**PRIVACIDAD DE DATOS PERSONALES: UNA PERSPECTIVA LEGAL**

Andrea Zúñiga1, Gleiston Guerrero2,

1Ministerio de Educación, El Empalme, Ecuador

[andrear.zuniga@educacion.gob.ec](mailto:andrear.zuniga@educacion.gob.ec)

<https://orcid.org/0000-0002-6231-262X>

3Universidad Técnica Estatal de Quevedo, Quevedo, Ecuador

2[gguerrero@uteq.edu.ec](mailto:gguerrero@uteq.edu.ec)

**Correspondencia**: andrear.zuniga@educacion.gob.ec

## Resumen

El acceso a la información pública, especialmente en los contratos públicos, es esencial para la transparencia y la democracia. Sin embargo, las cláusulas de confidencialidad suelen limitar este derecho. Aunque existen leyes que protegen el acceso a la información, es fundamental analizar los límites de estas cláusulas para evitar que se utilicen indebidamente para ocultar información relevante.

En Ecuador, los desafíos relacionados con la ciberseguridad y los delitos informáticos incluyen una legislación insuficiente, definiciones imprecisas de delitos informáticos y una falta de promoción de protocolos seguros. Para enfrentar estos problemas, se requiere fortalecer el marco legal, educar a la población sobre ciberseguridad y destinar recursos para combatir estos delitos.

Para evaluar la justificación de una cláusula de confidencialidad, se puede usar el principio de proporcionalidad y la prueba del daño. El principio de proporcionalidad analiza si la restricción es adecuada, necesaria y equilibrada, mientras que la prueba del daño evalúa si la divulgación causaría un daño específico. Este análisis debe ser continuo y flexible, permitiendo divulgaciones parciales cuando sea posible.

El acceso a la información pública, especialmente en los contratos públicos, es esencial para la transparencia y la democracia. Sin embargo, las cláusulas de confidencialidad suelen limitar este derecho. Aunque existen leyes que protegen el acceso a la información, es fundamental analizar los límites de estas cláusulas para evitar que se utilicen indebidamente para ocultar información relevante.

Promulgar y actualizar leyes específicas que regulan la recolección, almacenamiento, uso y transferencia de datos personales, alineadas con estándares internacionales como el Reglamento General de Protección de Datos (GDPR).

Promover la anonimización y cifrado de datos, cada gobierno debe asegurar de que los datos personales sean tratados de manera que no puedan identificar directamente a los individuos, empleando técnicas de anonimización o cifrado; el mismo debe establecer políticas claras de acceso a la información, que equilibren la transparencia con la protección de los datos personales, evitando la divulgación indebida.

Crear campañas de sensibilización sobre los derechos de privacidad y las mejores prácticas para proteger datos personales en entornos digitales.

Establecer una institución encargada de monitorear el cumplimiento de las leyes de protección de datos, investigar violaciones y sancionar incumplimientos, implementando revisiones periódicas en sistemas que manejen información personal para identificar y mitigar posibles vulnerabilidades.

En conclusión, garantizar la transparencia y el acceso a la información pública debe ir de la mano con el fortalecimiento de la privacidad de los datos personales. Aplicar herramientas como el principio de proporcionalidad, la prueba del daño y las recomendaciones mencionadas refuerzan los pilares de una sociedad democrática y responsable.

**Introducción**

Desde un enfoque legal, las medidas de seguridad para proteger la privacidad de los datos incluyen el cumplimiento de normativas como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea, Ley de Privacidad del Consumidor de California (CCPA) en EE. UU y la Ley Orgánica de Protección de Datos Personales LOPDP en Ecuador, que regulan la recopilación, almacenamiento y procesamiento de datos personales (Duong Dang & Tero Vartiainen, n.d.).

Entre las principales amenazas se encuentran el robo de información, phishing, ingeniería social y ciberataques, los cuales comprometen la sostenibilidad de los sistemas y generan pérdida de confianza. Para mitigar estos riesgos, es crucial implementar medidas técnicas, capacitar a los usuarios y establecer políticas organizativas que garanticen la gestión integral de la seguridad. (Duong Dang & Tero Vartiainen, n.d.)

En la era digital, la privacidad de los datos personales es crucial debido al avance tecnológico que ha transformado su recopilación y uso. Aunque la digitalización mejora la eficiencia y personalización de los servicios, también plantea desafíos éticos, legales y sociales que exigen una mayor protección de la privacidad. (Renuka et al., 2025).

La tecnología ha transformado sectores como el laboral, ampliando la recopilación de datos personales a espacios antes privados, como en el teletrabajo. Esto resalta la necesidad de regulaciones robustas y tecnologías para proteger la privacidad, como herramientas de anonimización y encriptación (Karkout, 2024).

La revisión sistemática sobre protección de datos personales implica definir un objetivo claro, establecer criterios de selección, buscar literatura relevante en bases de datos académicos, evaluar críticamente los estudios seleccionados y sintetizar los resultados. Esto permite identificar tendencias, vacíos y propuestas en aspectos legales, tecnológicos y sociales, proporcionando una visión integral del tema.

El presente trabajo de revisión sistemática sobre protección de datos personales contiene una introducción que justifica la importancia del tema y establece las preguntas de investigación. Luego, se describe la metodología, explicando cómo se seleccionaron y analizaron los estudios incluidos. En la sección de resultados, se presentan los hallazgos organizados por categorías clave, como marcos legales, herramientas tecnológicas y retos sociales. La comparación de los resultados, destaca las limitaciones de los estudios y sugiere áreas para futuras investigaciones. Finalmente, la conclusión resume los principales aportes de la revisión y su relevancia para el campo de estudio.

**Contextualizar en el Ecuador. (artículos de revisión del estado del arte)**

En Ecuador, la protección de datos personales es crucial ante amenazas como ciberataques y delincuencia. Este documento tiene el objetivo de examinar bibliografía sobre las seguridades de datos para garantizar la privacidad de datos personales.

Solo el 3% de las empresas cuenta con herramientas avanzadas de ciberseguridad, aunque las grandes organizaciones invierten en personal capacitado. El cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD) y la adopción de tecnologías avanzadas, junto con la capacitación y colaboración estratégica, son esenciales para mitigar riesgos, fortalecer la confianza y garantizar(Sánchez Ramírez & Andaluz Granda, n.d.-a)

Código Orgánico Integral Penal (COIP, 2014): Este código define y penaliza varias formas de delitos informáticos, incluyendo el acceso no autorizado a sistemas informáticos y la violencia sexual digital. Un ejemplo específico es el artículo 232, que se centra en el "Ataque a la integridad de sistemas informáticos". Este artículo penaliza a quienes destruyan, dañen, alteren o supriman datos informáticos o mensajes de correo electrónico, con penas de prisión que pueden llegar hasta 7 años si se afecta infraestructura crítica.(Ponce Tubay, 2024)

Ley Orgánica de Protección de Datos Personales (2021): Esta ley regula la gestión y protección de datos personales.

Ley Orgánica de Telecomunicaciones (2015): Esta ley incluye disposiciones sobre la seguridad de las redes y la información.

Esta revisión se enfoca en los temas clave que conforman el campo de estudio sobre privacidad de datos personales, a incluir desde los marcos regulatorios y las teorías que explican el concepto de privacidad, hasta las implicaciones de tecnologías emergentes como la inteligencia artificial, y el análisis predictivo. El análisis también considera aspectos éticos, conductuales y técnicos, subrayando la necesidad de un enfoque integral para abordar esta problemática compleja y en constante evolución.

La revisión de la literatura sobre privacidad de datos personales destaca su constante evolución ante la digitalización y el creciente uso de tecnologías que procesan datos personales. El avance tecnológico ha transformado la organización laboral, permitiendo trabajar desde ubicaciones distintas al centro de trabajo, adaptándose a las nuevas realidades digitales y laborales.​(Javier Martín Jiménez, n.d.)​

**Trabajos relacionados**

Aguirre Sánchez (2021) realiza una revisión sistemática de la base de datos IEEE sobre tecnologías de seguridad en bases de datos, analizando 34 artículos de 2015-2020 relacionados con modelos de seguridad, vulnerabilidades y fragmentación de datos. Sin embargo, el estudio no aborda específicamente la seguridad de datos personales en Ecuador.

Rosas-Lanas & Pila-Cárdenas (2023) presenta información relevante sobre la protección de datos personales en Ecuador, pero no se enfoca en estudios de revisión sistemática, encuestas o mapeos específicamente sobre este tema. El enfoque principal del artículo es la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador en 2021 y la revisión histórica del reconocimiento de este derecho fundamental en el país.

El artículo también menciona que el derecho a la protección de datos personales en Ecuador se reconoció por primera vez en la reforma constitucional de 1996, pero no fue hasta 2008 que se reconoció como un derecho autónomo en la Constitución. (Rosas-Lanas & Pila-Cárdenas, 2023)

Finalmente, el artículo analiza los desafíos de la era digital para la protección de datos personales, incluyendo la desactualización normativa, la falta de observancia del principio de minimización de datos y la resistencia a adoptar mecanismos de autorregulación. (Rosas-Lanas & Pila-Cárdenas, 2023)

Sánchez-Henarejos (2014) menciona un caso específico de la seguridad de datos personales protege la información sensible contra accesos, usos o divulgaciones no autorizados, garantizando confidencialidad, integridad y disponibilidad. Busca mitigar amenazas que puedan comprometer la privacidad y generar repercusiones legales o éticas. Es fundamental para salvaguardar derechos en entornos digitales. ​​

Sánchez Ramírez & Andaluz Granda, los autores mencionan que, en Ecuador, la seguridad de datos personales enfrenta desafíos como infraestructura deficiente y falta de inversión en tecnologías de protección. En el ámbito digital, destacan la baja adopción de medidas de ciberseguridad y la escasez de talento especializado. Estos factores exigen estrategias dinámicas para enfrentar amenazas en evolución.

Los estudios en mención destacan que los artículos no proporcionan información específica sobre estudios de revisión sistemática, encuestas o mapeos sobre datos personales en Ecuador.

**Estado del arte**

Los avances en IA, blockchain e IoT plantean desafíos legales como la falta de normativas actualizadas, la transparencia en decisiones automatizadas y la eliminación de datos en sistemas descentralizados. Además, la interoperabilidad regulatoria transnacional complica su gestión. Es crucial equilibrar innovación y protección de la privacidad. (Espinoza Solorzano & Bernabeu Aubán, 2024)

Los desafíos legales en la adopción de tecnologías avanzadas, son una preocupación importante en el contexto de la soberanía de datos. La ausencia de normativas específicas para tecnologías como la IA, blockchain e IoT, junto con la falta de transparencia en las decisiones automatizadas, presenta un desafío para garantizar la privacidad y seguridad de los datos(Espinoza Solorzano & Bernabeu Aubán, 2024)

En el Marco legal en desarrollo, si bien existen leyes y regulaciones relacionadas con la protección de datos y la ciberseguridad en Ecuador, el marco legal aún está en desarrollo. La interpretación y aplicación de las leyes a las nuevas tecnologías, como la IA y el blockchain, puede ser un desafío. (Espinoza Solorzano & Bernabeu Aubán, 2024)

En Ecuador, la falta de colaboración entre empresas, gobierno e instituciones educativas dificulta enfrentar los desafíos de seguridad de datos personales. Compartir recursos y promover mejores prácticas es esencial para crear un entorno digital confiable. Es crucial invertir en tecnologías robustas, capacitar al personal y fomentar políticas que impulsen un ecosistema seguro.(Sánchez Ramírez & Andaluz Granda, n.d.-b)

Además de estas leyes, las reformas al Código Orgánico Integral Penal en 2019 y 2021 han fortalecido la lucha contra los delitos informáticos, especificando y ampliando las definiciones y sanciones relacionadas con estos crímenes. Sin embargo, a pesar de estos esfuerzos legislativos, la legislación ecuatoriana en materia de ciberseguridad presenta algunas debilidades como:

* Falta de precisión en las definiciones legales: La amplitud en la definición de "acceso no autorizado" en el COIP (2014) puede llevar a aplicaciones desproporcionadas de la ley, criminalizando actividades sin intención maliciosa.
* Falta de alineación con los estándares internacionales: A pesar de las reformas, la legislación ecuatoriana no está completamente alineada con los estándares internacionales en materia de ciberseguridad.
* Falta de recursos para la aplicación de la ley: La Policía Nacional de Ecuador y otros organismos encargados de la seguridad pueden carecer de recursos adecuados para investigar y perseguir delitos informáticos.
* Falta de conciencia pública: La falta de conocimiento sobre los delitos informáticos y sus consecuencias puede dificultar la prevención y la denuncia de estos delitos.
* Penas insuficientes: Las penas para los delitos informáticos pueden no ser lo suficientemente severas para disuadir a los delincuentes.

La implementación de medidas de seguridad para garantizar la privacidad de datos personales es crucial en el panorama digital actual. A continuación, se evalúan las buenas prácticas legales y regulatorias en este ámbito:

**Marco Legal Robusto:**

Las leyes de protección de datos garantizan derechos y regulan el tratamiento de información personal bajo principios como licitud, finalidad y transparencia. Ejemplos clave son el RGPD[[1]](#footnote-1) en Europa y la LOPD[[2]](#footnote-2) en España. En Ecuador, la Ley Orgánica de Protección de Datos Personales (2021) representa un avance, aunque requiere constante evaluación para garantizar su efectividad.

Leyes Sectoriales: Además de las leyes generales, las regulaciones específicas del sector, como las que rigen la atención médica o las telecomunicaciones, pueden proporcionar protecciones adicionales para los datos personales. Por ejemplo, las normas HIPAA en los Estados Unidos establecen requisitos estrictos para la seguridad y privacidad de la información de salud.

Convenios Internacionales: La adhesión a convenios internacionales sobre protección de datos, como el Convenio 108 del Consejo de Europa, puede ayudar a armonizar las prácticas de privacidad de datos y facilitar la cooperación transfronteriza en la aplicación de la ley.

Principios de Privacidad desde el Diseño y por Defecto:

Incorporación de la Privacidad en las Etapas Iniciales: El principio de "privacidad desde el diseño" aboga por la integración de consideraciones de privacidad en las primeras etapas del desarrollo de sistemas y tecnologías. Esto implica evaluar el impacto en la privacidad, minimizar la recopilación de datos y adoptar medidas de seguridad proactivas en lugar de reactivas.

Configuración Predeterminada de Privacidad: El principio de "privacidad por defecto" exige que la configuración de privacidad más estricta esté habilitada de forma predeterminada, sin que los usuarios tengan que realizar acciones adicionales para proteger sus datos.

Evaluaciones de Impacto en la Privacidad:

●Evaluaciones Obligatorias: Las evaluaciones de impacto en la privacidad (EIP) deben ser obligatorias para los tratamientos de datos que impliquen un alto riesgo para los derechos y libertades de las personas. Estas evaluaciones ayudan a identificar y mitigar los riesgos para la privacidad antes de que se produzca el tratamiento de datos.

Supervisión y Cumplimiento:

●Autoridades de Protección de Datos: Las autoridades de protección de datos independientes desempeñan un papel crucial en la supervisión del cumplimiento de la legislación de privacidad de datos. Estas autoridades deben tener poderes suficientes para investigar las infracciones, imponer sanciones y emitir directrices sobre las mejores prácticas.

●Mecanismos de Rendición de Cuentas: Los responsables del tratamiento de datos deben ser responsables de sus prácticas de privacidad de datos. Esto implica implementar medidas de seguridad apropiadas, documentar sus procesos de tratamiento de datos y someterse a auditorías regulares para demostrar su cumplimiento.

Formación y Concienciación:

●Educación Continua: La formación y la concienciación sobre la privacidad de datos son esenciales para todos los actores involucrados en el tratamiento de datos personales. Los empleados, los desarrolladores y los responsables de la toma de decisiones deben estar al tanto de sus responsabilidades legales y éticas, así como de las mejores prácticas para proteger los datos personales.

●Campañas de Concienciación Pública: Las campañas de concienciación pública pueden ayudar a informar a los ciudadanos sobre sus derechos de privacidad de datos y sobre cómo proteger su información personal en línea.

**Herramientas y Recursos:**

●Guías y Estándares: Las guías y los estándares, como el estándar ISO 27002 sobre seguridad de la información, pueden proporcionar un marco útil para la implementación de medidas de seguridad y la gestión de riesgos para la privacidad de datos.

●Tecnologías de Mejora de la Privacidad: Las tecnologías de mejora de la privacidad (PET) pueden ayudar a minimizar la recopilación y el uso de datos personales, como las técnicas de anonimización y seudonimización.

En resumen, la implementación de medidas de seguridad eficaces para garantizar la privacidad de datos personales requiere un enfoque holístico que abarque un marco legal sólido, la incorporación de principios de privacidad desde el diseño y por defecto, evaluaciones de impacto en la privacidad, mecanismos de supervisión y cumplimiento, y una cultura de formación y concienciación. La protección de los datos personales en la era digital es una responsabilidad compartida entre los gobiernos, las empresas y los ciudadanos.

**Materiales y Métodos**

En una investigación sistemática describen las herramientas, procedimientos y enfoques utilizados para garantizar una recopilación y análisis de datos riguroso y transparente. Incluyen:

1. **Búsqueda de Información:**
   * Bases de datos seleccionadas (e.g., PubMed, IEEE Xplore, Scopus).
   * Criterios de búsqueda (palabras clave, operadores booleanos, filtros de fechas).
2. **Criterios de Inclusión y Exclusión:**
   * Definición clara de qué estudios serán considerados (e.g., idioma, rango temporal, diseño del estudio).
   * Exclusión de duplicados y artículos irrelevantes.
3. **Selección y Evaluación:**
   * Métodos para evaluar la calidad de los estudios (e.g., herramientas como PRISMA).
   * Procedimientos para minimizar sesgos en la selección.
4. **Análisis de Datos:**
   * Métodos cualitativos o cuantitativos para sintetizar resultados (e.g., metaanálisis).
   * Uso de software o herramientas específicas para organizar la información (e.g., Excel, R, NVivo).

Estos métodos garantizan que los resultados sean reproducibles y se ajusten a estándares científicos.

4o

Bases de datos, y buscadores

Protocolo de revisión de Kitchenham

Objetivo:

Preguntas de investigación

**Resultados**

Resultados de las búsquedas

Una tabla con los los resultados

Base de datos cadena de búsqueda resultados artículos diferentes Criterios de inclusión/exclusión

Web of Science 100 100 50

Scopus

IEEE

ACM

**Conclusiones**

Es necesario que el gobierno ecuatoriano mejore y actualice el marco legal, se necesitan leyes más concretas y adaptadas al entorno cambiante de las tecnologías y las amenazas en el ciberespacio. El COIP no contempla sanciones económicas para los delitos informáticos, por lo que debe establecer sanciones económicas. Es importante concienciar a la ciudadanía sobre las amenazas en internet y promover el uso de protocolos de seguridad, también la colaboración internacional es fundamental para combatir los ciberdelitos y evitar la impunidad, por lo que se recomienda firmas de nuevos convenios internacionales.

Ecuador ha realizado esfuerzos para abordar la ciberseguridad a través de la legislación, existen áreas de mejora significativas para fortalecer la protección de la información y combatir los delitos informáticos de manera efectiva.

Considerando normativas y estándares internacionales, así como los desafíos tecnológicos actuales, se pueden extraer las siguientes conclusiones sobre el análisis de las medidas de seguridad aplicadas para garantizar la privacidad de los datos desde un enfoque legal:

El gobierno ecuatoriano necesita actualizar el marco legal en materia de ciberseguridad, adaptándolo a las tecnologías emergentes y amenazas actuales. Es crucial que el COIP incluya sanciones económicas para delitos informáticos, fortaleciendo así las medidas de disuasión y las herramientas legales para combatir estos crímenes.

La concienciación ciudadana es otro pilar fundamental en esta lucha, promoviendo el uso de protocolos de seguridad y educando sobre los riesgos en internet. Además, la colaboración internacional mediante nuevos convenios es clave para enfrentar los ciberdelitos, evitando la impunidad y mejorando las capacidades del país en este ámbito.

Aunque Ecuador ha tomado medidas legislativas para abordar la ciberseguridad, aún existen importantes áreas de mejora. Es necesario reforzar la protección de la información y establecer estrategias efectivas para prevenir y sancionar los delitos informáticos, garantizando un entorno digital más seguro.

En definitiva, garantizar la privacidad de los datos en el entorno digital actual requiere un compromiso continuo por parte de todos los actores involucrados. La combinación de un marco legal sólido, la aplicación de estándares internacionales, la adopción de principios proactivos, la supervisión constante, y la educación continua, son elementos esenciales para afrontar los desafíos presentes y futuros en la protección de la privacidad de los datos.

Bibliografía

Aguirre Sánchez, M. J. (2021). *TECNOLOGÍAS DE SEGURIDAD EN BASES DE DATOS: REVISIÓN SISTEMÁTICA*.

Duong Dang, & Tero Vartiainen. (n.d.). *Exploring Socio-technical Gaps in the Cybersecurity of Energy Informatics for Sustainability*.

Espinoza Solorzano, R., & Bernabeu Aubán, J. M. (2024). *Soberanía de datos: Un Análisis Comparativo de Conceptos y Prácticas en un Mundo Digital Globalizado*.

Karkout, W. (2024). Strategic Innovations in Diplomacy. In Mohamad Zreik (Ed.), *Innovations and Tactics for 21st Century Diplomacy* (pp. 51–72). IGI Global. https://doi.org/10.4018/979-8-3693-6074-3.ch003

Ponce Tubay, M. A. (2024). Delitos informáticos: Caso Ecuador. *Revista San Gregorio*, *1*(58), 119–123. https://doi.org/10.36097/rsan.v1i58.2667

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data Privacy and Protection. In Gulshan Shrivastava, Rudra Pratap Ojha, Shashank Awasthi, Himani Bansal, & Kavita Sharma (Eds.), *Emerging Threats and Countermeasures in Cybersecurity* (pp. 433–465). Wiley. https://doi.org/10.1002/9781394230600.ch19

Rosas-Lanas, G., & Pila-Cárdenas, G. (2023). The protection of personal data in Ecuador A historical-normative review of this fundamental right in the South American country. *VISUAL Review. International Visual Culture Review / Revista Internacional de Cultura* , *10*. https://doi.org/10.37467/revvisual.v10.4568

Sánchez Ramírez, F. P., & Andaluz Granda, L. M. (n.d.-a). *TECNOLOGÍAS DE SEGURIDAD PARA EMPRESAS EN GUAYAQUIL*. *6*, 250–263.

Sánchez Ramírez, F. P., & Andaluz Granda, L. M. (n.d.-b). *TECNOLOGÍAS DE SEGURIDAD PARA EMPRESAS EN GUAYAQUIL*. *6*, 250–263.

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & Carrillo De Gea, J. M. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atencion Primaria*, *46*(4), 214–222. https://doi.org/10.1016/j.aprim.2013.10.008

1. Reglamento General de Protección de Datos [↑](#footnote-ref-1)
2. la Ley Orgánica de Protección de Datos Personales [↑](#footnote-ref-2)