BYTIC MEDIA

NÚMERO 50 | SEPTIEMBRE 2026

La gestión de los datos en la AAPP

ENTREVISTA

Lola Rabollo, responsable de Administración Pública en Cloudera

ENCUENTROS BYTIC

Cómo avanzar hacia un modelo de Zero Trust en las administraciones

V TORNEO DE PADEL

BY TIC MEDIA

Plazas limitadas
Reserva la tuya

8 DE OCTUBRE

EUROINDOOR ALCORCON

ÍNDICE DE CONTENIDOS

Sobre **NOSOTROS**

ByTIC es una plataforma de comunicación independiente que dedica su actividad a la información y creación de una comunidad de profesionales para el fomento de la tecnología y la innovación en las Administraciones Públicas en España.

Nuestra misión

Nuestra misión es unificar e incrementar el conocimiento sobre tecnología e innovación en Sector Público entre los profesionales TIC del país.
Desde ByTIC trabajamos con el objetivo de aumentar la transparencia sobre los proyectos tecnológicos en la Administración ante profesionales y directivos TI de empresas proveedoras de tecnologías.

Nuestra visión

Nuestra visión como plataforma referente de información de tecnología en Sector Público, es crear una comunidad que ayude tanto a proveedores de tecnologías como profesionales de la Administración Pública, aportando un marco de conocimiento que facilite y optimice la relación entre todas las partes.

BYTIC MEDIA

contacto@bytic.es
www.bytic.es

COMITÉ DE EXPERTOS

Carmen García Roger

Subdirectora Gral. de Estadística de Servicios. Ministerio de Hacienda y Función Pública

Ángel Luis Sánchez García

Jefe de Servicio de Arquitectura y Normalización. CTO del Servicio Madrileño de Salud [SERMAS]

Montaña Merchán Arribas

Coordinadora de informática [tecnologías emergentes] Secretaría General de la Administración Digital

Pedro M. Galdón Conejo

CIO & CISO de EMASA

Ildefonso Vera Gómez

Executive Advisor of Defense & Public Security de NTT Data

Andrés Prado Domínguez

Director del Área TIC UCLM

Concepción García Diéguez

Sistemas de Información Madrid Digital

Lucía Quiroga Rey

Asesora Técnica Delegación del Gobierno. Junta de Andalucía

Nacho Santillana Montal

exDirector de sistemas de la información del Ayuntamiento de Barcelona

Concepción Campos Acuña

Presidenta de la asociación de mujeres en el Sector Público

Sebastian Puig Soler

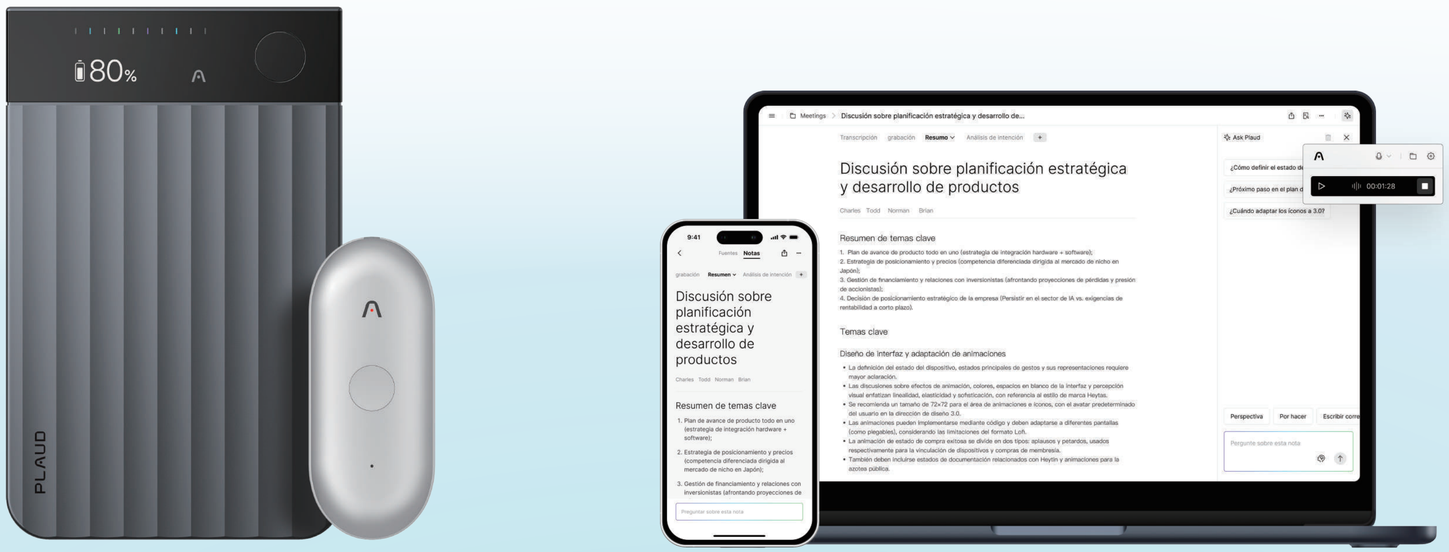
Jefe del Órgano de Dirección - Dirección General Asuntos Económicos. Ministerio de Defensa

María Luisa Ulgar

Coordinadora Iniciativa WomANDigital en Junta de Andalucía

PLAUD

Las mejores decisiones tienen lugar en conversaciones que no se deben olvidar.

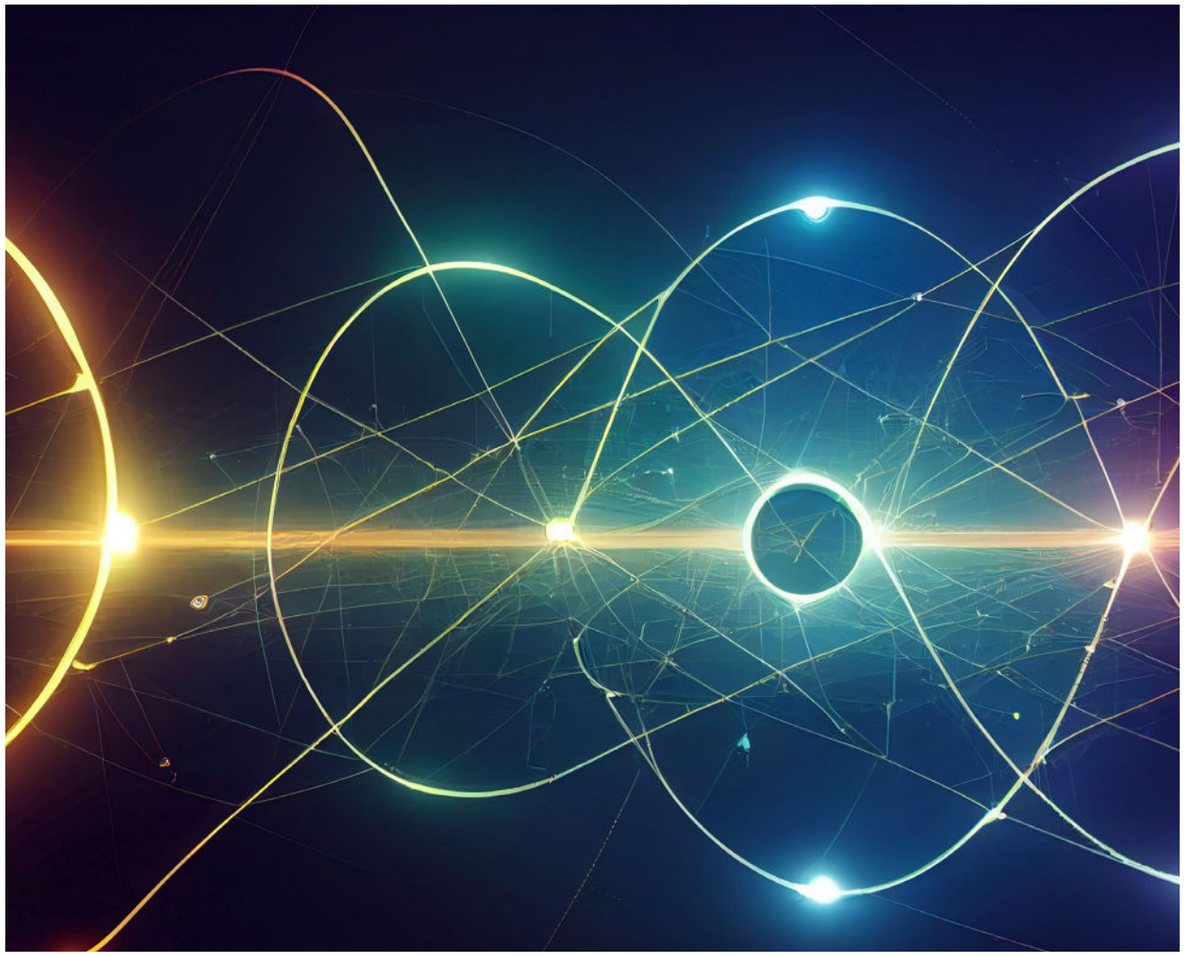


El dispositivo de IA que te libera de tomar notas.

reddot winner 2024 | reddot winner 2025 | reddot winner 2026 | iF DESIGN AWARD 2025 | iF DESIGN AWARD 2026 | GOOD DESIGN AWARD 2025 | 4.9 Rating on Apptopia | 4.7 Rating on Amazon | Sensaio ISO/IEC 27034 Certified | Sensiba ISO/IEC 27034 Certified | GDPR | SOC 2 | HIPAA | EN 18031

Para más información

El CCN fija 2030 como horizonte para migrar los sistemas públicos de mayor riesgo a criptografía poscuántica



El Centro Criptológico Nacional (CCN) ha situado la transición hacia criptografía postcuántica entre las prioridades de ciberseguridad para las administraciones y organizaciones que gestionan información sensible.

En su guía CCN TEC 009/BP 37, el organismo vinculado al Centro Nacional de Inteligencia (CNI) plantea que los sistemas clasificados como de riesgo alto deberán completar la migración hacia criptografía postcuántica antes del 31 de diciembre de 2030, mientras que los de riesgo medio contarán con plazo hasta el 31 de diciembre de 2035.

La recomendación parte de una previsión: la posible disponibilidad, hacia mediados de la próxima década, de ordenadores cuánticos con capacidad suficiente para comprometer buena parte de la criptografía asimétrica actualmente extendida. Este tipo de tecnología sustenta funciones esenciales en los entornos digitales, como el cifrado de comunicaciones, la autenticación, el intercambio de claves y la firma electrónica.

Para las administraciones públicas, el impacto potencial trasciende la protección técnica de las redes. Afecta a procedimientos administrativos electrónicos, servicios de identidad digital, relaciones con proveedores, custodia documental, plataformas de intercambio de datos y sistemas que manejan información con largos periodos de conservación. La guía del CCN advierte de que el riesgo no se limita al momento en que exista una capacidad cuántica operativa, ya que datos cifrados hoy pueden ser interceptados, almacenados y descifrados más adelante.

Este escenario, conocido como «almacenar ahora y descifrar después», introduce una variable temporal en la planificación de la seguridad. Información que mantendrá valor o requerirá confidencialidad durante la próxima década puede quedar expuesta en el futuro si se protege exclusivamente con algoritmos vulnerables a capacidades de cálculo cuántico. El documento incluye entre esos activos potencialmente afectados la información protegida mediante cifrado y los mecanismos de firma electrónica.

Un calendario vinculado al riesgo

El CCN plantea un calendario diferenciado según la criticidad de los sistemas. Los entornos de riesgo alto deberán haber completado su transición antes de finalizar 2030. Para los de riesgo medio, el límite se establece en el 31 de diciembre de 2035. En el caso de los sistemas de riesgo bajo, la migración se plantea en la medida de lo posible.

La fecha de 2030 no supone únicamente un objetivo de sustitución tecnológica. La documentación divulgativa publicada por el organismo incorpora una primera referencia intermedia para el 31 de diciembre de 2026. Para

entonces, las organizaciones deberían contar con estrategia, modelo de gobernanza, inventario criptográfico, clasificación de casos de uso y proyectos piloto iniciados para los sistemas de riesgo alto y medio.

Este planteamiento obliga a tratar la transición como un programa de transformación con dimensiones técnicas, organizativas y presupuestarias. La criptografía está integrada en múltiples capas de los sistemas de información y, en muchos casos, no resulta visible desde la operación cotidiana. Puede encontrarse en aplicaciones propias y de terceros, certificados digitales, mecanismos de acceso remoto, comunicaciones entre organismos, dispositivos conectados, copias de seguridad, bases de datos, pasarelas de pago, expedientes electrónicos o componentes de infraestructura suministrados por distintos fabricantes.

La dificultad, por tanto, no reside solo en seleccionar algoritmos resistentes a la computación cuántica. La administración debe identificar dónde se utilizan mecanismos criptográficos, qué datos y procesos protegen, qué dependencias existen entre aplicaciones y qué impacto operativo tendría su actualización. El CCN recomienda iniciar cuanto antes las fases de descubrimiento, adquisición, despliegue y puesta en marcha para reducir el riesgo de migraciones incompletas o tardías.

Gobernanza e inventario criptográfico

La guía concede un espacio específico a la gobernanza. Según el CCN, las instituciones deben establecer quién lidera la transición, cómo se medirá el avance y de qué forma se mantendrá el cumplimiento normativo durante el proceso.

La asignación de responsabilidades adquiere relevancia en organizaciones con competencias tecnológicas distribuidas entre unidades de sistemas, seguridad, contratación, servicios jurídicos, responsables funcionales y proveedores externos. Un programa de transición poscuántica requiere, en ese contexto, criterios comunes para priorizar activos, aceptar riesgos residuales, definir requisitos en los contratos y verificar el cumplimiento de los plazos.

El inventario criptográfico aparece como uno de los instrumentos centrales de la preparación. La documentación del CCN aconseja identificar los activos criptográficos empleados y sus dependencias, junto con la información o los activos que protegen y su nivel de criticidad. También recomienda actualizar ese inventario durante todo el proceso.

En la práctica, este ejercicio permite distinguir entre tecnologías que pueden evolucionar mediante actualizaciones de software y otras cuyo reemplazo puede exigir renovaciones de equipamiento, cambios de arquitectura o sustitución de productos. También permite detectar sistemas heredados, integraciones con terceros y servicios cuya criptografía depende de decisiones adoptadas por proveedores.

Cifrado, firma y soluciones híbridas

El documento aborda las principales piezas de la transición, entre ellas los mecanismos de encapsulación de claves, las firmas digitales y las soluciones híbridas. Los mecanismos de encapsulación de claves son relevantes porque permiten establecer de forma segura las claves que se emplean para cifrar comunicaciones o datos. Las firmas digitales, por su parte, intervienen en la autenticidad, integridad y no repudio de numerosos trámites electrónicos.

La incorporación de soluciones híbridas responde a la necesidad de compatibilizar tecnologías existentes con mecanismos resistentes a la computación cuántica durante una fase transitoria. Este enfoque puede permitir que una comunicación o un procedimiento combine esquemas criptográficos convencionales y poscuánticos mientras se completa la adaptación del ecosistema tecnológico. La decisión sobre su aplicación dependerá de la arquitectura disponible, la interoperabilidad exigida y las recomendaciones técnicas vigentes del CCN.

La guía invita asimismo a consultar los algoritmos y protocolos recomendados por el organismo, así como los productos y servicios identificados como quantum resistant en el Catálogo de Productos y Servicios de Tecnologías de la Información y la Comunicación [CPSTIC]. Para las administraciones, esta referencia puede trasladarse a los procesos de compra pública, los pliegos tecnológicos, las renovaciones de contratos y los requisitos de interoperabilidad con otras entidades.

Editorial

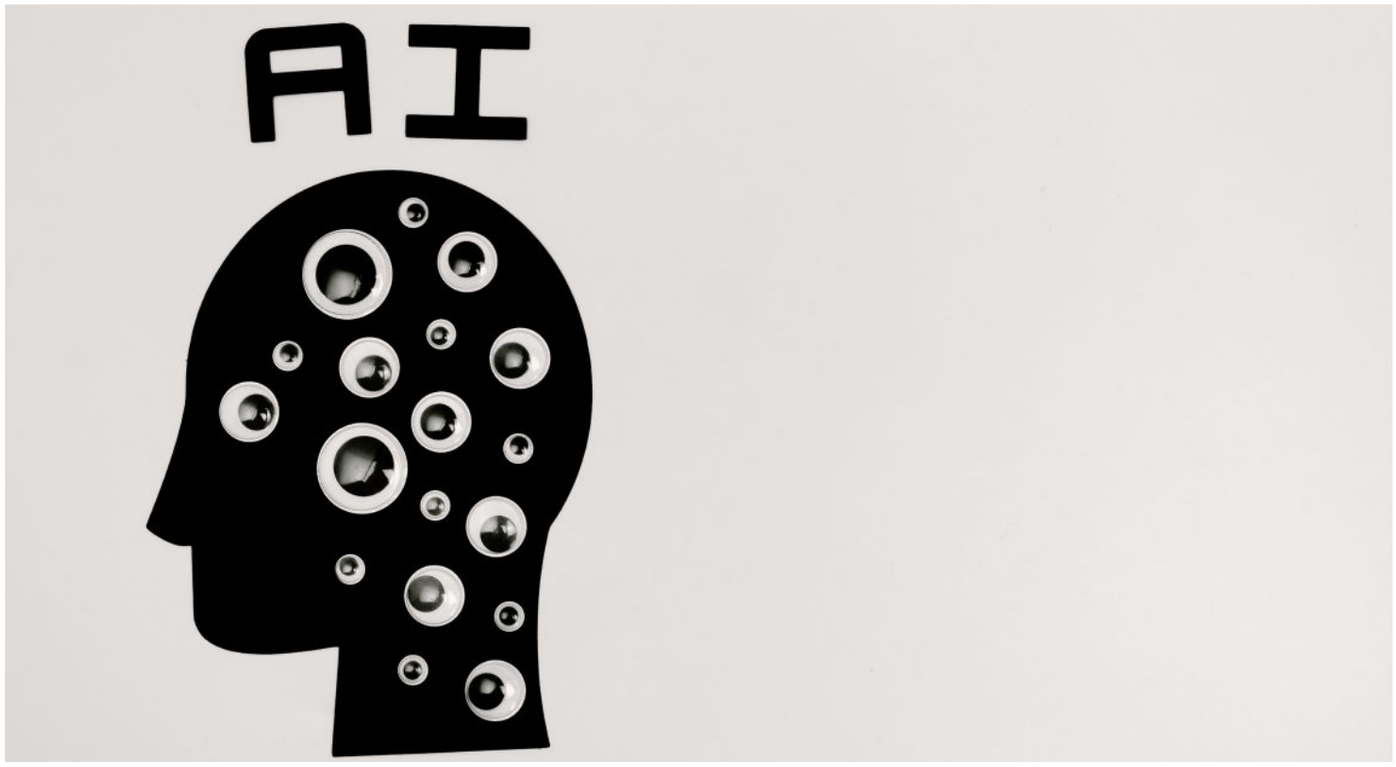
La transformación digital de la Administración en España ha logrado avances indiscutibles en la tramitación electrónica e infraestructuras. Sin embargo, la gestión estratégica y el gobierno integral del dato se mantienen como la gran asignatura pendiente del sector público. En la actualidad, nos encontramos ante una madurez asimétrica donde conviven iniciativas avanzadas con silos departamentales, una acusada deuda técnica y una notable falta de liderazgo transversal.

El obstáculo de fondo no reside en las herramientas tecnológicas disponibles, sino en barreras culturales y organizativas muy arraigadas. Durante años se han automatizado procedimientos sin definir con claridad la propiedad, la trazabilidad ni la calidad de la información. Con frecuencia, el dato sigue percibiéndose como propiedad exclusiva del departamento que lo genera, en lugar de entenderse como un activo institucional compartido al servicio del interés general.

Para construir una Administración moderna con la vista puesta en 2030, es imprescindible abandonar el modelo de repositorio único y apostar por centralizar las reglas de gobernanza mientras se me mantiene la gestión operativa federada. Asimismo, la soberanía del dato debe desligarse de la mera ubicación física del servidor para centrarse en un control técnico, normativo y contractual efectivo que garantice la independencia operativa.

Solo superando la interpretación defensiva de las normativas y fijando pilares claros de gobernanza se logrará un cambio de paradigma definitivo: pasar de una tramitación reactiva y burocrática a la prestación de servicios proactivos que se anticipen a las necesidades reales de la ciudadanía con total transparencia.

Euskadi defiende una IA con control público, límites claros y supervisión humana



La consejera de Gobernanza, Administración Digital y Autogobierno, Maria Ubarretxena, ha participado en la ciudad francesa de Lille en el Grand Sommet (Gran Cumbre) 'L'IA avec NOUS'. Este foro internacional reúne a más de un millar de responsables públicos, empresas tecnológicas y expertos de todo el mundo para analizar los retos de la inteligencia artificial desde una perspectiva social, económica y democrática.

Ubarretxena ha intervenido en el panel titulado 'Regiones impulsadas por la inteligencia artificial: cinco regiones, una ambición compartida', donde ha detallado la estrategia del Gobierno Vasco. En el encuentro ha compartido mesa con representantes institucionales de Maryland (Estados Unidos), Turingia (Alemania) y la Región de Bruselas-Capital (Bélgica), que han abordado el papel fundamental de las administraciones en la gobernanza ética de esta tecnología.

Las personas en el centro

Durante su intervención, la consejera ha subrayado que la clave del modelo vasco es situar a las personas en el centro "de forma innegociable". Bajo este principio, ha remarcado la importancia de mantener el mando institucional ante una transformación tecnológica irreversible.

"En Euskadi tenemos claro que la inteligencia artificial nos ayuda, pero no nos sustituye: no va a tomar decisiones sobre derechos, salud, empleo o condiciones de vida de las personas, porque esa responsabilidad es y seguirá siendo siempre humana", ha afirmado.

Ubarretxena ha explicado que el objetivo prioritario es utilizar la IA para eliminar tareas repetitivas y agilizar procesos, reforzando así el trabajo de los empleados públicos sin sustituir en ningún caso su criterio y experiencia. En este sentido, ha señalado que "el reto para las instituciones no es incorporar tecnología sin más, sino gobernarla para mejorar los servicios y consolidar la confianza de la ciudadanía".

Transparencia y control democrático

Como un ejemplo concreto de esta apuesta por la transparencia, la consejera ha destacado el Catálogo de Algoritmos y Sistemas de IA del Gobierno Vasco. Euskadi fue la primera comunidad del Estado en publicar este registro que actualmente cuenta con 16 sistemas en uso en áreas como salud, empleo, euskera o atención ciudadana. Esta iniciativa busca hacer comprensible y auditable el uso de algoritmos.

"Este catálogo responde a un estándar de transparencia significativa porque creemos que

publicar no basta; hay que publicar lo necesario para el control democrático", ha explicado Ubarretxena. El catálogo, que recibió el Premio Audaz 2026, permite conocer la finalidad de cada sistema, los datos utilizados y la supervisión humana de cada proceso, evitando que el uso de algoritmos se convierta en una herramienta opaca para la ciudadanía.

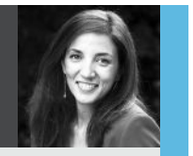
Soberanía del dato

Otro de los ejes de la estrategia vasca es la consideración del dato como un activo esencial para ofrecer servicios públicos, lo que requiere una gobernanza. Ubarretxena ha defendido la soberanía del dato entendida como control público para asegurar que los datos de las personas se gestionan con reglas claras y pleno respeto a los derechos fundamentales. Sólo así se podrán ofrecer mejores servicios, cada vez más personalizados cuando la ciudadanía así lo decida.

Para asegurar este despliegue ético, Euskadi cuenta con una estructura de soporte liderada por la Oficina de Gobierno de la IA y del Dato, la sociedad pública tecnológica EJIE, la iniciativa ADI [Atlantic Data Infrastructure] y el Basque Artificial Intelligence Center [BAIC]. Todas ellas están contribuyen a reforzar la autonomía digital estratégica europea.

Finalmente, la consejera ha resaltado que la cercanía de las instituciones vascas permite adaptar la tecnología a necesidades reales y específicas de la sociedad y ha citado como ejemplo el uso de la IA para reforzar la atención en euskera en los servicios digitales.

La opinión de Arantxa Herranz



Para muchas personas, el verdadero comienzo del año no es enero, sino septiembre. Quizá porque nos recuerda a la vuelta al cole, porque hemos podido descansar y el verano siempre parece una época más alegre que las navidades, en las que la nostalgia invade a muchas personas y nos les permite disfrutar de esos días señalados.

Sea como fuere, lo cierto es que este no me parece un septiembre cualquiera. El reloj para la convocatoria de elecciones generales ya se ha puesto en marcha e, independientemente de cuando sean y el resultado que arrojen, es más que evidente que producirá una pequeña parálisis en la AGE y casi por extensión en muchas otras entidades públicas, a la espera de que la lotería diga si hay cambio de destino o responsabilidades.

Si a esto añadimos el fin de los fondos europeos, el tablero puede estar más parado que nunca, lo que no es buena señal.

Ante este escenario incierto, resulta imprescindible no bajar la guardia ni dejar que la inercia institucional frene las inversiones estructurales pendientes. Es momento pues de agudizar el ingenio y seguir remando para que, llegado un nuevo informe DESI, España salga favorecida en la foto.

Drones e IA para mejorar el control de la calidad del agua

La Generalitat Valenciana ha puesto en marcha un proyecto piloto para reforzar la monitorización de la calidad del agua mediante el uso combinado de drones, cámaras hiperespectrales, inteligencia artificial y trabajos de validación sobre el terreno que permiten obtener datos en tiempo real ante posibles vertidos o episodios de contaminación.

El vicepresidente tercero y conseller de Medio Ambiente, Infraestructuras, Territorio y de la Recuperación, Vicente Martínez Mus, ha presentado esta iniciativa en la Gola de Pujol de l'Albufera, que se enmarca en la estrategia de la Generalitat para reforzar el control y seguimiento de las zonas de baño de la Comunitat Valenciana mediante la incorporación de nuevas tecnologías y una mayor capacidad de vigilancia.

Martínez Mus ha destacado que este plan supone un nuevo paso en la apuesta de la Generalitat por la innovación, la tecnología y los datos para mejorar la gestión ambiental y proteger nuestros ecosistemas acuáticos". Denominado 'Ocean Watcher', el proyecto desarrolla un sistema avanzado de seguimiento que permitirá obtener información más rápida, precisa y completa sobre el estado de las aguas y reforzar la capacidad de detección temprana ante posibles episodios de contaminación.

El sistema combina teledetección mediante drones, cámaras hiperespectrales, modelos de inteligencia artificial y muestreos de agua realizados sobre el terreno. La información obtenida mediante los vuelos se correlacionará con los resultados de las muestras para calibrar y validar modelos basados en el análisis espectral.

"La tecnología nos permite avanzar hacia una gestión ambiental basada en más información y en una mayor capacidad de anticipación", ha señalado el vicepresidente tercero, quien ha subrayado que el objetivo es "contar con mejores herramientas para conocer el estado de nuestras aguas y actuar con mayor rapidez ante posibles episodios de contaminación".

Martínez Mus ha remarcado que este sistema esta basado en "la inmediatez", ya que se actúa en el momento para dar una solución. Además, el sistema permitirá también mejorar los tiempos de detección y respuesta ante posibles episodios de contaminación.

En la actualidad, cuando una muestra analítica detecta parámetros que no se corresponden con los valores establecidos, puede haber transcurrido alrededor de 24 horas desde la toma de la muestra, de modo que la situación detectada puede haber evolucionado cuando se recibe la señal de aviso. 'Ocean Watcher' busca avanzar hacia una detección más temprana que permita conocer con mayor rapidez el estado de las aguas y actuar ante posibles episodios de contaminación.

Seis puntos de seguimiento

El proyecto piloto, que se complementa con la medición en tiempo real presentada en Meliana hace unas semanas, se desarrolla en seis puntos de la costa valenciana seleccionados por su posible afección por vertidos urbanos. En concreto, los trabajos se realizan en las acequias Sangonera y Nova, en Meliana; la acequia Sant Vicente y el barranco del Carraixet, en Alboraya; las golas del Pujol y del Perellonet, en València, y la Gola del Rey, en Sueca.

En estos puntos se realizan campañas de muestreo de agua superficial y vuelos con drones equipados con cámaras hiperespectrales. Los trabajos incluyen el registro de parámetros básicos como la temperatura y la turbidez, además de la localización mediante GPS y las condiciones ambientales. La información obtenida permitirá relacionar los datos de los vuelos con los resultados de los análisis realizados sobre el terreno.

'Ocean Watcher' complementa la red de vigilancia de la calidad de las aguas de baño de la Generalitat que está en vigor y realiza casi 5.000 análisis en cada temporada de baño. Además del control de las zonas de baño, la red de vigilancia incluye el seguimiento de efluentes que vierten al mar y que pueden incidir en la calidad del agua, como golas, acequias, aliviaderos de conducciones de vertidos y colectores de pluviales.

La incorporación de nuevas herramientas de teledetección e inteligencia artificial permitirá complementar estos sistemas de control con nuevas fuentes de información y avanzar en la detección temprana de posibles episodios de contaminación.

La administración pública frente al reto de implementar una estrategia 'Zero Trust'

El avance del teletrabajo, la explosión de servicios en la nube y la creciente complejidad de los ecosistemas tecnológicos han desdibujado por completo el perímetro de seguridad tradicional, obligando a las instituciones a repensar sus estrategias. Así se puso de manifiesto en un encuentro ejecutivo de ByTIC patrocinado por Trend Micro, donde responsables de ciberseguridad del sector público debatieron sobre la implantación de modelos de «confianza cero» (Zero Trust), una filosofía basada en no confiar por defecto en ningún usuario o dispositivo y verificar siempre cada acceso.

La desaparición del perímetro tradicional

Pablo Mattern, responsable de ciberseguridad del Hospital La Paz de Madrid, describió el cambio de paradigma en el ámbito sanitario: «venimos de una arquitectura en la que la persona que estaba fuera del hospital era siempre un externo». «Alrededor de las administraciones poníamos un muro muy alto, un perímetro. Cualquier persona que estuviera dentro podía tener acceso a la mayoría de recursos», señalaba. Sin embargo, con el teletrabajo y la telemedicina, «esta barrera que ponemos alrededor de nuestra organización desaparece». Mattern añadió que «no es algo ya que sea opcional. Es algo que tenemos que trabajar para que nuestros sistemas estén empapados».

Frente a esta apertura, existen organismos con necesidades de aislamiento extremo. Juan Luis Vicente, del área de organización y planificación digital de la Agencia Tributaria, detalló: «En la Agencia Tributaria los entornos son totalmente aislados. Solamente determinados puntos están permitiendo ese intercambio de datos. El resto son, perfectamente, podríamos definirlo, como silos». En su organización, la protección prima sobre la agilidad: «No permitimos el envío de correos o adjuntos, salvo determinadas personas, y bajo un permiso previo. Por lo tanto, estamos penalizando de alguna forma esa velocidad respecto a lo que sería la seguridad».

El desafío cultural y la visibilidad

Transitar hacia la «confianza cero» implica un choque cultural. Miguel Ángel Abeledo, CISO de Tragsa, lo calificó como «un reto muy complicado desde un punto de vista tecnológico y, sobre todo, cultural». De acuerdo con Abeledo, «en organizaciones tan grandes como la nuestra, 30.000 empleados que están ubicados en cualquier parte de España, es complicado», situando el problema «fundamentalmente por la parte de la cultura, de que los usuarios entiendan que desconfías de ellos por defecto y por naturaleza. No es algo que va a costar muchísimo».

Por su parte, David Guijas, del área de operaciones de seguridad en el Centro Criptológico Nacional (CCN-CERTIC), enfatizó la pérdida de los entornos corporativos cerrados: «Ya no vamos a datos on-prem, sino que ya incluso la propia industria te está redirigiendo hacia datos que están en la nube. Entonces ya el perímetro está difuminado, prácticamente no existe». Para lograr cambios efectivos, Guijas subrayó que «es muy importante también que la directiva esté involucrada y dé el apoyo concreto a que se puedan implantar

estas medidas».

El equilibrio entre la protección y la operatividad diaria de las instituciones genera roces constantes. Juan Luis Vicente reflexionó sobre esta tensión: «Si yo quisiera una seguridad completa, basta con que yo estuviera aislado de todo, lo cual es imposible». Explicó que «si yo doy flexibilidad, eso empieza a abrir puertas, donde es muy difícil ver todas las casuísticas que se pueden producir», y advirtió: «Si tú al usuario le pones impedimentos y dificultades, obviamente va a rechazar esa tecnología».

En el sector sanitario, este dilema alcanza cotas críticas. Pablo Mattern ejemplificó cómo la seguridad no puede bloquear la atención de urgencia: «En un ordenador de urgencias no puedes estar haciendo que el equipo funcional esté logueándose y poniendo su contraseña cada vez que quiere hacer algo». Bloquear un equipo tras varios intentos fallidos es inviable en ciertos dispositivos: «Tú eso no lo puedes hacer, por ejemplo, en un ordenador que esté conectado a un respirador o una bomba de insulina, porque que se bloquee ese ordenador supone que puedes poner en riesgo la vida de una persona».

Ante estas realidades, contar con una visión integral de los activos resulta imprescindible. Beatriz Burgos, Regional Account Manager de Trend Micro, resumió: «antes de toda la parte de Zero Trust, hay algo que es bastante más valioso e importante, que es la visibilidad. Visibilidad de toda tu infraestructura, de quién se conecta a ella, de quién accede a ella». Y añadió: «Una vez que ya tienes la visibilidad de tu entorno es cuando ya puedes tomar medidas y en algunos casos será Zero Trust, en otros casos será otra cosa».

Convivencia con sistemas heredados y nuevas amenazas

La presencia de sistemas obsoletos supone un riesgo recurrente. David Guijas expuso el caso de un equipo con «Windows 7 que a lo mejo ya está fuera de soporte y ya no tienes parcheo. Tienes que empezar a buscar, puedes meterlo por ahí para que esté lo menor expuesto posible. Tienes que buscar alternativas para que puedas tú con cierta comodidad, por decirlo de alguna manera, convivir con un entorno que sabes que es por defecto inseguro».

Juan Luis Vicente describió la inercia organizativa que perpetúa estos sistemas: «Estás con ese entorno diciendo: 'el año que viene lo quitamos, ya lo tenemos planificado'. El año que viene ya son dos. Ahora me surge otra necesidad. Sigo, sigo. Ahora resulta que no lo voy a tocar». La parálisis técnica puede llevar a un punto crítico: «Ha llegado un momento en que has pegado dos saltos hacia delante y ya no hay forma de hacer nada con eso, rezar que no se rompa».

Javier Díaz coincidió en los riesgos de depender de desarrollos antiguos: «Ya no existe la empresa que lo desarrolló, no hay evolución, no se ha adaptado a las necesidades actuales, no se ha pensado en la seguridad en el desarrollo». Para paliarlo, se recurre al parcheo virtual, algo que Miguel Ángel Abeledo validó: «Sí, tenéis virtual patching para ahora Windows 7. Sí, lo hay».

En paralelo, el cibercrimen utiliza inteligencia artificial ofensiva, lo que obliga a extremar las precauciones. «Con lo de la IA del ataque, lo que hablábamos de la IA ofensiva, está muy preocupado con el tema este del perímetro difuso y cobra mucho más valor el tema de tener los sistemas parcheados», señaló Díaz. Abeledo añadió la necesidad de priorizar los parches: «No es cazar toda la vulnerabilidad, sino que a ti [la] inteligencia te diga dónde tienes que parchear prioritariamente, que es más complicado».

El factor humano y la "tecnología en la sombra"

Las restricciones suelen chocar con las expectativas del personal. Pablo Mattern explicó la presión que ejercen los profesionales en los centros de salud: «Nos vienen facultativos y nos dicen: '¿pero por qué no lo podéis hacer si en el hospital tal ya lo tienen?'. Y claro, nosotros decimos: '¿cómo lo han conseguido?'».

Esta insatisfacción fomenta la aparición del Shadow IT. Miguel Ángel Abeledo apuntó que «el que no le das lo que quieres, pues ellos buscan las habichuelas para implementar sus propios métodos». Mattern lo confirmó: «Los médicos son muy listos y de repente, además, pasa mucho que ellos vienen ya con la solución».

El desarrollo informal de aplicaciones por parte del propio personal complica el control técnico. Juan Luis Vicente advirtió: «Esto ha hecho una aplicación en Visual, en JavaScript, ha metido algo en Python. Ves que te han empezado a abrir brechitas». Beatriz Burgos complementó señalando la incorporación de modelos lingüísticos caseros: «Su modelo es LLM que se hacen los propios informáticos en los hospitales específicos para analítica de imágenes y demás. Y además modelos LLM que pueden tener también brechas de seguridad».

La jerarquía interna también dificulta la aplicación estricta de las normas. Javier Díaz comentó: «Nos han llegado a decir que según qué usuario, pues no le puedes cortar, tiene acceso libre a según qué cosas simplemente por el perfil que tiene. ¿Cómo se le va a cortar la navegación a la ministra?».

Brechas, atajos e inmediatez

Los atajos operacionales por comodidad son habituales. Juan Luis Vicente confesó: «Ya están creando esas mínimas brechas de seguridad por comodidad, pero todo el mundo sabe que en un departamento IT hay muchos atajos que no los cuentas y los utilizas como ayuda, pero al final es un problema».

Por su parte, Pablo Mattern detalló hallazgos sorprendentes en la red hospitalaria: «Hemos llegado a detectar nodos Tor dentro de la infraestructura del hospital». En otro caso, identificaron «usuarios que estaban cursando en un máster de ciberseguridad y se pusieron a hacer un test de pentesting a uno de los servidores del hospital», concluyendo que «el propio trabajador es el vector principal por el que la arquitectura podría desmoronarse en cualquier momento».

David Guijas resaltó que la exigencia de inmediatez lleva a puentear las reglas: «Por no encontrar muchas veces la necesidad de la inmediatez por la jerarquía que tienen los militares, pues se buscan las habichuelas por otras rutas y al final te están buscando a ti el problema». La lentitud administrativa motiva el uso de dispositivos no autorizados. Juan Luis Vicente explicó: «Entre los tiempos que manejamos nosotros, cada vez que alguien te pide algo hasta que le respondes, pasa una semana o dos [...] la gente se cansa». De este modo, «tú crees que tienes todo controlado, [...] pero está entrando cosas».

Para revertir esta situación, se reclama mayor concienciación directiva y la aplicación del marco normativo continental. Miguel Ángel Abeledo remarcó: «Lo que nos viene de Europa pone en primera fila de responsabilidad a la alta dirección, ser conscientes de que un error en una toma de decisión les afecta a ellos». Subrayó además que «un error en una mala política, por un fallo de velocidad de querer ser más productivo, puede provocar que todo lo que habías hecho se caiga abajo», asegurando que «la gente tiene que saber que no puede hacer lo que quiera por defecto y que tiene que esperar».

No obstante, la autoridad del perfil profesional influye en el cumplimiento. Juan Luis Vicente expuso la encrucijada: «Si tú pones limitaciones a un médico, ¿quién es importante en el hospital, el médico o el ordenador?». Agregó que algunos usuarios simplemente «se ponen pies en pared y te dicen que ya puedes marcar la directriz, que esto lo vamos a hacer de esta forma».

Finalmente, se abordó el reto presupuestario y la justificación del gasto en prevención. Juan Luis Vicente admitió: «Cuando no pasa nada y pasa más de dos años o un año sin incidentes, empiezas a ver que es un coste». Ante ello, Miguel Ángel Abeledo sostuvo: «Lo que los responsables de seguridad tenemos que tratar de aprender o mejorar es la venta hacia los que toman las decisiones de que esto va dinero. Proyectar que lo que tú estás gastando en prevención es más barato que lo que te cuesta el incidente».

Para concluir, David Guijas destacó el valor disuasorio de la protección: «Simplemente la idea de que le va a costar más entrar en tu entorno que en otro le puede ser suficiente para que vaya a otro entorno más que al tuyo, aunque tú seas goloso». es el vector principal por el que la arquitectura podría desmoronarse en cualquier momento».

Juan Luis Vicente justificó esta impaciencia por la lentitud de los procesos burocráticos. «Entre los tiempos que manejamos nosotros, cada vez que alguien te pide algo hasta que le respondes, pasa una semana o dos [...] la gente se cansa», explicó. Esta frustración lleva a soluciones improvisadas como usar el móvil personal para transferir datos, burlando los controles del portátil corporativo. «Tú crees que tienes todo controlado, [...] pero está entrando cosas», sentenció.

ENTREVISTA

Lola Rebollo,

Head of Public Sector de Cloudera en España

"El mayor reto es acabar con la fragmentación para poder organizar, entender y proteger los datos que están dispersos"

Lola Rebollo, actual responsable de sector público en Cloudera, tiene una dilatada experiencia en el sector tecnológico en general y en la aproximación al sector público en particular. Graduada en Ingeniería Electrónica y especializada en semiconductores por la Universidad de Wilkes de Estados Unidos, fue directora para el Sector Público y Ciberseguridad en NEORIS y ha ocupado cargos de responsabilidad en entes públicos como subdirectora de Impulso a la Industria, Talento e I+D en el Instituto Nacional de Ciberseguridad [INCIBE] y ha formado parte del Consejo Asesor del Alto Comisionado de España Nación Emprendedora, iniciativa dependiente de Presidencia de Gobierno. En esta entrevista con ByTIC repasa la visión de Cloudera sobre algunos de los asuntos principales que están encima de la mesa de los responsables de tecnología e innovación del sector público.

¿Cómo está posicionada Cloudera actualmente en el mercado español y, en particular, en el ámbito de las administraciones públicas?

Dentro del ecosistema tecnológico de 2026, España ha evolucionado de un papel de adoptante para convertirse en un referente de innovación digital en el sur del continente. Para las Administraciones Públicas, somos un socio clave, ya que permitimos unificar ingestión, procesamiento analítico y gobierno del dato en un único entorno, manteniendo el control y la soberanía de la información crítica de este sector.

Con la llegada de la Ley de IA de la Unión Europea, nuestra

tecnología habilita a nuestros clientes a que los datos se usen de forma ética y controlada. Esto es vital para proyectos con impacto social, permitiendo que la administración sea más proactiva y se adelante a lo que necesitan los ciudadanos.

¿De qué manera la evolución hacia modelos basados en datos abiertos y compartidos está influenciando la oferta de Cloudera?

Nuestra oferta ha cambiado para adaptarse a un mundo donde los datos se comparten en lugar de estar aislados. Ya no somos un simple 'contenedor' de datos, sino que ayudamos a crear ecosistemas de colaboración. La clave ahora es la federación: en lugar de mover los datos a una plataforma central, nuestra tecnología va directamente a donde están guardados los datos.

Al facilitar que la administración comparta información con el sector privado de manera segura, ayudamos a que los datos públicos sirvan para crear aplicaciones que mejoren la salud, la movilidad, la eficiencia energética o el transporte.

¿Cuáles son las principales barreras que las administraciones públicas españolas encuentran a la hora de aprovechar sus datos de forma integral?

El mayor reto es acabar con la fragmentación para poder organizar, entender y proteger los datos que están dispersos. En el sector público esto es crítico, ya que se trabaja con información muy sensible y personal de los ciudadanos.

Según nuestro estudio 'The Data Readiness Index', solo el 20% de las administraciones públicas tiene sus datos bajo un control total. Los obstáculos principales que impiden usar bien la información son: no saber exactamente dónde están los datos, tener procesos de acceso demasiado complicados y la falta de una cultura interna que valore el uso del dato.

¿Qué propuestas o tecnologías ofrece Cloudera para impulsar una gestión unificada, segura y escalable del dato dentro de organismos públicos?

Cloudera, como única plataforma híbrida de datos e inteligencia artificial, permite alcanzar una interoperabilidad real entre diferentes entornos: on-premise, nube pública, nubes soberanas... Además, integra capacidades avanzadas de gestión, seguridad y gobernanza que permiten mantener el control y la soberanía de la información crítica, garantizando que los datos permanezcan protegidos en todo su ciclo de vida. Nuestra tecnología está sustentada en datos gobernados para impulsar la analítica avanzada e inteligencia artificial.

En un contexto de soberanía digital europea, ¿cómo se gestiona el equilibrio entre cumplimiento normativo, interoperabilidad y uso de soluciones en la nube?

Hoy el debate ya no está en dónde residen los datos, sino en cómo gobernarlos de forma unificada y segura, independientemente del entorno. La soberanía digital, por tanto, va mucho más allá de la ubicación: implica mantener el control sobre la infraestructura, el software, las operaciones y el marco regulatorio que los protege.

La verdadera soberanía digital se define como la capacidad de una organización para mantener el control sobre sus datos, infraestructura y decisiones tecnológicas sin interferencias de gobiernos extranjeros o proveedores externos. Requiere autoridad jurisdiccional, operativa y técnica absoluta sobre todo el ciclo de vida de los datos y la IA.

La estrategia de Cloudera está enfocada en integrar la soberanía a lo largo de todo el ciclo de vida de la IA, desde los datos utilizados para entrenar los modelos hasta los activos generados, garantizando siempre el control por parte de la organización. Para ello, nuestra plataforma está diseñada para abarcar todas las etapas del ciclo de vida de la IA, desde la preparación e integración de datos hasta el desarrollo, el entrenamiento y la implementación de modelos.

¿Qué papel debe jugar la inteligencia artificial en la modernización de los servicios públicos y cómo puede Cloudera ayudar a implementarla de manera responsable?

La inteligencia artificial tiene el potencial de transformar profundamente a las administraciones públicas, optimizando la toma de decisiones y proporcionando mejores servicios al ciudadano. Sin embargo, en este sector, en el que se gestiona información especialmente sensible, no basta con innovar, es imprescindible hacerlo de forma responsable.

Desde Cloudera apostamos por un enfoque de IA privada. Esta estrategia supone desplegar modelos de inteligencia artificial en entornos controlados por las propias organizaciones, donde la seguridad, la privacidad y la soberanía del dato están garantizadas en todo momento.

Para explicar de forma sencilla la diferencia entre los modelos de IA públicos y la IA privada, podemos compararlo con la experiencia en un restaurante. Los modelos de IA públicos serían como un buffet abierto, donde todos los comensales acceden a los diferentes platos y comparten un entorno común. La IA privada, en cambio, se asemeja a un chef que diseña un menú exclusivo para un grupo concreto de personas: selecciona cuidadosamente los ingredientes, adapta cada plato a las necesidades de los comensales y proporciona una experiencia personalizada. Del mismo modo, esta estrategia permite desarrollar modelos ajustados a los objetivos de la organización, manteniendo siempre el control y la confidencialidad de sus datos.

¿Cómo afronta Cloudera los retos de confianza y explicabilidad de la IA en un

contexto reglado como el del sector público?

La confianza en la inteligencia artificial empieza por la confianza en los datos. Sin una base de información gobernada, de calidad y segura, no es posible construir modelos fiables ni generar valor real. En el sector público, además, la exigencia es mayor: los ciudadanos necesitan entender cómo se toman las decisiones y qué datos intervienen en ese proceso. Sin transparencia, no hay confianza.

Por ello, resulta imprescindible habilitar canales informativos accesibles y garantizar que siempre exista supervisión humana sobre los sistemas de IA, así como disponer de los mecanismos de control necesarios, para asegurar una actuación correcta por parte de los modelos.

En este sentido, como comentaba anteriormente, Cloudera incorpora herramientas de gobernanza y de linaje del dato que salvaguardan la privacidad y la seguridad de la información se mantengan durante todo su ciclo su vida.

¿Qué ventajas aporta un modelo de "plataforma abierta de datos" frente a otros entornos más cerrados o propietarios?

El principal valor de una plataforma abierta de datos es la flexibilidad. Las plataformas híbridas permiten implementar arquitecturas de forma flexible, tanto on-premise, en la nube, o en entornos híbridos. Esto facilita la movilidad de conjuntos de datos entre entornos según las necesidades de procesamiento o analítica y reduce el riesgo de vendor lock-in.

¿Cómo encaja la ciberseguridad dentro de la propuesta de Cloudera, especialmente ante los crecientes riesgos vinculados a la gestión de datos sensibles ciudadanos?

El enfoque de Cloudera consiste en garantizar que la seguridad esté integrada desde el origen, a través de la estrategia "secure by design". En este sentido, abordamos la seguridad como un requisito prioritario a través de los siguientes pilares: autentificación, autorización, auditoría y anonimización.

La autentificación se integra con los directorios de cada empresa, por lo que se delega en el elemento correspondiente que valida y devuelve el control a Cloudera. A ello se une la autorización en función de proyectos, grupos o etiquetas semánticas. Junto a estas dos capacidades, realizamos una auditoría que registra todos los componentes que actúan en nuestra plataforma. Y los datos son anonimizados en función del usuario y de las características de la información mediante diferentes técnicas.

Cloudera Shared Data Experience (SDX) es la arquitectura que incorporamos a todas nuestras soluciones para proporcionar esas capacidades de seguridad y gobernanza de la información desde el punto de partida.

¿Podría compartir algún caso de uso concreto donde se haya demostrado el impacto de la analítica avanzada o del machine learning en administraciones públicas?

Un proyecto especialmente relevante es el desarrollado junto al Servicio Madrileño de Salud, que ha supuesto la creación del mayor repositorio de datos sanitarios de Europa. Este proyecto está permitiendo mejorar la atención al paciente, impulsar la investigación y optimizar la gestión sanitaria.

ENTREVISTA

Además, tomando como referencia esta iniciativa, Cloudera y la Comunidad de Madrid han creado el Madrid Data & AI Hub, que permite integrar y tratar datos de las distintas consejerías y los organismos del Gobierno autonómico para facilitar su acceso a los ciudadanos y mejorar la toma de decisiones de la administración.
También en el ámbito sanitario destaca el proyecto junto al Servicio Catalán de la Salud para la creación de una plataforma de IA que permite compartir y analizar datos médicos de forma segura entre distintos centros hospitalarios europeos, facilitando diagnósticos más precisos mediante algoritmos aplicados a imágenes médicas históricas.
Otro caso especialmente significativo es el de Metro de Madrid donde gracias a la analítica avanzada y al uso de algoritmos, se pueden reducir aglomeraciones, mejorar el control de aforos durante grandes eventos y avanzar en mantenimiento predictivo, aumentando así la eficiencia del servicio y la experiencia de los usuarios.
A ellos se añade la colaboración con la Agencia Tributaria en la mejora de sus capacidades de procesamiento y análisis de grandes volúmenes de información. Esto ha permitido acelerar el tratamiento de millones de documentos y conjuntos de datos, incorporar modelos analíticos más avanzados y reforzar al mismo tiempo la gobernanza, trazabilidad y seguridad de la información para garantizar el cumplimiento normativo.

¿Cómo imagina Cloudera la administración pública española dentro de cinco años si logra aprovechar plenamente el potencial de los datos?

En Cloudera imaginamos una administración pública española más conectada, donde los datos se conviertan realmente en un activo estratégico para impulsar servicios más eficientes, transparentes y personalizados.
Para ello, será imprescindible disponer de una infraestructura preparada, gobernada y segura, que permita aprovechar plenamente el potencial de la analítica avanzada y la inteligencia artificial para tomar decisiones más estratégicas y alineadas con las necesidades de los ciudadanos, optimizar la gestión de recursos públicos y acelerar la innovación en ámbitos clave como la sanidad, donde la IA puede impulsar avances muy relevantes en investigación y diagnóstico.
Todo ello debe ir acompañado de una apuesta decidida por el talento y la capacitación tecnológica. En este sentido, iniciativas como la convocatoria de 1.700 plazas especializadas en inteligencia artificial, ciberseguridad y ciencia del dato por parte del Ministerio de Transformación Digital y Función Pública representan un paso importante hacia una administración preparada para afrontar los retos del futuro.

¿Qué mensaje trasladaría a los CIOs y responsables de innovación pública que aún ven la analítica avanzada como un reto más que como una oportunidad?

Para los responsables públicos que contemplan la analítica avanzada con indecisión, la premisa es fundamental: la tecnología ha dejado de ser una barrera para convertirse en el pilar de la gobernanza moderna. Evolucionar del concepto de desafío al de oportunidad trasciende lo económico; es un cambio de mentalidad. Históricamente, la analítica se entendía como una complicación extra para sistemas ya sobrepasados. No obstante, en este 2026, el paradigma se ha transformado: el peligro real para las instituciones no reside en la adopción de modelos de vanguardia, sino en la persistencia de métodos obsoletos ante una ciudadanía globalmente conectada.. La gran ventaja competitiva es la transición de una gestión reactiva hacia una gestión predictiva. El objetivo no es la acumulación de datos por inercia técnica, sino la capacidad de prever necesidades sanitarias o perfeccionar los sistemas de transporte antes de que impacten negativamente en el usuario.
Ante el temor de que la IA y el Big Data comprometan la soberanía o la privacidad, la realidad demuestra que un esquema de gobierno de datos robusto ofrece una seguridad sin parangón. Actualmente, se puede auditar la trazabilidad de la información bajo los estándares europeos más rigurosos, asegurando que la soberanía institucional permanezca intacta mientras se aprovecha el máximo potencial computacional.
En última instancia, el valor reside en la humanización de la tecnología. La analítica avanzada es el medio para suprimir procesos burocráticos estériles y permitir que el capital humano se enfoque en servicios de alto valor añadido para el ciudadano. En esta era del conocimiento, la verdadera meta es emplear la inteligencia para edificar una administración pública sincronizada con el ritmo de vida actual.

ENTREVISTA

Diego Solier,

eurodiputado y ponente principal del CADA

"La soberanía no significa aislarse: el sector privado debe ir por delante y lo público facilitar que las cosas pasen"

Es el único eurodiputado español que actúa como ponente en el reglamento europeo conocido como Cada [Cloud and AI Development Act]. Diego Solier, ingeniero en excedencia [como le gusta definirse a sí mismo] nos concede una entrevista en el marco del 40 Encuentro de Economía Digital y Telecomunicaciones que AMETIC ha celebrado en Santander, donde explica las posiciones que está defendiendo su grupo [ECR], de los liberales y reformistas, en los que quiere que España juege un papel primordial.

¿Cuál es tu papel dentro del grupo de trabajo de CADA?.

Dentro del Parlamento Europeo, hay dos grandes grupos: el Partido Popular Europeo y los Socialistas y Demócratas. Nosotros somos el cuarto grupo en número. Que un file, una normativa de este calibre tan transversal, llegue al ECR es algo importante.

El grupo ha apostado por nosotros porque ha visto todo el trabajo que llevamos haciendo en los últimos dos años. No solo como ponentes ahora principales del CADA, sino como ponentes en la sombra del Digital Omnibus y del CSA2, del Cybersecurity. Al final, lo que hacemos en Europa es trabajar por Europa y, en este caso, por España.

Nuestro papel va a ser principalmente escuchar a la industria. Venimos de ella, soy ingeniero informático, director de tecnología. Ahora estoy sirviendo a mi país en una excedencia forzosa por servicio público y estoy muy contento.

Hay un reto muy importante en esta normativa de la Comisión: triplicar la capacidad de computación en los próximos años, con horizonte 2035. Para hacer eso necesitas otra palanca muy importante: la velocidad. El inversor quiere invertir, tener una rentabilidad y saber cuándo se produce. En tecnología ya no avanzamos en línea recta; vamos en exponencial, y muy pronunciada. La IA evoluciona mes a mes con capacidades impensables tres meses atrás. La velocidad es clave y, en Europa, tenemos un hándicap importante: la lentitud normativa y regulatoria. Debemos ser realistas y simplificar al máximo esa normativa para que las inversiones se conviertan en realidad a corto plazo.

Pero no podemos forzar a que el sector privado invierta donde queremos...

Lo que hay que generar es estabilidad y seguridad para que esas inversiones quieran venir. El inversor invertirá donde quiera invertir. Pero tenemos datos de la necesidad de cómputo que vamos a tener en el medio y corto plazo, y en Europa, por sí sola, no tenemos esa capacidad. Hay que generar una industria del data center que aporte ese cómputo que necesitaremos en este corto espacio de tiempo, hablo de los próximos dos o tres años.

¿Cuál sería la proporción que consideráis que debería invertir el sector privado y cuánto el público?

Para conseguir estos retos no te puedo dar un número exacto. Pero, obviamente, la inversión privada tiene que ser mucho más fuerte que la pública. Ahora mismo el sistema público de deuda está como está. No podemos seguir inyectando dinero para crear un ecosistema totalmente público. Tenemos que ir de la mano del capital privado.

¿Cómo evitar los incrementos de precios como está sucediendo en tokens ahora mismo? ¿Cómo se tiene soberanía si no es pública?

Como en todo, hay diferentes tipos de servicios. No podemos moverlo todo a un cloud público. En el entorno de las administraciones públicas pasa lo mismo. Hay servicios que pueden estar en un ente más comercial, más privado, y otros (por ejemplo, datos de salud) que son más críticos y deberían estar en una parte más controlada, pública. Esos son los cuatro niveles diferentes que dentro del file Cada están estipulados por la Comisión. Tenemos que revisarlos, ver cómo armonizarlos y que tenga sentido. No podemos poner todos los huevos en la misma cesta. No vamos a decir: "toda la demanda pública debe ir a datacenters públicos". No podemos, porque asesinaríamos a una industria europea que aún no está madura: hablo de data centers y computación europeos.

Generar demanda no significa generar capacidad. Para generar capacidad tienes que establecer un ecosistema y un entorno donde las empresas tengan seguridad jurídica y de inversión, y ese ecosistema hay que ayudarlo. Europa tiene que trabajar en dos líneas paralelas: por un lado, generar ese ecosistema de industria tecnológica (que aparezcan, crezcan, escalen y se queden); por otro, trabajar en partnership con los grandes players del sector, que nos tienen que ayudar a que la industria europea también crezca. Breton lo dijo en uno de los primeros debates sobre este file: soberanía no significa aislarse. No podemos aislarnos de los grandes players. Sobre la proporcionalidad público-privada: entiendo que para ciertas cosas puede haber un ente público, pero no podemos dejarlo todo en manos de lo público.

¿Confiáis en que se pueda regular menos en Europa?

Debería ser el objetivo, y es algo que venimos diciendo en diferentes áreas en estos dos últimos años: simplificación. En Europa tenemos un problema: somos 27 países, comparados con Estados Unidos (un país, aunque con estados) y China (un país en sí mismo). La velocidad que tienen esos dos vehículos no la tenemos. Debemos buscar cómo tener esa velocidad: construir un framework que luego los países apliquen, con homogeneidad en las reglas, como ha dicho Vicente antes. Si no, no jugamos con las mismas reglas en todos lados. La única cifra emblemática que aparece aterrizada en el borrador es el objetivo de triplicar la capacidad de computación y centros de datos europeos de aquí a 2030 y tantos. Es la cifra más clara que viene en el file.

¿Dónde sitúa el límite de la soberanía? Puedo ser una empresa europea que se dedica a hacer centros de datos. Pero ¿qué informática voy a tener dentro de ese centro de datos? ¿HPE, Dell...?

Aquí hay diferentes capas. La capa de hardware, del chip, la hemos pseudoperdido porque hemos querido, ya que tenemos a la única empresa en el mundo que fabrica las máquinas para hacer los microchips. Pero esa empresa, ahora mismo, su principal cliente está en Estados Unidos. Digamos que la capa de hardware la hemos perdido. No vayamos a perder la segunda capa, que es la que llamo de software. La aplicación de la IA no la hemos perdido, estamos jugando esa carrera. Tenemos capacidad de ingenieros y de empresas en Europa como para no perderla. Obviamente, que tu centro de datos tenga dentro un hierro que está hecho en otro sitio significa que no tienes independencia al cien por cien. La soberanía al cien por cien para mí no existe; siempre vas a tener unos mínimos de dependencia con terceros y ahí es donde entran las alianzas que tienes que tener.

Para mí, pensar que Europa puede ser cien por cien soberana en toda la parte tecnológica es una quimera. Va a ser imposible en el momento en el que estamos ahora mismo. Pero sí que veo posible ese crecimiento de la industria tecnológica en esa capa de aplicación de la IA. Sí que veo posible un crecimiento de la industria en esa parte, en esa capa de centros de datos que tengan la computación, que ahora mismo viene de Nvidia porque es lo que hay, o de quien sea. Pero vamos a intentar generar una industria de chips en Europa. Tenemos el conocimiento de las máquinas que hacen esos chips. Obviamente, va a ser muy mínima ahora, pero igual en quince años puede estar compitiendo con otros. Pero tenemos que empezar, y empezar significa ayudar desde la parte regulatoria y normativa a que se genere ese entorno para que esas inversiones vengan y se generen esas empresas.

¿Cómo se regula, entonces, el libre mercado en su opinión?

El libre mercado se rige por una base estructural legislativa que se cumple, pero tú no intervienes. Un teléfono ha sido desarrollado por una empresa privada donde naciones que están enfrentadas colaboran de una manera súper eficiente para que tú lo tengas. Pero ese libre mercado que ha creado el iPhone se ha creado en un entorno de competencia igual, pero regulado. Se permite que sigan compitiendo con las mismas reglas del juego.

Sí, pero si se regula para favorecer a unas empresas locales, ya no estamos liberalizando tanto el mercado.

Yo no quiero favorecer, quiero crear un sistema. Este problema es más intrínseco, de base estructural. Europa no tiene una unidad fiscal y, al no tenerla, no puede competir en igualdad de condiciones con China o con Estados Unidos, porque lo principal es el capital. Lo que tienen que hacer las instituciones públicas es promover que se den las circunstancias para que todos los actores (startups, pymes, que son la columna vertebral europea) puedan acceder a eso. Actualmente, Silicon Valley está lleno de europeos con un talento brutal porque en Europa tenemos un capital brutal. ¿Qué ocurre? Que no hay unas reglas del juego en Europa que permitan jugar igual. Los dos países con mayor inversión española en este momento son Estados Unidos e Inglaterra. ¿Por qué? Porque tienen unas reglas del juego claras para que el capital privado sepa a qué atenerse. Y por la incertidumbre legal. Cuando hay incertidumbre legal, las empresas huyen porque no saben qué se van a encontrar, no quieren que de un día para otro los políticos les cambien las reglas del juego. Eso es intervenir el libre mercado y la competencia, y los deja fuera de juego. Eso no ocurre en muchos países anglosajones.

¿Qué nos está pasando con la industria en general en Europa? Nos estamos quedando sin industria por las reglas del juego que hemos puesto en los últimos quince o veinte años. Estamos hablando de los ETS y de muchas cosas más; son impuestos que les ponemos a nuestras empresas aquí, pero que si se van fuera, no los tienen. Por eso se están deslocalizando de Europa. Tenemos que deshacer todo eso que se ha hecho anteriormente, simplificarlo y, en lugar de dar ayudas, no quitarles a las empresas. Hay una sutil diferencia entre favorecer y promover.

Pero, ¿cuál es esa incertidumbre legal que tienen las empresas para no invertir en Europa? ¿Qué es lo que vosotros consideráis que debería eliminarse?

Si nos centramos en la industria del data center, ¿qué necesita para su desarrollo? Una de las vías angulares es la soberanía energética. Ha pasado en Extremadura en los últimos meses: allí se ha parado una inversión de más de 4.000 millones por no tener la certeza de que la Central de Almaraz iba a seguir abierta en los próximos años para poder alimentar esos centros de datos. Ahora, con los cambios que ha habido, hemos generado que esa incertidumbre se convierta en certidumbre, por lo menos hasta más allá de 2030. En eso es en lo que hay que trabajar: en que las empresas vean un horizonte seguro. Hay muchos players europeos, nórdicos, que ven en esto una oportunidad de quitarle parte del pastel a las americanas, porque China está en cierta parte vetada. Los sistemas de inteligencia artificial chinos públicos son abiertos, los privados son cerrados y se pagan a través de cuotas, y no nos fiamos de los chinos ni queremos introducirlos. Pero este es el sistema global que tenemos. Entonces, volvemos a lo mismo: es una colaboración. No puedes quitar de en medio a quien ahora mismo nos sustenta en nuestro día a día tecnológico. No tenemos la capacidad. Decir lo contrario es inviable. ¿En qué lo fundamentas? ¿Quién lo paga, quién lo hace, quién innova y quién crea esos hubs de investigación y desarrollo? No queda más remedio que colaborar.

En el diagnóstico del problema todo el mundo está de acuerdo, pero evidentemente se discute cómo llegar a la solución.

Claro, hay una solución intermedia, que son esas cuatro capas. Hay partes, como defensa o asuntos gubernamentales, donde tienes que tener esa capacidad de decisión y soberanía y no depender, en caso extremo, de que el señor de Microsoft o de Meta nos desenchufe y nos quedemos todos aquí vendidos. Pero tiene que haber confianza. Aquí no puedes vender que son nuestros enemigos, porque yo en el Departamento Europeo trabajo con Outlook, con AWS. Sería un poco incoherente que estos señores dijeran ahora que vamos a quitar esto de en medio.

¿Hasta dónde confiar? Si llega un tribunal de Estados Unidos y dice "no, por mi ley yo puedo acceder a tus datos"...

Ahí entran más factores. Las tecnológicas grandes como AWS o Microsoft están trabajando en ese entorno de independencia Europa-Estados Unidos porque lo veían venir. Ellos te garantizan que tu soberanía va a estar protegida porque son empresas diferentes, la europea versus la americana. Pero siempre vas a tener la mosca detrás de la oreja. Por eso es lo que decía la comisaria: trabajemos en paralelo con alianzas, fortaleciendo esas alianzas con los actores clave, mientras que, poco a poco, ayudamos a que se genere esa industria en Europa para que, si se hacen las cosas bien, podamos casi equipararnos. Nunca vamos a estar a la misma altura, es imposible, pero hay que empezar. Si no empiezas, no vas a estar nunca en un término medio.

¿De aquí a 2030 se pueden conseguir esos objetivos?

Te voy a dar una foto: actualmente, oficialmente, el pistoletazo de salida aún no ha sido. Será ahora, durante septiembre u octubre de 2026, que es cuando pasa toda la fase de preparación y de trabajo del Parlamento. Hay que involucrar a todos los lobbies, hay que aterrizarlo. Se ha sacado un borrador antes del verano que no está del todo terminado. Todavía no se han empezado las negociaciones. A medida que vaya avanzando, surgirán más temas y se irá a la letra pequeña. Lo que te estamos dando es una foto desde arriba. Es estratégico, es transversal y creemos que España puede aprovecharse de tener un español liderando esto para posicionarse como país estratégico en todo este desarrollo.

La gestión de los datos detrás de la transformación de la Agencia Tributaria Canaria

La Agencia Tributaria Canaria está inmersa en una competa transformación digital, en la que se está promoviendo el uso estratégico de la analítica de datos, la automatización de procesos y el uso de la inteligencia artificial aplicada. El objetivo es lograr una administración tributaria más eficiente, innovadora y orientada al servicio público, así como mejorar la lucha contra el fraude.

Así al menos lo expuso Raquel Peligero Molina, Directora de la Agencia Tributaria Canaria [ATC] desde 2019, durante un encuentro de SAS.

Cabe señalar que esta entidad es Adscrita a la Consejería de Hacienda y Relaciones con la Unión Europea del Gobierno de Canarias, y que Raquel Peligero es también Vicepresidenta de su Consejo Rector. Asimismo, es Consejera Delegada de ASISTENCIA INTEGRAL TRIBUTARIA, S.A. [ASISTA Canarias], sociedad mercantil pública que actúa como medio propio de la Comunidad Autónoma de Canarias, y vocal del Pleno del Consorcio de la Zona Franca de Tenerife y del de Gran Canaria. Inspectora de Hacienda del Estado desde 2001 y licenciada en Ciencias Económicas y Empresariales por la Universidad de Las Palmas de Gran Canaria, cuenta con una dilatada trayectoria en la Agencia Estatal de Administración Tributaria, donde ha ejercido responsabilidades directivas en los ámbitos de inspección, recaudación, gestión económica y recursos humanos.

En la actualidad, lidera el impulso de la transformación digital de la Agencia Tributaria Canaria, promoviendo el uso estratégico de la analítica de datos, la automatización de procesos y el uso de la inteligencia artificial aplicada, con el objetivo de

lograr una administración tributaria más eficiente, innovadora y orientada al servicio público, así como mejorar la lucha contra el fraude.

Datos e IA

Durante este encuentro, esta responsable expuso los avances de la estrategia de transformación de la ATC, que se apoya fundamentalmente en la analítica de datos y la inteligencia artificial (IA). Peligero detalló que hay un especial énfasis en la gobernanza, la confiabilidad y la seguridad de la información tributaria.

Esta responsable repasó el origen y evolución de la estrategia de datos de la ATC, que en 2017 decidió implantar una herramienta de análisis masivo. "En la implantación nos dimos cuenta de que, para garantizar la potencia de la herramienta, necesitábamos mirar al dato. Algunos eran de distinta calidad, otros estaban atrasados; había que ordenarlos", explicó. De ahí surgió un proyecto de gobierno del dato, incorporado al Plan Estratégico 2022-2024 y ya en su fase final de implantación. "Tenemos nuestra plataforma y hemos detectado la necesidad de dar un paso más allá, migrando hacia la nueva plataforma SAS Viya", añadió.

En el ámbito de la IA, la ATC inició su acercamiento entre 2022 y 2023, con una visión centrada en beneficios y riesgos. "La IA arroja comportamientos no deterministas según el contexto y los datos; existe opacidad y nuevos escenarios de vulnerabilidades. En el sector público se nos exige confianza. Los resultados que arroja la IA han de ser confiables", recalcó.

Para ello, la institución se ha alineado con la legislación aplicable y con una estrategia clara. "La implantación de la IA necesita nuevas estrategias de gobernanza y control. El cumplimiento normativo es clave. La normativa europea está en despliegue por niveles de riesgo, y los Estados miembros deben crear organismos de supervisión y control. En España aún se requiere transposición, con una Ley Orgánica que está en trámite. Hace dos días, el Consejo de Ministros aprobó el proyecto de decreto; ya está en información pública".

La ponente subrayó las limitaciones específicas del ámbito tributario en materia de protección del dato. "El artículo 25 de la Ley General Tributaria protege el dato tributario: es reservado. Tenemos la obligación de custodiarlo; no puede salir a ningún lado. No podemos ir a la nube: las soluciones deben estar on-premise", afirmó.

También insistió en la necesidad de transparencia y trazabilidad de los algoritmos y en la capacitación de los funcionarios para gestionar el cambio. "En el sector público hay más aversión al cambio; debemos formar y acompañar".

Respecto a los riesgos, enumeró fuga de datos, usos indebidos y ventilación de propiedad intelectual, "comunes a todos los sistemas", y remarcó una conclusión clave: "El mayor riesgo, en todo caso, es no usar la inteligencia artificial. Debemos hacer un uso responsable, ético y seguro".

Una IA confiable

Tras una primera etapa con pilotos aislados, la ATC ha formalizado una estrategia de IA confiable.

"Ya no es una decisión tecnológica sobre usar o no usar IA; ahora la decisión estratégica es cómo implantamos la IA y dónde la aplicamos", comentó. Es más, esta misma responsable aseguraba que estuvo en un reciente foro con miembros de consejos de administración de empresas cotizadas donde

identificó las mismas tres preocupaciones entre sector privado y público. "Situación geopolítica, cómo implantar la IA en la organización, y la retención y captación de talento. En el sector público estamos más constreñidos; es difícil competir con la empresa privada en perfiles tecnológicos". La ATC ha aprobado su estrategia que define compromisos, principios rectores, líneas de actuación y recursos organizativos. "El gobierno de la IA es esencial: establecer roles y responsabilidades, mapear cuándo y para qué se usa, medir y gestionar riesgos", detalló. Entre los casos ya implementados, citó respuestas asistidas a consultas de contribuyentes ["siempre con supervisión humana"], asistencia virtual para cumplimentación de modelos tributarios y extracción de información de documentos notariales y judiciales para detectar imponibles no declarados. "Iniciamos cotejando las escrituras con la ficha resumen para detectar incongruencias, y ya estamos en el siguiente paso: detectar imponibles no declarados", indicó.

En la analítica avanzada, la IA se usa con fines preventivos: "Realiza clasificación automática de solicitudes de devolución del IGIC [el equivalente canario del IVA] y nos ofrece un mapa de riesgo para priorizar expedientes". También apoya la detección de tramas de fraude mediante visualización de redes societarias: "Antes lo hacía a mano en Inspección de Hacienda, con escrituras y planos. Ahora la IA te lo muestra; tú lo compruebas, pero ya tienes una base".

La IA contribuye igualmente a la toma de decisiones de política fiscal: "Si bajo el tipo del Impuesto de Transmisiones del 7 al 6,5 y añado una deducción, ¿cuánto menos voy a recaudar? Es una decisión política, pero hay que conocer el coste para ajustar el presupuesto de la comunidad autónoma".

La expansión alcanza áreas transversales y la propia base de datos institucional. "Estamos creando un asistente para la gestión de indicadores. Trabajamos por objetivos con 399 indicadores: queremos ver dónde vamos peor, dónde mejor y ajustar nuestra actuación", explicó. En desarrollo y seguridad, la IA se aplica a la documentación de aplicaciones y a auditorías conforme al Esquema Nacional de Seguridad: "Nos ayuda a documentar la aplicación de indicadores y puede reducir necesidades de programación: que la IA programe y un funcionario revise. También detecta incongruencias e inseguridades en nuestras bases de datos; esperamos que nos sugiera soluciones".

La visión de conjunto es la de una IA integrada en todos los estratos de la organización, no encapsulada. "La estamos usando prácticamente en toda la estructura tecnológica y de negocio. No sé dónde estaremos en ocho meses si vuelvo: esto se mueve muy rápido", concluyó, reafirmando el compromiso de la ATC con un despliegue responsable, robusto y transparente de la IA y los datos para ofrecer un mejor servicio al ciudadano.

TEMA DE PORTADA

El dato como asignatura pendiente de la Administración digital

Igual que los datos tienden al infinito, la gestión de este activo es algo que puede complicarse por momentos. Por eso, ni todos los organismos públicos están igual en lo que a la gestión del dato se refiere ni las soluciones a esta situación son ecuánimes.

La transformación digital del sector público español ha avanzado con solidez en la última década, especialmente en la disponibilidad de trámites electrónicos y en la modernización de infraestructuras informáticas. Sin embargo, cuando se pregunta a los responsables de tecnología del sector privado que trabajan con las administraciones públicas (AAPP) por el grado de madurez real en la gestión del dato, la respuesta es prácticamente unánime: se trata de un proceso desigual, todavía inacabado y con diferencias notables entre los distintos niveles administrativos.

José Alberto Pérez Cueto, director de área de Gobierno en Babel España, resume esa realidad con la idea de que "la digitalización ha avanzado, pero en muchas administraciones el dato continúa ligado a aplicaciones y expedientes concretos, sin una visión común ni responsables claramente definidos". Según Pérez Cueto, la Administración General del Estado (AGE) cuenta con más escala y capacidad de coordinación, mientras que las comunidades autónomas destacan en ámbitos

como sanidad, servicios sociales o administración electrónica, y en el nivel local la diferencia es mayor porque "los grandes ayuntamientos avanzan con rapidez, mientras que muchos municipios dependen de diputaciones, consorcios o servicios compartidos".

Julia Bernal, Regional Leader Mediterranean Region de Red Hat, plantea una lectura complementaria al señalar que la madurez "es asimétrica" y que "esta desigualdad refleja la complejidad de sus infraestructuras y su capacidad de automatización, más que el tamaño de la organización". Bernal detalla que la AGE gestiona grandes volúmenes de datos y sistemas de alto impacto, donde "el principal reto no es la adopción de nueva tecnología, sino la gestión de la deuda técnica y la conexión de sistemas heredados aislados sin comprometer la seguridad". En las comunidades autónomas, apunta, el desafío reside en "conectar entornos multicloud e híbridos heterogéneos sin fragmentar la información del ciudadano", mientras que en el ámbito local "la automatización de la infraestructura representa la única vía práctica para gobernar los datos de manera eficaz" para los equipos con menos recursos.

Desde VASS, José María Ibáñez Bote, Public Services Director, coincide en que la madurez media se sitúa "en una fase intermedia" en la que "hay inventarios de datos, catálogos e infraestructura de interoperabilidad [la Plataforma de Intermediación, el ENI], pero el gobierno del dato como función transversal [con roles, políticas y calidad garantizada de extremo a extremo] es todavía la excepción". Ibáñez Bote añade que la AGE lleva la delantera en estrategia y normativa "gracias al Plan de Recuperación y la Oficina del Dato", que las comunidades autónomas presentan una madurez muy desigual entre áreas como sanidad, hacienda o empleo frente a otras que gestionan el dato por silos departamentales, y que las entidades locales son "las más rezagadas porque tienen recursos y talento digital limitados, salvo en grandes ayuntamientos que actúan como referentes".

Por su parte, Alfredo García, responsable de AAPP en NetApp, aporta una matización relevante al hablar de "una fase de transición" en la que las administraciones "han avanzado mucho en digitalización, administración electrónica y prestación de servicios en línea,

pero no siempre han acompañado ese progreso con un gobierno integral del dato". García insiste en que "el reto es realmente transformar los datos en un activo accesible, protegido, trazable y reutilizable, y no tanto en almacenar más, como se ha pensado en muchos casos".

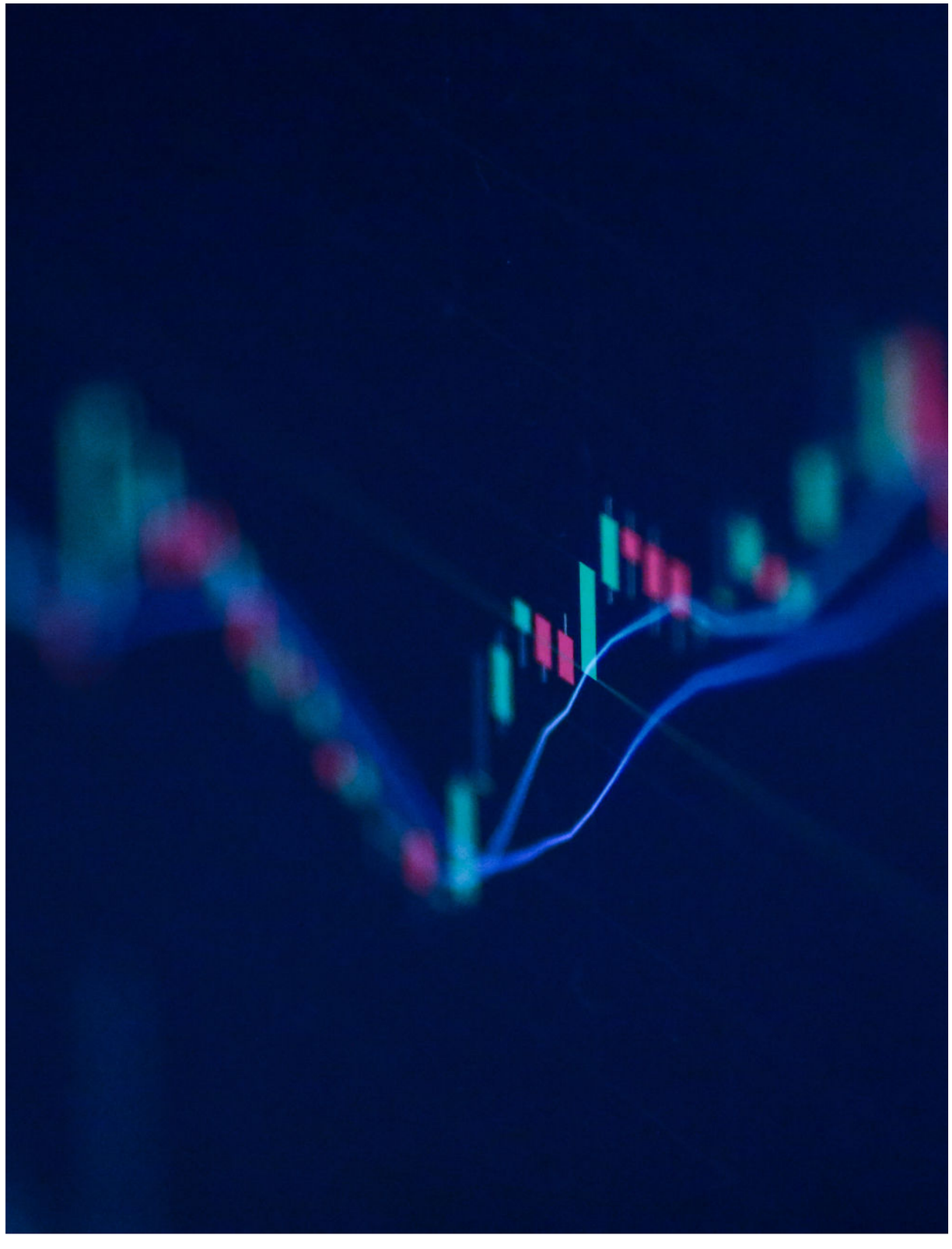
Los obstáculos que frenan el aprovechamiento del dato público

Al margen de la tecnología disponible, los cuatro proveedores coinciden en que las barreras principales tienen un componente organizativo y cultural muy marcado.

Pérez Cueto, de Babel, sitúa el problema en que "durante años se han gestionado sistemas y procedimientos, pero no siempre se ha definido quién responde por cada dato, cómo debe mantenerse o qué nivel de calidad necesita", a lo que se suman sistemas heredados, información repartida entre organismos y perfiles especializados escasos.

Mientras, Julia Bernal, de Red Hat, agrupa los frenos en cuatro grandes bloques: la gobernanza fragmentada y el aislamiento de los datos, la deuda técnica asociada al almacenamiento y al llamado "data gravity", el cumplimiento normativo y la predictibilidad de los costes, y la brecha de talento especializado. Sobre el primero de ellos advierte que "sin un modelo claro de propiedad, las iniciativas tecnológicas se paralizan en debates organizativos internos", mientras que en relación con el cumplimiento normativo recuerda que "las brechas de cumplimiento conllevan riesgos significativos y dañan la confianza pública".

Julio Estévez, Global Head of Data & AI en VASS, es especialmente directo al describir la raíz del problema, asegurando que "el obstáculo de fondo no es tecnológico, es organizativo: el dato sigue siendo propiedad de quien lo genera, no un activo compartido de la institución". Estévez enumera además presupuestos ligados a proyectos concretos y no a una capacidad continua de gestión del dato, escasez de perfiles data en la plantilla pública y una cultura en la que "compartir dato se percibe como riesgo (legal, de seguridad, de pérdida de control) antes que como oportunidad". Además, sostiene que "la normativa de protección de datos, bien aplicada, no es el



obstáculo: la interpretación defensiva que se hace de ella, sí".

Alfredo García, de NetApp, asegura, desde un punto de vista más técnico, que la fragmentación como el obstáculo más visible, "puesto que muchas administraciones mantienen sistemas heredados, herramientas poco integradas y datos distribuidos entre centros propios, aplicaciones departamentales y distintos entornos cloud". García añade que "cuando una organización desconoce qué datos posee, su sensibilidad o su calidad, resulta muy difícil gobernarlos, protegerlos y prepararlos para proyectos de analítica o inteligencia artificial", y apunta a la separación excesiva entre tecnología, negocio público, seguridad, contratación y áreas jurídicas como una de las trabas organizativas más persistentes.

Los pilares de una estrategia de dato más allá de la infraestructura

Preguntados por los elementos imprescindibles de una estrategia de dato que trascienda la mera capa tecnológica, los cuatro proveedores cinciden en la necesidad de un modelo de gobierno con responsabilidades definidas, aunque cada uno matiza el orden de prioridades. De hecho, Alfredo García, de NetApp, insiste en que la estrategia debe partir de los objetivos de servicio público, "así, antes de seleccionar herramientas, la administración tiene que determinar qué decisiones desea mejorar, qué trámites quiere simplificar y qué resultados espera obtener para ciudadanos, empleados y empresas". García añade que todo ello debe acompañarse de "indicadores que midan mejoras concretas, no únicamente actividad tecnológica: tiempos de resolución, disponibilidad de los servicios, reducción de errores, calidad de los datos o satisfacción ciudadana".

Para Julio Estévez, de VASS, hay cinco pilares clave: una gobernanza sólida con responsabilidades claramente definidas (Data Owner, Data Steward y CDO institucional), un catálogo de datos dinámico, políticas de acceso e intercambio basadas en el principio "once only", un modelo orientado al dato como producto, y la capacitación continua del personal. Estévez resume su planteamiento afirmando que "la tecnología es una condición necesaria, pero no suficiente: sin una gobernanza efectiva y sin profesionales preparados para aprovecharla, la infraestructura corre el riesgo de permanecer infrautilizada".

Por su parte, Julia Bernal, de Red Hat, plantea tres elementos esenciales relacionados con la confianza tecnológica: la seguridad y la gestión de vulnerabilidades desde el diseño, la interoperabilidad basada en estándares

abiertos y la independencia operativa frente a un proveedor concreto. Sobre el primero afirma que "puesto que la IA acelera tanto el descubrimiento como la explotación de los fallos de seguridad, gobernar los datos públicos exige proteger la cadena de suministro de software de código abierto, donde nace la innovación". Respecto a la interoperabilidad, defiende que "los datos públicos deben ser capaces de fluir sin fricciones entre administraciones, niveles de gobierno y aplicaciones heterogéneas", y en cuanto a la independencia tecnológica sostiene que "las entidades públicas no deberían asumir que un proveedor específico de infraestructura o tecnología mantendrá sus servicios en los mismos términos a lo largo del tiempo".

Pérez Cueto, de Babel, considera que debe incluir "un modelo de gobierno con responsabilidades concretas, un catálogo que permita saber qué información existe y unas reglas comunes de calidad, seguridad, acceso y trazabilidad", y advierte de que "una estrategia de dato no puede quedarse en ordenar información: debe establecer para qué se va a utilizar, cómo se medirá su impacto y qué cambios organizativos hacen falta para incorporarla a la toma de decisiones".

Centralizar las reglas, no necesariamente los datos

Uno de los debates más recurrentes en el diseño de estrategias de dato es el equilibrio entre la centralización necesaria para la gobernanza y la autonomía que requieren los organismos que mejor conocen su propio contexto. Las cuatro compañías consultadas apuestan, con matices, por un modelo federado o híbrido antes que por un almacén único de información.

De esta forma, Julia Bernal, de Red Hat, defiende que "el equilibrio no se logra construyendo un único e inmenso almacén de datos centralizado", ya que históricamente "este modelo ha tenido dificultades en el sector público por su rigidez organizativa". Bernal describe una nube híbrida bien diseñada que permite que "cada carga de trabajo se ejecute allí donde lo exijan los requisitos operativos" y pone como ejemplo casos como el del Gobierno Vasco, donde EJIE "desplegó inteligencia artificial para fomentar la inclusión lingüística, procesando miles de consultas ciudadanas diarias con total autonomía sobre sus sistemas", o el del Ayuntamiento de Valencia, que "modernizó los servicios municipales de administración electrónica, reduciendo los tiempos de tramitación".

Julio Estévez, de VASS, es especialmente explícito al describir el modelo que propone: "gobernanza y estándares comunes (nomenclatura, calidad, seguridad, interoperabilidad) definidos de forma centralizada, con la gestión operativa del dato descentralizada en cada organismo, que conoce mejor su contexto y sus usuarios". Estévez advierte de que "centralizar la ejecución suele generar cuellos de botella", y relaciona su propuesta con el concepto de "data mesh" del sector privado, "adaptado a la naturaleza jurídica y competencial de la Administración".

Mientras, Pérez Cueto, de Babel, remite a experiencias ya consolidadas en la Administración española, como "el Esquema Nacional de Seguridad (ENS) o el Esquema Nacional de Interoperabilidad (ENI): marcos comunes que fijan criterios compartidos, mientras cada organismo mantiene la responsabilidad de aplicarlos en su ámbito". Considera que en el gobierno del dato "debería ocurrir algo similar: cada unidad sigue siendo responsable de los datos que conoce y genera, pero dentro de un marco común que permita compartirlos y utilizarlos con garantías", y subraya que este modelo federado "encaja bien con el principio europeo de subsidiariedad".

Quien plantea una fórmula parecida es Alfredo García, de NetApp, al

sostener que "la solución no pasa por reunir físicamente todos los datos en un único repositorio, más bien por centralizar las reglas y federar la gestión". García remarca que este enfoque evita "dos extremos poco eficaces: una centralización rígida que ralentice los proyectos y una autonomía sin coordinación que multiplique los silos", y añade que requiere "una plataforma capaz de ofrecer visibilidad y políticas coherentes a través de entornos locales, nubes privadas y servicios de nube pública".

Soberanía del dato: control efectivo antes que ubicación física

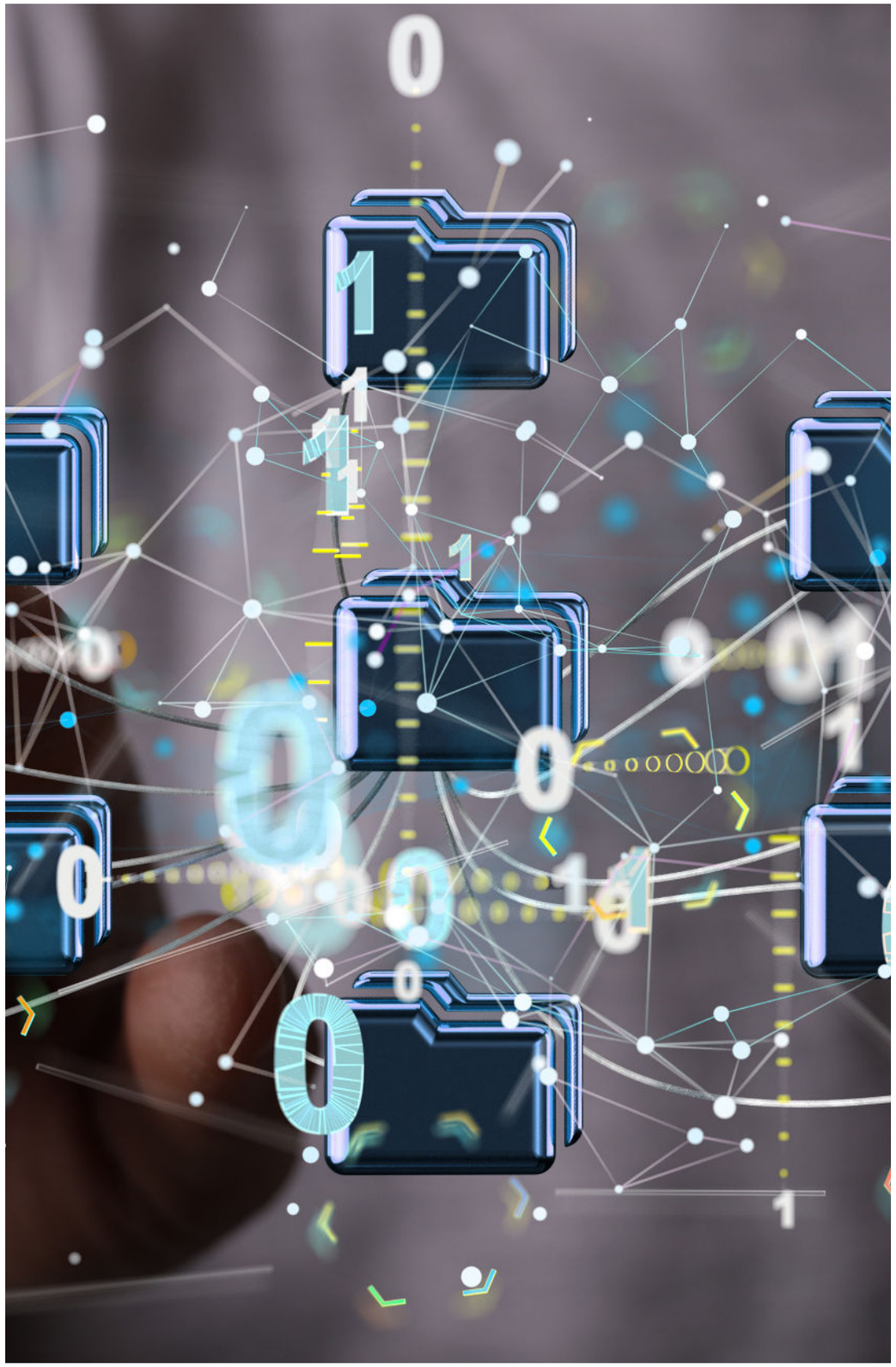
Pero, ¿qué entendemos por soberanía del dato?

Julio Estévez, de VASS, señala que la soberanía "no debe entenderse como la obligación de alojar la información en infraestructuras físicamente

ubicadas dentro del territorio nacional, sino como la capacidad real de mantener su control en todo momento". Estévez detalla condiciones concretas para que sea compatible con la nube pública global, como "el cifrado con claves bajo control de la Administración, la residencia y trazabilidad de los datos, salvaguardas contractuales frente a normativas extraterritoriales como el Cloud Act y estrategias híbridas o multicloud para los entornos más críticos", y concluye que "el verdadero riesgo no radica en adoptar soluciones cloud globales, sino en hacerlo sin una gobernanza técnica y contractual que asegure la autonomía, el control y la protección efectiva de la información".

Para Pérez Cueto, de Babel, "la soberanía del dato consiste en conservar un control efectivo sobre la información: quién puede acceder, bajo qué jurisdicción se trata, cómo se cifra, cómo se audita y cómo puede trasladarse a otra plataforma". Considera que es compatible con proveedores cloud globales, "pero no de forma automática", ya que requiere "una arquitectura adecuada, control sobre los accesos y las claves, cumplimiento del marco normativo y un plan de salida que reduzca la dependencia de un proveedor concreto".

Por su parte, la deficinión que hace Alfredo García, de NetApp, es que es un asunto que "no se limita a saber en qué país está ubicado un servidor", sino que "implica conocer qué legislación se aplica, quién puede acceder a la información, dónde se procesan las copias, quién controla las claves de cifrado, cómo se auditan los accesos y si la administración puede trasladar o repatriar sus datos cuando lo necesite". García explica que su compañía "plantea la soberanía como un espectro que combina ubicación, jurisdicción, control, seguridad y portabilidad", y defiende una estrategia híbrida que permita "utilizar



servicios cloud sin renunciar al control del dato ni asumir que toda la información debe recibir exactamente el mismo tratamiento".

Julia Bernal, de Red Hat, va más allá al afirmar que la soberanía "va más allá de la mera residencia física de la información" y que "almacenar los datos dentro de las fronteras españolas ofrece poca protección si el stack tecnológico subyacente es propietario, si los contratos continúan sujetos a normativas extraterritoriales o si las propias administraciones no pueden auditar ni migrar sus sistemas de manera independiente". Bernal precisa que "soberanía no significa reemplazar a los proveedores de nube globales como AWS, Microsoft Azure o Google Cloud", sino "poner fin a la dependencia exclusiva de un único proveedor mediante un enfoque de nube híbrida abierta".

Del expediente reactivo al servicio proactivo

Más allá de la eficiencia interna, los cuatro proveedores coinciden en que el verdadero cambio de paradigma consiste en que la Administración deje de esperar a que el ciudadano reclame y pase a anticiparse a sus necesidades. Esta transformación está vinculada, según Julia Bernal, de Red Hat, al principio europeo de "solo una vez", que "establece que la ciudadanía solo debe entregar información a los organismos públicos una única vez", y sostiene que "una infraestructura de datos madura también ayuda a las entidades públicas a pasar de una tramitación reactiva a un servicio público proactivo", permitiendo identificar "la elegibilidad para recibir prestaciones sociales antes de que el ciudadano lo solicite".

Mientras, Pérez Cueto, de Babel, explica que una estrategia bien diseñada "puede reducir trámites, evitar que el ciudadano presente información que la Administración ya posee y permitir que determinados servicios se activen de forma más proactiva", con especial relevancia en "ayudas públicas, sanidad, dependencia y servicios sociales".

José María Ibáñez Bote, de VASS, describe ese cambio con una formulación especialmente ilustrativa: "el impacto de una estrategia bien diseñada se notará cuando el ciudadano deja de ser quien reclama derechos y pasa a ser la Administración quien los identifica y activa". Ibáñez Bote menciona entre los beneficios "resoluciones más rápidas y personalizadas en ayudas, becas o prestaciones" y "detección proactiva de ciudadanos en riesgo de exclusión o con derecho a prestaciones que no solicitan por desconocimiento"

Coincide Alfredo García, de NetApp, en que el beneficio "no consiste únicamente en tramitar más deprisa, más bien en evitar desplazamientos, reducir incertidumbre y mejorar la igualdad de acceso", y añade una dimensión de continuidad del servicio al señalar que "una plataforma resiliente ayuda a que hospitales, servicios sociales, sistemas tributarios o canales de atención sigan disponibles ante una incidencia".

Recomendaciones para quien empieza a diseñar su estrategia

Ante la pregunta sobre qué recomendaciones concretas darían a un responsable de tecnología e innovación de una AAPP que inicia este recorrido, las respuestas comparten un mismo eje: comenzar por problemas acotados antes que por transformaciones integrales. Pérez Cueto, de Babel, aconseja "elegir uno o dos problemas concretos y demostrar valor antes de ampliar el alcance", "asignar responsables a los datos desde el inicio y acordar criterios medibles de calidad, acceso y actualización" y "diseñar una arquitectura interoperable y escalable, pero también reversible".

Julia Bernal, de Red Hat, propone "empezar por el inventario de datos antes de seleccionar la plataforma de software", ya que "las inversiones tecnológicas realizadas sin un punto de partida preciso sobre los datos conllevan un riesgo arquitectónico significativo". En segundo lugar recomienda "diseñar pensando en la portabilidad y la independencia desde el primer día" y, en tercer lugar, "considerar los marcos normativos como el punto de partida del diseño y no como una obligación secundaria".

Julio Estévez, de VASS, plantea "empezar por el gobierno del dato y los casos de uso, no por la plataforma tecnológica", "priorizar dos o tres casos de uso de alto impacto y visibilidad rápida para generar tracción política y presupuestaria" e "invertir en capacitación y en figuras de gobierno del dato (CDO, data stewards) antes que en ampliar infraestructura"

Alfredo García, de NetApp, sugiere "empezar por una auditoría realista: identificar los datos existentes, sus ubicaciones, su sensibilidad, su calidad, sus propietarios y los sistemas de los que dependen", "seleccionar pocos casos de uso prioritarios, vinculados a objetivos medibles de servicio público" y "establecer desde el inicio un modelo común de gobierno, seguridad e interoperabilidad que pueda aplicarse de forma automatizada a todos los entornos".

La mirada hacia 2030

Pero, ¿y si miramos más allá, a cuatro años vista? Al proyectar el horizonte de 2030, las cuatro compañías dibujan una Administración que comparte información entre organismos con garantías, que utiliza inteligencia artificial con supervisión humana y que actúa de forma anticipatoria.

Desde VASS, José María Ibáñez Bote y Julio Estévez comparten la visión de "una Administración donde el dato se comparta por defecto entre organismos con la seguridad, ante todo, donde la IA generativa y predictiva ayude a tomar decisiones sin sustituir la responsabilidad última del funcionario, y donde el ciudadano interactúe con una Administración que ya sabe lo que necesita antes de que lo pida".

Por su parte, Alfredo García, de NetApp, considera que "una administración verdaderamente orientada al dato debería ser capaz de tomar decisiones apoyadas en información fiable y actualizada, compartirla de manera segura entre organismos y ofrecer servicios más preventivos que reactivos", y subraya que "la gobernanza, la soberanía y la ciberresiliencia serán condiciones previas para innovar, no componentes añadidos al final de los proyectos".

Pérez Cueto, de Babel, sostiene que en 2030 una administración orientada al dato "debería haber pasado de la transaccionalidad a la proactividad: no limitarse a responder a los trámites que inicia el ciudadano, sino anticipar determinadas necesidades y ofrecer servicios en el momento adecuado", aplicando "la inteligencia artificial con transparencia y supervisión humana".

Mientras, Julia Bernal, de Red Hat, prevé que "la IA en el sector público evolucionará más allá de los resúmenes automatizados de documentos para convertirse en sistemas inteligentes colaborativos capaces de ejecutar flujos de trabajo complejos entre departamentos", y remarca que "las decisiones respaldadas por sistemas automatizados deben seguir siendo verificables, transparentes y estar sujetas a la supervisión humana".

TENDENCIAS

Europa, ¿está en forma para participar en la carrera tecnológica frente a Estados Unidos y China?

Por Óscar Salazar, Managing Director European Funds, Euro-Funding

Durante años, Europa ha sido sinónimo de estabilidad, regulación, calidad industrial y protección social. Sin embargo, cuando observamos el mapa global de la innovación tecnológica, surge una pregunta incómoda: ¿está Europa perdiendo la carrera tecnológica frente a Estados Unidos y China?

La tecnología ya no es solo un sector económico. Es poder geopolítico, influencia cultural y soberanía estratégica, donde actualmente destacan Estados Unidos y China.

Estados Unidos domina las plataformas digitales, la inteligencia artificial y el capital riesgo con compañías como OpenAI, NVIDIA, Google, Microsoft o Tesla. Por el contrario, China ha construido una estrategia nacional agresiva basada en inversión masiva, planificación industrial y velocidad de ejecución. Ya no copia tecnología: compite por liderarla.

¿Y Europa?

Europa lidera la regulación tecnológica mundial —privacidad, ética, competencia— pero todavía no lidera la creación de gigantes tecnológicos propios. Europa sigue teniendo talento, universidades excelentes y capacidad

industrial. Pero cuando hablamos de gigantes tecnológicos globales o liderazgo en IA, parece haberse quedado atrás. El desafío europeo no es la falta de talento, sino la dificultad para transformar innovación en compañías tecnológicas globales, dado que muchos de los mejores ingenieros, investigadores y emprendedores europeos terminan desarrollando sus carreras en ecosistemas más dinámicos.

Mientras Silicon Valley premia el riesgo, Europa muchas veces penaliza el fracaso con burocracia, fragmentación y lentitud. Estados Unidos innova primero y regula después, China escala primero y controla después. Europa, muchas veces, regula antes de competir, y la inteligencia artificial está acelerando todavía más esta diferencia, pues la IA no trata solo de chatbots, sino que la IA es productividad, defensa, energía, educación, salud y soberanía económica.

Entonces, la gran pregunta es si Europa puede mantener su independencia estratégica si depende tecnológicamente de plataformas y modelos desarrollados fuera del continente.

Aunque vayamos con retraso, aún no está todo perdido, pues Europa tiene mercado, talento, ciencia, industria y estabilidad institucional, pero necesita más ambición, más inversión, más velocidad, menos burocracia y una visión tecnológica verdaderamente estratégica, porque esta carrera no trata solo de empresas, sino del ecosistema europeo de innovación, manteniendo las virtudes europeas de estabilidad, calidad industrial y protección social.

Europa también está reaccionando

Aunque muchas veces se presenta a Europa como un actor rezagado, la realidad es que la Unión Europea ya ha empezado a mover ficha, y probablemente estemos entrando en una nueva etapa de política industrial y soberanía tecnológica europea. En los últimos años, la UE ha lanzado iniciativas estratégicas relevantes, como la ley europea de chips, el reglamento europeo de inteligencia artificial, y el futuro programa marco europeo FP10, donde se van a priorizar áreas donde Europa depende mucho de potencias extranjeras tales como inteligencia artificial, semiconductores, computación cuántica, biotecnología, espacio, defensa, baterías y energías limpias, aumentando significativamente el presupuesto europeo y movilizando inversión privada para startups y empresas tecnológicas. Además, se va a fomentar la integración entre investigación, industria y defensa para el desarrollo de tecnologías de doble uso (civil y militar).

Como conclusión, Europa tiene que dejar de ser solo un mercado consumidor de tecnologías extranjeras para pasar a ser una potencia capaz de desarrollar, producir y controlar tecnologías críticas propias. El objetivo no debería ser aislarse de EEUU o China, sino competir con mayor autonomía y menor dependencia estratégica.

TENDENCIAS

El EIC se abre a tecnologías de defensa y de doble uso: qué cambia para startups, pymes y scaleups europeas

Por Carolina Aragoneses, Technical Manager European Funds de Euro-Funding

El European Innovation Council ha dado un paso relevante en la estrategia europea de innovación: desde el 17 de junio de 2026, el EIC abre nuevas vías de financiación para tecnologías de doble uso y defensa, tras la modificación del EIC Work Programme 2026 adoptada por la Comisión Europea. El objetivo es reforzar la autonomía tecnológica, la seguridad y la capacidad industrial de Europa en ámbitos estratégicos.

La novedad no afecta por igual a todos los instrumentos. El EIC Accelerator y el EIC STEP Scale Up se abren a innovaciones de uso dual, es decir, tecnologías con aplicaciones civiles y de defensa.

En cambio, la nueva convocatoria EIC STEP Scale Up Defence está dirigida a tecnologías con aplicación primaria de defensa. Pathfinder, Transition y Advanced Innovation Challenges mantienen su foco exclusivamente civil.

¿Qué tipo de proyectos encajan?

Para proyectos de uso dual, el encaje natural estará en EIC Accelerator o EIC STEP Scale Up. Estas convocatorias son para tecnologías como inteligencia artificial, computación cuántica, robótica, espacio, ciberseguridad o materiales avanzados, con potencial de mercado civil y posible aplicación en defensa. EIC indica que esta vía es la indicada para startups, pymes y small mid-caps en fases desde TRL 6, con acceso a subvención e inversión según el instrumento.

Para proyectos de defensa exclusivamente, la convocatoria específica es EIC STEP Scale Up Defence. Está pensada para startups, pymes y small mid-caps de hasta 499 empleados establecidas en la UE, Ucrania o en países del Espacio Económico Europeo asociados a Horizon Europe. Los proyectos deben centrarse en tecnologías críticas de defensa como defensa aérea y antimisiles, drones y counter-drones, ciberdefensa, inteligencia artificial, guerra electrónica, movilidad militar, combate terrestre, marítimo o aéreo, y tecnologías médicas y contramedidas.

¿Qué financiación está disponible?

En EIC Accelerator, las startups y pymes pueden acceder a una subvención inferior a 2,5 millones de euros para actividades de innovación entre TRL 6 y 8, y a un componente

de inversión de 1 a 10 millones de euros para escalado y otras actividades.

El EIC STEP Scale Up proporciona apoyo exclusivamente en forma de inversión (equity), gestionada por el EIC Fund, con importes de entre 10 y 30 millones de euros por empresa. El instrumento está diseñado para apoyar el escalado de tecnologías estratégicas y catalizar rondas de financiación de entre 50 y 150 millones de euros o más. La convocatoria funciona mediante evaluaciones trimestrales y, tras la modificación del Work Programme, puede apoyar también innovaciones de uso dual.

El EIC STEP Scale Up Defence mantiene las mismas condiciones de elegibilidad, evaluación y apoyo financiero, pero está específicamente dirigido a empresas que desarrollan tecnologías con aplicaciones en defensa. Para 2026 cuenta con un presupuesto de 100 millones de euros y dispone de un presupuesto indicativo adicional de 100 millones de euros para 2027, sujeto a la adopción del correspondiente Work Programme.

Si quiero presentarme, ¿qué debo revisar?

La primera decisión será estratégica: uso dual no es lo mismo que defensa pura. Si la tecnología tiene una aplicación civil definida y una aplicación potencial en defensa, puede tener sentido analizar EIC Accelerator o EIC STEP Scale Up. Si la aplicación principal es defensa, la vía adecuada será EIC STEP Scale Up Defence.

Para el EIC Accelerator de uso dual, el proceso de evaluación sigue siendo el mismo, y las propuestas completas (Step 2) podrán presentarse a partir del 2 de septiembre de 2026.

En el EIC STEP Scale Up, la primera evaluación de propuestas de uso dual será el 9 de septiembre de 2026.

Para EIC STEP Scale Up Defence, la convocatoria abre el 30 de junio de 2026 y permite presentar solicitudes hasta el 28 de octubre de 2026.

Qué hacer si tenías una propuesta preparada

No necesariamente hay que empezar de cero, pero sí revisar el posicionamiento. Una propuesta preparada para EIC Accelerator debe reforzar la aplicación civil si se presenta como uso dual. Si el proyecto es predominantemente defensa, conviene evaluar si debe redirigirse a EIC STEP Scale Up Defence.

También será clave revisar la estructura societaria, la propiedad intelectual, la cap table, la presencia de inversores de terceros países y la freedom to operate. El EIC Fund podrá aplicar salvaguardas para proteger intereses europeos y asegurar que el valor estratégico, incluida la IP, permanezca mayoritariamente en Europa, EEA países asociados a Horizon Europe o Ucrania.

GRACIAS

contacto@bytic.es | www.bytic.es