

Verificación de edad con minimización de datos

Presentado por Diego Urrutia — Ingeniero en Sistemas.

1. El problema

Hoy la verificación de edad en línea se mueve entre dos extremos igualmente malos. O la plataforma pregunta la edad y confía en la respuesta —lo que equivale a no verificar nada—, o exige documento, selfie o escaneo facial, obligando a niñas, niños y adolescentes a entregar datos identificatorios y biométricos a empresas privadas para acceder a un servicio. Terminamos eligiendo entre desprotección o vigilancia. Existe una tercera opción, técnicamente madura, y es la que se propone.

2. La propuesta

Que Uruguay implemente un sistema nacional de prueba de edad con doble anonimato, apoyado en la identidad digital que el Estado ya emite (Usuario gub.uy, TuID, ID Uruguay)¹, mediante el cual una plataforma reciba únicamente la afirmación **«esta persona supera tal edad»**: sin nombre, sin cédula, sin fecha de nacimiento y sin ningún dato adicional.

3. Cómo funcionaría

Intervienen tres partes que nunca comparten información entre sí:

- **Emisión (una sola vez).** La persona, con su identidad digital ya validada, obtiene en su dispositivo una credencial criptográfica con atributos de edad (por ejemplo «mayor de 13», «mayor de 16», «mayor de 18»). El Estado interviene solo en este momento.
- **Presentación (muchas veces).** Cuando un servicio necesita comprobar la edad, el dispositivo genera una prueba criptográfica del atributo requerido. El servicio recibe un resultado verificable de tipo verdadero/falso.
- **Doble anonimato.** El emisor no puede saber en qué sitios se usó la credencial, y el sitio no puede saber quién es la persona ni correlacionar sus visitas entre servicios. Se garantiza con criptografía de conocimiento cero (zero-knowledge proofs)², de modo que el dato no existe para ser filtrado, hackeado ni requerido.

Es importante subrayar lo que la propuesta **no** es: no se trata de «iniciar sesión con gub.uy» en cada plataforma. Ese esquema le daría al Estado la traza de navegación de cada niño y a la plataforma un identificador estatal. La credencial se emite una vez y se presenta de forma desvinculada.

4. Principios de diseño no negociables

- **Minimización estricta:** se transmite el umbral consultado y nada más; nunca la edad exacta ni la identidad.
- **No vinculabilidad:** dos presentaciones de la misma persona no deben poder asociarse entre sí.
- **Sin registro de uso:** prohibición legal expresa de conservar trazas de dónde se presentó cada prueba.
- **Múltiples umbrales:** la vida digital de un adolescente de 16 no es la de un niño de 9; el sistema no puede reducirse a «menor o mayor de 18».

¹Agesic — Identidad Digital (Usuario gub.uy e ID Uruguay): <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tematica/identidad-digital>. En el sector privado existen además soluciones de identidad digital como TuID.

²EU Digital Identity Wallet — «The Age Verification Manual», Comisión Europea (Digital Building Blocks).

- **Pluralidad de métodos:** debe ser una alternativa gratuita y disponible, no el único camino, para no excluir a quien carece de dispositivo, conectividad o acompañamiento adulto.
- **Código abierto y auditable,** con auditorías públicas periódicas de seguridad y privacidad.

5. Por qué ahora: la ventana de oportunidad

La Comisión Europea publicó y está pilotando durante 2026 su Age Verification Blueprint³: una aplicación de verificación de edad que revela a los servicios en línea solo si la persona alcanza el umbral solicitado, con pruebas de conocimiento cero como método de presentación preferido, integrada a las billeteras de identidad digital nacionales de Francia, España, Italia, Dinamarca, Grecia, Chipre e Irlanda⁴.

Esto tiene una consecuencia práctica decisiva. **Las grandes plataformas deberán construir esa integración de todos modos para operar en Europa.** Por lo tanto, la estrategia realista no es pedirles que se integren a un desarrollo uruguayo a medida —un mercado de nuestro tamaño no tiene poder para exigir integraciones exclusivas—, sino **alinearnos con el estándar internacional ya existente** (credenciales verificables W3C, OpenID for Verifiable Presentations, el blueprint europeo)⁵, de modo que cumplir en Uruguay les represente un costo adicional prácticamente nulo.

Uruguay parte además con una ventaja concreta: a diferencia de varios países europeos, emite documento de identidad desde el nacimiento y cuenta con infraestructura de identidad digital operativa. Eso resuelve el problema más difícil del modelo, que es cómo dotar de credencial a los propios menores.

6. Medidas concretas que se proponen

1. **Definir por norma un estándar nacional de prueba de edad que preserve la privacidad,** interoperable con el blueprint europeo, encomendando su especificación e implementación de referencia a Agesic junto con la Unidad Reguladora y de Control de Datos Personales.
2. **Establecer la obligación legal de que los servicios digitales que operen en el país acepten toda prueba de edad conforme a ese estándar,** con la prohibición correlativa de exigir documento, biometría facial o datos identificatorios cuando exista una prueba conforme disponible.
3. **Prohibir expresamente la conservación y el tratamiento secundario** de los datos generados en el proceso, tanto por el emisor estatal como por el servicio verificador, con régimen sancionatorio.
4. **Habilitar la emisión de credenciales de edad para personas menores,** con participación de quienes ejercen la responsabilidad parental cuando corresponda y previendo la autonomía progresiva del adolescente.
5. **Impulsar la interoperabilidad regional** en el Mercosur y en los foros de gobierno digital de América Latina, para que la región no negocie plataforma por plataforma sino como bloque.
6. **Realizar una prueba piloto acotada y evaluada públicamente** antes de cualquier exigencia general, con métricas de cobertura, exclusión, usabilidad y efectividad real.

³Comisión Europea — Age Verification Blueprint, portal técnico oficial. <https://ageverification.dev/> (consultado en setiembre de 2026).

⁴Comisión Europea — «Commission makes available age verification blueprint». <https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint>

⁵W3C Verifiable Credentials Data Model y OpenID for Verifiable Presentations (OpenID4VP), estándares abiertos sobre los que se apoya la solución europea.

7. Límites que corresponde reconocer

Ninguna verificación de edad resuelve todo, y presentar esto como solución completa sería deshonesto. Una credencial puede ser prestada por un hermano mayor o por un adulto; el sistema mitiga ese riesgo vinculándola al dispositivo y limitando la frecuencia de uso, pero no lo elimina. Tampoco alcanza a servicios que operan fuera de toda jurisdicción, ni evita el uso de VPN, y existe un riesgo real de exclusión de quienes no dispongan de un dispositivo compatible.

Por eso esta propuesta debe entenderse como **una capa dentro de una estrategia más amplia** —que incluye diseño seguro por defecto, alfabetización digital, mediación adulta y canales de ayuda— y nunca como sustituto de ellas.

8. ¿Qué se solicita?

Que el Parlamento incorpore la prueba de edad con doble anonimato como línea de acción explícita del informe final de esta Consulta, y encomiende a Agesic, junto con la URCDP y el Consejo Nacional Consultivo Honorario de los Derechos de la Niñez y Adolescencia, un estudio de factibilidad técnica y normativa con plazo definido, tomando como base el estándar internacional ya disponible.