

Debate OSPI

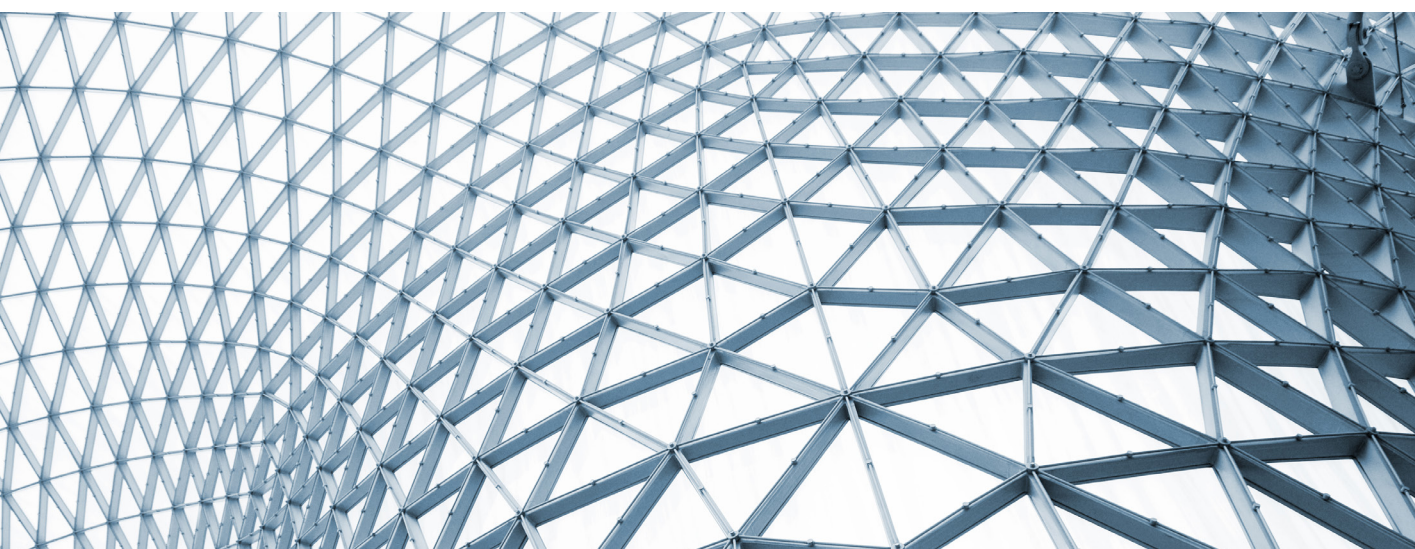
Identidades digitales fiables. Facilidad de uso, privacidad y seguridad en el Sector Público

Marzo 2024

OSPI ■

Observatorio
del sector público

inetum ■



El Observatorio de Sector Público de Inetum ha celebrado un nuevo debate de expertos sobre la importancia de la facilidad de uso, la privacidad y la seguridad en los sistemas de identificación digital en el sector público.

Las intervenciones destacaron la evolución de los sistemas de identidad digital, desde el DNI electrónico hasta iniciativas de la Unión Europea, como el **Reglamento eIDAS¹**, que el pasado 29 de febrero recibió el respaldo del Parlamento Europeo². Asimismo, se discutió la importancia de ofrecer soluciones accesibles y fáciles de usar para todos los ciudadanos.

Ha contado con la participación de los siguientes expertos:

- **Juan Crespo Sánchez**, comisario jefe de la Unidad de Informática y Comunicaciones de la Policía Nacional.
- **Ángel L. Martín Bautista**, subdirector adjunto de Planificación y Gobernanza de la Administración Digital (Ministerio para la Transformación Digital y de la Función Pública).
- **Izaskun Urrestarazu**, directora general de Izenpe.
- **Carlos Pastor Matut**, director de Estrategia Blockchain de Inetum.

Moderado por **Víctor M. Izquierdo**, presidente del Observatorio de Sector Público de Inetum.

1. Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea.

2. European Parliament. (29 febrero 2024). MEPs back plans for an EU-wide digital wallet.

<https://www.europarl.europa.eu/news/en/press-room/20240223IPR18095/meps-back-plans-for-an-eu-wide-digital-wallet>

Adicionalmente, el 26 de marzo, eIDAS2 fue aprobado por el Consejo. European Council. (26 marzo 2024). European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans

<https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>

Evolución de la identidad

En el primer bloque del debate los expertos abordan la evolución del documento de identidad gracias a la incorporación de capacidades electrónicas, la importancia de la infraestructura de registro, y la expansión de estas capacidades a diversos grupos de ciudadanos, tanto en España como en el extranjero.

Juan Crespo, comisario jefe de la Unidad de Informática y Comunicaciones de la Policía Nacional, destaca el papel histórico de la Policía Nacional en la emisión de documentos de identidad con garantías de seguridad y su evolución a lo largo de los años, hasta llegar al momento actual.

“Con el avance tecnológico, a principios del siglo XXI, se buscó dotar al documento de identidad de capacidades criptográficas para la identificación y firma electrónica remota”, explica.

Menciona como antecedente la Ley 59/2003 de firma electrónica (actualmente derogada), que habilitó el marco jurídico para transmitir la fortaleza y garantías de seguridad del registro físico del DNI a los certificados electrónicos.

Crespo subraya la importancia de la infraestructura de las Oficinas de Registro para la verificación de identidad y destaca el proyecto del Ministerio del Interior para la emisión de certificados para ciudadanos residentes en España, incluyendo extranjeros con tarjeta de identidad, con el objetivo de dotar a estos documentos de capacidades criptográficas. Además, planean extender estas capacidades a ciudadanos españoles en el extranjero sin DNI, mediante el pasaporte español, que contendrá certificados electrónicos.

En este sentido, destacamos en este documento de conclusiones la activación de un **Plan de la Policía Nacional³ para potenciar la identidad digital de los ciudadanos**. Entre las diversas actuaciones que se van a llevar cabo, destaca la renovación de 351 Puestos de Actualización de Documentación instalados en las comisarías, que son los que permiten renovar los certificados del DNI, cambio de contraseña para acceder a los certificados electrónicos y llevar a cabo operaciones de consulta de datos y verificación del DNI-e.

3. Ministerio del Interior (29 febrero 2024). La Policía Nacional activa un plan para potenciar la identidad digital de los ciudadanos. [Comunicado de prensa].

<https://www.interior.gob.es/opencms/va/detalle/articulo/La-Policia-Nacional-activa-un-plan-para-potenciar-la-identidad-digital-de-los-ciudadanos/>

Otra de las actuaciones, ya plenamente operativa, es la posibilidad del pago de las tasas de expedición de documentos de identidad y viaje (DNI y Pasaporte) a través de terminales de punto de venta (TPV) y la implementación de la pasarela de pago con la Agencia Tributaria, un sistema que facilitará y agilizará este trámite a la ciudadanía.

“El proyecto conocido con el nombre **DNI virtual**, que permitirá llevar el DNI en el móvil, va a suponer una transformación del modo de relación de los ciudadanos con la Administración Pública o con el sector privado, lo que requiere ineludiblemente que no se vea comprometida la garantía de la identidad segura que la legislación vigente atribuye al DNI-e”.

El DNI en el móvil, una actuación en dos fases

Respecto a este proyecto, el DNI en el móvil, Crespo subraya que es una actuación en dos fases. La primera fase es la de identificación física, es decir, acreditar la identidad del ciudadano de forma física con el DNI en el móvil sin tener que llevar encima su DNI físico. Aquí, explica, existen tres condicionantes. “Uno de ellos está cumplido, los otros dos estamos en vías de darles solución en breve”. El primer condicionante, ya solventado, era contar con la aprobación de la Agencia Española de Protección de Datos. El segundo condicionante era la certificación criptográfica. En este punto, el Centro Criptológico Nacional, CCN, está evaluando los sistemas centrales para verificar el cumplimiento de unas garantías de seguridad para dar luz verde a esa aplicación. En tercer lugar, menciona la validez jurídica. Un real decreto que aporte soporte jurídico constituye la última fase.

En paralelo, han trabajado con la ONCE para preservar los derechos de las personas con discapacidad. Desde esta organización valoran muy positivamente la iniciativa del DNI en el móvil. Facilitará a estos usuarios saber cuándo se están acreditando o cuándo alguien accede al DNI en el móvil.

En detalle, explica **Juan Crespo**, que se facilitará la información en forma de códigos QR, y un *token* que permitirá a los prestadores acceder a esa información básica según la necesidad. Uno de los QR contendrá toda la información impresa en el DNI. El siguiente QR permitirá el acceso solo a media afiliación (número de DNI y datos básicos) y el tercero servirá solo para mostrar si el titular es mayor de edad y regular así el acceso a juego, contenidos para adultos, etc. “Los dos primeros estarán disponibles en una primera fase y en una inmediata segunda fase se abordará el *token* relativo al acceso a contenidos en función de edad, que no ha salido en la primera fase para no retrasar la certificación”.

Estos avances, coinciden los expertos, ponen en valor la destacada posición de España en materia de identificación digital.

Sistemas de identidad digital

El segundo bloque se centró en los sistemas de identidad digital disponibles, en particular el *onboarding online*, destacando la importancia de aprovechar los avances tecnológicos para mejorar la experiencia del usuario.

Ángel L. Martín Bautista, del Ministerio para la Transformación Digital y de la Función Pública, puso en valor la posición privilegiada de España con el DNI electrónico, que otorga una identificación única a los ciudadanos, subrayando, además, la seguridad asociada al proceso de obtención del DNI, que requiere la presencia física y la demostración de identidad.

Mencionaron los expertos las diversas formas de identificación digital, desde contraseñas hasta certificados electrónicos, con énfasis en el sistema "Cl@ve" que involucra a varias entidades públicas y cuenta actualmente con cerca de 20 millones de usuarios registrados y gran cantidad de autenticaciones mensuales.

Importante cambio en la vida online de las personas

Izaskun Urrestarazu, de Izenpe, resaltó el desarrollo que ha llevado a cabo su entidad, como prestador de servicios de confianza, extendiendo la identidad a empresas y entidades jurídicas, llevando los certificados a la nube y preparando la adaptación al Reglamento eIDAS2 una vez haya entrado en vigor. La digitalización del proceso de identificación, especialmente con certificados en la nube, sin duda ha supuesto un "avance significativo", que ha contribuido a la mejora de la usabilidad. También mencionó la complejidad previa asociada a los certificados en tarjetas locales y cómo el nuevo enfoque en la nube facilita su manejo. "Estamos en un momento retador, un momento de cambio. Aún faltan incógnitas que despejar en el nuevo modelo de identidad", afirma.

Carlos Pastor, añade dos reflexiones a las manifestaciones anteriores. En primer lugar, destaca que, desde su creación, Internet ha carecido de una capa de identidad. "Por primera vez vamos a alcanzar una solución de uso común ante todos los interlocutores, e incluye no solo los datos *core* identificativos, sino cualquier otro atributo". Añade, además, que también el sector privado está sujeto a esta regulación, algo positivo para el sector público, ya que, "si estoy acostumbrado a usar esta identificación, cuando vaya a utilizarla en un trámite administrativo, será más sencillo", manifiesta.

Se refiere también a la relevancia de la tecnología NFC (Near Field Communication) como un elemento adicional que facilitará el uso de la identidad digital, especialmente en el nuevo modelo de *wallet* europeo. Cabe esperar que estos cambios transformen la vida *online* de las personas, proporcionando un mayor control y registro de las interacciones con la identidad digital.

Reglamento europeo

El tercer bloque, dedicado a iniciativas europeas en la materia, aborda tanto la transformación en el control ciudadano de datos como la prevención del fraude mediante la implementación del Reglamento eIDAS2 y, en particular, de la cartera digital europea. Los expertos pusieron énfasis en la estandarización, la seguridad mejorada y la minimización de datos como aspectos clave para el éxito del sistema.

Reglamento ambicioso, de futura obligatoriedad para todas las empresas que operan en Europa

Los panelistas del debate describen el Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea, conocido como el Reglamento eIDAS2, como una propuesta legislativa ambiciosa, con el potencial de fortalecer la cohesión territorial en Europa y consolidar el mercado único, ya que será de aplicación en todos los países, porque es la única manera de que sea interoperable, unificando así la forma de identificarse tanto ante el sector público como ante el sector privado.

La cartera digital se conceptualiza como un medio de identificación interoperable para ciudadanos en la Unión Europea, asegurando que la información no esté en manos de terceros, sino controlada por el ciudadano. El enfoque de la Comisión Europea, matizan los expertos, es otorgar al ciudadano el control y la propiedad de sus datos, en contraste con la situación actual, en la que terceros gestionan esta información.

Afirman, además, que el reglamento europeo podría seguir una dinámica similar a la que ha seguido el Reglamento General de Protección de Datos, de modo que las empresas que operan en la Unión Europea, en particular las grandes plataformas, deben cumplirlo, independientemente de si tienen regulaciones similares en sus países de origen. La futura obligatoriedad para estas grandes plataformas de aceptar la cartera digital europea impulsará la armonización de los medios de identificación y verificación de edad en la Unión Europea.

Prevención del fraude y Servicios de confianza

Otro caso de uso analizado por los panelistas se refiere a la convalidación de títulos académicos obtenidos en el extranjero. Los expertos apuntan que la cartera digital europea se presenta como una solución que simplificará y agilizará este proceso, contribuyendo a la validación legal de títulos académicos en diferentes países de la Unión Europea y la consiguiente reducción del fraude.

Efectivamente, manifiestan los ponentes, las credenciales digitales se comprueban de forma automática y con un nivel de seguridad altísimo. Ello es aplicable no solo a títulos universitarios, sino a cualquier otro tipo de títulos.

Simplificar para una mejor gobernanza

En este punto del debate emerge la importancia de la gobernanza. Existirán dos tipos de “listas de confianza”, explican los expertos, de aquellos registros que emiten información de un ciudadano. Por ejemplo, sobre un título académico, o datos recogidos en un registro de la propiedad, registro civil... etc. En el caso de España, contamos con el Registro Nacional de Titulados Universitarios Oficiales (RNTUO), que contiene información sobre los titulados universitarios en nuestro país. Con el nuevo reglamento, las anotaciones en dicho registro tendrán validez europea.

Otro tipo de lista, de gestión más complicada, contendrá las entidades que pueden solicitar información sobre ese título académico, por ejemplo, una empresa para un proceso de selección de personal. Según el nuevo reglamento, “en el *wallet* quedará registrado quién me pidió ese título y para qué lo pidió. Estos registros que almacenan información permitirán la verificación de quién pide qué y para qué”, matizan los expertos.

Crespo menciona la Plataforma de Intermediación de Datos que tenemos en España, “que, como país, nos sitúa muy por delante de otros países de nuestro entorno”. Todo ello, explica, debido a nuestra complejidad administrativa, que nos ha permitido conectar los tres niveles de administración que existen en nuestro país. “Algo que han intentado replicar en Europa mediante la Pasarela Digital Europea (SDB, Single Digital Gateway), con funciones similares de intermediación de datos a nivel europeo”.

Reflexionan los panelistas sobre la dificultad de conectar la diversidad de registros de los distintos países europeos, ya que la representación y la forma de organizarlos difiere de unos a otros. Por ello, explican, se avanza hacia un modelo más simple, de modo que, en lugar de crear una complicada red que conecte los registros de unos países con los de otros, se opta por que la información quede en manos del ciudadano. “Es decir, si este certificado es válido en mi país, también será válido en el tuyo”. Y concluyen que “al igual que existe ese reconocimiento mutuo a nivel de identificación en cada país, esos mismos pasos se dan en el caso de la validación de otros atributos de la identidad”.

La importancia de la estandarización para alcanzar la interoperabilidad

En la segunda parte del bloque se destaca la importancia de la estandarización para la interoperabilidad, señalando que todas las fuentes auténticas pueden convertirse en servicios de confianza y, además, deben facilitar el acceso a los terceros de confianza a la información que gestionan, siempre a petición del usuario. La discusión se centra en la creación de servicios de confianza especializados, como empresas que emitan credenciales en nombre de las fuentes auténticas, simplificando el proceso para el ciudadano.

En relación al papel de las Administraciones Públicas, los expertos sugirien que, debido a su condición de fuente auténtica, ya tienen un rol clave. Por otro lado, la estandarización de formatos se percibe como un avance esencial para facilitar la interoperabilidad entre diferentes tipos de credenciales y su intercambio entre organizaciones de distintos países.

Destacan, además, que, aunque existen servicios de confianza establecidos, el Reglamento podría impulsar la creación de nuevos servicios especializados en los nuevos tipos de credenciales. En este escenario, la gobernanza futura se plantea como un desafío, con la estandarización como elemento crucial para el éxito del sistema.

Un ejemplo mencionado en el debate es la dificultad para estandarizar los apoderamientos. Así, manifiestan que, en este caso, si se consigue estandarizar el 80% de los apoderamientos que se utilizan en el 99% de las ocasiones, podría ser suficiente. Por tanto, creen los expertos que es importante alcanzar un equilibrio entre rigor y practicidad a la hora de continuar avanzando. Mencionan también, como un aspecto positivo del Reglamento, “que se hayan dejado para actos de ejecución la concreción de los detalles más técnicos del reglamento, lo que ocurre habitualmente con la regulación europea, permitiendo así mayor agilidad en la modificación”.

También en este aspecto España ha tenido una contribución destacada, con trabajos en paralelo en el ámbito privado en esta materia. En este sentido, destaca **Carlos Pastor**, director de Estrategia Blockchain en Inetum, los avances realizados con grandes proyectos que son reconocidos a nivel europeo y que comenzaron con estándares españoles. “Hemos trabajado en colaboración público-privada en grandes iniciativas, como Alastria, que empezaron en nuestro país y han contribuido a consolidar la identidad en el ámbito europeo y en grandes proyectos como Dalion⁴, la solución de identidad digital autogestionada de once grandes empresas en la que participa Inetum”.

4. Inetum (30-06-2023). Dalion, la solución de identidad digital autogestionada, premio en los Blockchain Awards de Alastria. [Comunicado de prensa]

<https://www.inetum.com/es/spain/noticias/dalion-la-solucion-de-identidad-digital-autogestionada-premio-en-los-blockchain>

Brecha digital

En el último bloque del debate los expertos discutieron sobre la facilidad de uso de los sistemas de identificación para colectivos afectados por la brecha digital.

Juan Crespo detalló los esfuerzos de la Policía Nacional para acercar servicios de actualización de documentos a la “España vaciada”. Según explicó, están tramitando un convenio con la FEMP para desplegar **300 puestos de actualización de documentación** en distintos municipios que sean cabeza de partido judicial, situados a más de 30 kilómetros de una comisaría o de una oficina de documentación, a los que el ciudadano pueda acercarse para renovar el DNI y sus certificados sin necesidad de desplazarse a la capital de la provincia. Añade, además, otro plan con **85 unidades móviles** para la expedición de DNI y pasaporte en un solo acto. Este enfoque busca facilitar el acceso a servicios digitales, especialmente para colectivos afectados por la brecha digital.

Ángel L. Martín Bautista resaltó la importancia de esfuerzos que no solo beneficien a colectivos vulnerables, sino a toda la población, considerando la variedad de usuarios y la complejidad de desarrollar servicios digitales intuitivos para todos. También elogió la iniciativa de acercar la administración a los ciudadanos, reconociendo que no todos ellos adoptarán soluciones digitales.

Por su parte, **Izaskun Urrestarazu** puso en valor la iniciativa de una *App* móvil del Departamento de Servicios Sociales del Gobierno de Navarra que contempla medidas de accesibilidad, basada en la propia intuición para facilitar el acceso a los servicios.

En esta línea, **Carlos Pastor** mencionó iniciativas en las que Inetum está implicada, con Incibe y con la Unión Europea, y en todas ellas destaca un análisis de la facilidad de uso, de valoración de la experiencia de usuario, para que, efectivamente, esta sea lo más sencilla posible. A modo de conclusión de este bloque, relacionado con la facilidad de uso de la tecnología y los servicios a los que se accede, considera Pastor que, si el sector privado hubiese puesto servicios encima de la mesa para ser usados mediante el DNI electrónico, todos nos habríamos adaptado y habríamos aprendido a usarlo. Destacó, finalmente, en su intervención la importancia de contar con soluciones en el mundo físico para quienes tengan dificultades para adoptar los servicios digitales.

Conclusiones

Los siguientes titulares reflejan perspectivas clave presentadas durante el bloque.

Facilidad de uso en lo digital: Se destaca la importancia de que lo digital no solo sea accesible, sino también fácil de usar. Se busca que la tecnología digital redunde en la facilidad de uso, priorizando la experiencia del usuario.

Un mundo digital unificado: Se señala que estamos en un mundo digital, y, por primera vez, muchos países se ponen de acuerdo en identificar a sus ciudadanos de la misma manera. La información identificativa es reconocida y válida en todos esos países por igual.

Encrucijada digital en la Unión Europea: Se describe la situación de Europa como una “encrucijada digital”, donde la soberanía digital es esencial. La identidad digital se presenta como una pieza clave para la adopción generalizada y exitosa, destacando la importancia de la facilidad de uso como elemento clave.

Identidad digital para todos: Se enfatiza que la identidad digital debe ser igual para todos y utilizarse de manera habitual. La facilidad de uso se presenta como el elemento más importante para lograr la adopción exitosa de soluciones de identidad digital.

En general, las conclusiones subrayan la necesidad de abordar la facilidad de uso, la adopción generalizada y la importancia de la identidad digital en el contexto europeo.

Sobre el Observatorio del Sector Público

Con el foco puesto en la transformación digital de las Administraciones Públicas, el Observatorio del Sector Público lleva a cabo tareas de identificación, ordenación, valoración y difusión de políticas públicas, planes de acción, proyectos y servicios exitosos para la transformación digital, provenientes principalmente del ámbito internacional, a partir de los cuales se pueden efectuar propuestas aplicables al sector público español, dando lugar a un verdadero centro de conocimiento de la Administración Digital.

www.ospi.es



OSPI ■

Observatorio
del sector público

inetum 