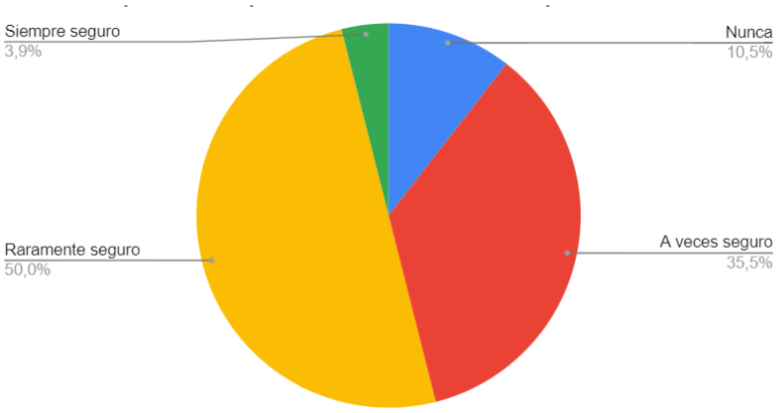
Facebook enfrentó críticas por su manejo de la situación. Mark Zuckerberg, CEO de la Compañía, en una audiencia realizada en el Congreso de los Estados Unidos, admitió errores y expresó: "No hemos hecho lo suficiente para evitar que estas herramientas se utilicen de manera perjudicial". (Zuckerberg, M. 2018). Esta admisión destacó las deficiencias en las prácticas de privacidad y seguridad de Facebook.

El incidente de Facebook y Cambridge Analytica no solo puso de manifiesto las preocupaciones sobre la privacidad de los datos, sino que también impulsó un debate más extenso acerca de la responsabilidad de las plataformas tecnológicas en la protección de la privacidad de sus usuarios. Este caso subrayó la necesidad de establecer regulaciones más rigurosas en la industria tecnológica. Como consecuencia, surgieron fuertes demandas por una mayor transparencia y regulación en el sector, con el objetivo de asegurar una adecuada protección de los datos y mantener la integridad en el manejo de información personal en el ámbito digital.

Pregunta 6 Al navegar por internet, ¿cuán seguros se siente respecto a la protección de sus datos personales?

Figura 21

Sensación de Seguridad al Navegar en Internet



La creciente preocupación por la evaluación crítica de la seguridad de la información personal en línea se hace evidente, con un 50% de los participantes manifestando raras sensaciones de seguridad durante su navegación por internet, el presente hallazgo representa una llamada de atención sobre la urgencia de fortalecer la seguridad y confianza en el entorno digital, el hecho de que solo el 3.9% de los participantes se sienta siempre seguro sugiere que existe una brecha significativa en la falta de seguridad en línea.

La variabilidad en las respuestas revela una diversidad de experiencias y percepciones. El 35.5% que se siente a veces seguro y el 10.5% que nunca se siente seguro indican una falta de consistencia en las garantías percibidas de la protección de datos personales en la red, el presente panorama destaca la necesidad de estrategias integrales que aborden las inquietudes específicas de los usuarios y promuevan un entorno digital más seguro y confiable.

En 2019, un grave fallo en la seguridad de Facebook resultó en una brecha que dejó expuestos los datos privados de una gran cantidad de usuarios. Este incidente, resaltó las deficiencias en las medidas de seguridad de la mencionada red social, permitió que los ciberdelincuentes accedieran a información sensible como nombres, números telefónicos y direcciones de correo electrónico. Posteriormente, en enero del año en curso, se utilizó un bot para recopilar información en una base de datos en Telegram, incluyendo más de 500 millones de números telefónicos asociados a los perfiles afectados. Sorprendentemente, esta

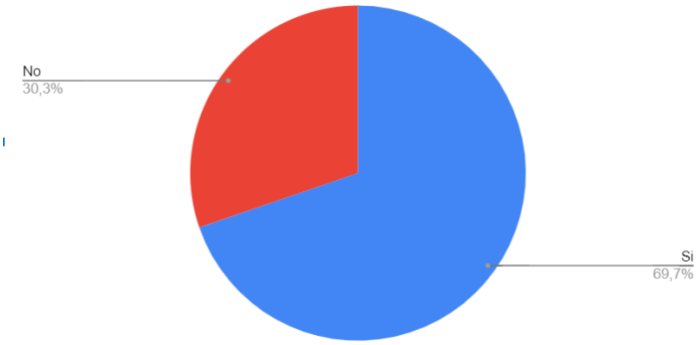
información se comercializó en la misma plataforma a precios que variaban entre 20 y 10.000 dólares estadounidenses. (Semana 2021, párr. 1,2).

Es necesario implementar medidas proactivas que aborden las áreas de vulnerabilidad identificadas y que promuevan una cultura de seguridad en línea, esto no solo contribuirá a generar más confianza digital, sino que también fortalecerá la resiliencia de los usuarios ante las crecientes amenazas cibernéticas.

Pregunta 7 ¿Ha experimentado alguna situación en la web donde sintió que sus datos personales estaban en riesgo legal?

Figura 22

Experiencias de Riesgo en la Web



La contundente mayoría, cifrada en un 69,7%, ha experimentado situaciones que les han hecho sentir que sus datos personales estaban en peligro legal en la web, lo que evidencia varias extensiones generalizadas de inquietudes sobre la seguridad de los datos personales en línea, la constancia de estas experiencias señala una necesidad de aprender a abordar las vulnerabilidades percibidas y fortalecer las salvaguardias digitales.

Contrastando con esta cifra, apenas el 30,3% afirma no haber enfrentado ninguna situación en la que sus datos estuvieran en riesgo, lo que esta minoría refleja la excepción, subrayando aún más la omnipresencia de desafíos relacionados con la seguridad de los datos personales en el ambiente digital actual.

Los resultados resaltan la emergente necesidad de iniciativas que no solo mitiguen los riesgos existentes, sino que también eduquen y capaciten a los usuarios para navegar de manera segura por el ciberespacio, la conciencia sobre la vulnerabilidad de los datos destaca la urgencia de estrategias integrales que promuevan la seguridad digital y fomenten prácticas informáticas seguras para todos los usuarios.

Los resultados obtenidos revelan un panorama de escasa familiaridad con los derechos ARCO y la tecnología blockchain, junto con una marcada percepción de riesgo y preocupación en torno a la seguridad de los datos personales en el entorno digital. Estos hallazgos evidencian un claro déficit de conocimiento sobre los derechos y tecnologías que fundamentan la protección de datos en el entorno digital, subrayando la necesidad urgente de iniciativas educativas y de concienciación.

La falta de familiaridad con los derechos ARCO indica que los individuos pueden no estar plenamente conscientes de sus derechos sobre la información personal y cómo ejercerlos. Asimismo, la limitada comprensión de la tecnología blockchain sugiere la necesidad de esfuerzos educativos para desmitificar su funcionamiento y resaltar su relevancia en la protección de datos personales.

La alta percepción de riesgo y preocupación subraya la urgencia de fortalecer el marco legal y las medidas de protección de datos personales en Ecuador. Es esencial abordar estas preocupaciones desde una perspectiva integral, promoviendo no solo la educación individual, admás, la constante evaluación y perfeccionamiento de las politicas y normativas actuales.

En respuesta a estos resultados, se hace imperativo un enfoque multidimensional que combine la educación pública sobre derechos y tecnologías, acompañado de una actulizacion de la legislación de protección de datos personales y una mejor concienciación sobre prácticas

seguras en línea. Este enfoque integral contribuirá a construir una sociedad digital más informada, empoderada y segura en Ecuador.

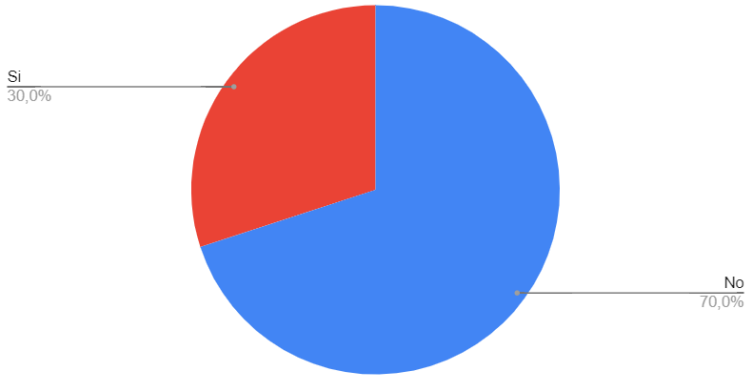
Análisis Descriptivo y Exploratorio de la Encuesta a Personas Jurídicas

***Población: 20 instituciones*.**

Pregunta 1 ¿Su empresa tiene un protocolo para gestionar los riesgos regulatorios asociados al tratamiento de datos personales, en especial los derechos ARCO (acceso, rectificación, cancelación y oposición)?

Figura 23

Existencia de Protocolo para Gestionar Riesgos Regulatorios (Derechos ARCO)



La ausencia de protocolos específicos para la gestión de riesgos regulatorios, especialmente en lo que respecta a los derechos ARCO, en el 70% de las empresas encuestadas, es un indicador preocupante. Esto puede señalar una falta de preparación para abordar los desafíos de LOPDP en Ecuador. La existencia de protocolos específicos es esencial para garantizar el cabal cumplimiento de la norma y para proteger los derechos de los titulares de los datos.

La Agencia Española de Protección de Datos en su "Informe Anual 2019" subraya la importancia de tener protocolos bien establecidos para el manejo efectivo de los derechos ARCO, destacando que la carencia de tales protocolos puede llevar a un manejo ineficiente de las peticiones de los titulares de datos y potencialmente a la violación de sus derechos

(Agencia Española de Protección de Datos, 2020, p.19). Este informe destaca la importancia de que las entidades establezcan procedimientos claros y efectivos para el tratamiento de datos personales y la gestión de riesgos asociados.

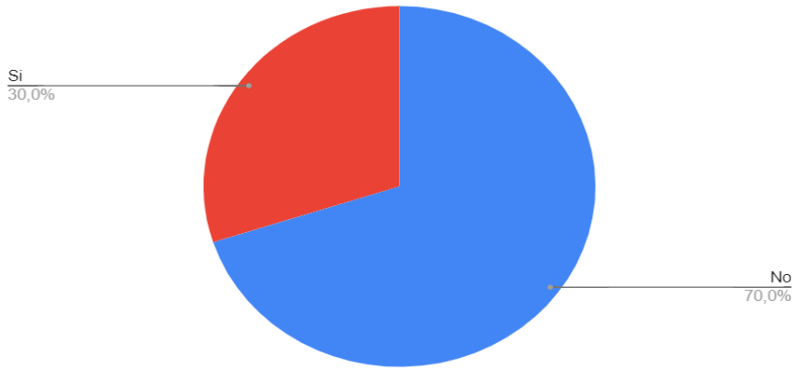
En el contexto ecuatoriano, la ausencia de protocolos específicos es preocupante, especialmente teniendo en cuenta el marco normativo establecido por la LOPDP. La ley ecuatoriana, al igual que el GDPR en Europa, exige que las organizaciones adopten medidas adecuadas para proteger los datos personales y garantizar los derechos de los titulares de datos personales. La ausencia de un protocolo adecuado para la gestión de riesgos regulatorios no solo expone a las organizaciones a posibles sanciones legales, sino que también influye de manera negativa en la confianza y la privacidad de los individuos cuyos datos manejan.

Para mitigar estos riesgos y mejorar el cumplimiento de la LOPDP, es esencial que las empresas ecuatorianas desarrollen e implementen protocolos específicos que aborden los riesgos regulatorios y aseguren el respeto de los derechos ARCO. Esto incluye la creación de políticas claras, la capacitación al personal y la adecuación de sistemas tecnológicos apropiados, como puede ser la tecnología blockchain, para el tratamiento seguro y eficiente de los datos personales.

Pregunta 2 ¿Considera que su empresa está adecuadamente preparada para identificar y mitigar los riesgos asociados al tratamiento de datos personales en el entorno digital?

Figura 24

Preparación para Identificar y Mitigar Riesgos en el Tratamiento de Datos



Dentro de la situación actual, donde el tratamiento de datos personales en el entorno digital es una tarea cotidiana para las empresas, la preparación adecuada para identificar y mitigar riesgos es crucial. Deacuerdo a los resultados, el 70% de las compañias encuestadas indican no estar adecuadamente preparadas para manejar estos riesgos. Esta cifra es alarmante, ya que indica una falta de conocimiento y de implementación de prácticas y estrategias de protección de datos personales en gran parte de las sociedades encuestadas.

Según un informe de IBM Security (2019), muchas organizaciones todavía están en las etapas iniciales de comprensión y adaptación a los retos de la seguridad en la marco digital. Este informe indica que solo el 23% de las organizaciones encuestadas cuentan con un enfoque de seguridad cibernética coherente y totalmente implementado (IBM, 2019, p. 45).

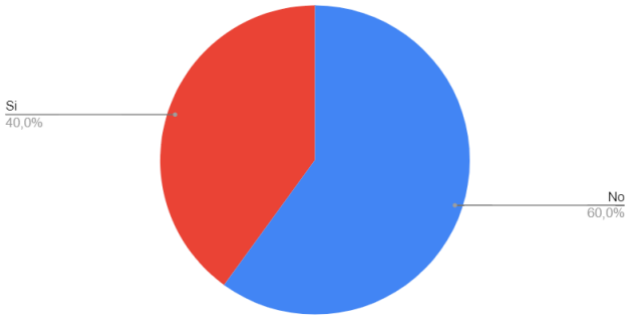
Para abordar esta brecha, las empresas pueden considerar la integración de la tecnología blockchain como parte de su enfoque para administrar riesgos. Blockchain ofrece características únicas como inmutabilidad, transparencia y descentralización, que pueden ser aprovechadas para mejorar la integridad y seguridad de los datos personales. Por ejemplo, un sistema eficiente de administración de identidades basado en blockchain podría proporcionar un método más seguro para almacenar y gestionar datos personales, reduciendo el riesgo de acceso no autorizado y manipulación de datos (Christidis & Devetsikiotis, 2016, p. 58).

Además, la implementación de contratos inteligentes en blockchain puede automatizar el cumplimiento de políticas de privacidad y consentimiento, garantizando que el tratamiento de datos personales se realice de acuerdo con las regulaciones vigentes (Savelyev, 2017, p. 117).

Pregunta 3 ¿Su empresa utiliza o considera el uso de tecnología blockchain para fortalecer la protección de datos personales?

Figura 25

Uso de Blockchain para la Protección de Datos Personales



El uso del blockchain en la protección de datos personales es un tema emergente en relación a la privacidad y la seguridad de la información. De 20 empresas encuestadas, 8 (40%) afirmaron que utilizan o consideran el uso de blockchain para robustecer la protección de datos personales, mientras que 12 empresas (60%) indicaron que no lo utilizan ni lo consideran. Esto sugiere que, aunque hay un interés creciente en la aplicación de blockchain para la protección de datos personales, todavía no forma parte de una práctica ampliamente adoptada en el sector empresarial.

Un estudio de KPMG (2020) reveló que el uso de blockchain en la protección de datos personales todavía está en una fase temprana, con un número limitado de implementaciones en el mundo empresarial (p.21). Esto refleja con los datos obstenidos de la encuesta, que la gran mayoría de compañias aún no han adoptado blockchain en sus estrategias de protección de datos personales.

Blockchain brinda ventajas significativas en lineamientos de seguridad y transparencia de gestión de los datos personales. Su estructura descentralizada y el registro inmutable de transacciones pueden mejorar la protección contra el acceso no autorizado y la manipulación de datos. Sin embargo, hay desafíos legales y técnicos, como la dificultad para modificar o eliminar datos, lo que podría entrar en conflicto con los derechos de protección de datos personales como el derecho al olvido (Morales Cáceres A., 2023, p.202-207).

Para abordar estos desafíos, las empresas podrían considerar el uso de blockchains privadas[4], donde el control de los datos y el acceso es más manejable. Además, se pueden implementar técnicas de anonimización[5] de datos en blockchain para el cabal cumplimineto de requisitos legales como el derecho a la supresión. Es esencial que las empresas que consideren implementar blockchain para la protección de datos personales realicen evaluaciones de impacto en la privacidad y consulten con expertos en protección de datos personales y tecnología blockchain.

El empleo de blockchain en la protección de datos personales muestra un potencial significativo, las compañias deben ser conscientes de los retos legales y técnicos asociados, por lo que deben buscar maneras de integrar esta tecnología de forma que cumpla con las normas de regulaciones de protección de datos personales actuales.

Pregunta 4 ¿Ha enfrentado su empresa alguna situación donde los derechos ARCO de los titulares de datos personales han sido comprometidos?

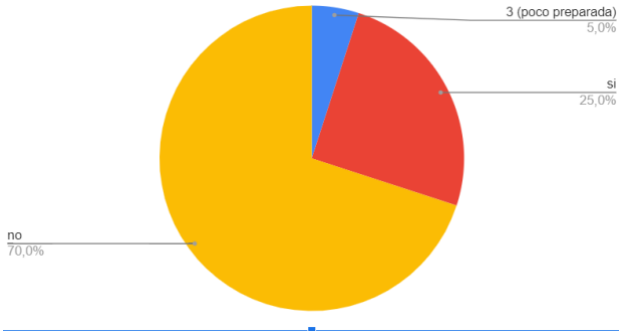
---

[4] **Blockchain privada:** Para evitar o minimizar estas desventajas del blockchain público existen también las redes blockchain privadas, a las que sólo se puede acceder por invitación de algún integrante de la red o de alguno de sus administradores. Aquí radica una de las principales diferencias: la administración y gestión de la red está a cargo de una entidad o corporación, que controla el acceso y los sucesivos registros en la cadena de bloques. ((https://www.orange.es/metaverso/noticias/curiosidades/tipos-de-blockchain-publica-privada-hibrida-y-federada) consultado 10-12-2023)

[5] **Técnicas de anonimización:** Pretenden ocultar la identidad y, por tanto, los identificadores de cualquier naturaleza. Los identificadores pueden aplicarse a cualquier persona física o jurídica, viva o muerta, incluidos sus dependientes, ascendientes y descendientes. A su vez, se incluyen otras personas relacionadas, directamente o a través de la interacción. (https://www.linkedin.com/pulse/pseudonimizaci%C3%B3n-y-anonimizaci%C3%B3n-de-datos-en-qu%C3%A9-se-diferencian/?originalSubdomain=es Consultado 10-12-2023)

Figura 26

Situaciones de Compromiso de los Derechos ARCO



La respuesta de las empresas, con un 25% indicando haber enfrentado situaciones de compromiso de los derechos ARCO, refleja un panorama preocupante respecto a la seguridad y el manejo de datos personales en Ecuador. Este porcentaje, aunque no mayoritario, es significativo y sugiere la existencia de brechas en las prácticas de tratamiento de datos personales y la aplicación de medidas de seguridad. Un estudio realizado por la Comisión de Protección de Datos de Irlanda (2020) indica que las violaciones de datos personales son un problema recurrente, que afecta tanto a grandes corporaciones como a pequeñas empresas, debido a la carencia de medidas de seguridad apropiadas y al gestionamiento ineficiente de los datos personales.

En este contexto, la tecnología blockchain surje como una potencial solución. Dada su naturaleza descentralizada, asi como tambien elementos característicos de inmutabilidad y transparencia; el blockchain mejorará significativamente la seguridad en la gestión de datos personales. Según Mendoza Enríquez, (2020)

> Técnicas como la cadena de bloques privada, permitiría asegurar el cumplimiento frente a derechos ARCO, considerando que una de las características del servicio, es la inmutabilidad de la información, lo cual, en principio, haría casi imposible la salvaguarda de derechos como el de cancelación del dato o la rectificación, por lo que, en la medida

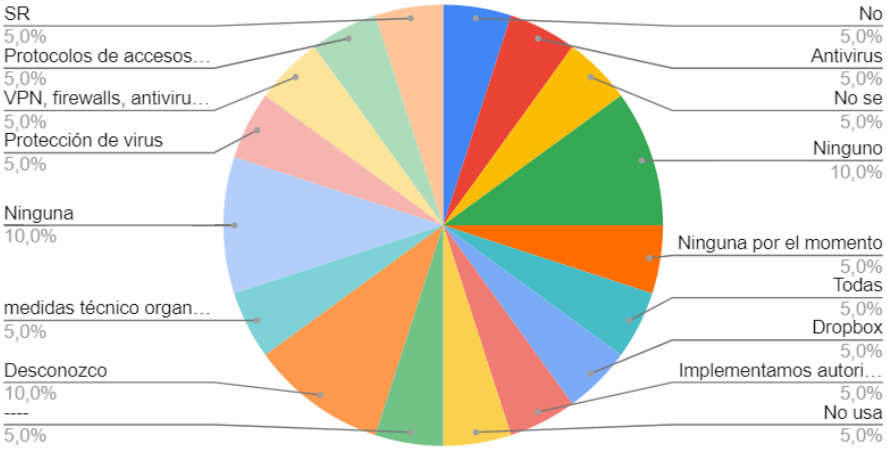
de control sobre los bloques, podría residir la posibilidad del nivel de cumplimiento normativo en materia de protección de datos personales (p.118)

La adaptación del blockchain a una estrategia integral de administración de riesgos y protección de datos puede ser una solución efectiva para las empresas en el Ecuador. No obstante, resulta importante reslatar que la tecnología blockchain debe ser implementada en conjunto con políticas claras, capacitación y una cultura organizacional que valore y proteja la privacidad y seguridad de los datos personales.

Pregunta 5 ¿Qué herramientas o soluciones utiliza su empresa para proteger los datos personales en la web y gestionar los riesgos regulatorios (legales)?

Figura 27

Herramientas y Soluciones para la Protección de Datos en la Web



Las respuestas de las empresas en la encuesta revela un patrón mixto en la aplicación de herramientas de protección de datos. Los resultados de la encuesta sugieren una diversidad de enfoques y un conocimiento limitado sobre herramientas específicas para la protección de datos personales en las empresas encuestadas en Ecuador. La ausencia de respuestas específicas o el desconocimiento expresado por un 45% de las empresas es indicativo de una posible falta de estrategias claras de gestión de amenazas regulatorias relacionadas con la

protección de datos. Este escenario es coherente con los hallazgos de un estudio de la Agencia Española de Protección de Datos, señala que muchas organizaciones aún no han adaptado completamente sus procedimientos relacionados a la protección de datos y requerimientos normativos vigentes (Agencia Española de Protección de Datos, 2021).

Es importante implementar estrategias más coherentes y efectivas para la protección de datos en Ecuador. De tal forma, la incorporación de tecnologías como el blockchain, destacada por su potencial en la mejora de la protección y la transparencia en la gestión de datos personales, podría ser una solución innovadora. Según Llamas Covarrubias (2021), el blockchain ofrece características como la inmutabilidad, la descentralización y la transparencia, lo que puede ser particularmente útil en el marco de la protección de datos personales (p.4) Sin embargo, para aprovechar plenamente estas tecnologías, las empresas en Ecuador deben adoptar un enfoque más integral que incluya la educación y la concienciación sobre la protección de datos, así como la actualización constante de sus prácticas y herramientas de seguridad.

Identificación de Tendencias Emergentes Basadas en Encuestas a Personas Naturales y Jurídicas

1. Conciencia sobre los Derechos ARCO

Existe una brecha significativa en el conocimiento y la implementación de los derechos ARCO tanto en individuos como en empresas. Mientras que las empresas parecen más conscientes y preparadas, una gran parte de la población general muestra falta de conocimiento sobre sus derechos fundamentales en relación con sus datos personales.

2. Ejercicio de Derechos ARCO y Preparación para Gestionar Riesgos

Personas Naturales: Solo 18 de 76 han ejercido sus derechos ARCO.

Personas Jurídicas: 6 de 20 empresas se consideran preparadas para identificar y mitigar riesgos regulatorios.

Existe una brecha entre la conciencia y la acción. Aunque algunas personas y empresas están conscientes de los derechos ARCO, son muy pocas las empresas que han tomado medidas necesarias para ejercerlos o prepararse para enfrentar los riesgos regulatorios asociados.

3. Percepción de Riesgos Regulatorios y Seguridad en la Web

Sesenta y una personas naturales, consideran que hay un riesgo regulatorio en la protección de sus datos personales. En seguridad web, 38 individuos raramente se sienten seguros.

Cinco de veinte empresas han enfrentado situaciones de compromiso de derechos ARCO.

Hay una creciente preocupación sobre los riesgos legales y la seguridad de los datos personales en el ambiente digital, tanto en individuos como en empresas. Esto sugiere una necesidad inminente de que se generen protocolos robustos sobre los riesgos regulatorios y una educación a la población por parte de la autoridad.

4. Uso y Conocimiento de Blockchain para Protección de Datos

Aunque el blockchain presenta un potencial significativo para la protección de datos personales, su comprensión y adaptación son todavía limitadas. Este escenario indica una oportunidad para fomentar el uso de tecnologías emergentes en el tratamiento de datos personales.

Los resultados de las encuestas revelan una necesidad urgente de mejorar la educación y la implementación de prácticas de protección de datos personales tanto a nivel individual y corporativo. La brecha en la conciencia y el ejercicio activo de los derechos ARCO, junto con la

preocupación por los riesgos regulatorios y la seguridad en la web, destaca la importancia de desarrollar protocolos efectivos de gestión de riesgos regulatorios y educar sobre tecnologías emergentes como la blockchain. La adopción y comprensión de estas tecnologías pueden ser clave para avanzar en la protección de datos personales en Ecuador.

Interpretación de las Tendencias en Protección de Datos Personales

1. Conciencia y Ejercicio de Derechos ARCO

La encuesta revela un conocimiento limitado y un ejercicio aún más reducido de los derechos ARCO entre las personas naturales. En contraste, las empresas muestran una mayor conciencia, pero aún con margen de mejora. Según Roldán Carrillo (2020), este desequilibrio resalta una "necesidad crítica de educación y formación en derechos de protección de datos para fortalecer la cultura de privacidad" (p. 102), por lo que adoptar una educación y una cultura de privacidad en la actual era digital son parámetros fundamentales para salvaguardar nuestra privacidad y datos personales. Esto incluye ser consciente de los riesgos, comprender nuestras responsabilidades y derechos, utilizar herramientas para proteger la información personal e incentivar una cultura que respete la privacidad.

Es fundamental establecer programas de sensibilizacion y formación dirigidos tanto para personas como para empresas con el din de fortalecer los derechos ARCO. Deberá ser imperativo para la autoridad competente instruir conscientemente a los titulares como a los responsables y encargados. A falta de esta conciencia y cultura, se deberá instruir a cada persona ayudando al fortalesimineto respecto a los derechos de protección de datos personales, que es parte de la idiosincrasia ecuatoriana. Comunicar por medio de iniciativas y educación sobre conceptos básicos e importantes en esta materia, los derechos de los titulares, las obligaciones de los encargados y responsables aplicando herramientas adecuadas (Roldán Carrillo, 2021, p. 200).

La mayor responsabilidad sobre la administración de los datos personales recae sobre los usuarios, los cuales son los encargados de suministrar la información a través de ficheros, dentro de los elementos que intervienen en los sistemas de comunicaciones, los usuarios representan el mayor volumen y el grupo que menos tiene conciencia sobre el uso y disposición de los datos personales (Remache Arias, 2019, p.47).

2. Percepción de Riesgos Regulatorios y Seguridad en la Web

La percepción elevada de riesgos regulatorios y la sensación de inseguridad en el entorno web destacan una paulatina preocupación por la protección de datos personales. Como señala Finck (2018), esta situación refleja "una alarmante desconfianza hacia las medidas de seguridad vigentes y subraya la urgente necesidad de reforzar las políticas de protección de datos" (p. 89). Dentro de una situacion donde la información digital fluye constantemente, las brechas de seguridad y el incumplimiento de normativas pueden tener consecuencias devastadoras tanto para los titulares de los datos asi como para los responsables del tratamiento.

El estudio de la Universidad de Cataluña (2021) resalta la importancia de la identificación y evaluación de riesgos como pasos fundamentales en la gestión de riesgos en la web. Este procedimiento involucra no solamente identificar los posibles riesgos que los datos personales pueden enfrentar a lo largo de su existencia, sino también analizar los factores que determinan el nivel de riesgo y valorar las consecuencias de su materialización. Esta evaluación debe tomar en cuenta tanto la posibilidad de que ocurra un evento desfavorable como las consecuencias que se podrían generar.

La web, como espacio de interacción global, presenta desafíos únicos en términos de riesgos regulatorios. Según un informe de la Comisión Europea (2020), la web es un terreno fértil para actividades como el phishing, malware y otras formas de ciberataques que pueden comprometer gravemente la integridad y confidencialidad de los datos personales. Además, la

complejidad de las regulaciones internacionales sobre protección de datos, como el RGPD en Europa, crea un mosaico normativo que las organizaciones deben navegar cuidadosamente para evitar sanciones y daños a su reputación.

Por lo que es necesario realizar acciones para mitigar riesgos tales como:

Identificación del Origen de Riesgos

Comprender las fuentes de riesgo en la web es crucial. Esto incluye riesgos internos, como errores de empleados o fallas en los sistemas, y riesgos externos, como ataques cibernéticos y cambios legislativos.

Análisis de Factores y Nivel de Riesgo

Evaluar los factores que contribuyen al riesgo, como vulnerabilidades en el software, prácticas de seguridad deficientes y el contexto regulatorio. Herramientas como análisis de vulnerabilidades y auditorías regulares son fundamentales en este proceso.

Evaluación del Impacto y Probabilidad

Medir tanto la probabilidad de un incidente como su posible impacto. Esto incluye el daño potencial a la privacidad de los individuos, así como las sanciones y costos asociados a la violación de las normativas.

La integración de tecnologías emergentes como el blockchain puede ser una estrategia prometedora para mitigar estos riesgos. Su aplicación en la protección de datos personales ofrece ventajas en términos de seguridad, transparencia y resistencia a manipulaciones, como sugiere Roldán Carrillo (2020). Sin embargo, es importante tener en cuenta que la implementación de nuevas tecnologías debe hacerse con una comprensión clara de las normativas aplicables y de cómo estas tecnologías pueden ayudar a cumplir con dichas regulaciones de manera efectiva.

El desarrollo y la implementación de protocolos efectivos de gestión de riesgos son cruciales, especialmente en un contexto digital que evoluciona rápidamente. Esta necesidad se hace aún más patente al considerar la alta percepción de riesgos regulatorios y la inseguridad en la web identificadas en el análisis anterior. Tal como subraya Finck (2018), la creciente desconfianza en las medidas de seguridad actuales exige una acción decidida para fortalecer la protección de datos (p. 89). El ambiente digital, con su potencial para riesgos como el phishing y otros ciberataques, requiere una estrategia proactiva y bien estructurada para la gestión de riesgos.

En Ecuador, la Ley Orgánica de Protección de Datos Personales ha introducido los derechos ARCO alineándose con los estándares internacionales. Sin embargo, los riesgos regulatorios en Ecuador se concentran en la implementación y ejecución efectiva de estos derechos. La novedad relativa de la LOPDP y la ausencia de una autoridad de protección de datos completamente funcional aumentan el riesgo de interpretaciones y aplicaciones inconsistentes de estos derechos. Esto se evidencia en la falta de preparación expresada por muchas empresas en las encuestas para manejar los desafíos relacionados con el tratamiento de datos personales (Acosta y Villamar, 2021, p. 110). Además, la transposición de los principios y derechos del RGPD al marco jurídico ecuatoriano implica desafíos únicos, como la adaptación a prácticas administrativas locales y la necesidad de sensibilizar a los titulares de datos y a los responsables de su tratamiento.

3. Uso y Conocimiento de Blockchain para Protección de Datos

A pesar del reconocido potencial del blockchain, su adopción y comprensión son limitadas. Martínez (2020) señala que "el desconocimiento de tecnologías emergentes como el blockchain es un obstáculo significativo para su implementación efectiva en la protección de datos" (p. 76).

Fomentar el conocimiento y aplicación práctica del blockchain puede ser una estrategia clave para avanzar en la protección de datos personales ofreciendo una solución innovadora para asegurar la integridad y la confidencialidad de la información personal.

4. Implementación de Protocolos de Gestión de Riesgos

Es evidente que la falta de preparación de las empresas en la gestión de riesgos relacionados al tratamiento de datos personales subraya la necesidad urgente de protocolos de gestión más efectivos. En este sentido, la afirmación de Ayudaley (2023) resalta que una gestión de riesgos eficiente es fundamental no solo para proteger la información personal, sino también para mejorar la confianza y la imagen de las empresas (párr. 34).

5. Blockchain como Tecnología Emergente

La descripción de Finck (2018) del blockchain como un libro de cuentas digitales distribuido pone de relieve su potencial disruptivo en el tratamiento y conservación de datos. La descentralización, transparencia e inalterabilidad son características clave de esta tecnología, lo que la hace atractiva para su uso en la protección de datos personales

6. Desafíos Normativos y Blockchain

La Ley 1581 de 2012 de Colombia y el RGPD en la UE ilustran la complejidad de adaptar la tecnología blockchain a los marcos legales existentes. Mientras la ley colombiana se concentra en un enfoque centralizado, el blockchain opera de manera descentralizada, generando desafíos en términos de anonimización y seudonimización de los datos personales (Martínez, 2020). Del mismo modo, el RGPD con su énfasis en la responsabilidad y el derecho al olvido presenta desafíos al carácter inmutable del blockchain. Sin embargo, las soluciones propuestas por Castelló (2019) demuestran que es posible alinear la tecnología blockchain con estos marcos legales, aunque requiere un enfoque innovador y flexible (Castelló, 2019).

7. Necesidad de Equilibrio entre Seguridad y Cumplimiento Normativo

La adaptación de las tecnologías emergentes como el blockchain a las normas juridicas de protección de datos personales es un desafío que no puede abordarse mediante un enfoque binario. Se necesita un equilibrio que permita el aprovechamiento de las ventajas de la tecnología blockchain mientras se respetan los derechos de protección de datos personales. La interpretación flexible de las leyes y el desarrollo continuo de la tecnología son fundamentales para alcanzar este equilibrio.

8. Aplicación en Ecuador

Es esencial en Ecuador la adopción de un protocolo para la administración de riesgos normativos que englobe los derechos ARCO. Este protocolo debe garantizar el cumplimiento efectivo de la LOPDP, adaptándose a las necesidades tanto de personas naturales como jurídicas. La tecnología blockchain, con su potencial para mejorar la seguridad y la gestión de datos personales, puede desempeñar un papel clave en este proceso, siempre que se aborden los desafíos normativos de manera proactiva y creativa.

Después de un análisis de los datos y en cumplimiento del objetivo de la presente investigación a continuación se detalla la propuesta de protocolo:

Protocolo de Gestión de Riesgos Regulatorios para la protección de los derechos ARCO asociados a la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador

1. – Objetivo

El propósito fundamental de este protocolo es establecer pautas y directrices claras para la gestión eficiente de los riesgos regulatorios asociados al ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) por parte de los titulares de datos personales, en pleno cumplimiento con la normativa establecida en la LOPDP.

2. – Alcance:

Este protocolo aplica a todos los responsables del tratamiento de datos personales que operen en Ecuador.

3. – ***Definiciones****:*

Confidencialidad: “Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.” (ISO / IEC 27000: 2018, 3.10).

Derechos ARCO: Derechos de acceso, rectificación, cancelación / eliminación y oposición al tratamiento de datos personales (Asamblea Nacional, 2021, LOPDP, Art.13 Acceso, Art.14 Rectificación, Art. 15 Eliminación y Art.16 Oposición).

Disponibilidad: “Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada”. (ISO / IEC 27000: 2018, 3.7)

Integridad*:* “La integridad de la información se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios” (ISO / IEC 27000: 2018, 3.36**)**

Responsable del tratamiento de datos personales: “Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.” (Asamblea Nacional, 2021, LOPDP, Art.4).

Riesgo: “Se entiende por riesgo la probabilidad y el impacto de que una amenaza se materialice, siendo una amenaza cualquier elemento o factor que potencialmente pueda provocar un daño o perjuicio.” (Universidad de Castilla de la Mancha 2020)

RIESGO = PROBABILIDAD X IMPACTO

Titular de datos personales: “Persona natural cuyos datos son objeto de tratamiento.” (Asamblea Nacional, 2021, LOPDP,Art.4)

4. - Identificación de riesgos

El primer paso para la gestión de riesgos regulatorios es identificar los riesgos que existen, los riesgos regulatorios pueden ser los siguientes:

Incumplimiento en el Plazo de Respuesta: No responder dentro del plazo de 15 días a las solicitudes de ejercicio de los derechos ARCO, según lo estipulado en los Artículos 13 al 16 de la LOPDP.

Falta de Provisión de Información: No proporcionar al titular de los datos personales la información requerida en el ejercicio de sus derechos ARCO.

Acciones Injustificadas sobre los Datos Personales: Rectificar, cancelar u oponer el tratamiento de datos personales sin justificación legal.

Negación Injustificada de Derechos: Rehusar rectificar, cancelar u oponer el tratamiento de datos personales cuando el titular tenga derecho a ello.

Denegación de Acceso a los Datos Personales: Rechazar el acceso al tratamiento de datos personales cuando el titular tenga derecho a ello.

En relación a lo señalado anteriormente, se sugiere se aplica la tabla 1 referente al tipo de amenazas inherentes a la confidencialidad, integridad y disponibilidad, debiendo responder a los siguientes cuestionamientos.

Tabla 1

Tipo de Amenaza

Tipo de Amenaza	Amenaza	Preguntas para Identificar la Amenaza

Confidencialidad	Acceso no autorizado	¿Quién tiene acceso a los datos personales? ¿Qué políticas y procedimientos existen para controlar el acceso a los datos personales?
Integridad	Alteración o destrucción de datos	¿Cómo se protegen los datos personales de la alteración o destrucción? ¿Cuáles son los procesos de respaldo y recuperación de datos?
Disponibilidad	Interrupción del servicio	¿Qué medidas se han tomado para garantizar la disponibilidad de los datos personales? ¿Qué sucedería si el sistema de información se cayera?

De igual manera, es importante identificar las amenazas relacionadas en forma específica con los derechos ARCO, por lo que se propone la aplicación de la tabla 2.

Tabla 2

Amenazas Derechos ARCO

Derecho ARCO	**Tipo de Amenaza**	**Amenaza**	**Preguntas para Identificar la Amenaza**
Acceso	Confidencialidad	Acceso no autorizado a los datos personales	¿Quién tiene acceso a los datos personales solicitados? ¿Cómo se controlan los accesos a los datos personales?
Rectificación	Integridad	Alteración o destrucción de los datos personales	¿Cómo se protegen los datos personales de la alteración o destrucción? ¿Cuáles son los procesos de respaldo y recuperación de datos?
Cancelación/eliminación	Confidencialidad	Acceso no autorizado a los datos personales cancelados/eliminados	¿Cómo se garantiza que los datos personales cancelados/eliminados no estén disponibles para terceros? ¿Cómo se garantiza que los datos personales cancelados/eliminados no sean utilizados para otros fines?
Derecho ARCO	**Tipo de Amenaza**	**Amenaza**	**Preguntas para Identificar la Amenaza**
Oposición	Integridad	Alteración o destrucción de los datos personales	¿Cómo se protegen los datos personales de la alteración o

			destrucción? ¿Cuáles son los procesos de respaldo y recuperación de datos?		

A continuación de describe en la tabla 3 un ejemplo de la probabilidad e impacto relacionados con los derechos ARCO

Tabla 3

Derechos ARCO Ejemplo de Probabilidad e Impacto

Derecho ARCO	**Tipo de Amenaza**	**Amenaza**	**Preguntas para identificar la amenaza**	**Probabilidad**	**Impacto**
Acceso	Confidencialidad	Acceso no autorizado a los datos personales	¿Quién tiene acceso a los datos personales solicitados? ¿Cómo se controlan los accesos a los datos personales?	Alta	Alto
Rectificación	Integridad	Alteración o destrucción de los datos personales	¿Cómo se protegen los datos personales de la alteración o destrucción? ¿Cuáles son los procesos de respaldo y recuperación de datos?	Media	Medio
Derecho ARCO	**Tipo de Amenaza**	**Amenaza**	**Preguntas para identificar la amenaza**	**Probabilidad**	**Impacto**
Cancelación/eliminación	Disponibilidad/ confidencialidad	Acceso no autorizado a los datos personales cancelados	¿Cómo se garantiza que los datos personales cancelados no estén	Alta	Medio

			disponibles para terceros? ¿Cómo se garantiza que los datos personales cancelados no sean utilizados para otros fines?		
Oposición	Integridad	Alteración o destrucción de los datos personales	¿Cómo se protegen los datos personales de la alteración o destrucción? ¿Cuáles son los procesos de respaldo y recuperación de datos?	Media	Bajo

5. - Evaluación de riesgos

Una vez que los riesgos han sido reconocidos, resulta fundamental analizar tanto su repercusión como la posibilidad de que ocurran. Esta valoración debe tener en cuenta:

- Probabilidad de Ocurrencia: Estimar la frecuencia con la que se espera que ocurra un riesgo.
- Gravedad del Impacto: Determinar el nivel de daño o las consecuencias adversas que el riesgo podría causar si se materializa.

5.1 Medición de la Probabilidad de los Riesgos

Para medir la probabilidad de ocurrencia de un riesgo, se utiliza una escala de calificación. Una metodología efectiva puede ser la siguiente:

Tabla 4

Probabilidad de los Riesgos

Probabilidad de Riegos	***Descripción***	***Criterio***

Bajo	La probabilidad de ocurrencia del riesgo es baja.	Ocurre 1 o 2 veces
Medio	La probabilidad de ocurrencia del riesgo es moderada	Ocurre 3 a 5 veces
Alto	La probabilidad de ocurrencia del riesgo es alta	Ocurre 3 a 5 veces

Para asignar una calificación a la probabilidad de un riesgo, se deben considerar varios factores tales como:

- Revisar los registros históricos de incidentes similares.
- Evaluar cómo los cambios recientes en el entorno operativo o tecnológico pueden afectar la probabilidad de ocurrencia.
- Considerar la eficacia de los controles actuales en la mitigación del riesgo.
- Utilizar datos y análisis de tendencias para prever posibles riesgos futuros.

En la tabla 5 se busca cuantificar la probabilidad de que se materialice un riesgo, basándose en la frecuencia, factores contribuyentes y la complejidad del sistema o proceso involucrado.

Tabla 5

Factores para Calificación a la Probabilidad de un Riesgo

Factor Evaluado	Descripción y criterios de evaluación
Frecuencia	Baja: Ocurre menos de una vez al año. Media: Ocurre entre 2 y 4 veces al año. Alta: Ocurre 5 o más veces al año.
Factores contribuyentes	Evaluar aspectos como nivel de capacitación del personal, calidad de los controles de seguridad y nivel de exposición a amenazas externas.
Complejidad del Sistema/Proceso	Baja: Sistemas o procesos simples con pocos componentes o pasos. Media: Sistemas o procesos con una complejidad moderada. Alta: Sistemas o procesos altamente complejos

Por ejemplo, La posibilidad de perder datos debido a una equivocación humana probablemente tendría una probabilidad baja, ya que los errores humanos son relativamente poco frecuentes. Sin embargo, un riesgo de pérdida de datos debido a un ataque cibernético probablemente tendría una probabilidad alta, ya que los ataques cibernéticos son cada vez más comunes.

5.2 Medición de la gravedad del impacto de los riesgos

En la tabla 6 se enfoca en evaluar la gravedad del impacto que un riesgo podría tener si se materializa, utilizando una escala de calificación cuantitativa.

Tabla 6

Medición Impacto de Riesgos con una cuantificación de 1 al 5

Gravedad del Impacto	Descripción y Ejemplos	Cuantificación (1-5)
Bajo	-Impacto mínimo en operaciones. - Pérdidas financieras menores. - Poca o ninguna afectación a la reputación.	1
Medio	- Interrupciones operativas manejables. - Pérdidas financieras moderadas - Impacto reputacional limitado.	2-3
Gravedad del Impacto	**Descripción y Ejemplos**	**Cuantificación (1-5)**
Alto	- Interrupciones graves en operaciones. - Pérdidas financieras significativas. - Daño reputacional grave.	4-5

Para asignar una calificación a la gravedad del impacto de un riesgo, se deben considerar los siguientes factores:

- Los recursos que se perderían o se dañarían si se produjera el riesgo.
- Los costes que se generarían si se produjera el riesgo.
- El impacto en la reputación de la organización si se produjera el riesgo.

Por ejemplo, un riesgo de pérdida de datos de clientes probablemente tendría un impacto alto, ya que los datos de los clientes son un activo valioso. Sin embargo, un riesgo de interrupción del servicio probablemente tendría un impacto medio, ya que los clientes podrían encontrar alternativas al servicio.

Tabla 7

Ejemplos de Medición de la Probabilidad y la Gravedad del Impacto:

Factor	Riesgo	Explicación
Probabilidad	Pérdida de datos debido a un error humano: Bajo	Los errores humanos son relativamente poco comunes. Sin embargo, cuando ocurren, pueden tener un impacto alto.
Probabilidad	Pérdida de datos debido a un ataque cibernético: Alto	Los ataques cibernéticos son cada vez más comunes y sofisticados, pues emplean una variedad de tecnicas para acceder a los datos como el phishing, el malware y las vulnerabilidades de seguridad
Factor	**Riesgo**	**Explicación**
Gravedad del impacto	Pérdida de datos de cliente: Alto	La pérdida de información de los clientes puede afectar considerablemente la imagen de la compañía y su habilidad para generar ganancias. Los clientes podrían perder la confianza en la empresa y decidir no mantener relaciones comerciales con ella.
Gravedad del impacto	Interrupción del servicio: Medio	La interrupción del servicio puede ser un inconveniente para los clientes, pero generalmente no tiene el impacto significativo en la reputación de una empresa o a su capacidad de generar ingresos.

Estas son solo algunas sugerencias para medir la probabilidad y la gravedad del impacto de los riesgos. La mejor manera de hacerlo dependerá de las circunstancias específicas de cada organización.

6. -Mitigación de riesgos

Para mitigar efectivamente los riesgos regulatorios asociados al ejercicio de los derechos ARCO, es esencial implementar una serie de medidas que no solo cumplan con la LOPDP, sino que también se alineen con las prácticas internacionales en la gestión de riesgos y seguridad de la información. Las medidas propuestas son:

Implementación de Procedimientos para el Ejercicio de Derechos ARCO: Desarrollar un procedimiento claro y sencillo que facilite el ejercicio de los derechos ARCO, conforme a lo establecido en el Art. 47, núm. 5 y núm. 7 de la LOPDP y el Art. 12 del Reglamento General de la LOPDP (RGLOPDP). Asegurar que estos procedimientos estén documentados, sean fácilmente accesibles para los titulares de los datos y cumplan con los principios de transparencia y eficacia.

Registro y Seguimiento de Solicitudes ARCO: Establecer un sistema para contabilizar todas las solicitudes de ejercicio de los derechos ARCO y asegurar su seguimiento efectivo, en línea con el Art. 51, núm. 9 de la LOPDP.

Implementar soluciones tecnológicas que permitan un registro detallado y una revisión sistemática de estas solicitudes.

Capacitación del Personal: Contar con personal debidamente capacitado para atender las solicitudes de ejercicio de los derechos ARCO, acorde con el Art. 10, Lit. K y Art. 52 de la LOPDP. ***Así como d***esarrollar programas de formación continua que abarquen tanto aspectos legales como técnicos relacionados con la protección de datos personales y el tratamiento de solicitudes ARCO.

Mecanismos de Registro y Conservación de Respuestas: Implementar mecanismos robustos para registrar y conservar las respuestas a las solicitudes de ejercicio de los derechos ARCO, tal como lo requiere el Art. 51, núm. 9 de la LOPDP.

Garantizar que estos mecanismos cumplan con los requisitos de integridad, confidencialidad y disponibilidad de la información, alineándose con los principios de seguridad de la información de la norma ISO 27001/27002.

7. - Capacitación y sensibilización

Es fundamental desarrollar programas de formación continua para todo el personal que maneje datos personales, estos programas deben centrarse en la importancia de los derechos ARCO y las obligaciones legales bajo la LOPDP. Los responsables del tratamiento de datos personales pueden implementar mecanismos de capacitación y sensibilización a través de cursos, talleres o seminarios, a fin de cubrir los siguientes temas:

- Los participantes deben comprender la importancia de los derechos ARCO para los titulares de datos personales y las obligaciones legales que les corresponden a los responsables del tratamiento.
- Los participantes deben conocer el procedimiento establecido para el ejercicio de los derechos ARCO, incluyendo los requisitos, plazos y términos.
- Los participantes deben conocer las buenas prácticas para el tratamiento de datos personales, incluyendo las medidas de seguridad y protección.
- Los participantes deben ser conscientes y conocer las sanciones leves y graves constantes en los Art. 71 y Art. 72 de la LOPDP.

8.- Sanciones

En la tabla 8 se describe las sanciones a las que serán objetos las empresas por incumplimiento a la LOPDP

Tabla 8

Sanciones Leves

Categoría del Infractor	Rango de Sanciones	Criterios de Proporcionalidad
Servidores o funcionarios del sector público	Multa de 1 a 10 salarios básicos unificados del trabajador en general	Además de la responsabilidad extracontractual del Estado, sujeta a su propia normativa.
Entidades de derecho privado o empresas públicas	Multa del 0,1% al 0,7% del volumen de negocio del año anterior	La multa se establecerá considerando la intencionalidad, reiteración, naturaleza del perjuicio y reincidencia.

La Autoridad de Protección de Datos Personales tendrá en cuenta los siguientes factores para determinar la multa:

- ***Intencionalidad:*** Evalúa la conducta del infractor y su intención al cometer la infracción.
- ***Reiteración:*** Considera si el infractor ha sido previamente sancionado por infracciones de menor o igual gravedad.
- ***Naturaleza del Perjuicio:*** Examina el impacto del daño ocasionado al derecho a la protección de datos personales.
- ***Reincidencia:*** Revisa si las infracciones anteriores son de la misma naturaleza que la actual.

De igual manera, en la tabla 9 se describe las sanciones graves a que serán objeto aquellas personas que incumplen con la LOPDP.

Tabla 9

Sanciones Graves

Categoría del Infractor	Rango de Sanciones	Consideraciones Adicionales

Servidores o funcionarios del sector público	Multa de 10 a 20 salarios básicos unificados del trabajador en general	Esto es además de la responsabilidad extracontractual del Estado, sujeta a su propia normativa.
Entidad de derecho privado o empresa pública	Multa del 0,7% al 1% del volumen de negocio del año anterior	La multa se establecerá en función de la proporcionalidad y se verificará la intencionalidad, reiteración, naturaleza del perjuicio y reincidencia.
Organización sin domicilio ni representación jurídica en Ecuador	Notificación a la autoridad del domicilio principal de la organización	El organismo correspondiente al lugar de domicilio principal sustanciará las acciones o procedimientos necesarios.

La Autoridad de Protección de Datos Personales considerará los siguientes elementos al establecer la multa:

Intencionalidad: Se evaluará la conducta del infractor.

Reiteración: Se considera si ya ha habido sanciones previas por infracciones de menor o igual gravedad.

Naturaleza del perjuicio: Las consecuencias dañinas para los derechos de protección de datos personales.

Reincidencia: Si la infracción anterior es de la misma naturaleza que la actual.

9. - Procesos de verificación

Para cumplir con este objetivo se deberán establecer procesos precisos y eficaces con el propósito de corroborar y asegurar el acatamiento de los derechos ARCO, por ende, se debe establecer mecanismos que posibiliten una respuesta ágil y precisa ante las solicitudes de los

titulares de datos, garantizando así el pleno respeto y ejercicio de sus derechos en conformidad con la legislación vigente.

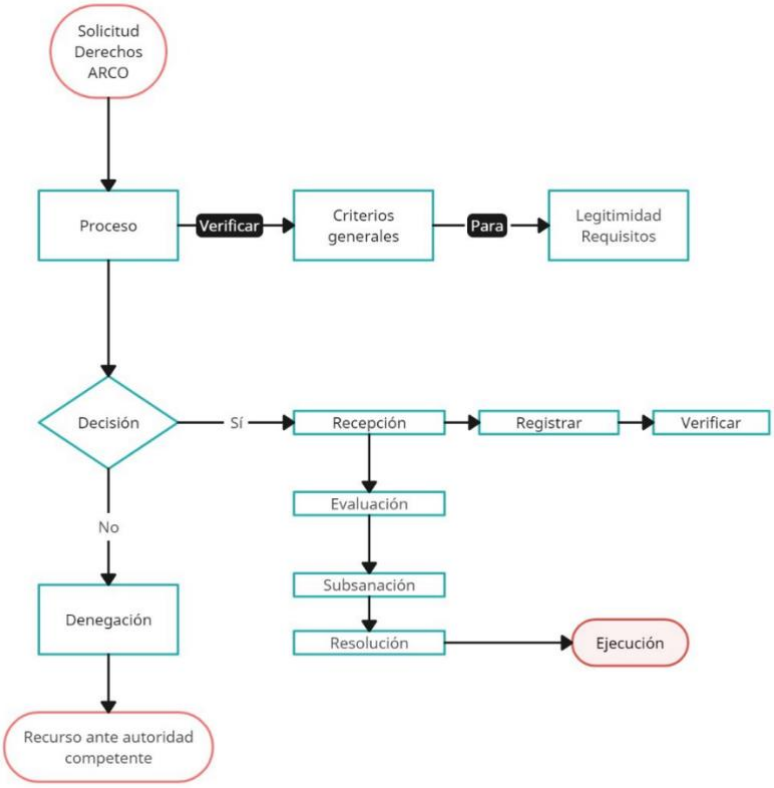
Los responsables del tratamiento de datos personales pueden implementar procesos (Anexo 1) de verificación para garantizar el cumplimiento de los derechos ARCO, los cuales pueden incluir los siguientes elementos:

- Un sistema de registro de solicitudes: El responsable del tratamiento debe registrar todas las solicitudes de ejercicio de los derechos ARCO, incluyendo la fecha de recepción, el estado de la solicitud y la fecha de respuesta. (Anexo 2)
- Un sistema de seguimiento: El responsable del tratamiento debe establecer un sistema para dar seguimiento al cumplimiento de las solicitudes de ejercicio de los derechos ARCO.
- Un proceso de revisión: El responsable del tratamiento debe establecer un proceso para revisar periódicamente el cumplimiento de los derechos ARCO.

A continuación, proponemos un proceso para el tratamiento de las solicitudes referentes a los derechos ARCO

Figura 28

Procedimiento Solicitudes Derechos ARCO



Nota: La descripción de este procedimiento consta en el Anexo 1

10. - Auditorías internas

Realizar inspecciones y evaluaciones internas regulares, este proceso debe analizar de manera completa todos los aspectos del manejo de la información, desde la fase de recopilación hasta la de almacenamiento y eliminación, e incorporar una evaluación del acatamiento de los derechos de (ARCO).

Los responsables del tratamiento de datos personales pueden realizar auditorías internas para evaluar el cumplimiento de los derechos ARCO, conllevando a que puedan cubrir los siguientes aspectos:

- Evaluar si el procedimiento para el ejercicio de los derechos ARCO es claro, sencillo y eficiente.

- Evaluar si el personal que maneja datos personales está capacitado y sensibilizado sobre los derechos ARCO.
- Evaluar si los procesos de verificación son adecuados para garantizar el cumplimiento de los derechos ARCO.

11. - Uso de blockchain

La aplicación de tecnologías innovadoras, como la incorporación del almacenamiento de información mediante la tecnología de cadena de bloques (blockchain), puede ayudar a reforzar la protección de la información personal, esta cadena de bloques proporciona un método seguro y transparente para el registro de datos, esto puede garantizar que exclusivamente personas debidamente autorizadas tengan acceso a la información personal.

Los encargados del tratamiento de datos personales tienen la opción de emplear la tecnología blockchain como medio seguro y descentralizado para almacenar información personal, proporcionando una diversidad de ventajas en términos de protección de datos personales, destacándose las siguientes:

- Utiliza un sistema de cifrado y autenticación que hace que los datos personales sean muy difíciles de alterar o eliminar, es decir a través del blockchain brinda mayor seguridad y protección de los datos personales.
- Registra todos los cambios realizados en los datos personales, lo que facilita la auditoría y el seguimiento porque la información es transparente y trazable.

Blockchain puede ayudar a los responsables del tratamiento de datos personales a demostrar el cumplimiento de las normativas de protección de datos de varias maneras:

En primer lugar, la claridad en el manejo de la información personal se refiere al hecho de que este registro distribuido es accesible para todos los participantes en la red. Esto puede ser beneficioso para quienes gestionan los datos, ya que les permite demostrar de manera

efectiva su cumplimiento con las obligaciones de transparencia, como la responsabilidad de informar a los propietarios de datos personales acerca de cómo se están tratando los mismos.

En segundo lugar, la seguridad del tratamiento de datos personales, utiliza un sistema de cifrado y autenticación que hace que los mismos sean muy difíciles de alterar o eliminar, facilitando a los responsables del tratamiento a comprobar que están cumpliendo sus obligaciones de seguridad, como la responsabilidad de proteger los datos personales contra el acceso no autorizado, el uso indebido, la divulgación, la alteración o la destrucción.

En tercer lugar, la trazabilidad del tratamiento de datos personales, en virtud que registra todos los cambios realizados en los datos personales, lo que facilita la auditoría y el seguimiento, cumpliendo con las obligaciones de trazabilidad, como la obligación de conservar registros de las actividades de tratamiento de datos personales.

Tabla 10

Ejemplos de Implementación de Blockchain

Derecho ARCO	Riesgo Regulatorio	Ejemplo de implementación con smart contracts y blockchain	Aplicación de blockchain
Acceso	El responsable del tratamiento no proporciona acceso a los datos personales a los titulares de datos personales cuando estos lo solicitan.	Un smart contract podría utilizarse para automatizar el proceso de acceso a los datos personales. El smart contract podría requerir que el responsable del tratamiento proporcione acceso a los datos personales al titular de datos personales en un plazo determinado.	Los datos personales se almacenarían en una cadena de bloques pública, lo que permitiría al titular de datos personales verificar que los mismos son correctos y se están utilizando de manera adecuada.
Derecho ARCO	**Riesgo Regulatorio**	**Ejemplo de implementación con**	**Aplicación de blockchain**

		smart contracts y blockchain	
Oposición	El responsable del tratamiento no suspende o limita el tratamiento de los datos personales cuando los titulares de datos personales lo solicitan.	Un smart contract podría utilizarse para automatizar el proceso de suspensión o limitación del tratamiento de los datos personales. El smart contract podría requerir que el responsable del tratamiento suspenda o limite el tratamiento de los datos personales en un plazo determinado.	Los datos personales se almacenarían en una cadena de bloques pública, lo que permitiría al titular de datos personales verificar que el tratamiento de sus datos personales ha sido suspendido o limitado.
Rectificación	El responsable del tratamiento no rectifica los datos personales cuando estos son inexactos o incompletos.	Un smart contract podría utilizarse para automatizar el proceso de rectificación de los datos personales. El smart contract podría requerir que el responsable del tratamiento rectifique los datos personales en un plazo determinado.	Los datos personales se almacenarían en una cadena de bloques pública, lo que permitiría al titular de datos personales verificar que los datos personales han sido corregidos.
Cancelación	El responsable del tratamiento no cancela/elimina los datos personales cuando los titulares de datos personales lo solicitan.	Un smart contract podría utilizarse para automatizar el proceso de cancelación de los datos personales. El smart contract podría requerir que el responsable del tratamiento cancele los datos personales en un plazo determinado.	Los datos personales se almacenarían en una cadena de bloques pública, lo que permitiría al titular de datos personales verificar que los mismos han sido eliminados.

La tecnología blockchain puede aplicarse a los smart contracts para los derechos ARCO de las siguientes maneras:

- Transparencia: Permite a las partes ver todos los cambios realizados en los datos personales, lo que incremente la transparencia y la confianza.
- Integridad: Implementan un mecanismo de acuerdo mutuo para asegurar que los datos personales solo se alteren con el consentimiento unánime de todas las partes involucradas.
- Inmutabilidad: Los datos personales almacenados en una cadena de bloques son inmutables, lo que significa que no pueden ser modificados o eliminados sin dejar rastro.

Estas características de la tecnología blockchain pueden ayudar a mitigar los riesgos regulatorios de los derechos ARCO asociados a la LOPDP en Ecuador. Por ejemplo, la transparencia de la tecnología blockchain puede ayudar a garantizar que los titulares tengan acceso a sus datos personales y que estos se estén utilizando de manera adecuada. La integridad de la tecnología blockchain permite que los datos personales no sean modificados sin el consentimiento del titular. La inmutabilidad garantiza que los registros de tratamiento de datos personales sean precisos y completos.

Es necesario considerar que la aplicación de la tecnología blockchain a los smart contracts para los derechos ARCO debe considerarse los requisitos de la legislación aplicable y las necesidades específicas de cada empresa u organización. Por ejemplo, es vital asegurarse que blockchain utilizada sea segura y robusta para garantizar que los datos personales estén protegidos adecuadamente.

12. – Seguimiento y Evaluación

La supervisión y análisis constante de la implementación del protocolo son cruciales para garantizar el cumplimiento efectivo de los objetivos establecidos. Esta vigilancia continua ofrece una oportunidad invaluable para identificar cualquier desviación, realizar ajustes necesarios y mejorar continuamente la efectividad del protocolo en tiempo real.

A su vez una evaluación periódica permite obtener una visión holística del rendimiento, pues identifica áreas de mejora y garantizar la alineación continua con los estándares y metas predefinidos. Por lo tanto, la diligente observación y evaluación del proceso no solo respaldan la consecución de los objetivos, sino que también permiten una gestión proactiva y adaptativa del protocolo en función de las circunstancias cambiantes.

Es necesario definir indicadores clave de rendimiento que permitan medir la efectividad del protocolo en términos de cumplimiento de la LOPDP y protección de los derechos ARCO. Estos indicadores pueden incluir el número de solicitudes de acceso, rectificación y cancelación procesadas, el tiempo de respuesta a estas solicitudes, y la cantidad y naturaleza de las incidencias de seguridad de datos reportadas.

Implementar auditorías periódicas para evaluar la adherencia al protocolo y la eficacia de las medidas de seguridad y privacidad implementadas. Estas auditorías pueden ser internas o realizadas por terceros independientes.

Crear canales para recibir comentarios de los titulares de datos y otros stakeholders. Esta retroalimentación es crucial para entender la eficacia del protocolo desde la perspectiva del usuario.

Basándose en los resultados de los indicadores de rendimiento, las auditorías y la retroalimentación, realizar revisiones periódicas del protocolo. Esto incluye actualizar las políticas y procedimientos para reflejar cambios en la legislación, avances tecnológicos o lecciones aprendidas de incidentes de seguridad.

13. Formación y Concienciación

Desarrollar y mantener programas de formación para garantizar de que todo el personal que participa en el tratamiento de datos personales asuma su rol y responsabilidades bajo el

protocolo y la LOPDP. Esto incluye formación sobre cómo gestionar adecuadamente los derechos ARCO y cómo responder a las solicitudes de los titulares de datos.

Asegurar que los materiales de formación estén actualizados con la legislación vigente, las mejores prácticas en la industria y cualquier cambio en el protocolo.

Realizar ejercicios y simulacros para evaluar la preparación del personal y la eficacia de los procedimientos del protocolo en escenarios realistas.

Promover una cultura de privacidad y seguridad de datos en toda la institución, resaltando la necesidad de proteger los derechos ARCO y la responsabilidad individual y colectiva en la protección de datos personales.

Implementar métodos para evaluar la efectividad de los programas de capacitación, como pruebas, encuestas de retroalimentación y evaluaciones de desempeño.

Capítulo 4

i. Conclusiones

La investigación se centró en cómo los responsables del tratamiento de datos personales en Ecuador pueden identificar y mitigar los riesgos regulatorios sobre los derechos ARCO. El objetivo general de desarrollar un protocolo integral de gestión de riesgos regulatorios, enfocado en los derechos ARCO y soportado por la tecnología blockchain, se ha cumplido satisfactoriamente, por cuanto este protocolo no solo aborda la identificación, evaluación y mitigación de riesgos en el tratamiento de datos personales, sino que también se alinea con la Ley Orgánica de Protección de Datos Personales de Ecuador, proporcionando un marco claro y efectivo para su aplicación. Su diseño permite a los responsables del tratamiento de datos en Ecuador identificar de manera precisa las áreas de riesgo y aplicar directrices claras para el tratamiento de datos personales, en conformidad con la LOPDP. La inclusión de

la tecnología blockchain en el protocolo permite brindar seguridad y transparencia en la gestión de datos personales; y que sea un medio eficiente para mitigar riesgos regulatorios.

La hipótesis de que si el protocolo es una herramienta eficaz para los responsables del tratamiento de datos personales se confirma a través de su desarrollo, que facilita la implementación de la LOPDP, mejorando la comprensión y el cumplimiento de los derechos ARCO.

Las estrategias y prácticas incorporadas en el protocolo han resultado en una mitigación de los riesgos identificados, contribuyendo a la protección de los derechos de los titulares de datos personales. Para lo cual, se realizó un análisis exhaustivo de la LOPDP, comprendiendo las disposiciones claves relacionadas con los derechos ARCO. Este análisis fue fundamental para diseñar un protocolo acorde con la normativa vigente.

Se examinaron detalladamente los riesgos regulatorios asociados a los derechos ARCO en Ecuador, identificando las principales áreas de riesgo y los desafíos específicos a abordar mediante la obtención de los resultados obtenidos a través de las encuestas y el análisis bibliográfico donde se obtuvieron los siguientes enfoques:

Conciencia sobre los Derechos ARCO

La encuesta reveló una brecha significativa en el conocimiento y la implementación de los derechos ARCO. Mientras que las empresas muestran mayor conciencia, una gran parte de la población general carece de conocimiento sobre estos derechos esenciales. Este desequilibrio, resalta la urgente necesidad de educación y formación en derechos de protección de datos personales.

Ejercicio de Derechos ARCO y Preparación para Gestionar Riesgos

Entre las personas naturales, solo una fracción ha ejercido sus derechos ARCO, y pocas empresas se consideran preparadas para enfrentar riesgos regulatorios asociados. Esto indica una desconexión entre la conciencia de los derechos y la acción para protegerlos.

Percepción de Riesgos Regulatorios y Seguridad en la Web

La percepción elevada de riesgos regulatorios y la inseguridad en el entorno web sugirió una necesidad de crear e implementar protocolos robustos para la protección de datos personales, así como la respectiva capacitación. La integración de tecnologías como el blockchain, podría ser clave para mitigar estos riesgos.

Uso y Conocimiento de Blockchain para Protección de Datos

A pesar de su potencial, la comprensión y adopción del blockchain son limitadas. Esto presenta una oportunidad para fomentar su uso en la gestión de datos personales, abordando los desafíos normativos y técnicos.

Los resultados de las encuestas, junto con la bibliografía analizada, revelaron una necesidad urgente de mejorar la educación en protección de datos y la implementación de prácticas adecuadas. La adopción de tecnologías como el blockchain y el desarrollo de protocolos de gestión de riesgos son esenciales para avanzar en la protección de datos personales en Ecuador. Es importante abordar estos desafíos de forma proactiva y creativa, asegurando el equilibrio entre seguridad y cumplimiento normativo, así como adaptando las soluciones a las necesidades específicas tanto de personas naturales como jurídicas.

La inclusión del blockchain en el protocolo se justifica técnica y legalmente por varias razones:

- Utiliza sistemas de cifrado y autenticación que protegen los datos personales de accesos no autorizados y manipulaciones, alineándose con los requisitos de seguridad de la LOPDP de Ecuador.
- Registra todas las transacciones de datos de manera transparente y trazable, lo cual es crucial para el cumplimiento de los derechos ARCO y las obligaciones de transparencia y responsabilidad bajo la LOPDP y otras normativas como el RGPD.
- La utilización de contratos inteligentes puede automatizar y agilizar los procesos relacionados con los derechos ARCO, mejorando la eficiencia operativa y el cumplimiento normativo.

En el contexto ecuatoriano, donde la protección de datos personales es un tema emergente, la integración del blockchain en el protocolo representa una solución innovadora y efectiva. Sin embargo, es crucial considerar las implicaciones legales y técnicas de su aplicación, asegurándose de que la tecnología se use de manera que respete las normativas vigentes y las necesidades específicas de cada organización

Por otra parte, en este proyecto se desarrolló sistemas adecuados para supervisar y evaluar la efectividad del protocolo, garantizando su adecuación y relevancia a lo largo del tiempo. También, se elaboró programas de capacitación enfocados en la importancia y el manejo adecuado de los derechos ARCO y la aplicación del protocolo, contribuyendo a una mayor conciencia y comprensión entre los responsables del tratamiento de datos y los titulares.

La incorporación de la tecnología blockchain en el protocolo plantea consideraciones éticas importantes, especialmente en términos de privacidad y autonomía de los titulares de datos. Mientras que la blockchain aumenta la transparencia y la seguridad, también requiere un manejo cuidadoso para proteger la privacidad de los individuos.

El protocolo promueve una ética de respeto a los derechos individuales y la confidencialidad, alineándose con el principio de que los individuos deben tener control sobre sus datos personales. Esto implica que cualquier uso de datos en la blockchain debe basarse en el consentimiento informado de los individuos.

Este estudio proporciona un apoyo valioso al campo de la protección de datos en Ecuador, ofreciendo un marco práctico y teórico para afrontar los desafíos actuales en el tratamiento de datos personales. La implementación efectiva del protocolo propuesto tiene el potencial de mejorar significativamente la confianza del público en las organizaciones que gestionan datos personales, fortaleciendo así la relación entre ciudadanos y entidades privadas o públicas en el contexto digital.

Este trabajo de investigación ha cumplido con su hipótesis y objetivos, proporcionando un protocolo integral y efectivo para la gestión de riesgos regulatorios asociados a los derechos ARCO, y ofreciendo un enfoque innovador y éticamente responsable en la protección de datos personales en Ecuador.

Finalmente, el estudio ha respondido afirmativamente a la pregunta central y ha confirmado la hipótesis planteada. El protocolo diseñado es una herramienta efectiva para los responsables del tratamiento de datos personales en Ecuador, facilitando la implementación de la LOPDP y mejorando la gestión de los riesgos regulatorios asociados a los derechos ARCO. Su implementación representa un paso significativo hacia una gestión más transparente, responsable y ética de los datos personales en el país.

ii. Recomendaciones

Se sugiere realizar estudios adicionales para evaluar el impacto a largo plazo del protocolo en la protección de datos personales en Ecuador, incluyendo el análisis de la

integración de tecnologías emergentes como la inteligencia artificial y el aprendizaje automático.

Cabe recalcar que aunque el enfoque hermenéutico y las encuestas proporcionaron una base sólida para el análisis; lo cual, amplió el marco metodológico para incluir métodos cualitativos adicionales, como entrevistas en profundidad o grupos focales con expertos y profesionales en el área de la protección de datos personales en Ecuador, podría enriquecer aún más el estudio, facilitando una comprensión más profunda de las actitudes, experiencias y expectativas de los actores clave en relación con la protección de datos personales y el uso del blockchain.

Referencias Bibliográficas

Cadwalladr, C. (2018). *Los archivos de Cambridge Analytica. El Guardián.* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Camacho Gutiérrez, P. J., & Velásquez Veloza, T. (2022). *Desafíos en la protección de datos personales.* Editorial Universidad de Bogotá.

Christidis, K., & Devetsikiotis, M. (2016). *Blockchains y contratos inteligentes para Internet de las cosas*. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Cisne, M. (2015). Blockchain: *El futuro de la integridad de datos. Blockchain Blueprint*.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *COSO ERM - Marco Integrado de Gestión del Riesgo*.

Departamento de Justicia de Estados Unidos. (2015). *Historia de la privacidad de datos en EE.UU. Gobierno de los Estados Unidos.*

International Organization for Standardization. (2018). *ISO 31000:2018 - Gestión del riesgo - Directrices.*

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2020). *Protección de datos y privacidad: El enfoque internacional.* Oxford University Press.

Asamblea Nacional, Ley Orgánica de Protección de Datos Personales de Ecuador. (2021).

Llamas Covarrubias, J. (2021). *Transparencia y protección de datos personales en la cadena de bloques.* Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM.

López Carballo, P. (2021). *Privacidad y protección de datos en la era d*igital. *Protección de datos y habeas data: una visión desde Iberoamérica.* Editorial Jurídica Andina.

Martínez, M. (2020). *Ley Orgánica de Protección de Datos Personales: comentario y concordancias.* Ediciones Legales.

Mendoza Enríques, O. (2020). *Blockchain y protección de datos personales*. Revista Iberoamericana de Derecho Informático, 8, 107-120.

Morales Cáceres, A. (2023). Blockchain: *Teoría y práctica, aspectos legales y técnicos.* Universidad Oberta de Catalunya.

Mougayar, W. (2016). *Blockchain y su aplicación en la protección de datos*. Revolución Blockchain.

Organización Internacional de Normalización. (2015*). ISO 9001:2015 - Sistemas de gestión de la calidad* - Requisitos. https://www.iso.org/standard/62085.html

Parlamento Europeo y del Consejo, de 27 de abril de 2016, Reglamento (UE) 2016/679

Remache Arias Jaily, S. (2019). Análisis de los aspectos tecnológicos del marco regulatorio para la protección de datos personales en Ecuador.

Roldán Carrillo, M. (2020). *Protección de datos personales en Ecu*ador. Ediciones Legales.

Savelyev, A. (2017). *Derecho de contratos 2.0: contratos inteligentes como el principio del fin del derecho de contratos clásico. Information & Communications Technology Law,* 26(2), 116-134. https://doi.org/10.1080/13600834.2017.1301036

Semana. (2021). *Facebook revela qué provocó la filtración de más de 530 millones de datos*. https://www.semana.com

Schwartz, P. M., & Peifer, K. N. (2017). *La evolución de la privacidad de datos: EE. UU. y la UE.* Cambridge University Press.

Solange Maqueo, R., & Viecens, M. F. (2022). *Protección de datos en América Latina: Un análisis comparativo.* Editorial Jurídica Latinoamericana.

The Open Group. (2018). Gestión de Riesgos.

Unión Europea. (1995). *Directiva de Protección de Datos de 1995*. Diario Oficial de la Unión Europea, L 281.

Unión Europea. (2018). *Reglamento General de Protección de Datos (RGPD*). Diario Oficial de la Unión Europea.

Zuckerberg, M. (2018). *Testimonio de Mark Zuckerberg ante el Congreso de Estados Unidos.* Cámara de Representantes de Estados Unidos.

12.- Anexos: Procedimiento y formato de solicitud para el ejercicio de los derechos ARCO

Procedimiento para el Ejercicio de Derechos ARCO de conformidad con la Ley Orgánica de Protección de Datos Personales en Ecuador (LOPDP) (Anexo1)

Para responsables del Tratamiento de Datos en Ecuador

1.- OBJETO:

Describir el procedimiento para que los titulares de datos personales ejerzan sus derechos ARCO (acceso, rectificación, cancelación/eliminación y oposición) en conformidad con la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador.

2.- DERECHOS ARCO (Artículos 13 al 16 de la LOPDP):

Derecho de acceso: Obtener información sobre sus datos personales tratados, la finalidad del tratamiento y las transferencias realizadas.

Derecho de rectificación: Corregir datos inexactos o incompletos.

Derecho de cancelación/eliminación: Solicitar la eliminación de datos personales cuando no sean necesarios o pertinentes.

Derecho de oposición: Oponerse al tratamiento de los datos personales en determinadas circunstancias.

3.- CRITERIO GENERALES:

3.1. Legitimidad: Solo el titular de los datos personales o su representante legal puede ejercer los derechos ARCO.

3.2. Presentación de la Solicitud: La solicitud debe dirigirse al responsable del tratamiento de datos, incluyendo la información y documentación necesaria.

3.3. Requisitos de la Solicitud:

- Identificación del titular de los datos personales.

- Domicilio o dirección electrónica para notificaciones.
- Detalle del derecho ARCO ejercido y especificación de los datos personales implicados.
- Documentación que sustente la petición, en caso de rectificación.
- Fecha y firma del solicitante.

4.-. PROCEDIMIENTO:

- Recepción: Registrar la solicitud ARCO y verificar la legitimidad del solicitante.
- Evaluación: Revisar si la solicitud cumple con todos los requisitos.
- Subsanación: Solicitar información adicional o corrección de errores, si es necesario.
- Resolución: Emitir una respuesta formal dentro de los plazos establecidos por la LOPDP (Artículos 13 al 16).
- Ejecución: En caso de aceptación, proceder con el acceso, rectificación, cancelación/eliminación u oposición del tratamiento de datos.

5.- DENEGACIÓN DE LA SOLICITUD:

El ejercicio de los derechos ARCO puede ser denegado en los casos especificados en el artículo 18 de la LOPDP, como cuando los datos no pertenecen al solicitante o cuando existen impedimentos legales.

6.- RECURSOS:

El titular de datos tiene derecho a recurrir ante la autoridad competente en caso de no estar satisfecho con la respuesta o si se incumplen los plazos establecidos para la resolución de la solicitud.

Una vez leído el “Procedimiento para el Ejercicio de Derechos ARCO de conformidad con la Ley Orgánica de Protección de Datos Personales en Ecuador (LOPDP)” sírvase descargar y presentar el formulario que se presenta a continuación:

Formulario de Ejercicio de Derechos ARCO (Anexo 2)

Datos del Titular

1. Nombre completo:
   _____
0. Identificación (CI/Pasaporte):
   _____
0. Domicilio (para recibir notificaciones):
   _____
0. Teléfono de Contacto:
   _____
0. Correo electrónico:
   _____

Datos del Representante (en caso de ser menor de edad)

1. Nombre Completo del Representante:
   _____
0. Identificación (CI/Pasaporte) del Representante:
   _____
0. Documento acreditativo de la representación:
   _____
0. Teléfono de Contacto:
   _____
0. Correo electrónico:
   _____

Derecho que desea ejercer (marque con una X el derecho que desea ejercer):

- Acceso – Solicito se me proporcione la información de los datos personales que son objeto de tratamiento.
- Rectificación – Solicito la corrección de mis datos personales que sean inexactos o incompletos.
- Cancelación – Solicito la eliminación de mis datos personales.
- Oposición – Manifiesto mi oposición al tratamiento de mis datos personales para determinados fines.

Descripción detallada de la solicitud:
(Especifique la información que desea acceder, los datos personales que desea rectificar o cancelar, o los motivos de su oposición al tratamiento).

_____
_____
_____

Documentación que adjunta (en caso de ser necesario para acreditar su identidad o la inexactitud de los datos):

- Copia de Documento de Identidad.
- Otros (específicos).

_____
_____
_____
_____

Autorizaciones

Consigno mi autorización para que mis datos personales sean tratados con el fin de dar trámite a la presente solicitud.

Fecha y Firma:

Fecha:

_____

Firma:

(Si el formulario se envía por medios electrónicos, incluya una declaración de conformidad).