



POLÍTICA DE DATOS EN TRABAJOS CON COMUNIDADES ÉTNICAS - INSTITUTO DATA GOYÁ



2025

Noviembre 2025

INSTITUTO DATA GOYÁ

Esta obra está sujeta a la licencia Creative Commons CC BY 4.0. Se permite a terceros distribuir, traducir, retocar y crear a partir de la obra licenciada de forma no comercial, y su distribución se tiene que realizar con una licencia igual a la que regula la obra original.

POLÍTICA DE DATOS EN TRABAJOS CON COMUNIDADES ÉTNICAS -
INSTITUTO DATA GOYÁ./ Denise Machado Leal-- Instituto Data Goyá, 2025. 8 p.

Texto en español.

Número de Identificación da Obra: 03.16112025- Versión de 01 de noviembre de 2025

1. Proteção de dados. 2. Comunidades étnicas. 3. Política de dados. 4. Pesquisa social - Aspectos éticos. 5. Instituto Data Goyá. I. Título.

CDD: 323.025
CDU: 004.738.5:323.1

Información de contacto:

Rubiataba, Goiás, Brasil.

Email: denise@datagoya.com.br

Más recursos disponibles <https://datagoya.com.br/>

POLÍTICA DE DATOS PARA TRABAJOS CON COMUNIDADES ÉTNICAS

Esta política establece los principios, salvaguardas y obligaciones éticas para el manejo de datos en proyectos desarrollados con comunidades indígenas y afrodescendientes, garantizando el respeto a su autodeterminación informativa, a la protección de sus datos y conocimientos colectivos. Basada en el Convenio 169 de la OIT, la Declaración de la ONU sobre los Derechos de los Pueblos Indígenas (UND RIP), las leyes nacionales de protección de datos y los Principios CARE, la política orienta procesos de consentimiento libre, previo e informado, gobernanza comunitaria, almacenamiento seguro y uso no extractivista de los datos. A través de acuerdos colectivos, comités de gobernanza y validaciones en lengua originaria, se asegura que la comunidad conserve control total sobre sus datos lingüísticos, personales, culturales y territoriales. La política también incorpora prácticas de transparencia, minimización de datos, auditorías éticas y mecanismos de retiro o corrección, promoviendo un enfoque feminista, intercultural e intergeneracional. Con ello, se fortalece la soberanía digital de las comunidades, se previene el uso indebido de la información y se crean condiciones para que la tecnología se desarrolle de manera justa, segura y alineada con los valores y prioridades comunitarias.

1. PRINCIPIOS RECTORES

Esta política establece lineamientos éticos, legales y operativos para el manejo de datos en proyectos realizados con comunidades étnicas, garantizando el respeto a sus derechos colectivos, culturales y territoriales. Se basa en los principios de **autodeterminación informativa, soberanía de datos, consentimiento libre, previo e informado, no extracción, minimización de datos y seguridad digital comunitaria**:

1.1 Consentimiento libre, previo e informado (CLPI)

Toda participación debe ser voluntaria. Se explicará, en las lenguas de los pueblos involucrados (ej.: castellano y quechua), el objetivo del proyecto, los posibles usos de la información y el derecho a retirarse en cualquier momento. El consentimiento será un proceso continuo, no un acto único.

1.2 Reciprocidad y beneficio mutuo

El proyecto buscará devolver valor concreto a la comunidad (diagnósticos útiles, herramientas conceptuales, fortalecimiento de capacidades, materiales bilingües), evitando cualquier forma de “investigación extractiva”.

1.3 Responsabilidad y rendición de cuentas

El equipo asumirá responsabilidad frente a la comunidad a través de espacios de devolución y evaluación colectiva, donde se puedan cuestionar decisiones, corregir rumbos y ajustar el proyecto.

1.4 Soberanía de datos y ética de datos comunitaria

Los datos lingüísticos, testimonios y materiales generados con la comunidad serán considerados un recurso colectivo, sobre el cual la comunidad ejerce soberanía. Cualquier uso fuera del alcance inicialmente acordado requerirá autorización comunal.

1.5 Ética feminista e interseccional

Se priorizará la participación y protección de las experiencias de mujeres, personas jóvenes, mayores y otros grupos históricamente marginados, reconociendo las múltiples capas de opresión (género, etnicidad, idioma, territorio, clase) y buscando que el proyecto contribuya a reducirlas, no a reforzarlas.

2. LOS FUNDAMENTOS LEGALES

- **Convenio 169 de la OIT** (1989): consulta previa, consentimiento informado y protección del conocimiento tradicional (arts. 6, 7, 13, 15).
- **Declaración de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas – UNDRIP** (2007): derecho a la autodeterminación y control de datos, conocimientos y expresiones culturales (arts. 18, 19, 31).
- **Pacto Internacional de Derechos Civiles y Políticos – PIDCP**: derecho a la privacidad (art. 17).
- **Pacto Internacional de Derechos Económicos, Sociales y Culturales – PIDESC**: derecho a participar en la vida cultural y proteger saberes colectivos (art. 15).
- **Reglamentos nacionales de protección de datos** del país correspondiente (Perú: Ley N.º 29733 – Ley de Protección de Datos Personales y su Reglamento; Brasil: Lei 13.709/2018 – LGPD).
- **Principios CARE para la Gobernanza de Datos Indígenas** (Collective Benefit, Authority to Control, Responsibility, Ethics).
- **Principios FAIR para manejo responsable de datos científicos**, adaptados desde un enfoque no extractivista.

3. TIPOS DE DATOS

Los datos recopilados en proyectos con comunidades étnicas incluyen:

- **Datos personales** (identificables o sensibles).
- **Datos colectivos** (información comunitaria, prácticas culturales, necesidades sociales).
- **Datos lingüísticos** (grabaciones, corpus, vocabulario, expresiones en lengua originaria).
- **Datos territoriales y ambientales**.
- **Conocimientos tradicionales** (sólo cuando la comunidad lo autorice explícitamente).

Todos estos datos están protegidos como bienes culturales colectivos según la UNDRIP (art. 31) y el Convenio 169 (arts. 2 y 13).

4. CONSENTIMIENTO LIBRE, PREVIO E INFORMADO (CLPI)

El uso de datos deberá basarse en procesos claros de **consentimiento libre, previo e informado**, conforme al Convenio 169 de la OIT (arts. 6 y 7).

El CLPI deberá:

1. Ser explicado en la lengua originaria predominante.

2. Detallar: qué datos se recopilan, para qué, cómo se almacenan, durante cuánto tiempo y quién los usará.
3. Incluir información sobre riesgos, límites y derechos de revocación.
4. Ser obtenido por escrito, grabación o acuerdo colectivo firmado.
5. Contemplar mecanismos diferenciados para mujeres, mayores y jóvenes.

5. SOBERANÍA DE DATOS

Siguiendo los **Principios CARE**, la comunidad mantiene la **autoridad para controlar**:

- Qué datos pueden o no ser compartidos.
- Quién puede procesarlos.
- Dónde se almacenan.
- Las reglas para su eliminación, anonimización o reutilización.

Se implementará un **Comité Comunitario de Gobernanza de Datos**, con representación de mujeres, autoridades locales y jóvenes, responsable de aprobar decisiones clave. También serán disponibilizados modelos/plantillas para mejor gobernanza de datos.

6. ALMACENAMIENTO Y SEGURIDAD

El almacenamiento seguirá las normativas nacionales de protección de datos (p. ej., Ley 29733 del Perú o LGPD de Brasil) y estándares internacionales de ciberseguridad (ISO/IEC 27001). Las medidas incluyen:

- Encriptación de datos en reposo y en tránsito.
- Acceso restringido basado en roles aprobados por la comunidad.
- Servidores seguros ubicados preferentemente en el país de origen o bajo jurisdicciones con protección equivalente o mayor (como Brasil).
- Copias de seguridad controladas por la comunidad.

7. USO ÉTICO Y NO EXTRACTIVISTA DE LOS DATOS

Queda prohibido:

- El uso comercial no autorizado.

- La transferencia a terceros sin aprobación explícita de la comunidad.
- La publicación de contenido que permita la identificación de personas sin consentimiento.
- La creación de modelos de IA basados en datos comunitarios sin gobernanza local.

Todo análisis o desarrollo tecnológico deberá priorizar **beneficio colectivo**, conforme al principio CARE de **Collective Benefit**.

8. TRANSPARENCIA Y RENDICIÓN DE CUENTAS

El equipo del proyecto deberá garantizar:

- Informes periódicos en lenguaje claro.
- Espacios de devolución comunitaria.
- Registro documentado de decisiones sobre datos.
- La posibilidad de auditorías éticas internas y externas.

Cumpliendo el art. 41 de la UNDRIP, que exige mecanismos adecuados de control y supervisión.

9. DERECHOS DE LA COMUNIDAD Y MECANISMOS DE RECLAMO

La comunidad tiene derecho a:

- Retirar su consentimiento en cualquier momento.
- Solicitar eliminación o devolución de datos.
- Exigir explicaciones sobre uso o almacenamiento.
- Presentar quejas ante autoridades de protección de datos.

El medio para las solicitudes son a través de correo del Instituto (denise@datagoya.com.br).

10. PUBLICACIÓN Y DIFUSIÓN

Toda publicación derivada del proyecto deberá:

- Atribuir de forma colectiva a la comunidad (UNDRIP art. 31).
- Respetar acuerdos previos de confidencialidad.
- Ser, siempre que posible, compartida en la lengua originaria.

- Ser aprobada por el Comité Comunitario antes de su difusión.

11. REVISIÓN Y ACTUALIZACIÓN

Esta política deberá ser evaluada y actualizada anualmente, o antes si la comunidad lo solicita, garantizando su alineación con marcos legales vigentes y estándares éticos contemporáneos.

Rubiataba, Goiás, Brasil.
Última revisión en 01 noviembre de 2025.
Denise Machado Leal, Presidenta del Instituto Data Goyá.