

Cuarta sesión 2026:
Conclusiones**Protección de la privacidad
en la era de la identidad
digital y los datos biométricos**

25 agosto 2026

Versión pública

En esta sesión del CEDIG contamos con la participación de Vicente Peredo Vázquez, titular de la Unidad de Protección de Datos Personales y de Aldo Fragoso, Director General de Normatividad y Prevención de la Unidad de Protección de Datos Personales de la Secretaría Anticorrupción y Buen Gobierno, junto a especialistas invitados y miembros del CEDIG. Se discutió el estado de la identidad digital en México a la luz de la biometría: como llave de acceso a servicios digitales, como categoría jurídica que exige protección reforzada, y como política pública ya en marcha. Fue una oportunidad valiosa para abordar la dirección por la que se está trazando la reforma a las leyes de protección de datos en el país, contrastando con el marco legal vigente, al tiempo que entra en operación de la CURP biométrica, con una pregunta de fondo: cómo construir confianza digital sin sacrificar derechos ni innovación.

¿De qué hablamos en la sesión?

- 1** **Sandbox.** La propuesta de nueva ley plantea espacios experimentales para probar usos de datos biométricos antes de su salida al mercado. Permite la innovación sin esperar a que la regulación alcance a la tecnología, y aprender de los errores antes de que tengan consecuencias masivas.
- 2** **Trazabilidad.** El uso de datos biométricos debe poder rastrearse de principio a fin para tener certeza sobre su uso, tanto para autoridades como personas usuarias.
- 3** **Enfoque preventivo.** El sentido de la reforma es anticipar riesgos, por lo que incluye reforzar medidas técnicas tales como el cifrado avanzado, la prueba de vida y el doble factor de autenticación, además de dar oportunidad de corregir antes de abrir un procedimiento sancionador.

4

CURP biométrica como detonador. El decreto que incorpora huellas, fotografía e iris al registro poblacional avanza con calendario propio: despliegue escalonado desde octubre de 2025 y obligatoriedad para trámites desde febrero de 2026. Es el proyecto que le da urgencia real a la discusión sobre el marco legal y la construcción de salvaguardas.

5

Minimización, borrado y consentimiento efectivo. Pedir permiso para usar datos biométricos no basta; debe haber avisos de privacidad claros y concretos, cumpliendo el principio de minimización para no pedir más de lo necesario, y ofrecer certeza sobre cuándo y cómo se eliminan esos datos una vez cumplida su finalidad.

6

Educar sobre el valor de los datos propios. Parte de la desconfianza hacia la biometría viene de que las personas no saben qué se hace con su huella o su iris una vez entregados. La reforma incorpora medidas para la alfabetización digital y la formación de habilidades relacionadas con la protección de los propios datos.

7

La agenda no debe diseñarse de forma aislada. La identidad digital biométrica se conecta directamente con la inclusión financiera y los pagos digitales que el propio CEDIG discutió en su sesión anterior: una identidad digital confiable ya había sido señalada como habilitador pendiente de esa agenda. La confianza es un elemento estructural, parte de la infraestructura que debe construirse a partir de acciones concretas y una relación permanente entre la ciudadanía y las entidades públicas y privadas que poseen datos personales.

Cuarta sesión 2026:
Conclusiones

**Protección de la privacidad
en la era de la identidad
digital y los datos biométricos**

25 agosto 2026

Versión pública

Perspectiva general

México está construyendo al mismo tiempo la infraestructura de identidad digital biométrica y el marco legal que debería gobernarla, en ese orden. La ventana para alinear ambos procesos existe, pero los procesos avanzan a distintas velocidades, con una ventaja en el despliegue de la CURP biométrica, y el desfase puede traer deficiencias en el diseño del marco de protección de datos que resulte muy costoso corregir. El reto para el país es acelerar la modernización del marco normativo de protección de datos y comenzar a construir una infraestructura de confianza ciudadana que potencie los beneficios de la identidad digital controlando adecuadamente sus riesgos, para lo cual es esencial la colaboración entre gobierno, sector privado y sociedad civil.