

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

[DOI 10.35381/noesisin.v7i2.598](https://doi.org/10.35381/noesisin.v7i2.598)

Consentimiento informado y afectación al principio de confidencialidad

Informed consent and impact on the principle of confidentiality

Ariana Dolores Calle-Morillo

arianacm35@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0009-0001-5925-9979>

Gladis Margot Proaño-Reyes

posgrado@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0000-0003-1653-5889>

Fernando de Jesús Castro-Sánchez

fernandodcs.ainv@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0000-0003-3937-8142>

Recibido: 15 de abril 2025
Revisado: 15 de mayo 2025
Aprobado: 15 de julio 2025
Publicado: 01 de agosto 2025

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

RESUMEN

La relación entre el consentimiento informado y el principio de confidencialidad en el marco de la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador resalta la importancia de proteger los datos personales, fundamentándose en la Constitución y la normativa vigente. El objetivo de la investigación consiste en analizar el consentimiento informado suscrito por el titular de los datos, enfatizando la necesidad de advertir que el almacenamiento de la información podría verse vulnerado y afectar, en primera instancia, el principio de confidencialidad. Se aplicó una metodología cualitativa con enfoque descriptivo y analítico, mediante análisis documental y entrevistas con expertos. Los resultados evidencian que, aunque el consentimiento informado es un requisito legal, su implementación presenta deficiencias. Se identificó la necesidad de incluir advertencias sobre posibles riesgos de seguridad, fortaleciendo la protección de la confidencialidad y garantizando que los titulares de datos conozcan el manejo y almacenamiento de su información personal.

Descriptor: Consentimiento informado; confidencialidad; protección de datos; privacidad de la información; normativa legal. (Tesoro UNESCO).

ABSTRACT

The relationship between informed consent and the principle of confidentiality within the framework of Ecuador's Organic Law on Personal Data Protection (LOPDP) highlights the importance of protecting personal data, based on the Constitution and current regulations. The objective of the research is to analyze the informed consent signed by the data subject, emphasizing the need to warn that the storage of information could be compromised and affect, in the first instance, the principle of confidentiality. A qualitative methodology with a descriptive and analytical approach was applied, using document analysis and interviews with experts. The results show that, although informed consent is a legal requirement, its implementation has shortcomings. The need to include warnings about possible security risks was identified, strengthening the protection of confidentiality and ensuring that data subjects are aware of how their personal information is handled and stored.

Descriptors: Informed consent; confidentiality; data protection; information privacy; legal regulations. (UNESCO Thesaurus).

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

INTRODUCCIÓN

En el contexto normativo ecuatoriano, el consentimiento informado y la confidencialidad son dos conceptos que han cobrado una relevancia significativa, no solo en el ámbito médico o jurídico, sino en todos los aspectos de la vida en los que se requiere el manejo de información personal. Estos principios fundamentales se encuentran entrelazados en una relación que asegura el respeto a la autonomía individual y la protección de los derechos fundamentales de las personas, tal como lo establece la Constitución de la República del Ecuador y otras leyes específicas. La importancia de estos conceptos se ve reflejada en la legislación reciente, que busca adecuarse a los desafíos que presenta la sociedad moderna, especialmente en lo que respecta a la protección de datos personales.

El consentimiento informado se define como un proceso mediante el cual una persona toma una decisión libre, voluntaria y consciente, basada en la información suficiente y comprensible sobre los riesgos y beneficios de una determinada acción. Este concepto se encuentra profundamente arraigado en el derecho a la autonomía personal y al respeto por la dignidad humana, principios reconocidos tanto en la Constitución ecuatoriana como en diversas leyes y regulaciones.

El artículo 66 de la Constitución del Ecuador garantiza el derecho a la integridad personal, incluyendo la integridad física, psíquica y moral, lo que se traduce en la obligación de obtener el consentimiento informado de una persona antes de someterla a cualquier tipo de intervención, ya sea médica, legal, o de cualquier otra índole. La Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021, refuerza esta obligación al establecer que el tratamiento de datos personales solo puede llevarse a cabo con el consentimiento explícito del titular de los datos, excepto en casos donde la ley disponga lo contrario (Art. 8, LOPDP).

El consentimiento informado no solo es esencial en el ámbito médico, sino también en la educación, la investigación científica, la publicidad y el marketing, y cualquier

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

actividad que involucre la recolección y uso de datos personales. En el ámbito educativo, las instituciones deben obtener el consentimiento de los estudiantes o sus representantes legales para la recopilación y uso de datos académicos y personales, asegurando que los interesados comprendan los fines para los cuales se utilizarán dichos datos (Ministerio de Educación del Ecuador, 2022).

A su vez, la confidencialidad es un principio que protege la privacidad y la seguridad de la información personal en todas las esferas de la vida. En Ecuador, este principio está garantizado por la Constitución y es regulado por la LOPDP. En ella se establece que los datos personales deben ser tratados de manera confidencial y que cualquier divulgación de esta información debe estar autorizada por el titular de los datos, a menos que la ley exija lo contrario (Art. 31, LOPDP).

La confidencialidad es un componente esencial en la relación entre individuos y organizaciones, ya que garantiza que la información personal compartida en confianza no será utilizada de manera indebida o divulgada sin permiso. Este principio es particularmente relevante en el sector de la salud, donde la confidencialidad de los datos médicos es fundamental para proteger la intimidad del paciente. No obstante, su aplicación es igualmente crítica en otros ámbitos, como el financiero, el laboral y el digital, donde la protección de la información personal es clave para evitar abusos y preservar la confianza de los usuarios.

En el sector financiero, por ejemplo, las instituciones están obligadas a proteger la confidencialidad de la información de sus clientes, lo cual incluye datos bancarios, transacciones y cualquier otra información sensible. La Superintendencia de Bancos del Ecuador ha establecido normativas estrictas para garantizar que estas instituciones implementen medidas de seguridad adecuadas y que solo accedan a los datos las personas autorizadas, bajo el principio de necesidad y proporcionalidad (Superintendencia de Bancos, 2021).

El consentimiento informado y la confidencialidad están intrínsecamente relacionados,

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

ya que el primero es un requisito esencial para garantizar el segundo. Cuando una persona otorga su consentimiento informado, lo hace con la expectativa de que la información proporcionada será manejada de manera confidencial y utilizada únicamente para los fines acordados. Cualquier violación de la confidencialidad sin el debido consentimiento no solo constituye una infracción legal, sino que también socava la confianza en la relación entre la persona y la institución o el profesional que maneja sus datos.

En el ámbito digital, esta relación adquiere una importancia crítica debido al manejo masivo de datos personales. La proliferación de plataformas en línea y servicios digitales ha generado nuevas oportunidades para la recopilación de datos, pero también ha aumentado los riesgos de violaciones de confidencialidad. La LOPDP establece que las empresas que operan en el entorno digital deben obtener el consentimiento informado de los usuarios para la recolección y uso de sus datos, asegurando que comprendan cómo se utilizarán sus datos y qué medidas de seguridad se implementarán para proteger su confidencialidad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2023).

Este marco legal también aplica en situaciones cotidianas, como el uso de aplicaciones móviles, redes sociales y plataformas de comercio electrónico. Los usuarios deben ser informados de manera clara sobre los datos que se recopilan, los fines de su uso, y los mecanismos disponibles para ejercer su derecho a la protección de datos, incluyendo la posibilidad de revocar su consentimiento en cualquier momento.

Aunque el marco normativo ecuatoriano proporciona una base sólida para la protección del consentimiento informado y la confidencialidad, existen desafíos significativos en su implementación práctica. Uno de los principales retos es la falta de conocimiento y concienciación por parte de la población sobre sus derechos en relación con el manejo de sus datos personales. Además, la rápida evolución tecnológica plantea nuevas amenazas a la confidencialidad, como el riesgo de ciberataques y el uso indebido de

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

datos por parte de terceros.

Para enfrentar estos desafíos, el gobierno ecuatoriano, a través del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), ha desarrollado iniciativas para fortalecer la seguridad cibernética y promover la educación digital entre la población. Estas iniciativas incluyen campañas de sensibilización sobre la importancia del consentimiento informado y la confidencialidad, así como la implementación de marcos de seguridad cibernética en el sector público y privado (MINTEL, 2023).

Por otro lado, la legislación ecuatoriana continúa evolucionando para adaptarse a los nuevos desafíos que surgen en el manejo de datos personales. La promulgación de normativas más específicas y detalladas, junto con la creación de organismos de control que garanticen el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD), constituyen pasos fundamentales para fortalecer la protección de estos derechos en todos los ámbitos de la vida. En este contexto, el objetivo de la investigación es analizar el consentimiento informado suscrito por los titulares de los datos, haciendo especial énfasis en la necesidad de advertir que el almacenamiento de la información podría verse vulnerado y, como consecuencia, afectar principalmente el principio de confidencialidad.

MÉTODO

Por su modalidad o enfoque, se trató de un estudio cualitativo, cuyo propósito fue el examen a profundidad conceptual y documental de una relación entre el consentimiento informado y su incidencia en el principio de confidencialidad. En cuanto a su alcance, se caracterizó por ser descriptiva y analítico - explicativa.

En su componente descriptivo, se procedió a identificar y detallar las normas legales, principios éticos y jurisprudencia que rigen el consentimiento informado y la confidencialidad en el contexto ecuatoriano. Se hizo un mapeo exhaustivo de la legislación vigente y de los casos judiciales que han abordado estos temas, con el fin

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

de establecer un marco claro de referencia. El aspecto analítico-explicativo de la investigación permitió ir más allá de la simple descripción, examinando críticamente las posibles tensiones y desafíos que surgen cuando el consentimiento informado entra en juego con la necesidad de proteger la confidencialidad. Este análisis buscó identificar situaciones donde el cumplimiento de uno de estos principios pueda comprometer el otro, lo que es crucial para entender las implicaciones prácticas y éticas en la protección de los derechos individuales.

Esta investigación fue realizada con el método de análisis documental, ejerciendo para el efecto la recopilación documental que abarcó normativas vigentes, análisis doctrinales de especialistas en derecho, y sentencias judiciales relevantes que discutieron o implementaron el consentimiento informado y la protección de la confidencialidad en diversas situaciones. Este enfoque fue crucial, ya que en dichos textos se encontró información necesaria para conceptualizar, caracterizar y concluir sobre la base de las posiciones y propuestas bibliográficas preexistentes respecto al consentimiento informado y su impacto en el principio de confidencialidad.

En cuanto a la población y muestra, el estudio se enfocó en la identificación y análisis de documentos relevantes y actores clave que proporcionaron una comprensión profunda y detallada sobre el consentimiento informado y el principio de confidencialidad en el contexto de la protección de datos personales.

En cuanto a la muestra de carácter objetual, se seleccionaron cuidadosamente leyes, decretos, y fallos judiciales que aborden de manera explícita los principios de consentimiento informado y confidencialidad. Esta selección incluyó tanto casos emblemáticos como normativas recientes que fueron fundamentales en la modificación o clarificación de estos conceptos, proporcionando un marco normativo actualizado y pertinente.

También se incluyeron documentos internos provenientes de hospitales, clínicas, y otras instituciones legales, que establecen procedimientos específicos para el manejo

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

del consentimiento informado y la confidencialidad. Estos documentos fueron cruciales para entender cómo se aplican estos principios en la práctica diaria, ofreciendo una perspectiva sobre los protocolos y directrices que guían las acciones de los profesionales de la salud y del derecho.

En lo que se refiere a la muestra de sujetos especialistas o expertos implicados, la misma se concentró en tres expertos y se empleó la técnica de entrevista para la recolección de la información valiosa que aportaron sobre el tema investigado. Los tres expertos han tenido una amplia trayectoria en el ámbito de la protección de datos personales, la cual se resume a continuación:

- **Experto N.º 1:** Reconocido profesional en protección de datos y ciberseguridad, con más de 30 años de experiencia en consultoría estratégica, mercantil, tecnológica y de cumplimiento. Ha ocupado roles clave como Delegado de Protección de Datos (DPO) en diversas instituciones, incluyendo el Colegio de Abogados de Las Palmas y el Consejo Canario de Colegios de Abogados. Además, dirige el Diplomado de Privacidad y Cumplimiento en la Universidad de Santiago de Chile (USACH). Especialista en la implementación de sistemas de gestión de ciberseguridad y protección de datos, contando con certificaciones internacionales como Lead Auditor en ISO 27001, ISO 27701 y otras normas ISO relevantes para la seguridad de la información y la continuidad del negocio. Es un firme defensor de la privacidad como derecho fundamental y enfatiza la importancia de la concienciación sobre los riesgos asociados al tratamiento de datos personales.
- **Experto N.º 2:** Se especializa en protección de datos y derechos digitales. Es doctor en Derecho por la Universitat de València, donde también ejerce como profesor de Derecho Constitucional y dirige la Cátedra de Privacidad y Transformación Digital, apoyada por Microsoft. Su investigación se centra en el derecho fundamental a la protección de datos y en los desafíos que presentan las tecnologías de la información y la comunicación, especialmente en ámbitos como la

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

salud y la inteligencia artificial. Ha sido un actor clave en la elaboración de la Carta de Derechos Digitales de España y ha participado en proyectos europeos relacionados con la innovación en el uso de datos, como BigMedilytics. Además, defiende la ética y la transparencia en la implementación de la inteligencia artificial, subrayando la necesidad de supervisión humana y la protección de los derechos fundamentales en este ámbito.

- **Experto N.º 3:** Profesional destacado en Derecho de las Tecnologías de la Información y protección de datos. Actualmente es CEO de la firma Govertis y Delegado de Protección de Datos (DPO) en el Ilustre Colegio de Abogados de Valencia. Posee una amplia trayectoria en el sector público y privado, desempeñando funciones relacionadas con el cumplimiento normativo y la ciberseguridad. Ha ejercido como DPO en diversas organizaciones, incluidas el Consejo Valenciano de Colegios de Abogados y Corts Valencianes, y ha sido docente en programas de maestría, como los de la UNIR. Cuenta con un Máster en Derecho Informático y otro en Inteligencia Artificial, y su experiencia abarca la privacidad, la seguridad de la información y el cumplimiento normativo en sectores regulados.

RESULTADOS

Análisis de la normativa

El análisis e investigación realizada revela que, aunque la Ley Orgánica de Protección de Datos Personales del Ecuador establece claramente la necesidad de obtener el consentimiento informado para el tratamiento de datos personales, existen brechas en su aplicación práctica. En varios casos, el consentimiento se obtiene de manera genérica y sin la debida explicación de los fines específicos para los cuales se utilizarán los datos. Esto puede llevar a situaciones donde la confidencialidad se vea comprometida, especialmente en contextos donde los datos son compartidos con

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

terceros sin el conocimiento o la aprobación explícita del titular.

Asimismo, se encontró que la ley promueve la protección de la confidencialidad, su inobservancia puede ser objeto de sanción civil, administrativa e incluso penal. La falta de supervisión adecuada contribuye a la vulnerabilidad de los datos personales frente a usos no autorizados.

Análisis de los resultados de la técnica de entrevista realizada

Las entrevistas realizadas a tres expertos en protección de datos señalaron que la Ley Orgánica de Protección de Datos Personales en Ecuador marca un avance importante en la defensa de los derechos digitales de los ciudadanos. Sin embargo, la implementación de la ley enfrenta varios retos significativos, especialmente en lo que respecta al consentimiento informado. Los expertos coinciden en que, aunque la normativa requiere el consentimiento explícito de los titulares de los datos, muchas organizaciones aún no comprenden plenamente qué constituye un consentimiento válido y suficientemente informado. Esta falta de comprensión compromete la base sobre la cual se fundamenta el tratamiento legítimo de los datos personales.

En relación con la protección de la confidencialidad, los especialistas señalan que, aunque la normativa es sólida en su formulación, su efectividad en la práctica está en duda. La supervisión del manejo de datos personales es insuficiente, y tanto las organizaciones como los ciudadanos muestran una falta de concienciación que limita la eficacia de la ley. Sobre el consentimiento informado los expertos, indican que las organizaciones ecuatorianas se encuentran en una etapa temprana en cuanto a la adopción de prácticas adecuadas para obtener el consentimiento informado. Aunque se han comenzado a utilizar formularios de consentimiento, estos a menudo son genéricos y no proporcionan la información necesaria para que los titulares de los datos puedan tomar decisiones realmente informadas. Los especialistas identifican una tendencia a obtener consentimientos de manera apresurada, sin detallar claramente los fines específicos del tratamiento de los datos.

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

Recalcan que los principales desafíos incluyen la falta de comprensión por parte de las organizaciones y los ciudadanos sobre lo que implica un consentimiento informado. Esta falta de entendimiento impide que los titulares de los datos reconozcan sus derechos y las implicaciones del consentimiento que otorgan. Además, las organizaciones a menudo carecen de procedimientos estandarizados y transparentes para obtener y gestionar el consentimiento, lo que puede llevar a incumplimientos inadvertidos.

Los expertos también observan que la mayoría de los ciudadanos aún no comprende completamente el concepto de consentimiento informado. Este déficit en la educación sobre privacidad y protección de datos limita la efectividad de la protección de la privacidad en el país.

En cuanto al principio de confidencialidad, los expertos en protección de datos consultados consideran que las medidas actuales para garantizar la confidencialidad de los datos personales en Ecuador son insuficientes. A pesar de que la ley establece claramente el principio de confidencialidad, en la práctica, muchas organizaciones no cuentan con sistemas adecuados para proteger los datos contra accesos no autorizados o filtraciones. La falta de formación especializada en ciberseguridad y la ausencia de auditorías regulares agravan esta deficiencia.

Un caso reciente en el Ecuador citado por los expertos ilustra la falta de confidencialidad como fue el caso de una institución financiera que experimentó una filtración de datos sensibles de miles de clientes debido a una vulnerabilidad en su sistema de gestión de datos. Este incidente afectó gravemente la confianza del público y resultó en sanciones legales y demandas colectivas, subrayando la necesidad de medidas más estrictas para proteger la confidencialidad.

Los expertos recomiendan que las organizaciones adopten políticas de seguridad de la información, capaciten continuamente a su personal en protección de datos y realicen auditorías regulares. Además, sugieren que las sanciones por incumplimientos deberían

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

ser más severas para incentivar el cumplimiento.

Sobre la interrelación entre consentimiento y confidencialidad, los expertos consultados coinciden en que la falta de un consentimiento informado adecuado impacta negativamente en el principio de confidencialidad. Si el consentimiento no se obtiene de manera adecuada, los titulares de los datos pueden no estar al tanto de cómo se utilizarán o compartirán sus datos, lo que puede resultar en divulgaciones no autorizadas. Sin un consentimiento claro y específico, las organizaciones pueden sentirse tentadas a utilizar los datos para fines no autorizados, violando así la confidencialidad.

Desde una perspectiva legal, los entrevistados destacan que la vulneración del principio de confidencialidad debido a un consentimiento inadecuado puede llevar a sanciones severas, incluyendo multas significativas y responsabilidad civil por daños. Éticamente, tal violación erosiona la confianza pública en las instituciones y puede tener consecuencias duraderas para la reputación de la organización implicada, afectando especialmente a individuos con información sensible.

En cuanto a mejoras y recomendaciones en la protección de la confidencialidad en el manejo de datos personales, los expertos recomiendan la implementación de campañas educativas dirigidas tanto a las organizaciones como al público general sobre la importancia del consentimiento informado y cómo debe gestionarse correctamente. También sugieren el desarrollo de guías y herramientas prácticas para ayudar a las organizaciones a obtener y gestionar el consentimiento de manera más eficaz y transparente. La creación de un sistema de certificación para organizaciones que cumplan con altos estándares de protección de datos podría ser un incentivo adicional para mejorar las prácticas de confidencialidad.

Recalcan que es necesario revisar y actualizar la normativa actual para abordar mejor los desafíos actuales y emergentes. En particular, se debería prestar atención a las disposiciones sobre el consentimiento informado para que sean más detalladas

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

y específicas. También es importante fortalecer las sanciones por incumplimientos y mejorar los mecanismos de supervisión.

La educación y concienciación de los ciudadanos son vistas como clave para mejorar la efectividad del consentimiento informado y la protección de la confidencialidad. Programas educativos en escuelas, universidades y campañas públicas pueden jugar un papel crucial en elevar el nivel de conocimiento sobre estos temas y fomentar una cultura de respeto por la privacidad.

En lo referido a la perspectiva futura los expertos, puntualizan que en los próximos cinco años haya un fortalecimiento del marco regulatorio en Ecuador, con una mayor adopción de buenas prácticas por parte de las organizaciones. La creciente digitalización y el uso de tecnologías emergentes, como la inteligencia artificial, harán que la protección de datos sea aún más crítica. Se anticipa un enfoque mayor en la transparencia, el empoderamiento del ciudadano y la implementación de tecnologías avanzadas para la protección de la confidencialidad.

Los expertos también sugieren que tendencias internacionales como la privacidad por diseño y por defecto, establecidas en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, y la aplicación de estándares internacionales de seguridad de la información, como la ISO/IEC 27001, podrían beneficiar a Ecuador. Además, la adopción de prácticas efectivas de supervisión y sanción observadas en otras jurisdicciones podría ser útil para mejorar la protección de datos en el país.

DISCUSIÓN

Los resultados obtenidos en este estudio refuerzan la importancia crítica de incluir advertencias sobre las vulnerabilidades en la seguridad del almacenamiento de datos dentro del consentimiento informado. Como señala Roldán (2021), la omisión de tales advertencias en el consentimiento informado puede generar una falsa sensación de seguridad entre los titulares de datos, lo que podría resultar en un manejo inadecuado

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

de la información personal. Este punto es particularmente relevante en el contexto ecuatoriano, donde la Ley Orgánica de Protección de Datos Personales (LOPDP) establece que el consentimiento informado debe ser libre, específico, informado e inequívoco (Art. 8). Sin embargo, la ley no detalla explícitamente la necesidad de advertir sobre posibles brechas de seguridad, lo que podría considerarse una laguna en la normativa.

La LOPDP refuerza el requisito de que el consentimiento debe ser informado. De conformidad con el artículo 10 literal c), el requisito de transparencia es uno de los principios fundamentales, estrechamente relacionado con los principios de lealtad y juridicidad. Si no se cumplen los requisitos relativos al consentimiento informado, el consentimiento no será válido y el responsable podrá estar incumpliendo el artículo 7 literal 1 de la LOPDP.

Como lo indica Meo (2010) facilitar información a los interesados antes de obtener su consentimiento es esencial para que puedan tomar decisiones informadas, comprender qué es lo que están autorizando, producto de esto por ejemplo puedan ejercer su derecho a retirar su consentimiento. Si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos.

Por tanto, es imperativo que las organizaciones ecuatorianas no solo cumplan con los requisitos legales mínimos establecidos en la LOPDP, sino que vayan más allá, incluyendo advertencias explícitas sobre las posibles vulnerabilidades de seguridad en el almacenamiento de datos. Esta medida no solo alinearía mejor las prácticas con las recomendaciones internacionales, como las directrices de la Organización de Estados Americanos (OEA) sobre privacidad y protección de datos, sino que también fortalecería el principio de confidencialidad, que es un pilar fundamental en la protección de los derechos de los titulares de datos. Además, el Reglamento de Protección de Datos Personales, que complementa la LOPDP, podría servir como una herramienta crucial

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

para establecer directrices más detalladas sobre cómo deben ser abordadas estas advertencias en el consentimiento informado.

Es importante considerar que este estudio se basa en un análisis normativo y documental, lo que limita la capacidad de observar cómo se implementan estas advertencias en la práctica diaria. Tal es así que Martínez (2019) destaca que las limitaciones inherentes a los estudios teóricos requieren que se realicen investigaciones empíricas que permitan evaluar la efectividad real de las normativas en la protección de la confidencialidad. Además, la evolución constante de las tecnologías y las amenazas cibernéticas sugiere que las recomendaciones presentadas aquí podrían necesitar ser revisadas y adaptadas en un futuro cercano para mantener su relevancia y efectividad.

Con base en las limitaciones y hallazgos de este estudio, se sugieren varias líneas de investigación futuras. Primero, sería valioso realizar estudios empíricos que recojan directamente las experiencias y percepciones de los ciudadanos y de las entidades que manejan datos sobre el consentimiento informado y la confidencialidad. Además, investigaciones comparativas entre diferentes países latinoamericanos podrían proporcionar una visión más amplia y revelar mejores prácticas que podrían ser adoptadas en Ecuador.

Otra área prometedora de investigación es el impacto de las nuevas tecnologías, como la inteligencia artificial y el *big data*, en la aplicación del consentimiento informado y la protección de la confidencialidad. Finalmente, estudios que analicen la efectividad de las campañas de sensibilización y educación sobre protección de datos podrían ofrecer estrategias para mejorar la aplicación de la LOPDP y fortalecer la protección de los derechos de los titulares de datos.

CONCLUSIONES

La investigación destaca la importancia de que el consentimiento informado no solo cumpla con los requisitos básicos de ser libre, específico, informado e inequívoco, sino

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

que también incluya advertencias sobre las posibles vulnerabilidades en la seguridad del almacenamiento de datos personales que tendría como consecuencias la afectación al principio de confidencialidad.

En un entorno donde las brechas de seguridad y los ciberataques son cada vez más comunes, es esencial que los titulares de datos comprendan plenamente los riesgos a los que pueden estar expuestos sus datos, incluso después de haber dado su consentimiento. Esto no solo aumenta la transparencia y la confianza de las instituciones que almacenan datos, sino que también permite a los individuos tomar decisiones más informadas y cautelosas sobre el manejo de su información personal y evitar litigios entre las partes.

La incorporación de advertencias en el consentimiento informado es decisiva para proteger y respetar el principio de confidencialidad que se basa en la promesa de que la información personal será resguardada y utilizada exclusivamente para los fines acordados, sin divulgación no autorizada. Sin embargo, si no se advierte adecuadamente a los titulares de datos sobre las posibles vulneraciones de seguridad, se corre el riesgo de comprometer gravemente este principio, lo que podría generar desconfianza en el sistema de protección de datos y en las instituciones responsables de su manejo.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTOS

A todos los actores sociales involucrados en el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Anónimo. (2019). Comentario al documental sobre el escándalo de Cambridge Analytica. Nada es privado. *Andina, Agencia Peruana de Noticias*. <https://n9.cl/6k8wk>

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

- Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador* (Registro Oficial N. 449). <https://n9.cl/5rpt3>
- Asensi Merás, A. (2022). Los riesgos asociados a las plataformas digitales de financiación participativa derivados de la privacidad y la protección de datos personales en el mercado. *RDSisFin*, (3), 151-180. <https://doi.org/10.32029/2695-9569.01.05.2022>
- BBC News. (2019, septiembre 16). Filtración de datos en Ecuador: La grave falla informática que expuso la información personal de casi toda la población del país sudamericano. *BBC News Mundo*. <https://n9.cl/2bpcl>
- Código Orgánico Integral Penal [COIP]. (2014). *Registro Oficial Suplemento* 180 (10 de febrero). <https://n9.cl/w5nul>
- Garriga, A. (2019). Nuevos retos para la protección de datos personales en la era del Big Data y de la computación ubicua. *Vlex*. <https://app.vlex.com/#WW/sources/14328>
- Machuca Vivar, S. A., Vinuesa Ochoa, N. V., Sampedro Guamán, C. R., & Santillán Molina, A. L. (2020). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, 14(2), 244-251. <https://n9.cl/vwqnl>
- Martínez, J. (2019). Vida privada sin intimidad: Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo. *Revista Derecho y Libertades*, (40), 1-20. <https://n9.cl/g4je6>
- Meo, A. I. (2010). Consentimiento informado, anonimato y confidencialidad en investigación social: La experiencia internacional y el caso de la sociología en Argentina. *Aposta. Revista de Ciencias Sociales*, 44, 1-30. <https://n9.cl/kgndlf>
- Organización de los Estados Americanos. (2021). *Principios actualizados sobre la privacidad y la protección de datos personales*. Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos. <https://n9.cl/7fxl6>
- Roldán Carrillo, F. N. (2021). Los ejes centrales de la protección de datos: Consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. *USFQ Law Review*, 8(1), 175-202. <https://doi.org/10.18272/ulr.v8i1.2184>

Ariana Dolores Calle-Morillo; Gladis Margot Proaño-Reyes; Fernando De Jesus Castro-Sánchez

Sanchez Campos, K. E. (2022). *Propuesta de un modelo de seguridad informática para la protección de datos en la Municipalidad distrital de Pinra, Huánuco 2022*. [Tesis de licenciatura, Universidad César Vallejo]. Repositorio UCV. <https://repositorio.ucv.edu.pe/handle/20500.12692/103456>

Vera Navas, N. A. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales*. [Tesis de maestría, Universidad Politécnica Salesiana]. Repositorio Institucional de la Universidad Politécnica Salesiana. <https://dspace.ups.edu.ec/handle/123456789/20949>

©2025 por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0) (<https://creativecommons.org/licenses/by-nc-sa/4.0/>)