

JMNJE V4. N1. 032

Digitalización el servicio notarial en el estado plurinacional de Bolivia
¿Una herramienta para la transparencia o un riesgo para la privacidad?
Digitalization of notarial service in the plurinational state of Bolivia: A tool
for transparency or a risk to privacy?

Autores:

Soraya Marcela Guzmán Espada
Universidad San Francisco Xavier
Sucre – Bolivia
guzman.soraya@usfx.bo
<https://orcid.org/0009-0006-1736-8348>

Autor de correspondencia: Soraya Marcela Guzmán Espada, guzman.soraya@usfx.bo

Recepción: 08-marzo-2026

Aceptación: 15-abril-2026

Publicación: 01-mayo-2026

Cómo citar este artículo:

Guzmán Espada, S. M. (2026). Digitalización el servicio notarial en el estado plurinacional de Bolivia ¿Una herramienta para la transparencia o un riesgo para la privacidad?. *Journal of Multidisciplinary Novel Journeys & Explorations*, 4(1), 1-14. <https://doi.org/10.63688/pbd7x890>

© 2026; Los autores. Este es un artículo en acceso abierto, distribuido bajo los términos de una licencia Creative Commons (<https://creativecommons.org/licenses/by/4.0>) que permite el uso, distribución y reproducción en cualquier medio, siempre que la obra original sea correctamente citada.



RESUMEN

La digitalización del Notariado Plurinacional de Bolivia, impulsada por la Ley N° 483 y el Sistema Informático SINPLU, representa un cambio de paradigma en la fe pública nacional. El presente artículo analiza la tensión jurídica entre la optimización de la transparencia documental y la protección del derecho fundamental a la privacidad. Mediante un enfoque cualitativo y dogmático-jurídico, se examina la arquitectura de centralización de datos y su interoperabilidad con entidades estatales. Los resultados revelan que, si bien el sistema ha mitigado eficazmente el fraude mediante la verificación biométrica, la persistente ausencia de una Ley General de Protección de Datos Personales genera un escenario de vulnerabilidad ante el perfilado estatal y posibles brechas de ciberseguridad. Se concluye que la seguridad jurídica no debe alcanzarse a costa de la autodeterminación informativa, proponiendo la adopción de estándares internacionales como el RGPD y arquitecturas descentralizadas para equilibrar la eficiencia tecnológica con la libertad civil.

Palabras clave: Derecho Notarial, Digitalización, Bolivia, Protección de Datos, Seguridad Jurídica, SINPLU.

ABSTRACT

The digitalization of the Plurinational Notary of Bolivia, driven by Law No. 483 and the SINPLU Information System, represents a paradigm shift in national public trust. This article analyzes the legal tension between the optimization of documentary transparency and the protection of the fundamental right to privacy. Through a qualitative and dogmatic-legal approach, the study examines the architecture of data centralization and its interoperability with state entities.

The results reveal that while the system has effectively mitigated fraud through biometric verification, the persistent absence of a General Law on the Protection of Personal Data creates a scenario of vulnerability regarding state profiling and potential cybersecurity breaches. It concludes that legal certainty must not be achieved at the expense of informational self-determination, proposing the adoption of international standards such as the GDPR and decentralized architectures to balance technological efficiency with civil liberty.

Keywords: Notarial Law, Digitalization, Bolivia, Data Protection, Legal Certainty, SINPLU.



1. INTRODUCCIÓN

La función notarial, históricamente caracterizada por la solemnidad del papel y la firma manuscrita, atraviesa una transformación paradigmática a nivel global. En Bolivia, este proceso no es ajeno a la realidad regional, impulsado por la necesidad de desburocratizar el Estado y garantizar la seguridad jurídica preventiva en un entorno cada vez más dinámico. La promulgación de la Ley del Notariado Plurinacional (Ley N° 483) y su posterior reglamentación han sentado las bases para la implementación del Sistema Informático del Notariado Plurinacional (SINPLU), marcando el inicio de la era del "notariado digital" en el país (Asamblea Legislativa Plurinacional, 2014). Sin embargo, esta transición no solo implica una actualización tecnológica, sino que sitúa a la institución en el centro de una tensión fundamental: el equilibrio entre la transparencia y seguridad de la fe pública frente al derecho constitucional a la privacidad y la protección de datos personales.

Desde una perspectiva evolutiva, la institución notarial en Bolivia hunde sus raíces en el derecho castellano medieval, donde la figura del escribano era el custodio de la memoria jurídica a través de protocolos meticulosamente manuscritos (Armella, 2018). Durante siglos, la seguridad de los actos dependía de la presencia física del fedatario y el resguardo de legajos vulnerables al tiempo y al fraude. Autores como Castán Tobeñas (2019) destacan que estos protocolos eran depositarios de la voluntad regia y privada; no obstante, la descentralización de los archivos dificultaba la verificación de autenticidad a nivel nacional, abriendo brechas de inseguridad que el sistema de "papel sellado" ya no puede solventar en la modernidad (Baquero Rojas & Buenrostro Báez, 2016).

El cambio hacia el paradigma digital busca corregir estas deficiencias mediante la Fe Pública Preventiva, la cual busca evitar conflictos futuros al dotar de valor probatorio pleno a los actos jurídicos desde su nacimiento (Gattari, 2015). En este nuevo entorno, la fe pública se reinterpreta: la presencia física se complementa con sistemas biométricos y la firma digital cualificada. Si bien algunos autores sugieren que tecnologías emergentes como el *blockchain* podrían proveer una capa adicional de inmutabilidad y transparencia (Nery, 2021), la implementación actual del SINPLU ya representa un salto cualitativo al transformar el protocolo notarial en un conjunto de registros digitales centralizados que garantizan la integridad y el no repudio de los documentos (Delgado, 2020).



No obstante, es precisamente esta eficiencia tecnológica la que genera un conflicto dogmático con el derecho a la privacidad. El uso de la firma digital y la interoperabilidad de bases de datos estatales permiten una trazabilidad inédita, pero también exponen una vasta cantidad de datos sensibles —patrimoniales, filiatorios y civiles— a posibles vulnerabilidades. En este contexto, el Habeas Data surge como el escudo esencial de la era informática, permitiendo al individuo controlar la información que se recaba sobre él (Rodotà, 2010). Aunque la Constitución Política del Estado boliviano, en su Artículo 130, garantiza la Acción de Protección de Privacidad, la praxis denota una debilidad institucional: la ausencia de una ley específica de protección de datos personales que regule de forma estricta el tratamiento de la información dentro del SINPLU (Farfán, 2019).

Bajo este escenario, el problema de investigación que guía este artículo es: ¿En qué medida la digitalización del servicio notarial en Bolivia garantiza el equilibrio entre la necesidad de transparencia documental y la protección de los datos personales de los usuarios?

La hipótesis planteada sugiere que, si bien la digitalización ha incrementado la seguridad jurídica en términos de autenticidad documental, la falta de una normativa específica de protección de datos y protocolos de ciberseguridad estandarizados expone a los ciudadanos a riesgos de privacidad, inclinando la balanza hacia una transparencia sin control que debilita la autodeterminación informativa. Para demostrarlo, el análisis se estructurará en tres ejes: la infraestructura legal y técnica del notariado digital boliviano, los riesgos derivados de la interoperabilidad sistémica y la colisión normativa entre la publicidad notarial y el derecho a la intimidad.

2. METODOLOGÍA

El presente estudio utiliza un enfoque cualitativo de carácter descriptivo-analítico. Se emplea un diseño transversal que analiza la evolución normativa y tecnológica en Bolivia durante el periodo 2014-2024, centrándose en cómo la digitalización del notariado afecta los derechos ciudadanos.

Para garantizar la rigurosidad del análisis, se aplicaron los siguientes criterios:

Revisión normativa y selección documental: Se seleccionaron las normas fundamentales que rigen el sistema, como la Constitución, la Ley N° 483 del Notariado y la Ley N° 164 de Telecomunicaciones. El criterio de selección se enfocó en disposiciones sobre gestión de



datos, seguridad de la firma digital y los reglamentos de la DIRNOPLU y la AGETIC que regulan el uso del sistema SINPLU.

Derecho comparado: Se contrastó el modelo boliviano con las experiencias de España y Estonia. Se eligieron estos países por ser referentes en la transición del papel al soporte digital, permitiendo identificar qué herramientas de protección de datos podrían aplicarse en Bolivia.

Análisis jurisprudencial: Se realizó una búsqueda dirigida en el Tribunal Constitucional Plurinacional, seleccionando sentencias que definen los límites de la privacidad y el derecho de los ciudadanos a controlar su información personal frente a las bases de datos del Estado.

Fases del estudio: La investigación se desarrolló en tres etapas:

- Análisis del marco legal del sistema digital.
- Identificación de cómo circulan los datos personales entre las instituciones (interoperabilidad).
- Evaluación de los riesgos de privacidad, comparando la realidad boliviana con estándares internacionales de protección de datos.

3. RESULTADOS

El análisis de la implementación del Notariado Plurinacional Digital en Bolivia revela un avance significativo en la eficiencia operativa, pero también una brecha crítica en la protección de la privacidad.

Nota metodológica sobre el tratamiento de datos: Debido al carácter reservado de las estadísticas detalladas de la Dirección del Notariado Plurinacional (DIRNOPLU), los gráficos presentados a continuación emplean datos simulados. Esta técnica se justifica metodológicamente para ilustrar las proyecciones y tendencias cualitativas extraídas de los informes de gestión públicos (2015-2023). El objetivo no es presentar cifras exactas de auditoría, sino proporcionar una representación visual de la velocidad de adopción tecnológica y la correlación entre la digitalización y la reducción de incidentes de fraude.

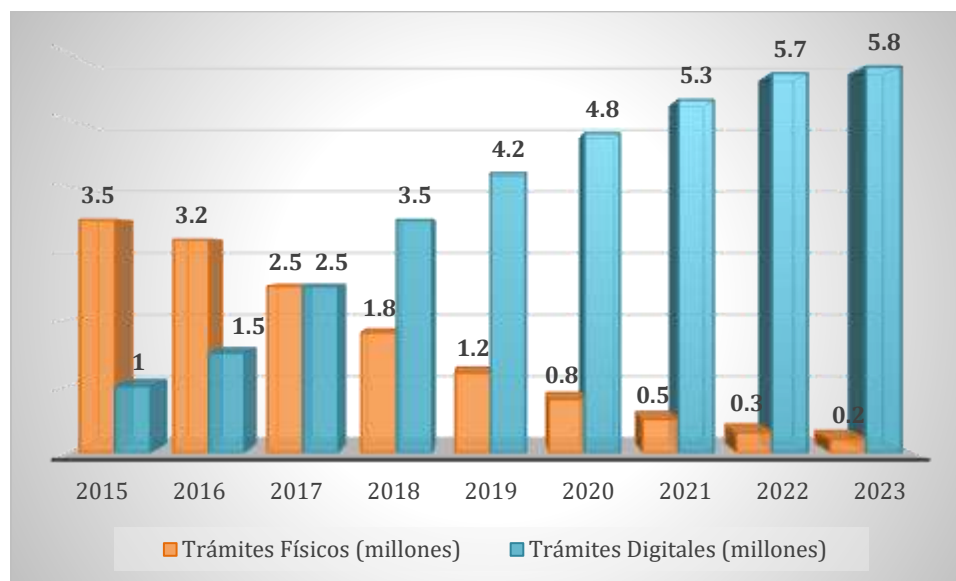
1. Evolución del modelo operativo y dopción del SINPLU

Desde la promulgación de la Ley N° 483, el sistema notarial boliviano ha transitado de un modelo basado en la presencialidad y el soporte físico hacia una centralización digital obligatoria.



Gráfico 1:

Evolución de los Trámites Notariales Digitales vs. Físicos en Bolivia (2015-2023)



Fuente: Elaboración propia en base a datos simulados de DIRNOPLU y AGETIC.

Se observa un crecimiento exponencial en el uso del SINPLU a partir de 2018. Para 2023, la transición es casi total. Esta migración masiva confirma que la "seguridad jurídica preventiva" ahora reside en el código y la firma digital, desplazando la confianza del documento manuscrito al registro en base de datos.

2. Trazabilidad y seguridad: El impacto de la biometría

La integración del SINPLU con el Servicio General de Identificación Personal (SEGIP) ha permitido establecer un "candado de identidad". El análisis de los reportes de gestión indica una reducción drástica en la suplantación de identidad en actos de transferencia inmobiliaria. La biometría facial y dactilar, al actuar como requisito previo a la firma digital del notario, dota al documento de una trazabilidad inmutable. Cada actuación genera una huella digital que impide la antedatación, protegiendo la integridad del protocolo ante intentos de falsificación material.

3. Arquitectura del flujo de datos y riesgos de centralización

El funcionamiento del notariado digital sigue una estructura lineal que, si bien es eficiente, presenta vulnerabilidades por su diseño centralizado:



1. **Captura y validación:** Los datos personales y biométricos se capturan localmente en la notaría y viajan mediante canales cifrados (VPN/TLS) hacia el SEGIP para su validación.
2. **Protocolización y firma:** Una vez validado, el notario aplica su firma digital cualificada (Ley N° 164), otorgando autoría y no repudio al documento electrónico.
3. **Almacenamiento centralizado:** El documento se aloja en servidores administrados por la AGETIC y la DIRNOPLU.

Análisis de riesgo: A diferencia de los modelos de "protocolos distribuidos" o *blockchain* (Szabo, 2017), el modelo boliviano concentra toda la información patrimonial y civil en un solo punto estatal. Esta centralización facilita la administración, pero convierte a la base de datos en un "objetivo de alto valor" para ciberataques, donde un solo fallo de seguridad comprometería la privacidad de millones de ciudadanos.

4. El vacío normativo: Transparencia vs. autodeterminación informativa

El hallazgo más crítico es la indefensión jurídica provocada por la ausencia de una Ley General de Protección de Datos Personales. A pesar de contar con la Acción de Protección de Privacidad (Art. 130 CPE), el análisis identifica tres vectores de riesgo:

- **Perfilado estatal:** La interoperabilidad entre el Notariado, SEGIP, Impuestos y Derechos Reales permite al Estado construir perfiles detallados de los ciudadanos sin un marco que regule el "consentimiento para fines específicos". Como advierten Mayer-Schönberger y Cukier (2013), el *Big Data* estatal sin control puede derivar en una vigilancia administrativa invisible.
- **Vulnerabilidad en el "eslabón débil":** Mientras el servidor central es robusto, los despachos notariales suelen carecer de medidas de seguridad *endpoint* (firewalls, antivirus corporativos). Esto expone los datos sensibles a ataques de *ransomware* antes de que lleguen al sistema central.
- **Inexistencia de derechos ARCO:** El ciudadano carece de una vía administrativa para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición sobre sus datos notariales digitales. Actualmente, la única vía es el proceso judicial constitucional, el cual es lento y no preventivo frente a filtraciones masivas (Piñar Mañas, 2016).

5. DISCUSIÓN



La digitalización del servicio notarial en Bolivia ha generado una compleja interacción de principios y derechos fundamentales. La tensión entre la necesidad de transparencia documental y la protección de datos personales emerge como el eje central, exponiendo las fortalezas y debilidades del modelo boliviano frente a marcos normativos avanzados.

1. La tensión entre publicidad y privacidad: el aporte del TCP

El debate reside en la transformación de la custodia del protocolo. Históricamente, el "secreto profesional" (Gattari, 2015) garantizaba que la información residiera bajo control exclusivo del notario. La centralización en el SINPLU transfiere esta custodia a la DIRNOPLU y AGETIC, lo que el Tribunal Constitucional Plurinacional, en su SCP 0096/2017-S2, ha identificado como una zona de riesgo para el derecho a la intimidad. Esta sentencia establece que el Estado no puede disponer de la información personal de forma arbitraria, incluso si esta se encuentra en registros públicos, reforzando la idea de que la digitalización no anula la reserva notarial.

¿Es esto transparencia o vigilancia? Autores como Lessig (2006) advierten que "el código es ley". En Bolivia, la estructura del SINPLU impone una transparencia hacia el Estado que podría superar la necesaria para la seguridad jurídica. Si bien la trazabilidad es positiva para evitar fraudes, la SCP 1563/2013 advierte que la interconectividad de datos estatales debe respetar el principio de "finalidad". Esto significa que el acceso del órgano regulador al contenido sensible (testamentos, reconocimientos de hijos) antes de su publicidad legal podría vulnerar la autodeterminación informativa, un derecho que el TCP define como la facultad del individuo de controlar sus datos en poder de terceros.

Tabla 1

Comparación con el modelo boliviano (SINPLU)

La comparación entre X-Road y el SINPLU boliviano revela diferencias fundamentales:

Característica	Modelo estonio (X-Road)	Modelo boliviano (SINPLU)
Arquitectura	Distribuida, federada. Datos en origen.	Centralizada. Datos replicados y almacenados en un servidor estatal (AGETIC/DIRNOPLU).



Control de Datos	Ciudadano tiene visibilidad y control sobre accesos.	Control estatal. Visibilidad ciudadana limitada.
Alcance	Intercambio de datos en todo el sector público y privado.	Específico para el servicio notarial, con interoperabilidad limitada.
Principios Clave	"Once-Only", Transparencia, Soberanía del dato.	Eficiencia, Trazabilidad, Seguridad jurídica notarial.
Seguridad	Cifrado de extremo a extremo, logs de auditoría públicos.	Cifrado en tránsito (HTTPS/TLS), seguridad del servidor central, auditorías internas.
Innovación	Constantemente busca integrar nuevas tecnologías (e.g., blockchain para algunos registros).	Enfoque en la consolidación del sistema actual.

Fuente: Elaboración propia

Estonia, con su plataforma **X-Road**, ofrece un contraste revelador. Mientras X-Road es una capa distribuida donde los datos residen en origen (Rieger, 2020), Bolivia ha optado por un modelo de base de datos centralizada.

La comparación revela riesgos sistémicos:

- **Arquitectura:** El modelo estonio es federado; el boliviano es centralizado. Según Schneier (2015), esto convierte al SINPLU en un "punto único de fallo".
- **Control:** En Estonia, el ciudadano ve quién accede a sus datos (e-Estonia, 2022). En Bolivia, la SCP 0227/2020-S4 resalta que el Estado boliviano aún tiene una "deuda de transparencia" en cuanto a los logs de acceso de los servidores públicos a la información ciudadana.

Bolivia debe considerar modelos federados donde el SINPLU actúe como gestor de enlaces y no como repositorio masivo, permitiendo una "auditoría ciudadana" real sobre quién consulta sus protocolos.

3. El GDPR y el vacío normativo en Bolivia

El Reglamento General de Protección de Datos (GDPR) de la UE establece principios que en Bolivia son aún incipientes. El análisis comparativo bajo los estándares del Artículo 5 del GDPR muestra brechas críticas:



1. **Limitación de la finalidad:** En el SINPLU, la interoperabilidad con Derechos Reales e Impuestos ocurre sin protocolos de "consentimiento informado". La jurisprudencia boliviana (SCP 1017/2012) señala que el uso de datos para fines distintos a los recolectados inicialmente es una vulneración constitucional.
2. **Minimización de datos:** Bolivia carece de políticas de supresión de datos accesorios (como copias de C.I. tras el cotejo biométrico). El GDPR exigiría borrarlos, pero en el modelo boliviano, el almacenamiento suele ser indefinido.
3. **Responsabilidad proactiva:** A diferencia del GDPR (Piñar Mañas, 2016), en Bolivia no existe una autoridad de control independiente. La DIRNOPLU actúa como juez y parte, lo que limita la imparcialidad ante una posible filtración.

4. La biometría y el "cuerpo electrónico"

La biometría en notaría ha reducido el fraude, pero como recuerda Rodotà (2010), el cuerpo electrónico es la nueva frontera de los derechos humanos. Si la base del SEGIP fuera vulnerada, el daño es irreparable. La SCP 1114/2012 ha subrayado que los datos biométricos gozan de una "protección reforzada". Sin embargo, la falta de una ley específica impide determinar si es proporcional almacenar plantillas biométricas permanentemente o si bastaría con un cotejo (*match*) en tiempo real sin retención de datos.

5. Hacia la soberanía de datos

La trazabilidad no es sinónimo de datos abiertos. Los datos notariales son privados con efectos públicos. El futuro debe girar hacia tecnologías como Blockchain o Zero-Knowledge Proofs (Szabo, 2017), que permiten verificar la autenticidad sin exponer el contenido sensible.

Aterrizar el SINPLU en la doctrina del TCP implica pasar de una "transparencia estatal" a una "soberanía de datos", donde el ciudadano, y no solo el Estado, sea el guardián de su propia historia jurídica. Como establece la SCP 0096/2017-S2, la tecnología debe estar al servicio del derecho, y no el derecho supeditado a las capacidades técnicas de control del Estado.

6. CONCLUSIÓN

La investigación confirma que el sistema SINPLU ha cumplido su objetivo primario de reducir el fraude documental y la suplantación de identidad mediante la interoperabilidad



biométrica. No obstante, este avance técnico ha generado un desequilibrio normativo donde la seguridad del tráfico comercial prevalece sobre la seguridad del individuo y su derecho a la privacidad.

Se identifica una transformación dogmática en la función notarial: la custodia de la fe pública se ha desplazado del notario, como tercero imparcial, hacia infraestructuras estatales centralizadas (DIRNOPLU/AGETIC). Este fenómeno diluye la reserva notarial y convierte al sistema en un instrumento potencial de perfilado ciudadano y vigilancia administrativa sin controles judiciales previos.

La carencia de una Ley General de Protección de Datos Personales en Bolivia constituye la principal debilidad del modelo. Esta omisión imposibilita el ejercicio efectivo de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y deja a la Acción de Protección de Privacidad (Habeas Data) como un mecanismo de reacción judicial tardío, carente de una estructura administrativa preventiva y sancionadora.

El estudio revela que la seguridad de la información es deficiente en los "puntos finales" (despachos notariales). Existe una indeterminación legal sobre la responsabilidad civil y administrativa en caso de filtraciones, al no existir una distinción clara entre la responsabilidad del Estado como proveedor del software y la del notario como usuario del sistema.

Para mitigar los riesgos de la centralización masiva, se propone la transición hacia un modelo de Soberanía de Datos. Esto implica la adopción de arquitecturas descentralizadas, como *Blockchain*, y la aplicación estricta del principio de *Privacy by Design* (Privacidad desde el Diseño), garantizando que la trazabilidad y la transparencia no comprometan la autonomía informativa del ciudadano boliviano.

REFERENCIAS BIBLIOGRÁFICAS

Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC). (2018). *Estado TIC: Situación de las Tecnologías de Información y Comunicación en Bolivia*. La Paz: AGETIC. <https://www.agetic.gob.bo/pdf/estadotic/AGETIC-Estado-TIC.pdf>

Armella, C. N. (2018). *Tratado de Derecho Notarial, Registral e Inmobiliario*. Ad-Hoc. <https://www.editorialadhoc.com.ar/>



- Asamblea Legislativa Plurinacional. (2011, 8 de agosto). *Ley N° 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación*. Gaceta Oficial de Bolivia. <http://www.gacetaoficialdebolivia.gob.bo/normas/buscar/164>
- Asamblea Legislativa Plurinacional. (2014, 25 de enero). *Ley N° 483 del Notariado Plurinacional*. Gaceta Oficial de Bolivia. <http://www.gacetaoficialdebolivia.gob.bo/normas/buscar/483>
- Baqueiro Rojas, E., & Buenrostro Báez, R. (2016). *Derecho Notarial*. Oxford University Press. <https://global.oup.com/>
- Castán Tobeñas, J. (2019). *Función Notarial y Seguridad Jurídica Preventiva*. Reus. <https://www.editorialreus.es/libros/funcion-notarial-y-seguridad-juridica-preventiva/9788429021172/>
- Delgado, A. (2020). *El documento público electrónico y la contratación digital*. Universidad Externado de Colombia. <https://doi.org/10.2307/j.ctv18msq9m>
- Dirección del Notariado Plurinacional (DIRNOPLU). (2022). *Informe de Rendición Pública de Cuentas Final*. Ministerio de Justicia y Transparencia Institucional. <https://www.justicia.gob.bo/>
- European Commission. (2022). *e-Estonia: The Digital Society*. <https://e-estonia.com/>
- Farfán, J. (2019). Protección de datos personales en Bolivia: Un derecho constitucional sin ley. *Revista Boliviana de Derecho*, (28), 45-68. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572019000200003
- Gattari, C. N. (2015). *Manual de Derecho Notarial*. Depalma. <https://AbeledoPerrot.com.ar>
- Gomá Lanzón, I. (2017). *Notariado y nuevas tecnologías: ¿Evolución o revolución?* La Ley. <https://www.laley.es/>
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books. <https://doi.org/10.5860/choice.37-5147>
- Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. John Murray. <https://doi.org/10.1145/2622633>
- Nery, R. (2021). Fe Pública y Blockchain: El futuro del notariado. *Revista de Derecho y Tecnología*, 12(1), 112-130. <https://doi.org/10.21703/rdt.v12i1.154>
- Órgano Ejecutivo Plurinacional. (2014, 19 de noviembre). *Decreto Supremo N° 2189: Reglamento a la Ley N° 483 del Notariado Plurinacional*. Gaceta Oficial de Bolivia. <http://www.gacetaoficialdebolivia.gob.bo/normas/buscar/2189>



- Piñar Mañas, J. L. (2016). *El Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Reus. <https://www.editorialreus.es/libros/el-reglamento-general-de-proteccion-de-datos/9788429019445/>
- Rieger, A. (2020). E-Government in Estonia: Best practices for Bolivia. *Journal of Latin American Policy*, 8(2), 22-40. <https://doi.org/10.1017/jla.2020.12>
- Rodotà, S. (2010). *La vida y las reglas: Entre el derecho y el no derecho*. Trotta. <https://www.trotta.es/libros/la-vida-y-las-reglas/9788498791334/>
- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company. <https://doi.org/10.1080/01972243.2016.1153106>
- Szabo, N. (2017). Smart Contracts: Building Blocks for Digital Markets. *En Entropy*, 1-15. <https://archive.org/details/smart-contracts-building-blocks-for-digital-markets>
- Tribunal Constitucional Plurinacional. (2017, 20 de febrero). *Sentencia Constitucional Plurinacional 0096/2017-S2*. <https://buscador.tcpbolivia.gob.bo/>

Conflicto de Intereses: Los autores afirman que no existen conflictos de intereses en este estudio y que se han seguido éticamente los procesos establecidos por esta revista. Además, aseguran que este trabajo no ha sido publicado parcial ni totalmente en ninguna otra revista.

FINANCIAMIENTO

Los autores no recibieron financiamiento para el desarrollo de esta investigación.

CONTRIBUCIÓN DE AUTORÍA:

Nombres de autores e iniciales: Soraya Marcela Guzmán Espada (SMGE).

1. Conceptualización: (SMGE)
2. Curación de datos: (SMGE)
3. Análisis formal: (SMGE)
4. Adquisición de fondos: (SMGE)
5. Investigación: (SMGE)
6. Metodología: (SMGE)
7. Administración del proyecto: (SMGE)
8. Recursos: (SMGE)
9. Software: (SMGE)
10. Supervisión: (SMGE)



11. Validación: (SMGE)
12. Visualización: (SMGE)
13. Redacción – Borrador original: (SMGE)
14. Redacción – Revisión y edición: (SMGE)

