

Resumen ejecutivo

Datos personales, poder institucional y apropiación ciudadana: hacia una cultura de protección de datos en Ecuador

Propósito y alcance

Este informe ofrece una fotografía integral del ecosistema de protección de datos personales en Ecuador: combina el análisis del marco normativo-institucional con evidencia cualitativa recogida en grupos focales con dos poblaciones particularmente expuestas a riesgos —personas LGBTIQ+ y comunidades amazónicas— para traducir experiencias reales en recomendaciones de política pública y herramientas ciudadanas.

Metodología

El estudio triangula (i) revisión documental del marco vigente y de planes nacionales, con (ii) dos grupos focales independientes, realizados en modalidad virtual, bajo consentimiento informado, confidencialidad y protocolos de no revictimización. Las dinámicas incluyeron mapas mentales, lluvia de ideas y priorización colectiva guiadas por cuatro bloques: conocimiento y contexto; experiencias y riesgos; expectativas institucionales; y soluciones requeridas. Los grupos estuvieron integrados por activistas y comunicadores LGBTIQ+ y por líderes y defensores de pueblos amazónicos.

Contexto normativo e institucional

Ecuador cuenta con un armazón jurídico actualizado (Constitución, LOPDP y normativa secundaria) y con una hoja de ruta nacional que, bien implementados bajo responsabilidad proactiva y privacidad desde el diseño, pueden cerrar la brecha entre el derecho formal y su garantía efectiva. El Plan Nacional de Protección de Datos Personales prevé ejes como gobernanza digital, universalización del derecho y creación de un Registro Nacional de Protección de Datos para robustecer trazabilidad y control. Para tratamientos de alto riesgo, el uso de Evaluaciones de Impacto (EIPD) opera como evidencia de cumplimiento y gestión de riesgos.

A la vez, la Superintendencia de Protección de Datos Personales (SPDP) —autoridad joven— requiere independencia, presupuesto adecuado y capacidades técnicas para pasar del “cumplimiento declarativo” a la rendición de cuentas demostrada en todos los sectores.

Hallazgos clave

- **Brechas de conocimiento y rutas confusas:** La población conoce poco la LOPDP, los derechos ARCO y cómo funciona el Sistema de Protección de Datos (roles de responsable/encargado, DPO, competencias de la SPDP), lo que desincentiva activar mecanismos formales y normaliza malas prácticas.
- **Prácticas problemáticas recurrentes:** Se reportan telemarketing con bases compradas, reuso de formularios, solicitudes injustificadas de datos sensibles y pérdida de control en plataformas. Estos patrones aumentan riesgos de discriminación, fraude, inseguridad digital y criminalización de defensores.
- **Desconfianza institucional:** La distancia entre avances normativos y su aplicación cotidiana alimenta la percepción de ineficacia y limita el ejercicio de derechos.

- **Reconocimiento de datos colectivos:** En territorios amazónicos se enfatiza la necesidad de proteger datos colectivos y culturales, con salvaguardas acordes a contexto, lengua y cosmovisiones.

Recomendaciones estratégicas

- 1. Responsabilidad proactiva y privacidad por diseño:** Impulsar metodologías de gestión de riesgos y EIPD a lo largo del ciclo de vida del dato; promover códigos de conducta/certificaciones; y asegurar minimización y transparencia como principios rectores.
- 2. Fortalecer actores clave:** Reforzar el rol del Delegado de Protección de Datos (DPO) en entidades públicas y privadas; y dotar a la SPDP de independencia, presupuesto y equipos técnicos para evaluar impactos, mitigaciones y riesgos residuales.
- 3. Transparencia y control ciudadano efectivos:** Exigir avisos de privacidad comprensibles, paneles de control para gestionar consentimiento, trazabilidad de fuentes y canales de reclamo accesibles; avanzar en un Registro Nacional de Protección de Datos que facilite supervisión y auditoría social.
- 4. Enfoque diferencial y territorial:** Reconocer y proteger los datos colectivos en pueblos amazónicos; adaptar políticas y servicios para superar barreras de idioma, cultura, discriminación y conectividad.
- 5. Educación práctica y multicanal:** Desarrollar campañas segmentadas por edad y territorio, con materiales multiformato (audio-radiales, infografías, cartillas bilingües, piezas para redes) y contenidos prácticos: cómo denunciar, configurar 2FA, reconocer phishing, ejercer revocatoria. Incluir rutas offline en zonas de baja conectividad.

Conclusión

El país ya dispone de bases jurídicas y una agenda nacional para proteger datos personales; el desafío es aterrizarlas en capacidades, procesos y cultura pública y organizacional. Con responsabilidad proactiva, transparencia aplicable y pedagogía práctica —especialmente en poblaciones históricamente vulneradas— es posible cerrar la brecha entre la promesa legal y la garantía efectiva del derecho a la protección de datos en Ecuador.