POLÍTICA DE PRIVACIDAD

Última actualización: Junio de 2025

Esta Política de Privacidad explica cómo **Consultora Blockchain S.R.L.**, con domicilio en la ciudad de La Paz, Bolivia, en su rol de Responsable del Tratamiento, recopila, utiliza, protege y conserva los datos personales de los usuarios que utilizan la aplicación **Wira Wallet**.

Wira Wallet es una aplicación diseñada para operar de forma completamente no custodial. Todas las claves privadas, credenciales y documentos se generan, cifran y almacenan directamente en el dispositivo del usuario. Ni Consultora Blockchain ni terceros poseen acceso técnico a estos datos tras la instalación.

La presente política se emite en cumplimiento de la legislación vigente en el Estado Plurinacional de Bolivia, incluyendo:

- **Ley N.º 1082** de Ciudadanía Digital
- **Ley N.º 164** de Telecomunicaciones y Tecnologías de la Información y Comunicación
- **Decreto Supremo N.º 3525** sobre Firma Digital

1. Datos Personales Recopilados

Wira Wallet recopila sólo la información imprescindible para crear su **identidad digital soberana** y permitirle usar la billetera sin custodia:

- **DNI (número y fotos anverso/reverso)**: capturados con la cámara, procesados por un OCR local y verificados mediante *Polygon ID*; el archivo cifrado (AES-256-GCM) queda en el Keystore del dispositivo.
- **Selfie**: capturada con la cámara; la comparación biométrica 1-a-1 se realiza en el dispositivo; imagen cifrada, y esta información no la guardamos.
- **Identificador Descentralizado (DID)**: generado en el teléfono, firmado con la clave local; sólo su *hash* se publica en la blockchain.
- **Credencial Soberana (VC)**: emitida con Polygon ID tras validar DNI + selfie; se cifra con una clave derivada de su PIN (Argon2) y se guarda en Ceramic. Su validez se demuestra mediante **pruebas de conocimiento cero (zk-SNARK)**, lo que significa que cualquiera puede comprobar que es auténtica **sin ver** sus datos.
- **Direcciones on-chain y hashes de transacciones**: se crean cuando firma operaciones; son públicas por naturaleza pero no contienen información personal.

Importante: Consultora Blockchain no puede descifrar las credenciales ni acceder a los documentos del usuario, ya que permanecen cifrados localmente o validados mediante pruebas sin revelar contenido.

2. Finalidades del Tratamiento

Los datos personales se utilizan exclusivamente para las siguientes finalidades:

- Verificar la identidad del usuario (DNI + selfie) y emitir su credencial soberana (VC).
- Activar y operar una billetera sin custodia mediante Account Abstraction.
- Permitir el inicio de sesión local mediante PIN o biometría.
- Implementar la recuperación on-chain con guardianes.
- Recopilar métricas técnicas anónimas para mejorar la seguridad y estabilidad de la aplicación.

3. Base Jurídica

El tratamiento de datos se basa en:

- **Consentimiento expreso** del usuario (Art. 21 de la CPE y Ley 1082).
- **Ejecución de un contrato digital** para el uso de la aplicación (Art. 78 de la Ley 164).
- **Firma electrónica avanzada**, conforme al DS N.º 3525, para autorizar transacciones on-chain.

4. Destinatarios de los Datos

Los datos personales no serán vendidos, transferidos ni compartidos con terceros no autorizados. Las únicas excepciones incluyen:

- Proveedores técnicos descentralizados (como nodos Ceramic o servicios RPC), exclusivamente para el funcionamiento de la red.
- Autoridades judiciales o administrativas, únicamente ante requerimiento legal debidamente emitido y previa autorización de la gobernanza de los usuarios. En otro caso no es posible técnicamente descifrar los datos del usuario.

5. Conservación y Almacenamiento de Datos

- Todos los datos sensibles se cifran localmente mediante algoritmos robustos (AES-256-GCM).
- Las credenciales se almacenan cifradas en la red Ceramic, y su validez se demuestra con pruebas zero knowledge.
- La eliminación de datos debe ser realizada por el propio usuario a través de funciones integradas y registradas en los contratos inteligentes en la App.

6. Derechos del Usuario

El usuario puede ejercer los siguientes derechos en cualquier momento:

- Acceso a sus datos personales cifrados.
- Solicitar la rectificación de errores detectados en los procesos de emisión.
- Ejecutar la portabilidad de sus credenciales entre dispositivos.

Estos derechos pueden ser ejercidos únicamente a través de las funciones habilitadas en la aplicación.

7. Seguridad de la Información

Implementamos múltiples capas de seguridad:

- Cifrado extremo a extremo de todos los datos sensibles.
- Almacenamiento local de datos sensibles (Android Keystore).
- Contratos inteligentes y pruebas de conocimiento cero para proteger la identidad.
- Autenticación reforzada mediante PIN y biometría.

8. Modificaciones

Esta Política podrá actualizarse para reflejar cambios regulatorios o tecnológicos. Notificaremos tales cambios a través de la aplicación y actualizaremos la fecha al inicio de este documento.