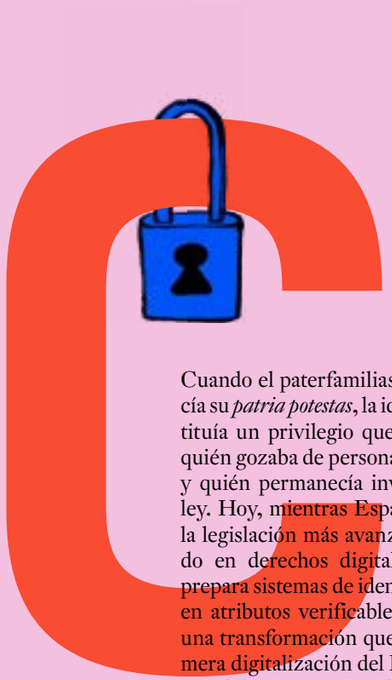
Palabras clave:
identidad digital, atributos verificables, seguridad jurídica, identidad autosoberana, carta de derechos digitales, eIDAS2 (electronic Identification, authentication and trust services.

La identidad digital: ¿Cómo demostrar quiénes somos en el espacio digital?

DEL PRIVILEGIO HISTÓRICO DEL PATERFAMILIAS ROMANO HASTA LA DEMOCRATIZACIÓN DEL SISTEMA DE IDENTIDAD DIGITAL EUROPEA

La identidad digital contemporánea no es simplemente la versión electrónica de nuestros documentos físicos, sino un ecosistema modular donde diferentes atributos verificados se combinan según el contexto específico de cada transacción. Se resuelve así uno de los problemas fundamentales del entorno digital: el equilibrio entre seguridad jurídica y experiencia de usuario.

TEXTO: **PALOMA LLANEZA**
ILUSTRACIÓN: **CINTA ARRIBAS**



Cuando el paterfamilias romano ejercía su *patria potestas*, la identidad constituía un privilegio que determinaba quién gozaba de personalidad jurídica y quién permanecía invisible ante la ley. Hoy, mientras España desarrolla la legislación más avanzada del mundo en derechos digitales y Europa prepara sistemas de identidad basados en atributos verificables, asistimos a una transformación que trasciende la mera digitalización del DNI: estamos redefiniendo qué significa verificar la identidad en el siglo XXI.

La transformación histórica de la identidad revela patrones que resurgen en el entorno digital. Por ejemplo, en la antigua Roma, solo los ciudadanos varones cabeza de familia gozaban de plena personalidad jurídica. Mujeres, esclavos y extranjeros carecían de identidad legal reconocida; existían únicamente en relación con el paterfamilias, que los representaba. Este sistema no era accidental: la identidad funcionaba como mecanismo de control social y exclusión política.

La Revolución francesa fracturó este paradigma al proclamar que "todos los ciudadanos son iguales ante la ley", aunque la verdadera universalización llegó con los registros civiles del siglo XIX. Francia creó, entre 1792 y 1795, los primeros sistemas estatales de registro, con los que se sustituyeron los archivos parroquiales por documentación secular.

Este modelo se extendió por Europa durante las guerras napoleónicas, estableciendo el principio según el cual la identidad debía ser un derecho ciudadano, no un privilegio aristocrático.

La paradoja contemporánea radica en que, tras dos siglos de democratización, los sistemas digitales actuales han recreado formas históricas de exclusión. Los 1.100 millones de personas sin identidad legal documentada enfrentan una invisibilidad que evoca a los *sine civitate* romanos, mientras que, en países como Estados Unidos, la dependencia del número de Seguro Social[1] ha creado vulnerabilidades sistémicas que facilitan la suplantación de identidad a escala masiva.

Identidad modular

La teoría contemporánea de identificación humana establece una distinción fundamental: la identidad representa quién es alguien[2], mientras que la identificación constituye el proceso de verificar esa identidad mediante la comparación de características observadas con referencias almacenadas.

Pero la verdadera revolución conceptual es reconocer que la identidad es inherentemente modular y evolutiva. Más allá de quiénes somos o cómo nos percibimos, la identidad se construye sobre conjuntos específicos de atributos que pueden combinarse de forma diferente según el contexto, y que varían con el tiempo. No necesito los mismos atributos para obtener una tarjeta de fidelidad que para firmar una hipoteca. En el primer caso, bastará con un identificador único y, tal vez, verificar mi mayoría de edad; en el segundo, necesitaré demostrar mis ingresos, un historial crediticio e identidad legal completa.

Esta aproximación modular permite construir distintas identidades digitales para diferentes propósitos, cada una optimizada para su contexto específico. Un profesional puede tener una identidad digital para servicios bancarios (con atributos financieros verificados), otra para redes profesionales (con credenciales académicas y laborales), y otra para servicios de ocio (con verificación mínima de edad). Cada una comparte únicamente los atributos necesarios para su función específica.

Desde la perspectiva psicológica, la identidad constituye un proceso evolutivo continuo, no un estado fijo. Esta naturaleza dinámica encuentra su expresión perfecta en los sistemas modulares, que pueden evolucionar añadiendo nuevos atributos o actualizando los ya existentes sin comprometer la coherencia del conjunto.

Los sistemas modulares y evolutivos, por tanto, pueden reflejar

La paradoja contemporánea radica en que, tras dos siglos de democratización, los sistemas digitales actuales han recreado formas históricas de exclusión

esta realidad permitiendo identidades profesionales, cívicas o sociales diferenciadas pero interoperables.

El ecosistema digital actual opera bajo un principio fundamental, pero problemático: la identidad presuntiva. Esta consiste en que, para evitar la fricción en el proceso de mantener una experiencia de usuario fluida, los sistemas digitales minimizan los requisitos de verificación y presumen que los usuarios son quienes dicen ser.

Esta aproximación crea un equilibrio perverso entre conveniencia y riesgo que determina la arquitectura de prácticamente todos los servicios *online*. Consideremos la paradoja de las compras digitales: puede comprar un libro en Amazon con un clic, pero no puede comprar un automóvil de 30.000 euros con la misma facilidad.

Esta diferencia no responde a limitaciones técnicas (la infraestructura de pagos digitales puede manejar ambas transacciones sin problemas), sino a una evaluación de riesgo basada en la debilidad de la verificación de identidad actual. Los comerciantes *online* calibran constantemente esta ecuación: gastar poco en verificar la identidad y, al mismo tiempo, asumir un riesgo proporcionalmente limitado.

Esta limitación tiene consecuencias económicas profundas. La brecha de confianza digital frena sectores enteros de la economía digital, manteniendo artificialmente procesos ineficientes y limitando el potencial de transformación digital en industrias tradicionales. La identidad presuntiva no es un problema técnico, sino un problema de seguridad jurídica: sin mecanismos robustos de verificación, las entidades no pueden asumir los riesgos asociados con transacciones de alto valor.

Por si esto fuera poco, la llegada de la inteligencia artificial generativa introduce vectores de suplantación completamente nuevos. Los *deepfakes* pueden eludir sistemas de verificación facial, las voces sintéticas engañan cada vez más a los sistemas de identificación por voz y los algoritmos pueden generar identidades completamente falsas, pero estadísticamente convincentes.

Identidad algorítimica

Más preocupante aún es que estos ataques escalan: lo que antes requería considerables recursos ahora está al alcance de actores individuales. La suplantación de identidad no es solo un problema de usuarios individuales, sino un riesgo sistémico para la economía digital. Cada caso de fraude incrementa los costes operativos de todas las entidades digitales, que deben incorporar estas pérdidas en sus modelos de negocio. Esto crea un efecto cascada: el fraude encarece los servicios legítimos y excluye del acceso a los servicios digitales a las poblaciones de menor renta.

Simultáneamente, emerge el fenómeno de la "identidad algorítmica": los perfiles que los sistemas automatizados construyen sobre nosotros basándose en patrones de comportamiento digital. Estos perfiles pueden utilizarse para suplantación sofisticada, donde el atacante no necesita robar credenciales específicas: le basta con imitar patrones de comportamiento para pasar desapercibido.

La arquitectura de los sistemas de identidad digital determina fundamentalmente la distribución del poder y la confianza. Los sistemas centralizados concentran el control en una autoridad única (típicamente gubernamental), como el sistema Aadhaar de India con 1.300 millones de usuarios. Aunque ofrecen eficiencia operativa y capacidad de implantar políticas sociales a escala masiva, crean vulnerabilidades sistémicas catastróficas. Por ejemplo, el fallo de seguridad de 2017 en las tarjetas eID de Estonia afectó a 800.000 documentos y es ilustrativa de este riesgo.

Los sistemas federados, por su parte, reparten la responsabilidad entre múltiples proveedores que crean relaciones de confianza para permitir la verificación entre dominios.

El modelo escandinavo, BankID, es un ejemplo que permite usar el usuario bancario para múltiples servicios *online*. Sin embargo, pueden crear múltiples puntos de vigilancia y su complejidad de coordinación entre actores puede generar fragilidades, como ilustró el fracaso del GOV.UK Verify.

Por último, la identidad autosoberana (SSI, en inglés *Self-Sovereign Identity*) permite que los individuos posean y controlen credenciales digitales sin depender de autoridades centralizadas. Este modelo maximiza el control individual mediante la "verificación y consentimiento criptográficamente demostrables", soportando "pruebas de conocimiento cero" para la divulgación selectiva de información. Los modelos SSI pueden "prevenir la correlación no deseada por terceros" mediante identificadores por pares y técnicas criptográficas avanzadas.

Sin embargo, los SSI también enfrentan desafíos. Los marcos jurídicos actuales están diseñados para sistemas centralizados o federados, no para arquitecturas donde los individuos actúan como sus propias autoridades certificadoras. Además, requieren que los usuarios

La identidad representa quién es alguien, mientras que la identificación constituye el proceso de verificar esa identidad

No es solo una cuestión técnica o legal: es una cuestión antropológica fundamental sobre qué significa actuar con seguridad jurídica en el siglo XXI

gestionen conceptos criptográficos complejos, lo que implica barreras de acceso considerables. A pesar de eso, es el modelo en el que se basa la nueva identidad digital europea, su *wallet* de identidad —aplicación que permite almacenar credenciales digitales y documentos oficiales para identificarse en las transacciones— y los elementos que se pueden cargar en él.

El Reglamento (UE) 2024/1183, sobre el Marco Europeo de Identidad Digital, que entró en vigor en mayo de 2024, establece que los Estados miembros deben proporcionar Carteras de Identidad Digital de la UE (EUDI Wallet)[3] para finales de 2026, con el objetivo de alcanzar el 80 % de adopción ciudadana para 2030.

El corazón técnico de este sistema, además del propio *wallet*, son las atestaciones de atributos: declaraciones criptográficamente verificables sobre características específicas de una persona emitidas a partir de fuentes auténticas (el registro civil, el registro de socios de un club de fútbol, la base de datos de clientes de una compañía de telecomunicaciones, los poderes otorgados ante notario, etc.) o no auténticas (prestadores de servicios de confianza —entidades que ofrecen servicios de verificación y validación de firma electrónica, regulados por estándares rigurosos que establece el Reglamento eIDAS de la Unión Europea—). Se almacenan en el *wallet* del usuario para que las use y las gestione sin trazabilidad.

Una atestación certifica, por ejemplo, que alguien es mayor de edad, sin revelar su fecha de nacimiento, que posee un título universitario sin especificar la institución, o que tiene ingresos superiores a cierto umbral sin detallar la cantidad precisa.

Las atestaciones son intrínsecamente modulares y están diseñadas como sistemas que protegen la privacidad por defecto. Mediante técnicas criptográficas como las pruebas de conocimiento cero, permiten demostrar que se cumple una condición, sin revelar los datos subyacentes que la sustentan.

La modularidad que ofrecen resuelve directamente el problema de la identidad presuntiva. En lugar de elegir entre verificación exhaustiva (con alta fricción) o verificación mínima (con alto riesgo), el sistema permite verificación graduada: cada transacción puede requerir exactamente el nivel de verificación que justifica su valor y riesgo asociado.

Identidad digital del futuro

El nuevo sistema debe resolver los desafíos de seguridad jurídica, eficiencia operativa, inclusión universal y confianza sistémica. Esto requiere superar la falsa dicotomía entre sistemas totalmente centralizados y completamente descentralizados, desarrollando arquitecturas modulares que combinen verificación robusta con experiencia de usuario fluida.

Así pues, los principios fundamentales incluyen verificación graduada (cada transacción requiere exactamente el nivel de verificación que justifica su valor y riesgo), modularidad basada en atributos verificados según contexto, interoperabilidad confiable (capacidad de funcionar a través de fronteras y sistemas, manteniendo garantías de seguridad) e inclusión universal (diseño que no excluya poblaciones por limitaciones técnicas, económicas o educativas).

Porque, al final, no se trata solo de una cuestión técnica o legal: es una cuestión antropológica fundamental sobre qué significa actuar con seguridad jurídica en el siglo XXI.

La pregunta no es si tendremos identidad digital universal (la tendremos), sino si será diseñada para ampliar nuestra capacidad de interactuar de manera confiable en el mundo digital o para perpetuar los riesgos y exclusiones del modelo presuntivo actual. La respuesta determinará el tipo de economía digital que construimos para las próximas generaciones.

Autora

PALOMA LLANEZA
Es abogada especializada en identidad digital y ciberseguridad. Editora de estándares ETSI sobre servicios de confianza, eIDAS2 y *wallet* europeo. Experta del Sandbox IA (SEDIA) y coordinadora SGT eIDAS2 del Foro Nacional de Ciberseguridad.

Notas

1 Identificador diseñado en 1936 para pensiones.

2 Las características fundamentales, atributos y cualidades que definen a una persona.

3 EUDIW, en inglés *European Digital Identity Wallet*.

Bibliografía

Allen, C. *"The Path to Self-Sovereign Identity"* en *Life with Alacrity blog* (2016). Disponible en: https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

Banco Mundial. *Identification for Development (ID4D) Initiative*. World Bank Group. Disponible en: https://id4d.worldbank.org/

Beduschi, A. *"Rethinking Digital Identity for Post-COVID-19 Societies"* en *Data & Policy*, 2021. Disponible en: https://www.cambridge.org/core/journals/data-and-policy/article/rethinking-digital-identity-for-postcovid19-societies-data-privacy-and-human-rights-considerations/0B9A65B889C341CF535E804256C2816A

Comisión Europea. *Reglamento (UE) 2024/1183 - European Digital Identity Framework*. Bruselas, Comisión Europea, 2024. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation

Council of Europe. *Guidelines on National Digital Identity: Enfoque centrado en derechos humanos*. Estrasburgo, Council of Europe, 2022. Disponible en: https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-identity.html

Llaneza, P. (2021): *Identidad digital*. Madrid, Bosch Editor (Wolters Kluwer).

Reed, D. & Preukschat, A. (2021): *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Nueva York, Manning Publications.

English

From the historical privilege of the Roman paterfamilias to the democratization of the European digital identity system

DIGITAL IDENTITY: HOW DO WE PROVE WHO WE ARE IN THE DIGITAL SPACE?

Contemporary digital identity is not merely an electronic replica of our physical documents, but rather a modular ecosystem in which verified attributes are selectively combined according to the specific context of each transaction. In this way, one of the fundamental challenges of the digital environment is resolved: achieving a balance between legal certainty and user experience.

Keywords: *digital identity, verifiable attributes, legal certainty, self-sovereign identity, digital rights charter, eIDAS2.*