



# Autenticación Digital en la Era de la IA: el Registro Civil como Raíz de Confianza

Panel 1: “Facilitando el acceso a servicios, autenticación digital en la era de la IA”

Gustavo Fiscarelli

Asociación de Registradores de Personas Naturales, Brasil

XXIII Encuentro del CLARCIEV

Tegucigalpa, Honduras, 2 de septiembre de 2026

# Lectura estratégica del título del panel

acceso a servicios → autenticación digital → era de la IA

## El riesgo de la discusión

Reducir autenticación digital a biometría, en particular al reconocimiento facial, y entender la Inteligencia Artificial sobre todo como tecnología de identificación biométrica o de detección de fraude.

## Una pregunta conceptualmente más rica

¿Cómo establecer, en el ambiente digital, una cadena de confianza entre una persona, su identidad fundacional, sus atributos, su autenticación y el acto digital que pretende realizar?

# Biometría no es identidad

La biometría responde principalmente a una pregunta. El registro civil puede responder a otras, complementarias.

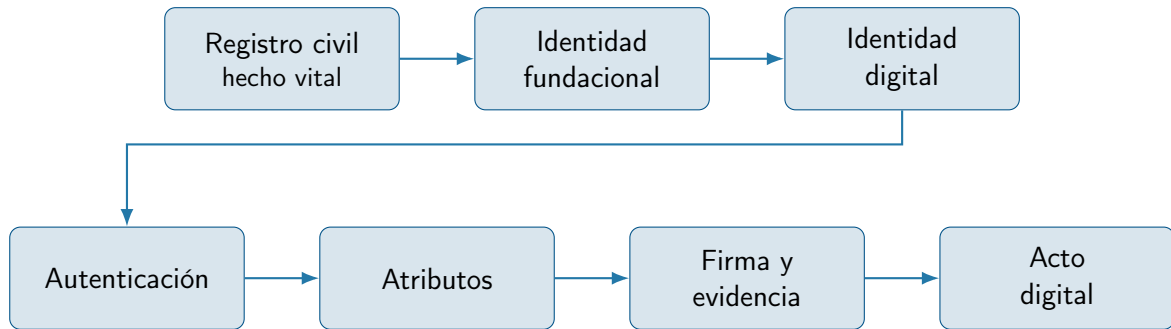
“¿Es la misma persona?”  
(biometría)

“¿Quién es jurídicamente esa persona?”  
(registro civil)

“¿Qué atributos registrales son actuales y confiables?”  
(identidad fundacional)

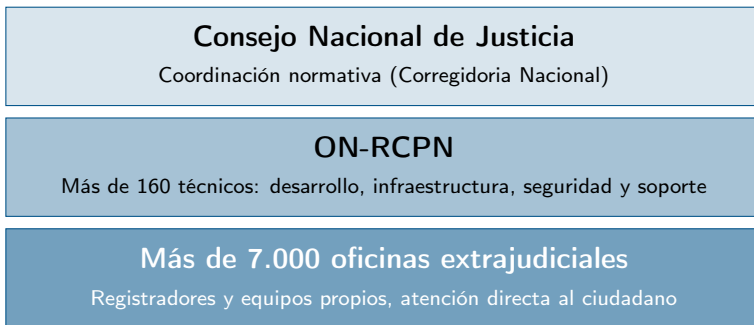
“¿Podemos atribuir este acto digital a esa persona?”  
(firma y evidencia)

# La cadena de confianza propuesta



La identidad digital no nace en una aplicación aislada. Nace del registro autoritativo de la persona, y esa raíz de confianza debe acompañar toda la cadena, hasta la atribución del acto digital.

# Tres capas institucionales



La capacidad de innovar, incluida la incorporación de IA, depende de una coordinación efectiva entre un equipo técnico nacional relativamente pequeño y una red descentralizada mucho mayor.

# El equipo humano detrás del registro civil

## ON-RCPN

Más de 160 profesionales técnicos: gobernanza de datos, desarrollo, infraestructura, seguridad y soporte

## Oficinas registrales

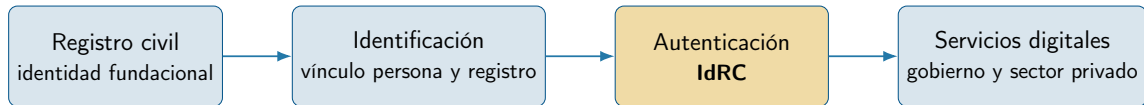
Más de 7.000 unidades autónomas, primera línea de identificación y autenticación de identidad en el país

## Ciudadanía

Personas registradas, cuya confianza en el sistema es el objetivo final de toda la arquitectura

Ninguna solución de inteligencia artificial sustituye a este conjunto de personas. El papel de la tecnología ha sido dar a esta red herramientas más seguras, más ágiles y más confiables.

# El IdRC en la cadena registro civil, identificación y servicios



## Qué es

Capa de autenticación electrónica apoyada directamente en la base del registro civil, desarrollada y mantenida con investigación aplicada, en cooperación continua entre el ON-RCPN y la universidad.

# Niveles de garantía y multifactor

- Evidencias explícitas de **nivel de garantía de identidad** y de **nivel de garantía de autenticación** para cada acceso (alineado con NIST SP 800-63-3)
- Cada servicio, público o privado, puede exigir el nivel compatible con el riesgo de la transacción
- **Multifactor y métodos alternativos**, dificultando ataques con IA generativa: deepfakes y clonación de voz

## Meta en desarrollo

Incorporar IA directamente en la operación del sistema para implementar **autenticación adaptativa**: el nivel de exigencia de verificación se ajusta conforme al riesgo identificado en cada intento de acceso.

# Riesgos: deepfakes e identidades sintéticas

- Avance consistente de las técnicas de manipulación facial y de generación de contenido sintético: intercambio de identidad, síntesis completa de rostro, manipulación de expresiones
- Impacto directo en la verificación remota de identidad, la prueba de vida y el reconocimiento facial usados en autenticación digital
- Exigen contramedidas específicas: detectores de manipulación, verificación de vivacidad robusta, combinación de múltiples factores

## Principio orientador

La IA puede apoyar los procesos de identidad. No debe convertirse en la raíz de confianza.

# Oportunidades: IA al servicio de la confianza

- Señales contextuales y conductuales de riesgo: ubicación, comportamiento, horario
- Verificación cruzada con bases de datos de socios
- Bloqueo del uso de credenciales de personas fallecidas, desde el origen del registro
- Búsqueda inteligente con preservación de privacidad sobre los índices nacionales
- Digitalización, transcripción y restauración inteligente de acervos en papel
- Chatbot y OCR especializados en legislación registral (plataforma ARIA)

Cada mecanismo refuerza una capa distinta de la cadena de confianza, sin sustituir a las fuentes autoritativas que sostienen todo el sistema.

# Lectura simplificada: riesgos frente a oportunidades

## Riesgos

- Deepfakes y manipulación facial en verificación remota
- Identidades sintéticas en registros y en el ingreso de usuarios
- Uso indebido de búsquedas amplias en bases de registro

## Oportunidades

- Niveles de garantía de identidad y de autenticación en el IdRC
- Multifactor y señales contextuales contra ataques con IA
- Verificación cruzada, bloqueo de credenciales de fallecidos, búsqueda con privacidad

El equilibrio entre confianza, seguridad e inclusión depende de tratar riesgos y oportunidades como parte de una misma agenda, no de forma aislada.

# Tres componentes de la propuesta brasileña

## **IdRC**

¿Quién es usted? Identidad y autenticación

## **ICP-RC**

¿Cómo atribuir confianza al acto? Firma, integridad, evidencia

## **ARIA e IA aplicada**

¿Cómo mejorar el servicio? Atención, OCR, automatización

# Cinco mensajes que deben permanecer

- 1 El registro civil es una fuente autoritativa de identidad fundacional. La identidad digital debe preservar una ligación verificable con esa fuente.
- 2 Biometría no es sinónimo de identidad. Es un mecanismo poderoso de vinculación y autenticación, no sustituye la identidad jurídica y registral.
- 3 Autenticación no es el fin de la cadena de confianza. Para actos relevantes, importan también atribución, firma, integridad y evidencia.
- 4 La IA debe reducir barreras, no crear una nueva raíz de confianza.
- 5 El desafío debe pensarse regionalmente.

# Mensaje final

*“El registro civil puede evolucionar de una institución que registra eventos de la vida civil hacia una infraestructura permanente de confianza para la vida digital del ciudadano.”*

identidad fundacional → identidad digital → autenticación → atributos → actos digitales confiables

La Inteligencia Artificial debe incorporarse de forma transversal a esa arquitectura para mejorar acceso, eficiencia y experiencia del ciudadano, sin sustituir las fuentes autoritativas ni los mecanismos verificables sobre los que descansa la confianza.

# Gracias

## Preguntas y discusión

Gustavo Fiscarelli

Panel 1, XXIII Encuentro del CLARCIEV  
Tegucigalpa, Honduras, 2 de septiembre de 2026