BYTIC MEDIA

NÚMERO 40 | OCTUBRE 2025

La urgencia de gestionar datos propios

ENTREVISTA

Benjamín Cogolludo, Responsable de Informática, Innovación y Comunicaciones en el Ayuntamiento de Castro-Urdiales

CASO PRÁCTICO

Cómo BIM y GIS ayudaron al Ayuntamiento de Madrid en el soterramiento de la A5

AI-NATIVE PREVENTION FOR TOMORROW'S DIGITAL THREATS

www.eset.es

ESET® Cybersecurity
Progress. Protected.

TABLA 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.

BYTIC MEDIA

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.

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

Director Innovación, Procesos y Transformación Digital. ISDEFE

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

BYTIC MEDIA

Forma parte de la comunidad ByTIC

Comunidad de innovación y tecnología exclusiva para la Administración Pública

- ✔ Acceso a todo el contenido **ByTIC Media**
- ✔ Acceso a **adjudicacionesTIC.com** para CIOs de la AAPP
- ✔ Suscripción a **Revista Byte TI**
- ✔ **Encuentros exclusivos** como torneos de golf y pádel
- ✔ **Mesas redondas** de fomento e innovación
- ✔ Visibilidad a proyectos de su organismo
- ✔ **Entrevistas**

🚀 **Exclusivo** para responsables de **Administración Pública**

adjudicaciones y licitaciones TIC | powered by byte TI

Andalucía presenta el Centro de Innovación en Tecnologías Exponenciales

El consejero de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, Antonio Sanz, ha anunciado en Granada, junto a la alcaldesa de Granada, Marifrán Carazo, la puesta en marcha casi de manera inmediata del nuevo Centro de Innovación en Tecnologías Exponenciales, que impulsará la Agencia Digital de Andalucía [ADA] en estrecha colaboración con las empresas IBM y Ayesa. Este centro permitirá a la comunidad andaluza erigirse en epicentro para la investigación y desarrollo de la computación cuántica.

Antonio Sanz ha anunciado, acompañado también por el presidente de IBM en España, Portugal, Grecia e Israel, Horacio Morell, y el director general de Ayesa, Germán del Real, que este espacio formará parte del Centro de Inteligencia Artificial de Andalucía, que cuenta con una inversión de 3,5 millones de euros y que tendrá su sede en el Parque Tecnológico de la Salud de Granada.

Este centro abrirá sus puertas el próximo mes de noviembre, coincidiendo con la celebración del III Congreso de Inteligencia Artificial de Andalucía en la ciudad, los días 10, 11 y 12, e iniciará su actividad con la coordinación y despliegue de los 65 casos de IA que actualmente funcionan en la Junta, gracias a una inversión de 36 millones de euros.

Potenciar el ecosistema digital

"Con el nuevo Centro de Innovación en Tecnologías Exponenciales queremos fortalecer el innovador ecosistema digital de nuestra región, impulsando el talento y la investigación en tecnologías cuánticas, acercando soluciones digitales innovadoras a la Administración y al sector investigador/productivo, y creando y fomentando nuevos

productores y consumidores de servicios cuánticos en Andalucía, abriendo oportunidades para empresas, startups, universidades y administraciones públicas", ha destacado el consejero en la reunión que ha mantenido esta mañana con el ecosistema andaluz de tecnologías exponenciales, que integra a representantes de la empresa, del mundo académico, de la investigación y de las instituciones que están impulsando el desarrollo de estas tecnologías.

Las líneas de trabajo del nuevo centro ya han sido definidas, según ha explicado el consejero. De este modo, se pretende interactuar con otros centros de conocimiento y ecosistemas de innovación (a nivel local, nacional e internacional) no sólo centrados en la cuántica sino también en otras tecnologías emergentes; plantear y desarrollar proyectos pilotos y casos de uso que hibriden la IA y la cuántica; aplicar un sistema de gobernanza y seguimiento de los resultados; y ofrecer acceso a computación cuántica real en modo uso por servicio, poniendo en marcha capacidades de emulación cuántica en el supercomputador Hércules, propiedad de la ADA, en funcionamiento desde diciembre de 2023 en el Centro Informático Científico de Andalucía.

Un modelo de gobernanza

Antonio Sanz ha destacado que la puesta en marcha del nuevo centro se asienta sobre el modelo de la gobernanza y de la colaboración público-privada, subrayando el papel estratégico que jugarán en las operaciones de este espacio "un gigante tecnológico como IBM y una empresa andaluza referente en el sector como Ayesa".

Por su parte, Marifrán Carazo ha afirmado que este centro "representa un hito que consolida a Granada como epicentro de innovación, tecnología e inteligencia artificial, situándola en el mapa regional y nacional". Y ha resaltado que "supone un salto cualitativo en materia de computación cuántica y en capacidades de investigación y desarrollo, que beneficiarán a toda la región".

La regidora ha destacado que "Granada es un enclave único en innovación, gracias al talento de nuestra universidad y al ecosistema de empresas tecnológicas que ya conforman una industria de primer nivel". También ha mencionado proyectos pioneros como el iQuantum y el I Plan Municipal de Inteligencia Artificial, con los que Granada "ayuda y fortalece al conjunto de Andalucía, posicionando a la ciudad como un referente nacional e internacional en tecnología avanzada".

Andalucía se integra en IBM Quantum Network

Gracias a esta colaboración con IBM, Andalucía pasa desde ahora a formar parte de la IBM Quantum Network, una red internacional de empresas, academias, startups, centros tecnológicos y agentes públicos que colaboran en el desarrollo de la computación cuántica y sus aplicaciones reales, "lo que nos va a permitir participar de esta comunidad y beneficiarnos de los avances producidos en ese colectivo internacional", ha resaltado el consejero.

IBM ha puesto en marcha más de 40 centros de innovación cuántica en el mundo, ha fabricado y puesto en servicio más de 60 ordenadores cuánticos desde 2016 y ha creado en Europa un Data Center cuántico que estará al servicio de investigadores y empresas andaluzas para desarrollar pilotos en los sistemas cuánticos más vanguardistas. "Gracias a ello Granada será un punto de acceso privilegiado a la computación más avanzada del planeta", ha destacado Sanz.

El objetivo último de este centro es aprovechar al máximo la capacidad de cálculo que brinda la computación cuántica en la simulación de procesos complejos para "lograr que las ideas se transformen en soluciones reales que contribuyan a mejorar la vida de los ciudadanos, que es lo que promovemos desde la ADA", ha culminado el consejero.

Editorial

La importancia de diseñar una estrategia de ciberseguridad sólida en las administraciones públicas es una cuestión prioritaria y urgente en España. Según el Instituto Nacional de Ciberseguridad (INCIBE), en 2025 se gestionaron más de 124.000 incidentes de seguridad, lo que supone un aumento del 28% respecto a 2024. El 34% de los ciberataques detectados en España en 2025 fueron dirigidos contra entidades públicas, afectando a ayuntamientos, diputaciones, ministerios y organismos nacionales.

El ransomware, las campañas de DDoS y el robo masivo de información han comprometido datos sensibles de funcionarios y ciudadanos, amenazando la continuidad y reputación del servicio público. Solo en la Comunidad de Madrid, la concentración de sedes administrativas ha potenciado el impacto de los ataques, con más de 47.000 incidentes y pérdidas económicas estimadas en 950 millones de euros.

Entre los retos clave figuran la protección de infraestructuras críticas, la adaptación a regulaciones como NIS2 y la formación constante de empleados para identificar amenazas. La falta de recursos técnicos y la rápida evolución del cibercrimen agravan la vulnerabilidad de las administraciones, que necesitan enfoques proactivos y colaborativos para mitigar riesgos crecientes. Sin una estrategia coordinada y proactiva, las administraciones seguirán vulnerables ante unos ciberdelincuentes que utilzan técnicas cada vez más sofisticadas para tener éxito.

Navarra impulsa TwIN Govtech para el desarrollo de gemelos digitales

Un total de ocho empresas y centros tecnológicos desarrollarán, a través del programa TwIN Govtech, diversos proyectos piloto de gemelos digitales que respondan a los actuales retos urbanos y que contribuyan a que Pamplona sea una ciudad más innovadora, sostenible y conectada.

Este programa se enmarca en la estrategia global del Gobierno de Navarra y del Ayuntamiento de Pamplona por impulsar una transformación digital que tenga efectos tangibles sobre la calidad de vida de la ciudadanía. Los gemelos digitales, modelo tecnológico en auge a nivel internacional, permiten crear réplicas virtuales de entornos físicos —una plaza, una red de transporte o una infraestructura energética— para simular su comportamiento en tiempo real, analizar datos y prever el impacto de distintos escenarios. De este modo, las decisiones públicas pueden fundamentarse en evidencias y datos, minimizando costes, mejorando la eficiencia y anticipándose a posibles problemáticas urbanas.

Las propuestas ganadoras, escogidas entre 113 candidaturas presentadas, pondrán a prueba sus soluciones innovadoras en cuatro áreas clave: energía, movilidad, urbanismo y calidad del aire; divididas a su vez en ocho retos: diseño de redes de calor y frío, cultura de eficiencia energética, medición de calidad del aire, gestión integral ambiental, mantenimiento del espacio urbano, diseño de la ciudad del futuro, planificación de infraestructuras de movilidad y mejora del transporte público urbano.

Esta convocatoria de amplio alcance refleja la gran respuesta que el ecosistema innovador navarro ha mostrado hacia la digitalización de la administración pública. El alto número de candidaturas evidencia el dinamismo de startups, pymes tecnológicas y centros de investigación, tanto locales como de otras regiones, interesados en colaborar con instituciones públicas en el desarrollo de soluciones tecnológicas de impacto inmediato.

Las entidades que resulten escogidas en su categoría recibirán adjudicaciones de pilotos de hasta 60.000 euros. De esta forma, tendrán la oportunidad de testar sus tecnologías en un entorno real, generando un impacto directo en la ciudadanía. En estos pilotos, podrán experimentar las soluciones

seleccionadas, con la idea de obtener aprendizajes y, si es posible, escalar aquellas propuestas que encajen con las necesidades de los equipos públicos. Esta metodología, orientada a la experimentación y mejora continua, sitúa a Pamplona entre las ciudades españolas pioneras en la adopción de modelos de innovación abierta dentro del sector público.

Las candidaturas finalistas han sido presentadas en el evento TwIN Govtech, que se ha celebrado en la sede de la sociedad pública Centro Europeo de Empresas e Innovación de Navarra (CEIN), ubicada en Noáin / Noain. En él, el consejero de Universidad, Innovación y Transformación Digital, Juan Luis García, ha destacado que "gracias a esta iniciativa hemos comprobado cómo la innovación digital, combinada con la colaboración público-privada, se convierte en una potente herramienta para transformar nuestro entorno, haciéndolo más sostenible, más eficiente y también más humano".

La jornada, que reunió a representantes institucionales, técnicos municipales, responsables de las empresas

participantes y agentes del ecosistema tecnológico, permitió compartir experiencias y debatir sobre cómo los gemelos digitales pueden ayudar a planificar una Pamplona más resiliente frente a los desafíos energéticos, climáticos y sociales del siglo XXI. Los asistentes coincidieron en que la colaboración entre el sector público, la empresa privada y el ámbito científico es clave para garantizar que la innovación no quede solo en el plano teórico, sino que se traduzca en mejoras reales para las personas.

Asimismo, García ha subrayado que el programa "abre la puerta a que la creatividad de nuestras empresas tenga un impacto real en la sociedad, poniendo la tecnología al servicio de la ciudadanía" y ha reafirmado la apuesta del Gobierno de Navarra por seguir impulsando este tipo de iniciativas que sitúan a la Comunidad Foral "como referente en innovación tecnológica aplicada". Esta filosofía refleja una visión madura de la gobernanza digital: no se trata únicamente de incorporar tecnología, sino de hacerlo con propósito, transparencia y valor público.

Por su parte, el gerente del Ayuntamiento de Pamplona, Iñigo Anaut, ha subrayado el valor de este concurso. "Este es un paso más hacia la Pamplona del futuro. La innovación y la colaboración son la clave para transformar nuestra ciudad", resaltó. Con esta declaración, Anaut enfatizó la intención del consistorio de seguir apostando por modelos de gobernanza colaborativa que integren la participación ciudadana en las decisiones estratégicas sobre el desarrollo urbano.

Las entidades seleccionadas

En el área de Energía, resultó ganadora del reto de cultura de eficiencia energética Mosaik Ubem, mientras que Suno lo hizo en el reto de diseño de redes de calor y frío. Ambas entidades aportarán su experiencia en el campo de la optimización energética, ámbito fundamental para reducir emisiones, optimizar consumos y promover una transición ecológica.

En Movilidad, DECIDE venció en el reto de mejora del transporte público urbano, con Hupi Ibérica en el de planificación de estructuras de movilidad. Estas iniciativas apuntan hacia una movilidad urbana más eficiente, digitalizada y adaptada a las necesidades de los ciudadanos, incorporando análisis predictivo y modelización avanzada mediante gemelos digitales.

En calidad del aire, la propuesta en colaboración entre Tesicnor y UNAV fue la ganadora del reto de gestión integral, con Ingreen, Naitec y Suez finalistas en medición de calidad del aire. El control y la mejora de la calidad atmosférica es un objetivo prioritario en la agenda ambiental de Pamplona, y estos proyectos permitirán profundizar en el análisis de contaminantes, establecer patrones de comportamiento y evaluar la efectividad de distintas políticas de mitigación.

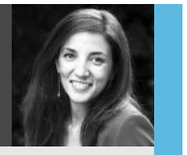
En la última área, urbanismo, la entidad ganadora fue BIM6D en diseño de la ciudad del futuro, quedando finalistas DECIDE, DCOD y Fuvex en mantenimiento del espacio urbano. Los trabajos desarrollados en este ámbito permitirán testar nuevas metodologías de gestión urbana a través de modelado digital del territorio, automatización del mantenimiento y creación de entornos virtuales que faciliten la participación ciudadana en el diseño urbano.

Programa TwIN

El programa TwIN Govtech forma parte de la iniciativa TwIN en Navarra, impulsada por el Gobierno de Navarra y el Ayuntamiento de Pamplona, cuya ejecución lidera la empresa pública Tracasa Instrumental, adscrita al departamento de Universidad, Innovación y Transformación Digital. Este proyecto se concibe como un marco integral para fomentar la innovación con impacto social a través del uso de tecnologías avanzadas.

Además del área Govtech, el proyecto TwIN en Navarra cuenta con la vertiente Lab, que ofrece un espacio de innovación para startups, pymes y emprendedores. A través de este laboratorio, los participantes pueden acceder a formación práctica, utilizar gemelos digitales sin necesidad de grandes inversiones y recibir acompañamiento para desarrollar y escalar un producto mínimo viable (MVP). Este componente formativo y experimental refuerza el carácter inclusivo de la iniciativa, al permitir que actores de diversos tamaños y sectores se beneficien de las ventajas que ofrece la digitalización avanzada.

La opinión de Arantxa Herranz



Primero fue el Covid. Luego la invasión de Ucrania por parte de Rusia. Más tarde, la llegada de Donald Trump a la Casa Blanca y la irrupción de los aranceles. El último acontecimiento que ha ocurrido es el de, la reacción de Washington a la multa europea a Google. Todos estos acontecimientos (entre otros) han espoleado un movimiento que llama a Europa a ser más resiliente. Esto es, a depender menos de terceros.

Unas veces con más sigilo, otras con menos, es el runrún que recorre la industria tecnológica. Y frente a las voces que niegan la posibilidad de que Europa pueda ser tecnológicamente independiente, cada vez surgen más voces (muchas veces desde Alemania, todo hay que decirlo, sin quitar un ápice de liderazgo a Reino Unido o Francia) que, de manera más o menos tajante, dan datos, cifras, muestras y realidades de que este "sueño" sí es alcanzable. Que todo es proponérselo. Que no somos tan pequeños como pudiera paracer y, en caso de que lo seamos, bien organizados nos podeos comer al pez grande.

Porque, o jugamos todos, o se rompe la baraja. Quizá solo es cuestión de poner boca arriba las cartas y comprobar quién va de farol.

El proyecto Altamira busca un centro de supercomputación cuántica en Cantabria

El consejero de Industria, Empleo, Innovación y Comercio de Cantabria, Eduardo Arasti, ha anunciado que el futuro Campus Tecnológico de Centros de Datos Altamira, promovido por Stoneshield Capital, podría albergar un centro de supercomputación cuántica, el primero de este tipo en Cantabria. Según Arasti, el promotor "explora activamente la introducción de supercomputación cuántica para dotar al proyecto de capacidades más allá del presente y mirando hacia el futuro".

Acompañado por el vicerrector de Transformación Digital de la Universidad de Cantabria, José Luis Bosque, y el CEO de XDC Properties, Javier García, Arasti destacó que Altamira "no solo será clave desde el punto de vista económico y social, sino que también transformará la investigación científica, la formación de los jóvenes y la competitividad regional". El consejero subrayó la buena disposición de Stoneshield para estudiar la implantación del centro cuántico, que situaría a Cantabria como referente en innovación.

Durante la mesa redonda celebrada, Arasti explicó que el proyecto Altamira "significará un giro de 180 grados en el sistema productivo de Cantabria, orientándolo hacia sectores de mayor valor añadido". La inversión prevista asciende a más de 3.600 millones de euros, "la mayor de la historia de Cantabria", equivalente al presupuesto del Gobierno regional y a un 25% de su PIB. Además, se prevé la creación de más de 1.500 empleos cualificados y bien remunerados. "Estamos ante un momento histórico", afirmó.

Entre las ventajas del proyecto, Arasti destacó su eficiencia energética "imbatible", ya que el centro consumirá menos electricidad que cualquiera de su tipo en España y no empleará agua para refrigeración, gracias al clima templado y húmedo de la región. También subrayó su conectividad estratégica, cercana a rutas de fibra óptica y al cable submarino Anjana, "el de mayor capacidad del mundo, que atraviesa Santander y conecta Europa con Estados Unidos", lo que garantiza baja latencia y múltiples rutas de conexión. Esta conectividad se reforzará con el nuevo cable submarino de Google, que también enlazará Santander con Estados Unidos.

El Campus obtendrá su energía de la subestación de Penagos, un nodo robusto y preparado para grandes demandas eléctricas, lo que permitirá descentralizar el consumo y reducir la concentración de centros de datos en el eje Madrid-Aragón-Cataluña. Además, se plantea una conexión directa a la red eléctrica con dos nuevas posiciones que "no implicarán ningún coste de ejecución", pendiente aún de aprobación por el Ministerio para la Transición Ecológica en la planificación 2026-2030.

Arasti defendió el papel de los centros de datos como "instrumentos esenciales para que las pymes compitan en igualdad de condiciones", fomentando ecosistemas de innovación junto a universidades y empresas. Recordó que tecnologías "disruptivas" como la Inteligencia Artificial y el Big Data requieren infraestructuras de baja latencia y soberanía digital, "con datos protegidos bajo jurisdicción española y europea".

Finalmente, reafirmó el compromiso del Gobierno cántabro con la IA, la ciberseguridad y la supercomputación, pilares de una transformación tecnológica que busca situar a Cantabria como referente en innovación aplicada a la industria y la administración pública. Con 637.000 m entre Piélagos y Villaescusa, el Campus Altamira se ejecutará en tres fases, centradas en inteligencia artificial y servicios cloud. La primera arrancará en enero de 2026, y el complejo prevé iniciar operaciones en 2032.

El Gobierno de Castilla-La Mancha apoya su Asociación de Inteligencia Artificial

El director general de Digitalización e Inteligencia Artificial, Juan Pedro de Ruz, ha dado a conocer que la Agencia de Transformación Digital será miembro honorífico de esta asociación, junto a la UCLM y los Colegios de Ingenieros de Telecomunicaciones y de Informática de Castilla-La Mancha.

El Gobierno de Castilla-La Mancha ha apoyado a la Asociación de Inteligencia Artificial de la región (AIACLM) en su presentación oficial. Un respaldo que ha corrido a cargo del director general de Digitalización e Inteligencia Artificial, Juan Pedro de Ruz, durante la clausura del acto que se ha celebrado en la Diputación de Albacete.

Junto al director general también han participado la presidenta de la Asociación de Inteligencia Artificial de Castilla-La Mancha (AIACLM), Dori López; el delegado de la Junta de Comunidades en Albacete, Pedro Antonio Ruiz; así como representantes de otras instituciones de la región, como la UCLM o los Colegios de Ingenieros de Telecomunicaciones y de Informática de Castilla-La Mancha.

Juan Pedro de Ruz ha dado a conocer que la Agencia de Transformación Digital de Castilla-La Mancha será miembro honorífico de esta asociación, al igual que formarán parte en esa misma calidad la Universidad de Castilla-La Mancha, el Colegio de Ingenieros de Telecomunicaciones de la región y el Colegio de Ingenieros Informáticos de la comunidad autónoma.

De Ruz ha señalado que para el Gobierno de Castilla-La Mancha la Inteligencia Artificial es una "tecnología que va a permitir seguir mejorando los servicios que se prestan a la ciudadanía desde la Administración regional". De este modo, ha precisado que esta oportunidad para mejorar se está trabajando desde dos puntos: "ofreciendo servicios proactivos", adaptados a las necesidades del ciudadano o en base a las preferencias de éste, y "mejorando los tiempos de respuesta de la Administración", ya que la Inteligencia Artificial permite desarrollar herramientas digitales o asistentes basados en IA generativa que ayude a los empleados públicos en su labor, en la tramitación y resolución de expedientes.

De este modo, el director general ha recordado que ya la pasada legislatura se hizo una apuesta decidida por parte del Ejecutivo autonómico por la adopción de la IA y su impulso creando un equipo especializado, un esfuerzo que en este mandato se ha visto reforzado con la creación de la Agencia de Transformación Digital y, dependiente de ésta, una Dirección General de Digitalización e Inteligencia Artificial.

El director general ha puesto algunos ejemplos, como la Plataforma Agroalimentaria en Red (PAN), un proyecto Retech que integra la IA en todos los eslabones de la cadena de valor en la industria agroalimentaria con el objetivo de mejorar la toma de decisiones, unificar oferta y demanda, facilitar y agilizar los intercambios comerciales, o garantizar la trazabilidad y la optimización de procesos en la cadena de valor del sector agropecuario. En el ámbito del medio ambiente y la sostenibilidad, ha puesto un tercer ejemplo con el proyecto Geneva, a través de la aplicación de la IA generativa para la mejora de los servicios públicos al ciudadano. Se trata de un asistente basado en IA para ayudar a la resolución de expedientes de Evaluación de Impacto Ambiental de una manera más ágil y eficiente.

Finalmente, el director general ha explicado que en la aplicación real de Inteligencia Artificial es muy importante considerar la formación y capacitación de los empleados públicos de forma estratégica, como es el caso de la Junta de Comunidades de Castilla-La Mancha, de forma que la IA generativa se convierta para ellos en una herramienta de apoyo en sus labores cotidianas. La Asociación de IA CLM es una entidad sin ánimo de lucro y entre sus fines tiene los siguientes: fomentar la educación en el uso de la IA tanto en el ámbito profesional como en el académico; democratizar el acceso a la IA, evitando brechas económicas y sociales; apoyar a autónomos, pymes y entornos rurales en la integración de soluciones de IA.

La EMT de Madrid usará la IA para detectar incidencias y anomalías a bordo

Los autobuses de la Empresa Municipal de Transportes de Madrid (EMT) de Madrid contarán con un sistema de visión artificial a bordo, una tecnología que persigue reforzar la seguridad de los usuarios y la eficiencia operativa de toda la flota municipal.

Este proyecto, basado en herramientas de Inteligencia Artificial (IA), es pionero en su ámbito y cuenta con prototipos propios. Además, es también un proyecto colaborativo con Nvidia, que ha participado en el diseño.

El sistema utilizará las cámaras que ya están presentes en el autobús dotándolas de una nueva utilidad: identificará posibles riesgos o situaciones inesperadas, así como usos incorrectos y será capaz de reaccionar de forma inmediata ante imprevistos que puedan comprometer la seguridad o el bienestar de los usuarios. Esta respuesta instantánea permitirá, por tanto, actuar rápidamente ante incidentes urgentes gracias al análisis de las imágenes a bordo.

Evitar la pérdida de objetos, caídas o aglomeraciones

EMT Madrid ha publicado el pliego de la licitación del proyecto y, una vez adjudicado el contrato, la fase de desarrollo tendrá una duración aproximada de 18 meses. Está previsto que las primeras analíticas estén operativas para el primer trimestre de 2027.

Algunos ejemplos de la utilidad de este novedoso sistema de detección son la identificación de objetos abandonados, de posiciones incorrectas en carritos de bebé y sillas de ruedas, la presencia de patinetes eléctricos que no están autorizados, las caídas o desvanecimientos de pasajeros, comportamientos violentos, frenadas bruscas y aglomeraciones en zonas específicas del vehículo, entre otras situaciones. Esta capacidad de anticipación permitirá una detección temprana y la reducción de riesgos antes de que se conviertan en incidentes reales. Finalmente, el sistema incorporará modelos de aprendizaje automático que evolucionarán con el uso y mejorarán progresivamente esta tecnología.

Además, dado el compromiso de EMT con la ética digital, el proyecto garantiza el máximo respeto por la privacidad de los usuarios, objetivo para el que se han revisado, a la hora de elaborar el pliego, todos los criterios legales vinculados a la tecnología (tanto en lo que respecta a la inteligencia artificial como al Reglamento General de Protección de Datos).

Beneficios operativos

Los incidentes generarán avisos en tiempo real, que llegarán, según corresponda, al conductor, al centro de control e, incluso, al propio viajero a través de la megafonía interna de los autobuses, facilitando la actuación inmediata y la optimización de los recursos. Esta detección en tiempo real constituye un ejemplo de movilidad conectada y segura, puesto que permite que los vehículos, conductores y usuarios estén interconectados en tiempo real.

La implantación del sistema será progresiva: los distintos usos se incorporarán por fases, priorizando primero los más críticos para garantizar una integración controlada. Un valor añadido del proyecto es que la infraestructura desplegada permitirá el desarrollo y evolución de nuevas estrategias para mejorar la accesibilidad y la experiencia del viaje.

La Generalitat Valenciana impulsa una nueva herramienta para mejorar la transparencia local

La Generalitat y las diputaciones provinciales de la Comunitat Valenciana han mantenido una reunión de trabajo en Moraira, presidida por el secretario autonómico de Relaciones Institucionales y Transparencia, Santiago Lumbreras, encuentro en el que se han definido las líneas de actuación conjunta para 2026 en materia de participación ciudadana, transparencia y buen gobierno.

Durante la sesión de trabajo, se ha anunciado una nueva herramienta de autodiagnóstico, diseñada para que los ayuntamientos puedan evaluar de forma sencilla y práctica su grado de cumplimiento en materia de transparencia. Esta iniciativa se enmarca en un conjunto de proyectos innovadores que incluyen también servicios de asistencia técnica, jornadas formativas y subvenciones específicas para municipios de menos de 20.000 habitantes.

El secretario autonómico de Relaciones Institucionales y Transparencia, Santiago Lumbreras, ha afirmado que la transparencia "no puede ser una carga burocrática, sino una oportunidad para acercar la administración a la ciudadanía. Con esta herramienta, los ayuntamientos podrán identificar sus fortalezas y áreas de mejora, y contar con apoyo técnico para avanzar", ha añadido Lumbreras.

Lumbreras ha destacado también que "por primera vez, las diputaciones han expuesto sus propuestas concretas sobre el destino de los fondos autonómicos, lo que permitirá una planificación más eficaz y ajustada a las necesidades reales de cada territorio".

"Queremos que los municipios, especialmente los más pequeños, tengan herramientas reales y eficaces para avanzar en transparencia y participación. Esta colaboración con las diputaciones nos permite sumar esfuerzos, evitar duplicidades y ofrecer soluciones adaptadas a las necesidades locales", ha asegurado el secretario autonómico.

Lucha contra la brecha digital

Entre las acciones acordadas en el ámbito de la participación ciudadana, se incluye la puesta en marcha de formaciones destinadas a reducir la brecha digital en el ámbito local. Estas formaciones estarán orientadas a capacitar a la ciudadanía en el uso de las plataformas de transparencia y participación de la Generalitat —GVA Oberta y GVA Participa—, así como en el manejo de sitios web municipales que canalizan la participación ciudadana. Además, se impartirán cursos específicos sobre el uso de aplicaciones móviles dirigidos a personas mayores, con el objetivo de fomentar su implicación en los procesos participativos.

La colaboración con las diputaciones provinciales durante el próximo ejercicio se orientará fundamentalmente a proyectos de transparencia y participación ciudadana, desarrollo de herramientas digitales para la evaluación municipal, formación y capacitación de personal técnico en buen gobierno, además de campañas de sensibilización.

La reunión se ha celebrado en el marco del convenio de colaboración entre Presidencia de la Generalitat, las diputaciones de Alicante, Castellón y València, y la Federación Valenciana de Municipios y Provincias [FVMP], reafirmando el compromiso institucional por una gobernanza más abierta, colaborativa y eficaz.

La Xunta refuerza la formación de los empleados públicos en materia de protección de datos

Un total de 70 empleados públicos participan desde hoy en la cuarta edición del Curso superior en protección de datos, organizado por la Agencia para la Modernización Tecnológica de Galicia (AMTEGA) y el Nodo CIBER.gal.

El curso fue inaugurado por la directora de la EGAP, Sonia Rodríguez-Campos; el director de la AMTEGA, Julián Cerviño Iglesia, y el jefe del subárea de seguridad de la AMTEGA y director de la acción formativa, Gustavo Herva Iglesias.

La directora de la EGAP, Sonia Rodríguez-Campos, destacó la gran acogida que tuvo el curso e incidió en la importancia de que el desarrollo de las nuevas tecnologías a nivel de la Administración pública "tiene que ir acompañado de una clara preocupación por la seguridad como factor decisivo en la implantación de la Administración electrónica y de la sociedad de la información".

Sonia Rodríguez-Campos resaltó que "ante el desarrollo de la Administración digital es preciso dotar al personal empleado público de las herramientas y los conocimientos necesarios para salvaguardar los datos personales que se almacenan y transmiten en línea, algo esencial para defender los derechos de la ciudadanía y preservar la confianza en nuestras instituciones".

Además, destacó que uno de los objetivos de la Xunta para continuar avanzando en la implantación de la e-Administración "es mejorar la seguridad para minimizar los posibles incidentes en este ámbito, garantizar la confidencialidad de la información y asegurar la continuidad del servicios prestados".

Por este motivo, según la directora de la EGAP, "se hace ineludible a convocatoria de actividades formativas que contribuyan a crear un escenario de seguridad jurídica".

Además, Sonia Rodríguez-Campos señaló que el curso "es una muestra más del esfuerzo y el compromiso por parte de la Escuela por ofrecer una formación anual completa, actualizada y de calidad en aquellas materias de relevancia para lo personal empleado público mediante cursos y acciones formativas en relación con el ámbito digital".

Por su parte, el director de la Agencia para la Modernización Tecnológica de Galicia, Julián Cerviño, recordó que "los datos deben usarse para mejorar la calidad de vida de las personas, pero, en todos los casos, tienen que ser gestionados desde la responsabilidad, la seguridad, la garantía de confidencialidad y desde el conocimiento de toda la información normativa y legal".

Objetivos

La cuarta edición del curso superior en protección de datos, con una duración de 118 horas, pretende ahondar en el conocimiento de la protección de datos, tanto desde una perspectiva técnico-jurídica cómo práctica. El curso finalizará el 10 de diciembre.

Los objetivos de esta acción formativa de modalidad mixta (presencial, telepresencia y teleformación) son concienciar al alumnado sobre la relevancia e importancia del derecho fundamental a la protección de datos personales para lo cual es necesaria la aplicación de buenas prácticas de acuerdo con la normativa vigente, respetar los derechos de las personas interesadas por el tratamiento de sus datos personales y gestionar adecuadamente posibles incidentes que puedan surgir en las distintas fases del tratamiento.

El curso también ahondará en los principios básicos de seguridad y las medidas que hace falta implantar en los sistemas de información desde la perspectiva del riesgo y en base al dispuesto en el Reglamento General de Protección de Datos y en el Esquema Nacional de Seguridad.

Cómo establecer una consexión segura a distanciay garantizar la continuidad de las operaciones

En el contexto actual de transformación digital y trabajo híbrido, las instituciones públicas enfrentan un reto creciente: garantizar la continuidad de sus operaciones a través del acceso remoto, sin poner en riesgo la seguridad de los datos que gestionan ni incumplir la normativa vigente. Desde ministerios y ayuntamientos hasta organismos de salud y educación, el uso de herramientas de soporte y acceso a distancia se ha vuelto imprescindible. Pero esta misma necesidad ha abierto nuevas puertas a amenazas, tanto internas como externas, que exigen una respuesta clara, estructurada y técnica por parte de los responsables de TI en el sector público.

El concepto de cumplimiento de seguridad en soluciones de acceso remoto no se refiere solo a mantener una plataforma funcional, sino a cumplir con marcos legales como el Reglamento General de Protección de Datos (RGPD), la Directiva NIS 2 o normativas específicas nacionales que regulan el tratamiento de datos, la infraestructura crítica o los sistemas de información

clasificados. Además, con el aumento de la presión normativa y las auditorías externas, las instituciones deben demostrar activamente que sus herramientas digitales están alineadas con buenas prácticas reconocidas, tanto en diseño como en operación.

AnyDesk surge en este escenario como una solución de acceso remoto que prioriza la seguridad y el cumplimiento normativo. A diferencia de otras plataformas más generalistas, AnyDesk ofrece características adaptadas a las necesidades del sector público, combinando robustez tecnológica con flexibilidad operativa. Su arquitectura incluye cifrado de extremo a extremo mediante TLS 1.2 y cifrado simétrico AES de 256 bits, tecnologías utilizadas a nivel bancario y militar para proteger la confidencialidad e integridad de los datos en tránsito. Además, todo el software está firmado digitalmente con certificados emitidos por Digicert, lo que garantiza su autenticidad y previene manipulaciones o inyecciones de malware.

Uno de los grandes valores que AnyDesk aporta a los organismos públicos es la posibilidad de instalar una solución completamente On-Premises. Esto significa que todos los datos, conexiones y registros se mantienen dentro de la red interna del organismo, sin pasar por servidores externos o nubes públicas. Esta opción resulta esencial para administraciones que deben cumplir con requisitos estrictos de soberanía digital, residencia de datos o control total sobre sus infraestructuras críticas. En muchos países, esta capacidad no solo es deseable, sino obligatoria para determinados tipos de instituciones.

Además del cifrado y la infraestructura, AnyDesk incluye funciones avanzadas de control de acceso y auditoría. El administrador puede definir exactamente qué dispositivos pueden conectarse, establecer políticas de acceso interactivo (que requieren aceptación del usuario) o acceso por contraseña, activar la autenticación de dos factores (2FA) y gestionar los derechos de cada usuario mediante integración con sistemas de identidad (IAM) y Single Sign-On (SSO). Todo esto se complementa con registros detallados de sesión, lo que permite auditar el uso del sistema y detectar comportamientos anómalos o accesos indebidos.

En entornos donde la privacidad de los datos es crítica —como en salud pública o servicios sociales—, AnyDesk también permite activar un modo de privacidad que oscurece la pantalla del dispositivo remoto mientras se realiza una conexión, evitando así que terceros visualicen información sensible. Estas funcionalidades son particularmente útiles para ofrecer soporte técnico a empleados sin comprometer datos confidenciales, especialmente cuando los dispositivos se utilizan fuera de oficinas seguras.

La amenaza de ciberataques dirigidos a entidades públicas no es teórica: cada año se reportan incidentes en los que herramientas de acceso remoto mal configuradas o vulnerables han sido utilizadas para robar información, cifrar sistemas con ransomware o manipular bases de datos institucionales. En este contexto, contar con una herramienta como AnyDesk, que realiza análisis automatizados de vulnerabilidades con Detectify y se desarrolla conforme a los principios de seguridad definidos por OWASP, representa una capa adicional de defensa frente a estas amenazas.

No cumplir con los requisitos legales o de ciberseguridad ya no es una opción menor. Las consecuencias pueden incluir desde sanciones económicas hasta la paralización de servicios esenciales o la pérdida de confianza de los ciudadanos. Además, en caso de una auditoría o incidente, los organismos deben poder demostrar no solo que eligieron una herramienta segura, sino que implementaron correctamente sus controles y políticas de uso.

Por esta razón, la elección de herramientas de acceso remoto no debe basarse únicamente en criterios de coste o facilidad de uso, sino en su capacidad de ofrecer seguridad certificada, control granular y cumplimiento con las normativas vigentes. AnyDesk, con su enfoque en la protección de datos, su capacidad de personalización para entornos públicos y su infraestructura de seguridad, se posiciona como una solución confiable para el sector público que no puede permitirse errores ni brechas.

La implementación de una solución segura como AnyDesk debe ir acompañada de políticas internas claras, formación continua del personal y monitoreo activo de las conexiones. Solo así se puede garantizar que el acceso remoto no se convierta en una debilidad, sino en una herramienta poderosa al servicio de una administración más eficiente, digital y responsable.

Además del cifrado y la infraestructura, AnyDesk incluye funciones avanzadas de control de acceso y auditoría.

ENTREVISTA

Benjamín Cogolludo,

Responsable de Informática, Innovación y Comunicaciones en el Ayuntamiento de Castro-Urdiales

"La inversión de dinero público debe ser exquisita y basada en retornos reales de mejora de la ciudadanía"

Benjamín Cogolludo es el Responsable de Informática, Innovación y Comunicaciones en el Ayuntamiento de Castro-Urdiales, cargo que desempeña desde abril de 1998, acumulando más de 27 años de experiencia en la función pública. Ingeniero en Informática por la Universidad de Deusto, cuenta con un Máster en Dirección de Sistemas y Tecnologías de la Información por la Universidad Politécnica de Madrid y el Instituto Nacional de Administración Pública.

Como director técnico de proyectos de innovación y tecnologías de la información en el Ayuntamiento, participando en iniciativas como "Castro-Urdiales Smart People 2020-2039" y gestiona equipos técnicos y proyectos subvencionados, aportando una gran experiencia y solvencia en el desarrollo de sistemas informáticos para la administración pública. Además, es vocal del Colegio Profesional de Ingenieros en Informática de Cantabria, lo que refleja su reconocimiento profesional y su papel activo en la comunidad tecnológica regional.

En esta entrevista con ByTIC nos cuenta cómo es su día a día, las particularidads de su rol y su visión de la innovación en el sector público

¿Puede describir su experiencia en la gestión de sistemas informáticos, especialmente en entornos de administración pública?

Trabajar en la Administración Pública es especialmente gratificante, porque el objetivo compartido es el bien común. En el caso del Ayuntamiento de Castro-Urdiales, se trata de buscar mejoras en el bien común de la ciudad, y por lo tanto, puedes colaborar para mejorar la calidad de vida de tus conciudadanos.

La gran diferencia en Gestión de Sistemas Informáticos en el ámbito público respecto del ámbito privado, es el modelo organizativo. Los jefes a los que tienes que plantear propuestas son políticos: alcaldesa/alcalde, o concejales. Pueden o no tener capacidades especiales de alta dirección. Es decir, no es el directivo tradicional de la empresa privada seleccionados para esos puestos directivos y que han demostrado experiencia

y capacidad para el puesto. Por otro lado, buscan el bien común de la sociedad a la que representan y existe un compromiso para ese objetivo.
Considero que es vital avanzar en la Dirección Pública Profesional en la AA.PP. y es por ello que soy socio de la Asociación para la Dirección Pública Profesional en España [ADPP]. Creo que es un reto vital para mejorar las AA.PP.

¿Cuáles son las principales responsabilidades que tiene en su cargo?
Actualmente soy Responsable de Informática, Innovación y Comunicaciones en el Ayuntamiento de Castro-Urdiales, como puesto de trabajo, pero adicionalmente ostento los siguientes roles dentro del Ayuntamiento de Castro-Urdiales: Representante técnico en la Red Española de Ciudades para la Agenda 2030 de la FEMP; Representante técnico en la Red Española de Ciudades Sostenibles de la FEMP; Coordinador y secretario de la Estrategia de Promoción de la Salud y Prevención [EPSP] de la RECS y el Ministerio de Sanidad. También soy Secretario del Colegio Profesional de Ingenieros en Informática de Cantabria y participo como evaluador de los premios de Innovación "Innovagloc" de la FEMP
En todo caso, y respecto al puesto de Responsable del Departamento de Informática, mi principal responsabilidad es velar porque los servicios a la ciudadanía funcionen con la eficacia y eficiencia requerida, dando soporte a toda la organización.

¿Y los principales retos o desafíos?
En primer lugar, como decía anteriormente, difundir y avanzar en una Dirección Pública Profesional que dirija a los funcionarios públicos. Los políticos tienen que responsabilizarse de los objetivos sociales y políticos, de su programa electoral, pero hay que separar el ámbito de la gestión directiva de la gestión política. No todas las personas serían seleccionadas para ser directivos en una organización, y en los Ayuntamientos existe el "conflicto de rol" cuando desde el ámbito político se confunden los roles profesionales con los técnicos.
Por otro lado, el gran reto para la mejora es aplicar modelos innovadores en todos los sistemas. Como dice Maite Covisa, "Si lo estás haciendo igual, lo estás haciendo mal". Seguimos realizando las tareas como hace mucho tiempo, cuando es evidente que ha cambiado la tecnología y el conocimiento y experiencia de las personas ha variado a lo largo del tiempo. Es vital, cambiar las formas de hacer las cosas aplicando "innovación disruptiva".

¿Qué experiencia tiene en la implementación de proyectos de innovación tecnológica?
Tras una experiencia profesional de casi 40 años, en el sector público y privado, en el ámbito de la Ingeniería en Informática, la Innovación, no sólo tecnológica, es parte de la savia natural de un profesional en este ámbito. Para cualquier diseño de un nuevo sistema desde la Informática, es necesario tener visión innovadora en la que no sólo diseñas soluciones tecnológicas, sino organizativas y humanas. Especialmente, remarquemos el término "humanas", dado que tenemos que interiorizar el avance hacia el bien común, en alineación total con la Agenda 2030 y los ODS.
Tras conseguir que "Castro-Urdiales, Smart People" fuera uno de los 14 proyectos seleccionados de entre los 736 presentados al Programa de Innovación Abierta [PIA] del 2019, de Fundación Cotec para la Innovación, se produjo un salto cualitativo y cuantitativo. A partir de ese momento, Castro-Urdiales empezó a ser conocida como una Ciudad Innovadora y por otro lado, a nivel personal, he sido invitado a participar en diferentes proyectos y ponencias.

¿Cómo se mantiene actualizado sobre las nuevas tecnologías y tendencias en el sector de la informática y las comunicaciones?
Especialmente a través de las redes de personas. Y en este concepto entran las asociaciones a las que pertenezco : [ADPP] Asociación para la Dirección Pública Profesional. [CPIIC] Colegio Profesional de Ingenieros en Informática de Cantabria, y [ATIAL] Asociación de Técnicos de Informática de Administración Local.
Adicionalmente, debe citarse la participación en redes sociales profesionales, grupos de trabajo,y proyectos de innovación. Por supuesto, la realización de cursos de formación con una media de dos a tres cursos anualmente, y la lectura habitual de documentación técnica en revistas, y publicaciones

¿Puede describir algún proyecto de innovación tecnológica que haya liderado o en el que haya participado activamente? ¿Cuáles fueron los resultados?
Destacaría el proyecto "Castro-Urdiales, Smart People" que desarrollamos en el Ayuntamiento de Castro-Urdiales junto a Fundación Cotec. Pretendía "diseñar el futuro" de los perfiles profesionales necesarios y de la organización más eficaz en un Ayuntamiento. Tratar de analizar los cambios que van a venir, y preparar planes de adaptación y formación de las personas en la ciudad para impulsar ese cambio fue un reto maravilloso. Respecto a innovación tecnológica, el diseño de un sistema propio, que llamamos MiCastro, tomando como referencia un proyecto personal, que llamé Marcocal, para desarrollar un software "multifunción" pueden ser reseñados en este apartado. En todo caso, todo esto no sería posible sin la colaboración del equipo de personas que forma parte de mi equipo y del que me siento orgulloso.

¿Cómo ve el papel de la tecnología en la mejora de los servicios públicos en un municipio como Castro-Urdiales?

Vital, con la reserva y crítica a los "proyectos megachulos" que acaban en despilfarros. La inversión de dinero público debe ser exquisita y basada en retornos reales de mejora de la ciudadanía. Casos de despilfarro como chatbot, marketplace locales, ciudades inteligentes que desaparecen al cabo de poco tiempo y que ha supuesto una inversión que no tiene ni estabilidad ni continuidad.

Y para ello, debe respetarse y fomentar que estos proyectos los dirijan los profesionales. Por ello, participé como uno de los fundadores del Colegio Profesional de Ingenieros en Informática de Cantabria, porque es imprescindible poner en la Dirección de Informática, Innovación, Atención a la Ciudadanía y Organización a Ingenieros en Informática, es decir, a los profesionales formados y capacitados para esta tarea.

¿Qué particularidades tiene el ser responsable de un ayuntamiento como el suyo?

Pues la verdad es que lo primero que debo destacar es existe un conflicto de rol que supone que el político toma decisiones técnicas, incluso en entornos de Ingeniería en Informática. Este problema es terriblemente dañino para las organizaciones públicas.

Tenemos la gran ocasión de hacer muchas mejoras, y así lo hemos hecho, pero es una queja generalizada la falta de escucha y atención al personal profesional del área de Informática

En la parte positiva, la colaboración con las áreas, basado en una vocación de servicio público innata a cualquier empleado público, es gratificante y sirve de palanca para el avance y la mejora de los servicios públicos.

¿Cómo es su relación con otras administraciones?

Fenomenal. Formo parte de grupos de trabajo con la Dirección General de Administración Local (DGAL) del Gobierno de Cantabria, participo en la Federación Española de Municipios y Provincias (FEMP), he realizado proyectos de innovación y colaboración con el Instituto Nacional de Administración Pública (INAP) de la Agencia General del Estado (AGE) y puedo constatar el alto nivel de calidad de los profesionales de todas estas organizaciones.

¿Qué ideas o proyectos de innovación tecnológica considera que podrían ser beneficiosos para el ayuntamiento de Castro-Urdiales?

Tener una visión innovadora disruptiva para producir localmente las necesidades

que ahora mismo se contratan fuera. La creación de Laboratorios de Innovación que generen productos que puedan ser utilizados por la sociedad en la Ciudad y que sean exportables y compartibles con otras organizaciones y ciudades. En este caso, sirva citar como ejemplo al proyecto Sedipualba de la Diputación de Albacete. Que las necesidades propias sean visionadas como oportunidades de desarrollo económico y social local. Sirva para ello, el ejemplo que aprendí del economista Emilio Ontiveros citando el desarrollo conseguido en la región de Bangolore apostando por la formación TIC de la ciudadanía en la zona.

¿Cómo abordaría la transformación digital del ayuntamiento?

En primer lugar, consiguiendo convencer a la dirección política que es necesario un "Director de Innovación Digital" (mañana podemos llamarle "Director de Inteligencia Artificial" u otro análogo), que lidere ese proceso. Y la selección de dicho perfil debe hacerse conforme a criterios de mérito, igualdad y capacidad sin nombrar personal de confianza como es habitual, tal y como fomentamos en la ADPP. Para poder hacer las tareas con eficiencia y eficacia, debemos tener un liderazgo transformador que sea el impulsor de la capacidad interna del personal empleado público y se necesitan líderes transformadores.

¿Qué estrategias implementaría para mejorar la ciberseguridad del ayuntamiento?

En primer lugar, apoyo político a la Política de Seguridad. En segundo lugar, la participación e implicación de todo el personal con grupos de trabajo, descentralización de esas responsabilidades para que sean de todos y no de una persona o grupo. Y, por supuesto, la formación y concienciación es vital y, en último lugar las dotaciones presupuestarias, que en mi opinión, no son tan difíciles de conseguir.

ENTREVISTA

Frank Karlitschek,

CEO de Nextcloud

“Las soluciones de código abierto refuerzan la resiliencia digital. El momento de aplicarlas es ahora”

Frank Karlitschek es, además de fundador y CEO de Nextcloud, un desarrollador alemán apasionado y defensor del software libre, la privacidad y el control de los datos por parte de los usuarios, elementos que considera fundamentales para la democracia y la soberanía digital. Como CEO de Nextcloud, Karlitschek promueve la idea de que la privacidad es un derecho básico y que el software abierto es clave para que los usuarios y organizaciones tengan soberanía digital. Su empresa ha ganado reconocimiento especialmente en Europa, al proveer soluciones que cumplen con regulaciones como el RGPD y al contar con una arquitectura modular que permite colaboración en tiempo real, con fuerte soporte comunitario. Ahora, hace una defensa encendida de Europa y de su potencial tecnológico, pero reclama más implicación también por parte de las administraciones públicas en un momento clave para la soberanía digital y el respeto por los valores europeos.

Nextcloud se ha posicionado como una alternativa europea a las grandes plataformas estadounidenses. ¿Qué ventajas concretas ofrece Nextcloud a las administraciones públicas españolas en términos de soberanía digital y cumplimiento del RGPD, frente a soluciones como Microsoft 365 o Google Workspace?

Nextcloud es la única plataforma de colaboración con la que las autoridades públicas conservan el control total de sus datos. Ellas mismas pueden elegir dónde alojarlos: en su propio servidor, en una nube privada o con un proveedor de alojamiento de confianza como por ejemplo Arsys. Así, las autoridades pueden decidir quién tiene acceso a los datos. Nextcloud es de código abierto y trabaja con estándares abiertos. Esto significa que cualquiera puede trabajar con el código fuente y que todos los datos son interoperables, por lo que pueden trasladarse fácilmente a otros proveedores.

Los proveedores de los EE.UU. al contrario siempre crean dependencia. Las autoridades estadounidenses pueden acceder en cualquier momento a los datos almacenados en los centros de datos de Microsoft, Google o AWS, incluso si estos centros están localizados en Europa. Además, Donald Trump podría utilizar estos servicios como herramienta

de negociación política. ¿Qué pasaría si la Administración Trump decidiera dejar de proporcionar actualizaciones a los clientes europeos?

¿Cómo garantiza Nextcloud que los datos de los organismos públicos españoles permanezcan bajo control europeo y no estén sujetos a legislaciones extranjeras?
Los usuarios, como las autoridades públicas, deciden dónde y cómo quieren alojar Nextcloud. Muchos clientes del sector público, por ejemplo, optan por instalar Nextcloud en sus propios servidores. Esto significa que no hay conexión con organizaciones no europeas sujetas a sistemas jurídicos diferentes. No es posible ser más conforme.
En España, entidades como la Xunta de Galicia, el Gobierno de Canarias o EducaMadrid ya utilizan Nextcloud.

¿Podría compartir aprendizajes o resultados concretos que hayan obtenido estas administraciones tras implantar su plataforma?
Las autoridades públicas son responsables de gestionar datos altamente sensibles de sus ciudadanos. Por lo tanto, la protección de datos y la prevención del acceso de terceros son máximas prioridades. Además, la plataforma debe ser fácil de usar para gestionar los procesos administrativos de manera eficaz. Una experiencia de usuario intuitiva y la escalabilidad son esenciales. En este sentido, la modularidad y el sistema personalizable de Nextcloud son de gran ayuda.
También recibimos comentarios de usuarios que nos cuentan lo sencillo que fue introducir una nueva plataforma de colaboración. Uno de nuestros clientes en España es, por ejemplo, Amnistía Internacional. Su equipo de activistas tenía conocimientos técnicos muy limitados, pero adoptó rápidamente la nueva tecnología. Antes de Nextcloud, les resultaba difícil colaborar y compartir documentos al escribir cartas a entidades gubernamentales. Sin embargo, una vez disponible Nextcloud, el equipo empezó a utilizar carpetas compartidas internas con sus colegas. También les resultó fácil compartir enlaces con activistas externos y pudieron trabajar desde casa.

¿Qué retos han encontrado en la implantación de Nextcloud en organismos públicos españoles y cómo los han superado?
Las soluciones existentes suelen estar profundamente integradas en los procesos y sistemas. Sin embargo, la migración no es un obstáculo insalvable, sino un proceso manejable. Ofrecemos asistencia para la migración y hay una serie de funciones de integración que permiten utilizar Nextcloud junto con otras soluciones, como Zoom, Teams o SharePoint.
Otra ventaja de Nextcloud que contribuye a su implantación es que se trata de una plataforma integrada con un diseño modular. Esto permite una adopción gradual de Nextcloud. Los clientes pueden empezar con Files para editar y compartir documentos antes de pasar a Groupware para gestionar correos electrónicos, calendarios y contactos. Después, pueden pasar a Nextcloud Office o Talk para chatear y hacer videoconferencias.

¿Cómo fomenta Nextcloud la colaboración con desarrolladores y empresas tecnológicas españolas para adaptar la plataforma a las necesidades específicas de nuestras administraciones?
El enfoque de código abierto de Nextcloud es una gran ventaja. Contamos con varios colaboradores españoles en nuestra comunidad. Por lo tanto, intercambiamos ideas con ellos con regularidad. Nuestros clientes también tienen la oportunidad de crear sus propios desarrollos y personalizaciones. Además, mantenemos un diálogo constante con ellos para definir juntos la hoja de ruta de desarrollo.

Usted ha defendido que Europa está lista para competir tecnológicamente y que es un mito pensar lo contrario. ¿Qué mensaje trasladaría a los responsables públicos que aún dudan de la capacidad de Europa para liderar en soluciones cloud y open source?
Muchas aplicaciones de empresas europeas de TI son competitivas y, a menudo, incluso mejores que las de las empresas tecnológicas estadounidenses. En realidad, estas grandes empresas tecnológicas no son tan innovadoras como mucha gente cree: rara vez crean cosas nuevas. Suele ser otras empresas las que desarrollan las innovaciones y las grandes tecnológicas las que compran o copian sus productos. La barrera para su uso no es la tecnología, sino una opción política.
No obstante, cada vez hay más casos que demuestran que es posible funcionar perfectamente sin proveedores estadounidenses y utilizar soluciones de código abierto. Algunos ejemplos son la ciudad de Lyon, el Ministerio de Economía de Austria y el estado federal de Schleswig-Holstein en Alemania.
Desde la cumbre de la OTAN, Donald Trump también ha amenazado a España. Las soluciones de código abierto refuerzan la resiliencia digital. El momento de aplicarlas es ahora.

¿Qué iniciativas o políticas considera prioritarias para que Europa y, en particular España, consoliden su independencia tecnológica en el sector público?
En primer lugar, Europa debe hacer cumplir sus propias normas. No me sorprende que seamos vulnerables al chantaje cuando oigo que la Comisión Europea quiere sacrificar legislaciones digitales como la Ley de Servicios Digitales y la Ley de Mercados Digitales para apaciguar a Donald Trump. Está claro que necesitamos una industria europea de TI fuerte.

Para conseguirlo, los gobiernos europeos deberían comprar más soluciones europeas. Los grandes proveedores estadounidenses también han crecido gracias a la adjudicación de importantes contratos gubernamentales. Curiosamente, una encuesta reciente de dos ONG revela que los ciudadanos son conscientes de la amenaza que supone nuestra dependencia de las grandes tecnológicas. En España, por ejemplo, más del doble de las personas encuestadas afirma que las grandes tecnológicas tienen un impacto negativo en la democracia europea que las que señalan un impacto positivo. La política tiene el respaldo de la ciudadanía para adoptar cambios al respecto.

Microsoft y Google están integrando inteligencia artificial en sus plataformas. ¿Qué planes tiene Nextcloud para incorporar IA de forma ética y alineada con los valores europeos de privacidad y transparencia?

La IA tiene el potencial de mejorar nuestras vidas. Sin embargo, solo será así si se alinea con nuestros valores. Por ejemplo, no debe discriminar, debe utilizar los recursos de manera eficiente, dar a los usuarios el control total sobre sus datos sensibles y no debe utilizarse en secreto para su formación.

Somos el primer proveedor de una plataforma de colaboración que integra un agente local de IA basado en estos criterios y ofrecemos a los usuarios una selección de modelos de IA de código abierto que pueden ejecutarse localmente. Los usuarios pueden resumir historiales de correo electrónico o chat, generar nuevos correos y respuestas, crear imágenes, traducir textos, transcribir videollamadas y mucho más. También colaboramos con algunas administraciones públicas para automatizar y simplificar determinados procesos especializados mediante el uso de la IA.

¿Cómo ve la evolución de la colaboración digital en el sector público europeo en los próximos cinco años y qué papel aspira a jugar Nextcloud en ese escenario?

Se acabó el tiempo de conformarse con las ofertas estadounidenses y los agresivos modelos de negocio de las empresas tecnológicas. Actualmente, asistimos a la aparición de la primera oleada de organizaciones públicas que se alejan de las grandes tecnológicas y exploran soluciones europeas de código abierto. Entre ellas se encuentran muchas universidades europeas, ciudades como Fráncfort, Ginebra o Lyon, y el estado federal alemán de Schleswig-Holstein. También se suman el Parlamento serbio y la policía islandesa.

Existen soluciones europeas adecuadas, como Nextcloud. Lo que necesitamos ahora es que los políticos decidan empezar a utilizarlas. Dentro de unos años, estoy seguro de que el sector público contará con una infraestructura tecnológica más diversa en la que el código abierto desempeñará un papel crucial.

Nextcloud se apoya en una comunidad open source activa. ¿Qué importancia tiene la comunidad en el desarrollo y seguridad de la plataforma, especialmente para organismos públicos que buscan máxima transparencia y control?

Nextcloud no existiría sin su comunidad y eso tiene un valor inmenso para nuestros clientes. Nuestro modelo de desarrollo abierto significa que nos beneficiamos de la contribución de un grupo mucho más amplio de personas inteligentes, creativas e innovadoras que nuestros ingenieros internos. Además, como ya trabajamos constantemente con personas externas a nuestra organización, colaborar estrechamente con los clientes u otros socios en las funcionalidades es algo que se nos da mucho mejor que a la mayoría de las empresas de TI. La tercera ventaja para los clientes es que la gran comunidad de miles de colaboradores les da la seguridad de que Nextcloud goza de buena salud y no depende de una sola empresa o cliente, ¡ni siquiera de la empresa Nextcloud!

Por supuesto, nuestro equipo de ingeniería se encarga de examinar y revisar todo el trabajo de la comunidad en un proceso estructurado. Nuestros clientes confían en nosotros para obtener un producto final empresarial, seguro y conforme a las normas, que pueden desplegar con confianza.

Dinero, talento, concienciación: principales retos de la ciberseguridad

Sin dinero no se puede invertir en tecnología ni en el talento necesario para gestionar la ciberseguridad, pero de nada sirve todo lo anterior sin llevar a cabo una buena política de concienciación. Esos son, a grandes rasgos, los principales retos de la ciberseguridad a los que se enfrentan ahora mismo buena parte de los responsables de seguridad de las diferentes administraciones públicas.

El reto de la ciberseguridad en las administraciones públicas españolas es, ante todo, un espejo de las transformaciones y fracturas que experimenta la sociedad digital, con factores presupuestarios, humanos, tecnológicos y organizativos en tensión permanente.

Así al menos se puso de manifiesto en un reciente encuentro ejecutivo de la comunidad ByTIC que patrocinaron Siedor y Eset, donde responsables de tecnología de distintas administraciones y expertos dibujaron un escenario lleno de dificultades estructurales y paradojas.

No es país sin presupuestos

La primera preocupación transversal es el presupuesto. Len Braga, subdirector de Tecnologías de la Información en INECO, lo anunciaba sin rodeos. "Para mí ahora mismo el principal reto es la finalización de los fondos de recuperación y la incertidumbre sobre si va a haber o no presupuestos generales del Estado. Si esto no se resuelve, la administración va a adolecer, especialmente en la parte de ciber, que es la última que ha llegado".

Según su experiencia, se ha invertido en servicios clave (desde SIEMs hasta Data Lakes) con fondos extraordinarios, pero nada garantiza la continuidad

cuando los recursos extraordinarios cesen. Para Braga, no existe por ahora una estrategia estatal que consolide la ciberseguridad como pilar estructural y no como simple resultado de la oportunidad de gasto. "El 2027 va a ser un año problemático si no hay un movimiento estratégico país".

Luis Samper, responsable de ciberseguridad en la Casa Real, ratifica ese diagnóstico, asegurando que "todos los organismos públicos estamos igual. Presupuestos congelados, esperando que llueva algo, y con la informática relegada siempre a la cola". Sin embargo, advierte también que "da igual el dinero que tengas" porque "hay entidades muy pequeñas que lo hacen muy bien y lo gestionan. No se puede asociar el dinero con las figuras de ciberseguridad, hay muchos factores". Esta idea, que desafía el lugar común de que más fondos implican automáticamente más seguridad, es uno de los leitmotivs recurrentes en el debate.

Hablamos de talento

Pero no solo la falta de presupuestos es uno de los principales retos a los quese enfrenta la ciberseguridad en las administraciones públicas españolas. De nuevo, el talento (o, más bien, la falta del mismo) vuelve a salir a la palestra.

La estructura salarial y las condiciones administrativas, otro punto crítico, pasan factura al reclutamiento y fidelización del talento en ciberseguridad pública. Víctor Balbás, Jefe de la División de Sistemas y Tecnologías de la Información - Ministerio para la Transición Ecológica y el Reto Demográfico, evidencia una brecha generacional y de capacitación preocupante. "El eslabón más débil en mi opinión son las personas. En la Administración General

del Estado, la edad media es bastante elevada y esto suele venir acompañado de mayor resistencia al cambio y peor adaptación a nuevas herramientas".

Además, reconoce que los nuevos perfiles que llegan son jóvenes, formados en lo digital, pero no lo suficientemente entrenados en cuestiones específicas del sector público. Y aún peor: "No somos competitivos en sueldo para atraer talento".

El problema trasciende a la propia administración y afecta también a los proveedores. Carlos Tortosa, Responsable de Grandes Cuentas Eset, define con crudeza una situación que no solo viven los organismos públicos, sino también los privados e, incluso, los propios proveedores de seguridad. "Nos cuesta muchísimo encontrar talento. Pocos y buenos. Una persona con ese talento posiblemente se vaya a Londres, a Ámsterdam, a Estados Unidos; el mercado nacional no está preparado para pagar esas cantidades". Por tanto, los esfuerzos por retener talento se ven lastrados no solo por el salario, sino por el propio atractivo del sector, donde la rotación y la fuga de cerebros son fenómenos constantes.

La cuestión de la formación y la concienciación del usuario ("el eslabón más débil" que citaba Balbás) articula buena parte de la conversación. Emilio González, responsable de sistemas en el Ayuntamiento de Alcorcón, subraya la dificultad de generar conciencia real. "Tenemos un problema de concienciación de los de arriba. Cuando hemos sido capaces de crear una política de seguridad y de aprobarla, que el responsable máximo sea nuestra alcaldesa ha supuesto que de repente exista una preocupación mayor


por todos estos temas, porque ya se ha subido a nivel de la corporación". En su ayuntamiento, los avances han sido posibles precisamente por esa implicación en la cúpula directiva.

Pero el compromiso personal no siempre basta. José Javier Marín, Jefe de área de la Dirección general de Infraestructura en Ministerio de Defensa, aporta su visión desde la experiencia militar de quien ha pasado por estos cuerpos durante muchos años de su trayectoria profesional. Según su experiencia, "hay que acreditar a la organización, pero empieza por la persona. Yo me he pasado 35 años como militar, y en el ejército funciona el 'búscate la vida'. Ahora, con 50, no es lo mismo. Necesitas formar a la gente, si no la formas no hay nada que hacer". Marín cree que la paciencia con el factor humano debe ser infinita. "No podemos pretender que todo el mundo tenga la misma conciencia que nosotros. Siempre será el factor humano el más débil de la ecuación. El mundo virtual tiene el problema de que no se percibe el peligro tan claramente como en el mundo físico".

Zonas grises

Pedro Alejandro Moreno, account manager en Seidor, subraya la complejidad de las zonas grises. "La pandemia nos llevó a securizar muchos equipos que no eran de las propias organizaciones. Cumpliendo la política de seguridad, no hay más remedio que pasar por ciertas soluciones, pero las fronteras entre lo personal y lo profesional se difuminan constantemente". En la administración, la permeabilidad de los dispositivos personales y la flexibilidad respecto a la norma generan riesgos añadidos que son difíciles de erradicar.

Willy Obispo, coordinador del CCMAD y con larga experiencia en la administración estatal, plantea una crítica al enfoque reactivo dominante. "Si esperas a que te ataquen para defenderte, te van a atacar primero; deberíamos ser proactivos, cambiar el momento, intentar ponerte por delante. Eso solo se consigue cambiando los procesos. Lo fundamental es que los procesos que se arrancaron perduren y mejoren, independientemente de las personas". Obispo reconoce que buena parte de la resiliencia digital de los ayuntamientos reside en la flexibilidad institucional y en una gestión que prioriza el compromiso más allá del cumplimiento formal. "Una certificación significa compromiso. Si desde arriba hacen esa tarea, me va a ser mucho más fácil concienciar a la organización porque ya están liderando el cambio", remarca.

Daniel Acuña, director de operaciones de ISDEFE, fue el encargado de introducir una nueva arista en la conversación: las presiones regulatorias. "Europa nos va a exigir pronto la transposición de su normativa y va a condicionar importantes progresos y mejoras en los sistemas de información. Ahí soy optimista". Pero alerta también sobre la responsabilidad de los directivos, incluso políticos, en las entidades públicas. "Antes era el CIO, ahora eres tú el responsable, y tienes que ser consciente de que eres tú el responsable. Cuando te aprietan, esa presión marca la diferencia".

Más inversión, ¿más defensa?

El debate en la celebración de este encuentro ejecutivo también dejó espacio para la relación entre inversión, tecnología y resultado en materia de ciberseguridad. Dado, sobre todo, que la jornada se inició con un lamento sobre la falta de presupuestos y la problemática que eso podía conllevar para todos los responsables de área, la pregunta lazada fue si tener más dinero para invertir en ciberseguridad conllevaba una correlación en estar más asegurado frente a las amenazas.

Rafael Carlos de Celada, coordinador de la gestión de pacientes y con experiencia en el sector hospitalario, plantea el desfase de los usos tecnológicos. "Conozco muchos casos donde la gente ni siquiera sabe que tiene un ecosistema digital entrelazado y que puede gestionarlo. Hay quienes no son conscientes de la protección del dato o de volcar datos de calidad en los sistemas. Inversión sí, pero formación y concienciación también. Todo debe ir de la mano".

En numerosos momentos de la discusión, los participantes pusieron sobre la mesa la dificultad de cubrir el ciclo completo de prevención, detección y respuesta ante incidentes. Luis Samper comparte un ejemplo claro: "Si hay una persona que recibe un correo malicioso y hace clic, el error gravísimo no es suyo, sino nuestro. Tenemos que hacer más cosas: los usuarios van a seguir cometiendo imprudencias, como quien pierde un punto del carné y sigue conduciendo". Este enfoque reparte la responsabilidad por toda la estructura de la organización.

Balbás refuerza la idea de responsabilidad compartida. "Los usuarios siempre pedirán más acceso, pero rara vez asumen la responsabilidad. Si conquisto el

compromiso de mi jefe, ya he ganado esa batalla. La facilidad para concienciar al personal depende totalmente de que la alta dirección asuma su parte".

En el plano técnico, salen a relucir las debilidades clásicas: desde tecnologías desfasadas o infraestructuras que no se renuevan ("el principio de los fondos nos ha permitido avanzar, pero ahora se están terminando y empezamos a ver el riesgo de retroceso", advierte Braga) hasta políticas poco adaptadas al entorno cloud y multiplataforma, donde la rapidez de adaptación es esencial. "Si funciona no lo toques" deja de ser un principio válido en un mundo digitalizado.

Va de personas

También surgen anécdotas que ilustran la profundidad de los riesgos. Carlos Tortosa narra el caso de una administración local que sufrió un incidente grave de seguridad. "El atacante había estado moviéndose por la red durante meses porque no tenían un EDR adecuado. Calculan que se llevó al menos 260 gigas de información". Para Tortosa, este incidente demuestra que la falta de tecnología básica y la conciencia del usuario son igual de peligrosas: "No es solo cuestión de política, sino de que el responsable de seguridad no estaba implicado".

La gestión de dispositivos personales y corporativos es fuente recurrente de incertidumbres. Moreno lo resume así: "Es tan clara la frontera entre lo profesional y lo personal, que aún hoy hay organizaciones en las que poner un USB implica un riesgo enorme". Aquí, la cultura de la seguridad choca con la comodidad o la resistencia al cambio, y la pedagogía nunca parece suficiente. "Conocemos las normas, pero todos las hemos incumplido alguna vez", asume.

Para muchos ponentes, la clave reside en el proceso más que en la persona. Obispo explica: "El primer enemigo soy yo mismo porque tengo acceso a más de lo que debiera. Por eso lo fundamental es primero restringirse a uno mismo y luego trabajar la cultura del cumplimiento, no solo de la concienciación". Frente a un contexto donde el usuario final sigue siendo la principal vía de acceso de los ciberdelincuentes

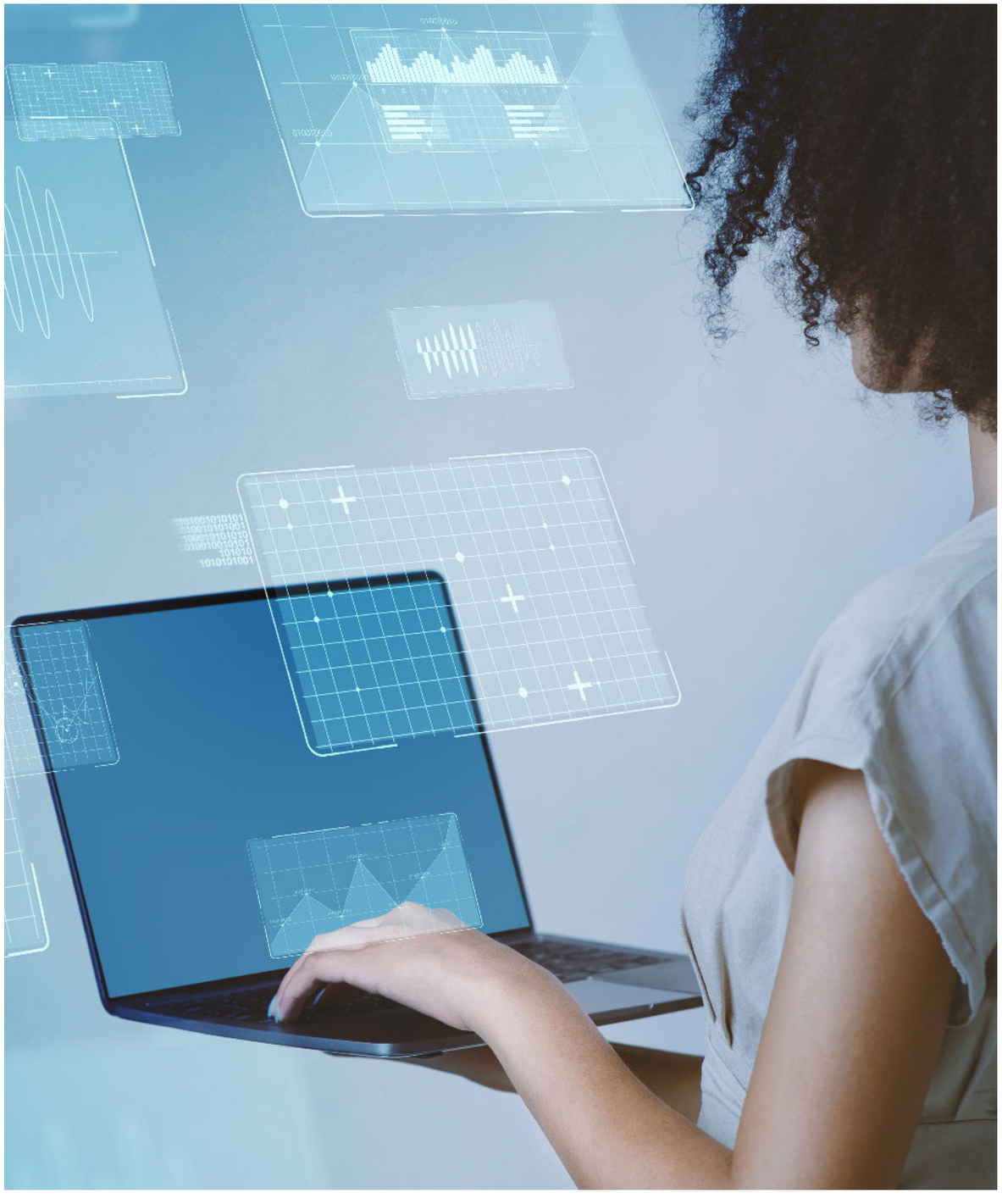
—"el gran vector de ataque sigue siendo el correo electrónico", confirma Samper—, la visión del experto gira hacia la arquitectura de los sistemas y la madurez de los procesos, entendidos como garantes de la seguridad.

A modo de síntesis de la cultura organizativa, Marín sentencia: "Todos somos nativos analógicos. Ahora unos están más concienciados, otros tienen más conocimiento, pero siempre el factor humano será la parte más débil de esta ecuación". Así, la realidad de las administraciones públicas en España denota avances notables, pero está profundamente condicionada por una suma de factores: ciclos presupuestarios imprevisibles, rigidez normativa, dificultad para retener talento, dependencia del compromiso directivo y la eterna batalla contra la fragilidad humana ante el riesgo digital.

Ahondando en el tema de la concienciación (por cierto, son numerosos los paralelismos que estos responsables realizan entre la seguridad y las normas de conducir), también sale a relucir la cuestión de quién debe liderar esta concienciación y hacer de poli bueno y poli malo. En palabras de Len Braga, "la concienciación no puede salir de la SGTIC, sino de la subdirección de personas, que sí tiene autoridad para cambiar comportamientos". Sin una implicación verdadera de toda la organización y una mirada estratégica (no oportunista= sobre la inversión, la ciberseguridad pública seguirá a expensas de la próxima crisis, del siguiente incidente mediático o de los vaivenes administrativos. El reto sigue siendo colectivo, multidimensional, y exige más que nunca un liderazgo comprometido y una ejecución determinante, no solo en la tecnología sino en la cultura y los valores compartidos.

TEMA DE PORTADA

La urgencia de gestionar datos propios



El futuro de la soberanía del dato en España pasará por innovar con control, regular con visión estratégica y construir alianzas que fortalezcan el entramado digital público, siempre con un foco firme en la protección, confianza y autonomía de la información que sustenta a la sociedad y sus instituciones.

La soberanía del dato se refiere al principio por el cual los datos están sujetos a las leyes y regulaciones del país o región donde se generan o almacenan. Esto implica que cada territorio tiene jurisdicción y autoridad sobre cómo se pueden utilizar esos datos y quién puede acceder a ellos.

Este concepto es clave en la gestión del dato porque determina el marco legal que protege la privacidad, regula el uso y garantiza la seguridad de la información, especialmente cuando los datos se almacenan o procesan en infraestructuras tecnológicas que pueden estar situadas en diferentes lugares geográficos.

La soberanía de datos es importante porque afecta directamente a la protección del derecho a la privacidad, la seguridad nacional y la confianza ciudadana en los servicios digitales. Al garantizar que los datos del país están bajo control local y regulaciones propias, se evita que actores externos puedan tener acceso no regulado a información sensible.

Asimismo, también permite cumplir con normativas como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que establece fuertes requisitos para la gestión de datos personales. De manera práctica, la soberanía del dato resguarda la autonomía tecnológica, defiende los intereses estratégicos del país y permite usar la tecnología para innovar sin sacrificar el control ni la transparencia sobre la información pública y privada.

Se trata de un concepto que resulta aún más crítico en el caso de las administraciones públicas, puesto que esta soberanía es crítica para asegurar que los datos de los ciudadanos y de las instituciones se manejan con total responsabilidad, evitando riesgos derivados del

acceso transfronterizo o de la transferencia de información a terceros países con regulaciones diferentes. Además, es fundamental para mantener la confianza en los sistemas públicos digitales y en la seguridad de los servicios públicos que dependen intensamente del dato.

Por todo ello, la soberanía del dato se ha convertido en un eje central de las políticas tecnológicas y de transformación digital en las administraciones públicas, pues establece los parámetros para que estos organismos gestionen la información con total control, cumpliendo con las leyes nacionales y europeas y preservando la autonomía frente a proveedores externos.

Gestión pública

La gestión de datos públicos es una responsabilidad inherentemente vinculada a la soberanía de las naciones. En España, donde el despliegue digital de las Administraciones Públicas avanza de manera acelerada, asegurar que los datos sensibles de los ciudadanos permanezcan bajo control nacional y europeo es una preocupación constante que involucra tecnología, regulación y una clara voluntad política.

"Las Administraciones Públicas son las auténticas responsables de garantizar que los datos de los ciudadanos se custodian en cada momento con las máximas garantías posibles," explica Alfredo García, responsable de Ventas para el Sector Público en NetApp Iberia. "No se trata únicamente de almacenamiento físico en territorio nacional; más bien, se trata de gobernanza, trazabilidad y disponibilidad frente a cualquier contingencia".

José Luis López Rodríguez, senior director OCI de Oracle España, coincide e incide en que la administración debe establecer marcos regulatorios claros y exigir a los proveedores estándares estrictos en protección y trazabilidad para los datos críticos. "La Administración Pública debe desempeñar un papel clave en garantizar que los datos públicos se gestionen con soberanía y dentro de nuestras fronteras". Desde Microsoft, fuentes responsables afirman que sus centros de datos europeas y su plataforma Microsoft Cloud for Sovereignty responden directamente a esta necesidad, permitiendo a las entidades públicas almacenar y procesar datos con altos estándares de seguridad bajo control local y europeo.

Esta demanda de soberanía no solo es un imperativo tecnológico, sino también de confianza social. No en vano, la información digital es la base de muchos de los servicios que ya consideramos esenciales, por lo que la percepción ciudadana respecto al control y protección de sus datos se transforma en un activo intangible pero fundamental para la gobernabilidad y la legitimidad digital.

La dependencia externa, un escollo complejo

A pesar de esta prioridad, España y la Unión Europea mantienen relaciones complejas con grandes proveedores internacionales de tecnología y servicios en nube.

Históricamente, la dependencia de plataformas cloud estadounidenses ha generado inquietudes respecto a la exposición a normativas extraterritoriales, como el Cloud Act, que permiten a Estados Unidos acceder a datos almacenados incluso en Europa, bajo condiciones que pueden vulnerar la legislación europea. Este conflicto significativo entre el Reglamento General de Protección de Datos (RGPD) y la Ley Cloud Act ha impulsado la búsqueda de alternativas soberanas y de infraestructuras cloud que garanticen control efectivo y respeto a la normativa europea.[

Oracle ha abordado esta tensión mediante la creación de una entidad jurídica europea que aloja datos dentro del territorio nacional y de la Unión, garantizando la soberanía sin renunciar a la innovación global. "Combinamos la innovación global con el cumplimiento normativo local," aclara José Luis López Rodríguez, explicando que esta aproximación permite equilibrar los beneficios tecnológicos con la garantía legal y operativa requerida.

Las arquitecturas híbridas, que combinan infraestructuras locales con nubes públicas, aparecen como el modelo predominante para afrontar este desafío. Alfredo García destaca que "cada vez más organizaciones adoptan arquitecturas híbridas que combinan infraestructuras locales con nube pública, garantizando flexibilidad sin renunciar al control". Este enfoque permite funcionar con eficiencia y escalabilidad, al tiempo que se asegura que los datos más sensibles permanezcan bajo jurisdicción europea y control directo.

Las regulaciones europeas marcan el ritmo

Resulta obvio decir que la creciente complejidad normativa europea, que, más allá del RGPD, incluye regulaciones determinantes para la soberanía de datos, establece el marco no solo normativo, sino también tecnológicos, que todas las partes deben seguir.

El Reglamento de Gobernanza Europea de Datos (Data Governance Act), vigente desde septiembre de 2024, busca establecer un marco común para facilitar la reutilización de

TEMA DE PORTADA

datos públicos protegiendo derechos y la confianza. Prevé, además, sanciones específicas para incumplimientos y regula el proceso administrativo para solicitar la reutilización, apuntando a procedimientos ágiles y transparentes.

Mientras, la Ley de Datos Europea (Data Act), que entró en vigor en 2025, redefine la titularidad funcional del dato, otorgando a usuarios derechos exclusivos de acceso y uso, y estableciendo mecanismos para que las autoridades públicas puedan acceder a datos bajo condiciones estrictas en emergencias o situaciones de interés público. Esto fomenta un acceso responsable y equitativo en el sector público, pero requiere que las infraestructuras y proveedores cumplan con altos estándares de privacidad y control.

Por su parte, el Reglamento DORA (Digital Operational Resilience Act), especialmente relevante para el sector financiero, impone medidas estrictas para gestión de riesgos TIC, gestión y notificación de incidentes, pruebas periódicas de resiliencia y supervisión de proveedores críticos, buscando robustecer la resiliencia operativa de sistemas críticos con impacto sistémico.

La normativa NIS2 amplía el alcance al sector público y sectores críticos, con obligaciones de gestión de riesgos, planes de continuidad y notificación rápida de incidentes, incluyendo sanciones que pueden superar los 10 millones de euros para entidades esenciales.

Estas normativas elevan el listón regulador y obligan a las AAPP a adoptar nuevas políticas, tecnologías y procesos, generando un marco que demanda altos niveles de gobernanza, auditoría y control que deben acompañarse de capacidades tecnológicas adecuadas.

¿Es la tecnología un pilar fundamental para la soberanía?

Aunque es cierto que muchas veces los proveedores tecnológicos, especialmente norteamericanos, han expresado sus quejas por esta complejidad normativa del marco europeo, no es menos cierto que estas mismas voces se erigen en muchas ocasiones como las herramientas que pueden garantizar el cumplimiento de las leyes.

Las soluciones tecnológicas específicas son mostradas como herramientas indispensables para materializar la soberanía. La combinación de cifrado avanzado, inmutabilidad de datos, recuperación ante incident

es, y replicación en múltiples ubicaciones controladas es cada vez más habitual. NetApp, por ejemplo, promueve su plataforma ONTAP como motor para asegurar que las infraestructuras híbridas y multicloud mantengan la soberanía sin perder elasticidad ni capacidad de innovación: "Garantizamos que la protección

y gestión se mantenga bajo control local," dice Alfredo García.

Oracle enfatiza el valor de las nubes soberanas, cifrado extremo a extremo y gestión avanzada de identidades como elementos inseparables para cumplir con los requisitos regulatorios y asegurar la trazabilidad e integridad del dato. Su estrategia contempla integración fluida con aplicaciones cloud para impulsar la innovación dentro del marco soberano.

Microsoft alude a tecnologías como Azure Confidential Computing, que permiten el análisis y explotación de datos sensibles sin exponer su contenido, ofreciendo así un equilibrio entre explotación de inteligencia artificial y protección de privacidad. Su enfoque híbrido es destacado por fuentes de Microsoft como la mejor opción para equilibrar innovación y cumplimiento normativo en la administración pública española.

La inteligencia artificial añade un valor fundamental reforzando la defensa frente a ciberamenazas mediante detección avanzada y automatización en la aplicación de políticas de seguridad, especialmente en entornos híbridos y multicloud complejos.

Espacio para la innovación dentro del cumplimiento

De igual manera, y aunque muchas veces se han tildado estas normativas como constringentes de la innovación, lo cierto es que estas leyes marcan cómo deben [también los organismos públicos] ser innovadores y útiles, pero respetando la legalidad.

En este sentido, ñas administraciones públicas deben desarrollar capacidades que les permitan innovar sin abandonar el cumplimiento exigido por nuevas regulaciones. El reto está en gestionar la complejidad de arquitecturas integradas que unen sistemas legados con modernas soluciones cloud, en un entorno normativo robusto pero evolutivo.

Alfredo García señala que esta integración es complicada: "La coexistencia de sistemas heredados con nuevos multiplica costes y dificulta la operación" y la importancia de la formación y capacitación en competencias digitales para estos entornos.

Desde Oracle y Microsoft se impulsan marcos de políticas públicas claros que definan estándares sobre clasificación, cifrado, gestión de identidades y auditoría, junto al desarrollo conjunto de herramientas y certificaciones que aportan confianza continua al sector público, facilitando la innovación segura y controlada.

Una característica común en las respuestas es la necesidad de construir una alianza efectiva entre administraciones y sector privado. José Luis López Rodríguez sostiene que "el modelo debe combinar la necesidad regulatoria de la administración con la agilidad y experiencia del sector tecnológico". Alfredo García añade que la colaboración debe ir más allá del suministro de tecnología, implicando cocreación en arquitecturas, estándares y adaptación normativa.[1][2]

Microsoft resalta que esta relación se debe basar en transparencia, formación continua y responsabilidad compartida para maximizar la autonomía del sector público sin generar dependencias prolongadas. Esta cooperación es vital para equilibrar innovación, cumplimiento y soberanía, creando ecosistemas abiertos y plurales capaces de dar respuesta a las crecientes demandas del sector público y la sociedad.

Formación y transferencia de conocimiento

Más allá de entregar tecnología, las empresas tecnológicas asumen un rol en transferir conocimiento y capacitar a los equipos públicos para gestionar con autonomía los datos soberanos.

NetApp desarrolla programas de formación y acompañamiento que buscan ampliar las competencias en la gestión de infraestructuras híbridas y multicloud, clave para mantener la soberanía. José Luis López Rodríguez concluye que "es imprescindible compartir innovación, conocimiento y herramientas abiertas para que las administraciones gestionen sus datos sin perder autonomía".

Microsoft resalta la apuesta por estándares abiertos e interoperabilidad como condición para mantener la evolución tecnológica sin quedar atadas a un único proveedor. La sostenibilidad de la soberanía digital requiere un equilibrio dinámico entre capacidades internas, apoyo externo y soluciones que promueven la independencia y seguridad.

Medidas técnicas y organizativas

Evidentemente, para poder hacer un buen compliance de la soberanía del dato, hay que tener en cuenta varias medidas técnicas y organizativas.

En el caso de las administraciones públicas, estas medias se centran en garantizar que los datos se gestionan y almacenan con control absoluto dentro de las fronteras nacionales o bajo marcos legales estrictos. Según José Luis López Rodríguez, senior director de OCI Oracle España, la

administración pública debe establecer marcos regulatorios claros e impulsar infraestructuras cloud seguras que exijan a los proveedores altos estándares en protección, disponibilidad y trazabilidad de la información crítica.

En el plano tecnológico, las plataformas que combinan seguridad avanzada, cifrado de datos de extremo a extremo, gestión de identidades, automatización de cumplimiento y herramientas de observabilidad son vitales. Oracle integra estas capacidades para garantizar protección sin sacrificar innovación, apoyándose en nubes soberanas y soluciones híbridas que permiten flexibilidad y control.

NetApp destaca el uso de tecnologías con cifrado avanzado e inmutabilidad nativa, como su plataforma ONTAP, para asegurar que los datos públicos estén siempre disponibles, protegidos y bajo control de la administración. Además, soluciones con inteligencia artificial ayudan a detectar anomalías en tiempo real, fortaleciendo la defensa contra amenazas como ransomware. La automatización y orquestación garantizan que las políticas de protección se apliquen de forma homogénea en todos los entornos, incluso en arquitecturas híbridas y multicloud. Por ejemplo, NetApp ofrece capacidades como Autonomous Ransomware Protection y SnapMirror para replicación y recuperación inmediata de datos en entornos soberanos.

Microsoft subraya la importancia de contar con centros de datos locales que cumplen con el Esquema Nacional de Seguridad y garantizan almacenamiento y procesamiento de datos dentro del territorio nacional y europeo mediante soluciones como Microsoft Cloud for Sovereignty. Aquí, la clave está en definir políticas públicas claras con estándares para clasificación, cifrado y control de accesos, junto a contratos con garantías, auditorías independientes y certificaciones nacionales e internacionales. Esta combinación técnica y organizativa permite aprovechar la innovación de la nube y la inteligencia artificial sin perder el control de los datos.

Las barreras señaladas por los responsables tecnológicos coinciden en que la coexistencia de sistemas heredados y modernos, junto al déficit de talento especializado, complican la integración y aumentan costes operativos. También se destaca la necesidad de una colaboración público-privada sólida, inversión sostenida y desarrollo de infraestructuras diseñadas específicamente para soberanía. A nivel normativo, regulaciones como DORA y NIS2 elevan las exigencias en gobernanza y ciberseguridad, lo que refuerza la necesidad de soluciones que simplifiquen la gestión, aseguren trazabilidad y garanticen el cumplimiento.

Cómo BIM y GIS ayudaron al Ayuntamiento de Madrid en el soterramiento de la A5

A lo largo de los últimos años, la integración de tecnologías avanzadas en la gestión y ejecución de infraestructuras públicas ha cambiado de manera radical la forma en que las administraciones españolas afrontan proyectos complejos y estratégicos. Atrás quedaron las barreras asociadas a la dispersión de datos, la falta de trazabilidad en obra o los procesos de decisión fragmentados. Hoy, herramientas como BIM (Building Information Modeling) y GIS (Geographic Information Systems) han permitido a los equipos municipales, empresas de ingeniería y proveedores tecnológicos operar bajo una lógica profundamente colaborativa, optimizando cada fase del ciclo de vida de los activos públicos y generando una nueva cultura de eficiencia, transparencia y servicio.

El caso de la A-5, impulsado por el Ayuntamiento de Madrid en colaboración con CEMOSA y Esri España, revela el alcance y las posibilidades de esta transformación digital. Los responsables municipales, desde el principio, buscaron dotar al proyecto de "una visión integradora que fuera más allá de la mera digitalización de planos o documentos", priorizando la coordinación multidisciplinar, la accesibilidad a la información y la capacidad de anticipación ante incidencias urbanas. "Nuestra meta era no solo facilitar la gestión técnica, sino también acercar la obra pública al ciudadano, convirtiendo la información técnica en valor social y operativo", resume uno de los portavoces del Ayuntamiento.

Integrar múltiples fuentes

Este enfoque estratégico encontró su aliado natural en la tecnología. Cristina Carrera, Team Leader de UtilitiesAEC en Esri España, describe el papel de su plataforma como "la infraestructura geoespacial sobre la que se articulan los datos del proyecto, estableciendo un único punto de acceso y habilitando una metodología altamente colaborativa". Al integrar información proveniente de múltiples fuentes (como entornos comunes de datos tipo Autodesk Construction Cloud, sensores, aplicaciones para toma de datos en campo o drones), el sistema GIS permitió eliminar los tradicionales silos departamentales y dotar de eficiencia a la gestión pública.

La interoperabilidad, según Carrera, constituye la piedra angular de esta nueva era. "ArcGIS ofrece no solo capacidades de visualización en 2D y 3D, sino una extensa batería de herramientas de análisis espacial que pueden operar tanto en escritorio como en web. Esto nos ha permitido situar los modelos BIM del proyecto en su contexto urbano real: el trazado actual de la A-5, la red de transporte adyacente, la ocupación del suelo, la topografía y la planificación urbana". La comprensión técnica (tanto de ingenieros como de gestores) se ve enriquecida por la posibilidad de comunicar, de forma clara y visual, cómo las actuaciones afectan a la globalidad de la ciudad. Herramientas avanzadas, como cuadros de mando interactivos y visores de acceso público, han materializado esta transparencia de forma tangible para la ciudadanía.

Para los equipos de obra y asistencia técnica, la integración BIM-GIS ha significado una profundización inédita en la capacidad de análisis y decisión. Desde CEMOSA, fuente crucial en el desarrollo metodológico, destacan los beneficios de contextualizar los modelos constructivos a través del GIS. "Transformar los planos técnicos en información situacional ha sido clave" explican, especialmente para "identificar afecciones reales en el entorno urbano, anticipar impactos sobre la movilidad, emergencias o el comercio local y tomar decisiones urbanas con mayor solidez".

Una de las herramientas emblemáticas ha sido la aplicación desarrollada por CEMOSA, capaz de superponer modelos 3D, cámaras de tráfico y capas de información de obra en tiempo real, optimizando la planificación de desvíos y la comunicación con la ciudadanía.
"No se trata solo de monitorizar el avance geolocalizado de la obra; se trata de que todos los perfiles técnicos y ciudadanos dispongan de herramientas adaptadas a sus necesidades para consumir la información en tiempo real", apunta uno de los responsables de CEMOSA. Así, la plataforma interactiva estructurada por áreas técnicas, con acceso a mapas, escenas 3D y documentación actualizada, ha revolucionado la forma en que el cuerpo técnico y el Ayuntamiento abordan la trazabilidad de cada fase del proyecto.

Gobernanza y colaboración

Este salto cualitativo no es fruto exclusivo de la tecnología, sino también de la gobernanza y la visión compartida entre los distintos actores. "El éxito de la colaboración reside en haber establecido un marco claro de roles, una comunicación fluida y una priorización constante de funcionalidades realmente útiles para los ciudadanos" subrayan desde CEMOSA.
La apuesta decidida del Ayuntamiento de Madrid por la digitalización, unida al soporte técnico y la capacidad de adaptación de Esri, ha permitido una integración sin fisuras y ha reducido la complejidad inherente a proyectos de esta envergadura.
La medición del retorno de la inversión, objetivo central para cualquier administración, encuentra correlato directo en los resultados operativos. "El uso combinado de BIM y GIS nos está permitiendo realizar análisis comparativos entre el estado actual y las propuestas de diseño, anticipando interferencias y optimizando siempre las decisiones previas a la ejecución", reconoce CEMOSA. Este enfoque, orientado a la anticipación y la minimización del error, ha permitido no solo reducir costes, sino también acortar plazos, incrementar la calidad y aumentar la seguridad.
Cristina Carrera confirma que la experiencia de integración tecnológica en proyectos como este ya ha dejado patente beneficios tangibles. "Estamos viendo cumplimiento —e incluso reducción— de los plazos de entrega; mayor coordinación entre técnicos, operarios y subcontratas; cumplimiento y seguimiento riguroso de medidas medioambientales; y una mayor transparencia, tanto con el cliente como con el ciudadano". Además, añade, "la reducción de la huella de carbono, gracias a la optimización de rutas y una gestión integral más eficiente, es uno de los valores añadidos más claros de la digitalización".
El alcance de las mejoras va más allá de la obra. En la fase de operación y mantenimiento, la plataforma permite inventariar activos, auscultar estructuras y actualizar información técnica de forma georreferenciada, algo esencial para el mantenimiento actualizado de infraestructuras complejas.
En palabras de Carrera, "la tecnología es esencial para manejar la cantidad ingente de datos que se genera día a día y establecer un marco colaborativo sólido entre cliente, asistencia técnica, constructoras, subcontratas y ciudadanía".
En este escenario, y mirando de cara al futuro, CEMOSA considera que "la integración BIM-GIS va camino de convertirse en un requisito estratégico, más que en una opción técnica. No se trata solo de saber qué construir, sino de saber dónde y con qué impacto sobre la ciudad, los servicios y las personas". Su estrategia de digitalización integral se apoya en el desarrollo de soluciones propias, la formación continua y la colaboración activa con administraciones y líderes tecnológicos, siempre con la vista puesta en estándares abiertos e interoperabilidad. La administración, a su vez, confirma que el avance hacia la gobernanza abierta, apoyada en plataformas intuitivas y accesibles, es una senda irreversible. El papel del ciudadano, entendido ahora como usuario activo y partícipe del proceso, se potencia al disponer de información interactiva en tiempo real sobre desvíos, avance de obras y afecciones al entorno. Esta comunicación, bidireccional y transparente, contribuye a una mayor confianza social y refuerza el control institucional sobre los costes, la seguridad y la calidad. En lo cotidiano, la eficacia de los nuevos procesos digitales se traduce en aspectos concretos y medibles. "Entre las mejoras más destacadas que estamos encontrando está la mayor coordinación entre los agentes implicados", aseguran desde CEMOSA. Algo que está "facilitando la visualización conjunta de modelos y datos geoespaciales". El uso combinado de BIM y GIS ha permitido realizar análisis complejos, optimizar recursos durante la planificación de espacios públicos y garantizar una ejecución mucho más eficiente.

Los retos

Esta revolución no viene exenta de retos. La complejidad de la coordinación multidisciplinar, el volumen de datos y la necesidad de protocolos alineados son retos constantes en la aplicación de tecnologías disruptivas a la obra pública, algo que los equipos han ido resolviendo con metodologías de roles definidos, validaciones recurrentes y, sobre todo, una cultura de mejora continua.
Al mirar hacia adelante, tanto CEMOSA como Esri identifican la consolidación del gemelo digital (con la combinación de BIM, GIS y datos en tiempo real) como horizonte estratégico. "La integración de datos en tiempo real mediante sensores, la aplicación de inteligencia artificial y la analítica predictiva serán claves para anticipar necesidades y mejorar la resiliencia urbana", afirma Carrera. La digitalización aborda así todo el ciclo de vida de la infraestructura, de la planificación y el diseño, a la operación y el mantenimiento, transformando las ciudades en entornos más sostenibles y centrados en las personas.
Esta experiencia, mejora los procesos y la eficiencia, y además proyecta a las instituciones hacia un nuevo paradigma de servicio público basado en la transparencia, la anticipación y el valor añadido para la sociedad.

TENDENCIAS

IA, gemelos digitales, edge computing: ¿por qué la industria necesita infraestructuras locales potentes?

Por Youssef Nadiri, Jefe de producto y BDM Ciudades y espacios inteligentes en PNY Technologies

La aceleración de la inteligencia artificial (IA) en la industria depende de infraestructuras de hardware y software adaptadas, capaces de soportar cargas de cómputo masivas, en local, en tiempo real y con una fiabilidad absoluta. En este contexto, el modelo centralizado de la nube, aunque omnipresente, muestra sus límites y no puede responder por sí solo a las exigencias operativas y regulatorias de la industria. Por ello, las infraestructuras locales vuelven a situarse en el centro de las estrategias de despliegue de la IA industrial.

Latencia, confidencialidad, soberanía: criterios determinantes

La IA se integra de manera casi natural en los procesos industriales. En casos como el control de calidad asistido por visión, la robótica inteligente o el mantenimiento predictivo, una latencia excesiva puede comprometer la precisión de las decisiones automatizadas e incluso generar riesgos operativos.

Más allá de los aspectos técnicos, las estrictas exigencias regulatorias en materia de seguridad y confidencialidad obligan a las empresas industriales a mantener un control total sobre sus flujos de datos. En sectores estratégicos como la salud, la defensa o la energía, externalizar datos hacia nubes públicas, a menudo sujetas a jurisdicciones extraterritoriales, no es una opción viable. Las infraestructuras locales permiten conservar el control absoluto de los datos al tiempo que garantizan el cumplimiento de las normativas locales de seguridad.

Gemelos digitales: la convergencia entre simulación, IA y edge computing

El auge de los gemelos digitales ilustra perfectamente esta necesidad de potencia local. Una encuesta de McKinsey mostró que el 86% de los directivos industriales identifican aplicaciones concretas en la implementación de gemelos digitales dentro de sus organizaciones, y casi la mitad ya habrían iniciado su despliegue. Estos entornos virtuales permiten simular cadenas de producción, predecir fallos y optimizar el mantenimiento de sistemas complejos.

Pero esta transformación solo es posible gracias a infraestructuras locales de alto rendimiento, que aseguran coherencia en tiempo real y reducen los riesgos asociados a la externalización del procesamiento. Para garantizar la fluidez entre la simulación y la realidad, el tratamiento debe realizarse donde se generan los datos: en el edge o en centros de datos locales, próximos a la producción.

Una arquitectura híbrida: datacenter local, edge e IA distribuida

La IA industrial evoluciona hacia arquitecturas híbridas que combinan centros de datos locales, edge computing e IA distribuida. Esta convergencia permite un procesamiento inteligente, seguro y en tiempo real de los datos industriales. Ante las crecientes necesidades de flexibilidad, agilidad y soberanía, las infraestructuras deben ser más inteligentes y capaces de evolucionar rápidamente. Las empresas dependen de un ecosistema que gestione el cómputo, se integre con entornos de código abierto y se adapte a las

particularidades de cada emplazamiento industrial.

Controlar la infraestructura para controlar la IA

Durante años, la nube pública se presentó como la solución ideal para ejecutar modelos de IA, pero sus límites son evidentes en aplicaciones industriales críticas. Las arquitecturas híbridas, que combinan centros de datos locales, edge computing e IA distribuida, permiten procesar datos en tiempo real y mantener el control sobre los flujos de información.

El edge computing desempeña un papel clave al posibilitar que las empresas procesen los datos donde se generan, optimizando recursos y reduciendo la dependencia de soluciones centralizadas. Estas tecnologías están siendo adoptadas masivamente para acelerar las cargas de trabajo de IA. Según un estudio de IDC patrocinado por NVIDIA, las empresas invierten en servidores acelerados por GPU para responder a las crecientes exigencias de la IA. La inversión mundial en servidores con GPU pasó de 6,9 mil millones de dólares en 2020 a 10,3 mil millones en 2022. El desafío actual para la industria es construir infraestructuras capaces de explotar todo el potencial de la IA, manteniendo un control total sobre los datos y procesos.

Construir las bases de una IA soberana, escalable y resiliente

El futuro de la IA, tal y como se perfila hoy, no será totalmente en la nube ni totalmente on-premise. Será híbrido, capaz de combinar la potencia de los centros de datos locales, la proximidad del edge y la agilidad de la nube. Para los industriales más avanzados, es esencial contar con socios tecnológicos de confianza que aporten experiencia en software y conocimiento de los entornos industriales, y que ofrezcan arquitecturas adaptadas a múltiples escenarios: centros de datos tradicionales, microcentros en edge computing o infraestructuras modulares embebidas. Así, las empresas industriales obtienen un soporte estratégico alineado con sus exigencias de flexibilidad, seguridad y escalabilidad.

GRACIAS

contacto@bytic.es | www.bytic.es