BYTIC MEDIA

NÚMERO 41 | NOVIEMBRE 2025

Hiperconvergencia en la Administración Pública

ENTREVISTA

María Isabel Urrutia, consejera de Presidencia y Simplificación Administrativa de Cantabria

TENDENCIAS

El apagón que señaló una brecha: Replanteamiento de la ciberseguridad

AI-NATIVE PREVENTION FOR TOMORROW'S DIGITAL THREATS

www.eset.es

ESET® Cybersecurity
Progress. Protected.

TABLA DE CONTENIDOS

ByTIC Media - Sobre nosotros 03

Comité de expertos- 05

Actualidad 07

Entrevista María José Urrutia,
consejera de Presidencia y
Simplificación Administrativa de Cantabria 15

Entrevista Lucas Ferrera Hernández,
gestor de proyectos TIC en el Cabildo de Gran Canaria 18

Entrevista Andrés Martín
Líder de Sector Público en Celonis 21

Encuentros
Sostenibilidad y eficiencia de procesos en la Administración 24

Tema de portada
Hiperconvergencia en la Administración Pública 27

Caso de éxito
TMB confía en ACKstorm su infraestructura cloud 33

Tendencias
Replanteamiento de la ciberseguridad en el sector público 35

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

Orange y el Ayuntamiento de Madrid ponen en marcha la primera burbuja táctica 5G SA para emergencias

Orange y el Ayuntamiento de Madrid han desplegado la primera burbuja táctica 5G SA operativa en España. Esta red privada 5G de última generación permitirá a los Cuerpos de Seguridad y Emergencias comunicarse de forma fiable, segura y efectiva incluso en situaciones críticas como incendios forestales o catástrofes naturales.

Esta nueva red, una de las primeras en Europa, representa un paso decisivo en la digitalización de las comunicaciones críticas en servicios esenciales ya que la red 5G Stand Alone (SA) garantiza comunicaciones de alta disponibilidad, baja latencia y máxima seguridad.

La solución se apoya en la red existente y se refuerza, cuando es necesario, mediante unidades móviles con conectividad vía satélite, capaces de mantener el servicio incluso si las estaciones base han sido destruidas por el fuego.

Apoyados en Ericsson y Nemergent

La colaboración entre Orange y el Ayuntamiento de Madrid se ha articulado mediante una licitación pública en la que se ha valorado la capacidad técnica del operador. El proyecto, respaldado por socios tecnológicos como Ericsson y Nemergent Solutions, especialistas en comunicaciones seguras y gestión de redes privadas, se financia con fondos NEXTGEN EU gestionados por el Ministerio de Transformación Digital y Función Pública, en el marco de las iniciativas de modernización y digitalización de los servicios públicos.

Esta iniciativa posiciona a Madrid como referente en el uso de tecnologías 5G para la gestión de

emergencias, y abre la puerta a futuras aplicaciones en movilidad urbana, protección civil y grandes eventos. La solución de Orange, con vehículos de intervención rápida equipados con tecnología 5G SA y conectividad satelital, permite restablecer las comunicaciones en tiempo récord, asegurando la operatividad de los servicios de emergencia en cualquier escenario. Estos vehículos, además de operar en frecuencias comerciales, incluyen bandas reservadas para emergencias (B68), lo que garantiza un canal exclusivo para los cuerpos de seguridad, incluso en situaciones de alta congestión de red.

Conectividad al servicio de la seguridad ciudadana

La red privada 5G desplegada en Madrid utiliza las bandas de 700MHz (n28) y 3,5GHz (n78), e incorpora funcionalidades avanzadas como el slicing de red y la priorización del tráfico de emergencias. Esto permite que Policía Municipal, SAMUR y bomberos del Ayuntamiento mantengan sus comunicaciones críticas incluso en eventos multitudinarios o situaciones de emergencia extrema.

Por ejemplo, los equipos de bomberos podrán retransmitir vídeo en tiempo real desde las cámaras instaladas en sus cascos o vehículos de intervención rápida. Esta capacidad permitiría al centro de mando recibir imágenes en directo del interior de edificios afectados por incendios o de zonas de difícil acceso, facilitando la evaluación inmediata de riesgos, la localización de víctimas y la toma de decisiones críticas para la seguridad de los efectivos y la eficacia del rescate. Además, la baja latencia y la alta disponibilidad de la red garantizan que la comunicación audiovisual no se interrumpa, incluso en escenarios de alta congestión o con infraestructuras dañadas.

Esta infraestructura ya contempla y hará efectivo también, el control remoto de drones en operaciones BVLOS (más allá del alcance visual del piloto), permitiendo retransmisión de vídeo en tiempo real desde zonas de difícil acceso, por ejemplo, durante un incendio, lo que mejora la toma de decisiones rápidas sobre el terreno.

Este enfoque integral convierte a Madrid en el primer municipio español en contar con una infraestructura de red de emergencias con cobertura real y operativa, más allá de entornos de prueba.

Una solución replicable para la España vaciada

La falta de cobertura y conectividad en zonas poco habitadas sigue siendo un obstáculo para la coordinación de efectivos en situaciones de emergencia. La solución desplegada en Madrid puede ser replicada en otras comunidades autónomas, especialmente en áreas rurales o de difícil acceso, donde la conectividad es limitada.

Gracias a su capacidad de despliegue rápido y conectividad satelital, esta tecnología puede ser clave para mejorar la respuesta ante incendios forestales, rescates o catástrofes naturales en la España vaciada. Con esta iniciativa, Orange se posiciona, una vez más, a la vanguardia en innovación, ofreciendo soluciones tecnológicas que garantizan la seguridad de todos los ciudadanos, estén donde estén.

"Este proyecto marca un hito en la modernización de los servicios de emergencias en España puesto que garantiza comunicaciones seguras e ininterrumpidas en los escenarios más exigentes y sitúa a Madrid a la vanguardia europea en innovación al servicio de la seguridad ciudadana. Estamos comprometidos con ofrecer soluciones robustas, escalables y preparadas para salvar vidas, reforzando así nuestro papel como aliado estratégico de las administraciones públicas", afirma Joaquín Colino, director de General de B2B en MasOrange.

Editorial

La sostenibilidad es un imperativo ineludible para las administraciones en la gestión de los procesos tecnológicos. La digitalización ha sido clave para modernizar servicios, pero la creciente demanda energética de centros de datos puede convertirse en un lastre para la transición ecológica si no se aborda con criterios responsables. La Comisión Europea estima que, si no se adoptan medidas efectivas, los centros de datos podrían consumir hasta un 3,2% de la electricidad total en la UE para 2030.

El Ministerio para la Transición Ecológica ha impulsado diferentes regulaciones para exigir a estos centros reportes detallados sobre consumo energético, uso de energías renovables y eficiencia en refrigeración, siguiendo la Directiva comunitaria 2023/1791.

La sostenibilidad es un apartado importante, sobre todo cuando hay muchos procesos anticuados y las administraciones deben liderar este cambio adoptando infraestructuras de cloud, reforzando la compra sostenible y racionalizando recursos tecnológicos para minimizar la huella digital.

Invertir en eficiencia energética no solo reduce costes, sino que también mitiga la presión sobre las redes eléctricas y contribuye a cumplir con los compromisos climáticos. Más allá de la tecnología, se requiere rediseñar procesos para optimizar recursos y evitar residuos digitales innecesarios. La digitalización responsable convierte a la administración en un referente ético y funcional, imprescindible para un futuro sostenible y resiliente.

Asturias agiliza la administración con la aplicación de inteligencia artificial en la contratación pública

La Administración del Principado de Asturias da un paso decisivo en su proceso de modernización con la incorporación de Tendios, una plataforma desarrollada para mejorar la gestión pública y los servicios que prestan las administraciones basada en inteligencia artificial que transformará la gestión de la contratación pública.

La herramienta permitirá automatizar tareas clave, como la elaboración de memorias justificativas o la redacción de pliegos rectores de la contratación, reduciendo los tiempos de tramitación y optimizando el proceso de licitación.

"La inteligencia artificial no es un fin, sino una palanca para mejorar la calidad de los servicios públicos. Con su aplicación en la contratación, avanzamos hacia una Administración más ágil, transparente y orientada a las personas", ha destacado la vicepresidenta y consejera de Presidencia, Reto Demográfico, Igualdad y Turismo, Gimena Llamedo.

Administración sin trabas

Esta actuación se enmarca en la Estrategia de Transformación Digital del Principado de Asturias, coordinada por la Dirección General de Estrategia Digital e Inteligencia Artificial, que tiene como objetivo situar a la comunidad como referente en innovación administrativa y en la guerra contra la burocracia.

Además, la implantación de esta tecnología refuerza el cumplimiento del Decreto 98/2025, que regula el uso de la inteligencia artificial en la Administración del Principado, y responde a los principios de simplificación,

seguridad y transparencia recogidos en la normativa autonómica.

Con la implantación de esta plataforma, los órganos de contratación podrán generar pliegos en minutos, analizar documentación de manera automatizada y gestionar expedientes con mayor eficiencia y trazabilidad. La inteligencia artificial facilitará, asimismo, el análisis predictivo, la detección de oportunidades y la elaboración automática de informes, garantizando procesos más abiertos, competitivos y con mayores garantías jurídicas.

El Gobierno de Asturias refuerza así su compromiso con una Administración sin trabas, en la que la tecnología se pone al servicio de la ciudadanía para ahorrar tiempo, ganar eficiencia y ofrecer servicios más proactivos, especialmente en los ámbitos con mayor carga burocrática.

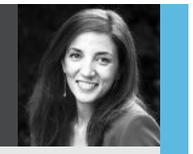
Esta medida forma parte de la hoja de ruta de transformación digital que impulsa el Principado, junto con otras iniciativas como la digitalización de los procedimientos administrativos, la sede electrónica avanzada o el despliegue del marco ético y de seguridad para el uso de la inteligencia artificial, aprobado este mismo año.

Formación y uso responsable de la inteligencia artificial

Además de aplicar la inteligencia artificial en los procesos administrativos, el Principado apuesta por formar a su personal público en el uso seguro y eficiente de estas herramientas. En este contexto, la Dirección General de Estrategia Digital e Inteligencia Artificial ha puesto en marcha el programa "Domina Copilot Chat", desarrollado en colaboración con Microsoft, que ofrecerá sesiones formativas periódicas sobre las aplicaciones prácticas de la IA en el trabajo diario. El objetivo es que el conjunto del personal empleado público aprenda a utilizar la inteligencia artificial como apoyo a sus tareas cotidianas, mejorando la productividad, el trabajo colaborativo y la calidad del servicio a la ciudadanía.

Con iniciativas como Tendios y Domina Copilot Chat, Asturias avanza hacia una Administración moderna, transparente y cercana, capaz de responder con agilidad a las necesidades de empresas y ciudadanía, y de situar la innovación al servicio del bien común.

La opinión de Arantxa Herranz

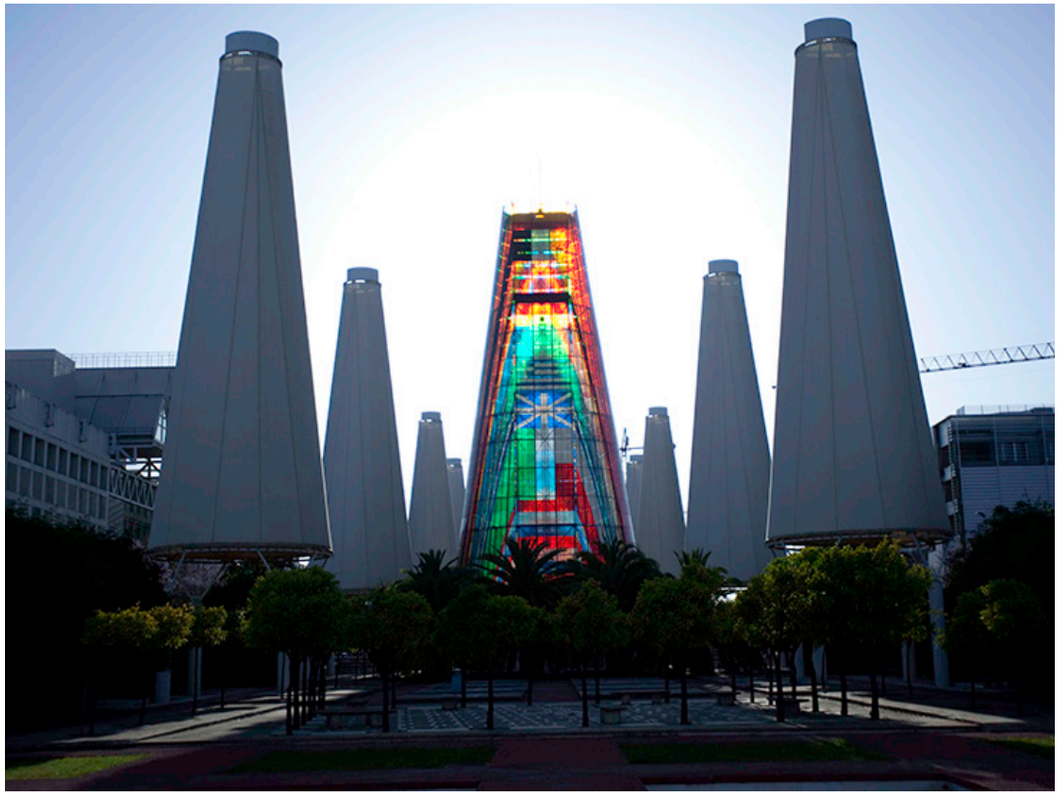


La confianza en la inteligencia artificial parece un camino empedrado de excusas. Cuando un sistema falla, cuando se produce un error o una cadena de los mismos, cuando algo no funciona, la culpa recae en "la informática". Una etiqueta amplia, casi mítica, que sirve para diluir responsabilidades (aunque siempre habrá quien diga que el problema no es el sistema informático, sino la persona que lo implementó, no vaya a ser que la culpa recaiga en el ingeniero que la ideó).

Es cierto que los algoritmos no despiertan un día con mala intención; operan dentro de los límites que los humanos les imponen. Cuando se dice que "es un error informático", en realidad lo que ha ocurrido es que alguien (un ingeniero, un equipo, una organización) diseñó mal el sistema o no previó las consecuencias. Pero reconocer eso implica admitir que el error no es de la máquina, sino de las personas que la crean, la implementan o la supervisan.

Hasta que no asumamos esa responsabilidad compartida, será difícil confiar de verdad en la inteligencia artificial. La confianza no se construye con discursos sobre innovación o eficiencia, sino con transparencia, control y rendición de cuentas.

Los proyectos de movilidad, energía y TIC de eCitySevilla, con 19,8 millones, se licitarán en 2026



El Consejo de Gobierno ha tomado conocimiento de las actuaciones en materia de movilidad, TIC y eficiencia energética de la Junta de Andalucía que se incluyen en el proyecto de Compra Pública de Innovación (CPI) eCitySevilla, que se lleva a cabo en el parque científico y tecnológico Sevilla TechPark y que se licitarán durante el primer semestre de 2026.

Estas intervenciones, que cuentan con una inyección económica de 19,8 millones de euros procedentes del programa Andalucía Feder 2021-27, contemplan desde la implantación de sistemas de alumbrado público inteligente hasta pilotos de robótica para limpieza urbana, pasando por servicios de autoconsumo compartido o sistemas de logística de última milla para mercancías.

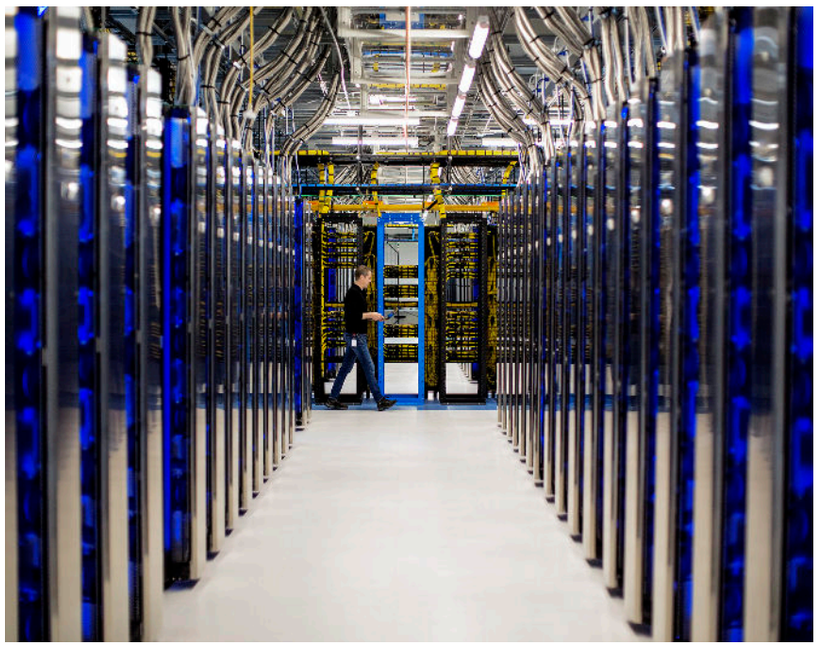
La iniciativa eCitySevilla está promovida por la Junta de Andalucía a través de las consejerías de Universidad e Industria, el Ayuntamiento de Sevilla, el propio parque científico y tecnológico y Endesa y a la que están adheridas 94 empresas del recinto; y tiene como objetivo transformar ese enclave en un ecosistema abierto, digital, descarbonizado y autosuficiente energéticamente. Dicha acción pretende anticipar los retos a los que deberán enfrentarse las ciudades del futuro mediante proyectos pioneros en los que convergen los sectores de la energía, el agua, el transporte y la edificación, apoyados por las tecnologías de la información y la comunicación.

El impulso económico de la Consejería de Universidad permitirá implementar las actuaciones contempladas mediante la fórmula de Compra Pública de Innovación, que es un novedoso sistema de contratación con el que la Junta de Andalucía pretende satisfacer una demanda de servicios y productos avanzados aún no disponibles en el mercado, fomentando las respuestas de la iniciativa privada. Con ello se reforzará, por tanto, la colaboración público-privada. En los últimos meses, se han lanzado las consultas preliminares al mercado de todas ellas, que es el proceso mediante el cual se puede conocer las soluciones innovadoras disponibles, informar a los operadores económicos de sus planes y requisitos futuros y preparar la licitación.

En ese conjunto de acciones se incluye un servicio de autoconsumo compartido y de recursos de energía distribuidos, con el que se busca aplicar nuevos modelos de negocio aprovechando los mercados energéticos de flexibilidad que no están desarrollados todavía. También destaca el impulso de un piloto de transporte eléctrico autónomo de personas, que posibilitará cambiar rutas y frecuencia de servicio en función de la demanda. De igual modo, se prevé impulsar un sistema de logística de última milla para mercancías con automatización avanzada que conllevará la creación de nuevas infraestructuras de almacenamiento y transportes automatizados. En este listado se encuentran, igualmente, una iniciativa centrada en la infraestructura digital del parque, una plataforma de datos y un sistema de alumbrado púbico inteligente.

A todo ello se suma, entre otros, la puesta en marcha de un piloto dirigido a mejorar los procesos de limpieza y mantenimiento del viario y espacios comunes del recinto tecnológico, así como el desarrollo de un sistema de gestión anticipada de eventos y emergencias. Todas esas actuaciones se aplicarán en las 200 hectáreas que conforma el parque, concebido como una ciudad en sí misma que alberga 575 entidades con 31.667 empleados y un impacto económico de 5.513 millones de euros.

Microsoft amplía su nube soberana y sus servicios



Microsoft ha anunciado un refuerzo de sus capacidades en nube soberana, asegurando que extiende y profundiza las garantías de residencia y control de datos dentro del perímetro europeo.

La propuesta de Microsoft Sovereign Cloud integra una doble vertiente: una nube pública soberana (con la que asegura garantizar la residencia y el procesamiento íntegro de datos en centros de datos europeos) y una nube privada soberana (que facilita la innovación mediante inteligencia artificial avanzada y mayor escalabilidad).

Esta estrategia se articula sobre un consejo de administración europeo que supervisa las operaciones de los centros de datos en cumplimiento exclusivo con la legislación europea, además de la reciente expansión de capacidad en centros de datos en países como Austria y Bélgica.

De este modo, Microsoft pretende mitigar las preocupaciones de soberanía vinculadas al uso de servicios en la nube gestionados por proveedores no europeos. No en vano, la confianza en proveedores de tecnología extranjeros sigue siendo un tema crítico para las administraciones públicas, en especial en la Unión Europea, donde la soberanía digital y el control sobre los datos tienen un peso regulatorio y estratégico cada vez mayor.

De extremo a extremo

Una de las novedades fundamentales es el procesamiento de datos de inteligencia artificial de extremo a extremo dentro del Perímetro de Datos de la Unión Europea.

Esto implica que todos los datos, tanto en reposo como en tránsito, permanecen alojados y procesados solo en territorio europeo salvo indicación expresa del cliente. Para las administraciones públicas esta garantía es indispensable para cumplir normativas como el GDPR y otras regulaciones específicas relacionadas con la protección, acceso y localización de datos. La extensión que Microsoft hace del procesamiento local para Microsoft 365 Copilot a 15 países (incluyendo España para 2026) refuerza esta narrativa de soberanía, al ofrecer procesamiento local de las interacciones con IA integrada en las herramientas de productividad.

En el plano técnico, la actualización de Sovereign Landing Zone, basada en la arquitectura Azure Landing Zone, proporciona una estructura jerárquica para la gestión de políticas y despliegue de controles de soberanía, simplificando la adopción de medidas regulatorias y asegurando la coherencia en el cumplimiento normativo. Esto resulta especialmente útil para las administraciones públicas que gestionan arquitecturas complejas con múltiples grupos administrativos y requieren estandarizar mecanismos de control.

La nube privada soberana, representada por Azure Local, también ha recibido mejoras significativas destinadas a facilitar cargas de trabajo intensivas en IA. La incorporación de la GPU NVIDIA RTX Pro 6000 Blackwell enable la ejecución de más de mil modelos de IA, desde GPT hasta modelos open source, permitiendo a las entidades públicas aprovechar la innovación en inteligencia artificial sin comprometer la protección de datos. Además, la ampliación de Azure Local para sostener clústeres de hasta cientos de servidores, junto con soporte para Storage Area Network (SAN), ofrece la flexibilidad necesaria para escalar entornos privados soberanos robustos y conectados a infraestructuras locales existentes.

Las operaciones desconectadas, con disponibilidad para 2026, suponen una innovación crucial para las entidades con altos requerimientos de control y resiliencia, al permitir la gestión segura y local de múltiples clústeres de Azure Local desde un plano de control totalmente local. Esta funcionalidad es especialmente relevante para administraciones públicas con entornos muy regulados o despliegues en ubicaciones remotas, donde la continuidad y la independencia operativa son esenciales.

Adicionalmente, Microsoft ha establecido una especialización en soberanía digital para sus partners, apoyando un ecosistema europeo que no solo se beneficie de las capacidades técnicas sino también de garantías de cumplimiento rigurosas, incluyendo auditorías y certificaciones focalizadas en residencia de datos y privacidad.

Navarra pone su Cybersecurity Center y el Polo Iris al servicio de la ciberseguridad

El consejero de Universidad, Innovación y Transformación Digital de Navarra, Juan Luis García, ha subrayado "la importancia de la colaboración público-privada para el impulso de áreas como la digitalización y la ciberseguridad, con el objetivo de que las empresas navarras crezcan, se fortalezcan y puedan desarrollar su actividad en un entorno más sólido y seguro".

El consejero García ha defendido este modelo en la apertura del 5o Foro Navarra de Seguridad Digital NASEC 2025, organizado por el Clúster de tecnología y consultoría ATANA, que se ha celebrado en Baluarte bajo el título '¿Sabes cómo blindar tu futuro en el mundo digital?'.

En su intervención, ha destacado que la misión tanto del Gobierno de Navarra como de las sociedades públicas es "acompañar, reforzar y hacer partícipe al sector privado de cada avance tecnológico", poniendo en valor el papel de dos agentes facilitadores como el Polo Iris y el Navarra Cybersecurity Center.

"Estos agentes abren puertas, coordinan recursos y canalizan el talento hacia el tejido empresarial. En el Polo, un 89% de los proveedores son empresas privadas. Y el Navarra Cybersecurity Center colabora, al igual que lo hace el Gobierno de Navarra, con empresas, asociaciones y clústeres", ha señalado.

Asimismo, ha llamado a las empresas a realizar un esfuerzo para poder absorber el talento generado en centros educativos, centros de FP y universidades navarras en vocaciones tecnológicas, como la ciberseguridad. "Todo este talento no pertenece al Gobierno ni tan siquiera a las universidades, pertenece a Navarra en su conjunto y debe encontrar su lugar natural en las empresas", ha resaltado.

De igual manera, ha invitado al tejido empresarial a cooperar para "reforzar el conjunto del ecosistema tecnológico" de la Comunidad Foral. "Los ciberataques son ya una amenaza real para nuestra economía, nuestra seguridad y, en definitiva, para nuestra confianza. Por eso, desde el Gobierno de Navarra estamos impulsando que la ciberseguridad sea una prioridad estratégica", ha destacado.

Durante el resto de la jornada, más de una decena de personas de diversas empresas y entidades han realizado breves ponencias en las que han compartido sus experiencias y casos de éxito en temas como el marco regulatorio actual, estrategias y retos del futuro, ciberamenazas, ciberseguridad en compañías e industria o ciberdelitos.

Final de la I Semana Navarra de la Ciberseguridad

El 5o Foro Navarra de Seguridad Digital NASEC 2025 ha supuesto el punto final de la primera Semana de la Ciberseguridad, una iniciativa organizada por el Navarra Cybersecurity Center [NavCC] que ha contado con más de 20 actividades gratuitas enfocadas a diferentes públicos y programadas en distintas localidades de la geografía foral.

No obstante, los actos continuarán con el espectáculo itinerante del mago Jorge Luengo titulado 'La ciberseguridad no es cosa de magia... ¿o sí?', que contará con funciones en el Teatro Gaztambide de Tudela, el próximo 3 de noviembre; en el Centro Cultural Tafalla, el día 4; en el Teatro Gayarre, el día 5; para finalizar la gira el 12 de noviembre en el espacio Cultural Los Llanos de Estella-Lizarra.

El objetivo de las actividades, que han ido desde la celebración de foros sobre ciberseguridad al mencionado espectáculo de magia, pasando por espacios itinerantes de formación, charlas técnicas, talleres especializados y competiciones, ha sido concienciar y sensibilizar a la ciudadanía navarra sobre la importancia de la ciberseguridad coincidiendo con la celebración del Mes Europeo de la Ciberseguridad.

La JCYL extiende la implantación de cruces inteligentes a 15 tramos de su red autonómica para reforzar la seguridad

La Junta de Castilla y León continúa avanzando en su compromiso con la seguridad vial y la atención a las necesidades reales de los ciudadanos, implantando medidas en la red viaria autonómica. En esta línea, la Consejería de Movilidad y Transformación Digital ha desarrollado 15 actuaciones en tramos de vías autonómicas con el objetivo de reducir la siniestralidad y modernizar la red de carreteras.

Dentro de estas actuaciones, el consejero de Movilidad y Transformación Digital, José Luis Sanz Merino, ha visitado hoy la finalización de las obras de un nuevo sistema de cruce inteligente en la carretera CL-527, a la altura de la localidad zamorana de Villar del Buey, que cuenta con un presupuesto de 48.008 euros. Allí ha subrayado que "las actuaciones de la Junta no se miden solo en cifras, sino en su capacidad para mejorar la vida de las personas. Cada intervención que realizamos en materia de seguridad vial responde a una necesidad concreta y busca prevenir accidentes y salvar vidas".

La actuación ha permitido mejorar la seguridad de la intersección entre la CL-527 y los accesos a Villar del Buey y Muga de Sayago, un punto con elevada peligrosidad, mediante la instalación de un sistema de advertencia dinámica que alerta a los conductores de la presencia de vehículos en los accesos.

La intervención surgió a raíz de la solicitud del Ayuntamiento de Villar del Buey, tras registrarse un accidente en la zona en 2024. La Junta decidió dar una respuesta eficaz y sostenible, apostando por una solución tecnológica, moderna y adaptada al entorno rural. Además del cruce inteligente, se ha actuado en la señalización, los arcenes y el pavimento, aplicando medidas experimentales que siguen las recomendaciones de la Dirección General de Tráfico (DGT). Se han implantado ya 15 cruces inteligentes en ocho provincias de Castilla y León. En la provincia de Zamora ya existía una intervención de este tipo en la ZA-104, en el P.K. 1+500.

Sanz Merino ha incidido en que "la seguridad vial no depende solo de grandes

infraestructuras, sino de la capacidad de escuchar y actuar allí donde los vecinos lo necesitan. Este es un ejemplo de cómo la Junta trabaja para dar soluciones reales a problemas reales".

La obra forma parte de la línea de actuaciones que la Junta impulsa en toda la Comunidad para implantar soluciones inteligentes de seguridad vial, con especial atención a las zonas rurales y tramos con mayor siniestralidad, reforzando la seguridad, la conectividad y la calidad de vida de los ciudadanos.

Inversiones en Zamora

La inversión prevista para el año 2025 en materia de carreteras supera los 10.600.000 euros en Zamora, con proyectos como el nuevo puente sobre el río Valderaduey, en la ZA-512, entre los puntos kilométricos 0+980 y 2+985, por valor de 2.285.252 euros, con un plazo de ejecución de 10 meses.

ENTREVISTA

María Isabel Urrutia,

consejera de Presidencia y Simplificación Administrativa de Cantabria

"El éxito de un proyecto es mejorar la administración o tener impacto real en los ciudadanos"

María Isabel Urrutia es la consejera de Presidencia, Justicia, Seguridad y Simplificación Administrativa del Gobierno de Cantabria. Licenciada en Derecho por la Universidad de Cantabria y en Ciencias Políticas y de la Administración por la UNED, ha desempeñado cargos relevantes en la administración cántabra, entre ellos la dirección del Instituto Cántabro de Servicios Sociales (ICASS) entre 2011 y 2015. Además, ha sido diputada del Parlamento de Cantabria en varias legislaturas, lo que le ha permitido acumular una amplia experiencia en gestión pública y política regional.

Como consejera de Presidencia y Simplificación Administrativa, Urrutia lidera la modernización de la administración pública cántabra, impulsando la digitalización y la reducción de trámites para ciudadanos y empresas. Entre sus logros más recientes destaca la aprobación de la nueva Ley de Simplificación Administrativa, que elimina trámites obsoletos, agiliza procesos y facilita la actividad económica en la región. Su gestión ha sido reconocida tanto a nivel autonómico como europeo, especialmente por su papel en la defensa de los intereses regionales en foros clave de la Unión Europea

¿Cuáles son las principales iniciativas tecnológicas que está impulsando su consejería para modernizar la administración pública?

La Ley de simplificación administrativa de Cantabria, aprobada el pasado 2 de abril de 2025, y su desarrollo reglamentario es, en la actualidad, uno de los proyectos principales de la acción de la Consejería de Presidencia, Justicia, Seguridad y Simplificación Administrativa del Gobierno de Cantabria.

En el ámbito tecnológico, esta Ley de simplificación prioriza las siguientes acciones:

- Optimización del gestor de expedientes corporativos, hoy en uso, de cara a ofrecer una mejor información al ciudadano sobre sus expedientes, a la vez que se mejoran las funcionalidades internas para agilizar la gestión.
- Creación de un espacio personalizado para ciudadanos y empresas en la sede electrónica de nuestra Administración y su integración con la carpeta ciudadana.

- Ofrecimiento proactivo de servicios públicos personalizados, a partir de la información disponible en la carpeta ciudadana y la utilización de aplicaciones móviles para hacer más fácil y accesible la relación entre los ciudadanos y la administración
- Creación de la Carpeta Empresarial en la que se integrarán todas las relaciones administrativas que se produzcan a lo largo de la vida de la empresa.
- Puesta en funcionamiento de una Plataforma de Gobernanza de Datos.
- Impulso del establecimiento de cuadros de mando que, junto con la Plataforma, tiene el objeto de proporcionar información real y permanentemente actualizada sobre el funcionamiento de los trámites y procedimientos.
- Potenciación de la Plataforma de Intermediación para garantizar el acceso a la información requerida por parte de los diferentes órganos y unidades de la Administración.
- Apoyo a la Digitalización de las Entidades Locales con el fin de que éstas puedan facilitar la accesibilidad de vecinos y empresas a los servicios públicos.
- Utilización de la Inteligencia artificial aplicada a la simplificación administrativa para fomentar el crecimiento económico y la mejora en la atención de los servicios públicos.

Fuera de este contexto, desde la Dirección General de Informática, dependiente de esta consejería, se está trabajando principalmente en garantizar la seguridad y disponibilidad de los sistemas de información corporativos. Igualmente, a primeros del mes de noviembre empezaremos los trabajos de renovación de los puestos de usuario corporativo con objeto de adaptarlos a la realidad tecnológica actual, fomentando el uso generalizado de portátiles y herramientas de colaboración, entre el personal de la administración.

En el contexto de la simplificación administrativa, ¿qué papel juegan las tecnologías emergentes como la IA y la automatización de procesos?

En el Gobierno de Cantabria no SOMOS ajenos a las novedades que, constantemente, se producen en el ámbito de las nuevas tecnologías y resulta absolutamente impensable que la Administración no se adapte ni utilice todos los medios a su alcance para facilitar al máximo las relaciones con los ciudadanos.

La ley de simplificación administrativa de Cantabria contiene, precisamente, una mención expresa al uso de la inteligencia artificial aplicada a la simplificación administrativa.

El uso de las tecnologías emergentes nos sirve para la automatización de algunos trámites de los procedimientos a fin de conseguir que nuestra administración sea más eficiente, además de permitirnos implantar un entorno de trabajo más ágil y adaptable para los empleados públicos, aunque siempre habrá trámites en los que la actuación del empleado público sea insustituible, si bien siempre podrá apoyarse en la tecnología para mejorar la precisión en la toma de decisiones.

¿Qué medidas se están implementando para garantizar la protección de datos ciudadanos en los procesos de digitalización?

En el Gobierno de Cantabria tenemos clarísima nuestra prioridad: garantizar la protección de los datos, una adecuada utilización de la información y garantizar los derechos de los ciudadanos en la protección de los datos que ponen a nuestra disposición. Esta prioridad ineludible tenemos que hacerla compatible con el uso de las tecnologías informáticas dada su utilidad para mejorar los servicios que prestamos a los ciudadanos y la eficiencia que nos aportan.

Desde el Gobierno de Cantabria hemos aprobado una Política Integral de Seguridad de la Información y una Organización competencial para la Protección de Datos Personales y para el desarrollo de nuestros sistemas informáticos que tiene en cuenta el Esquema nacional de seguridad informática.

La gestión de la protección de datos, al igual que la de la seguridad de la información, la entendemos como un proceso integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información, descartándose cualquier actuación puntual o tratamiento coyuntural.

Esta gestión implica directamente tanto al personal especialista en tecnología, como a los gestores con capacidad de decisión sobre la información o los servicios prestados, así como al resto de personas que usan o acceden de algún modo a los sistemas de información.

Por ello, prestamos la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni el desconocimiento, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

¿Cómo se está formando al personal público en materia de seguridad digital?

También en esta materia estamos en continua formación a los empleados públicos y en información a los ciudadanos que se relacionan con la administración. De hecho, desde nuestra Dirección General de Informática contamos con un servicio específico de seguridad de la información, que es el que marca la línea de acción en esta materia.

Esta Dirección General, con la colaboración de nuestro centro de formación de los empleados públicos, el Instituto Cántabro de Administración Pública que está adscrito a esta consejería, establece la estrategia de formación, tanto para el personal tecnológico como para el conjunto de los empleados del Gobierno que se refleja en

los programas anuales de cursos de formación que se ponen a su disposición. Asimismo, periódicamente, y a través del correo corporativo, se envían mensajes de aviso, advertencia, información o recordatorio sobre las principales medidas en materia de seguridad.
Y, muy recientemente, hemos puesto en funcionamiento una herramienta sobre formación informática accesible desde todos los puestos de trabajo. Una aplicación totalmente accesible desde el escritorio de todos los puestos de trabajo del personal al servicio de la administración.

¿Cuáles son los principales proyectos tecnológicos piloto que se están desarrollando en su consejería?
Actualmente tenemos pilotos en múltiples áreas con objeto de adecuar nuestros sistemas a las futuras tendencias.
Entre los más destacados tenemos los orientados a la aplicación de la inteligencia artificial en la mejora de procesos internos (automatización de tareas de negocio, migraciones tecnológicas de aplicaciones, etc.)

¿Cómo ve el futuro de la administración pública española en términos de transformación digital en los próximos 5 años?
No se puede plantear una mejora de los servicios públicos sin una transformación digital de estos. Y, creo, que esta es una idea que está plenamente arraigada en todos los sectores de la Administración pública. Estoy convencida de que tenemos una grandísima oportunidad para conseguir lo que llevo años escuchando, lustros diría yo, la modernización de la administración; y va a venir de la mano de la digitalización.
En Cantabria tenemos absolutamente claro que debemos impulsar un cambio profundo en la forma de trabajar de nuestra Administración. Y en ello estamos implicados desde nuestra llegada al Gobierno hace ya dos años.
También creo que la incorporación de las nuevas generaciones va a posibilitar este cambio de forma normalizada, porque es una generación digital que ha nacido y vivido con las tecnologías.
Pero nosotros ya estamos trabajando en ello por convencimiento. Se acabó el lema "siempre se ha hecho así" Queremos que nuestra Administración no actúe de espaldas a los ciudadanos. Queremos una Administración abierta, accesible, cercana y colaboradora con ciudadanos y empresas porque estos son los que crean empleo y riqueza para nuestra región.
De ahí nuestro proyecto de simplificación administrativa que tiene uno de

sus grandes elementos en la mejora de los procedimientos y de los sistemas de comunicación y de intercambio de información que he comentado al principio. Cualquier herramienta digital que esté a nuestra disposición y que sirva para agilizar las relaciones entre Administración y ciudadanos será estudiada para ser implantada en Cantabria
Así mismo, venimos colaborando con los ayuntamientos de la región, especialmente con los más pequeños, para que también ellos puedan contar con las herramientas tecnológicas adecuadas que agilicen y faciliten las relaciones con empresas y autónomos.
La mejora, simplificación y racionalización de los servicios públicos debe ir, sí o sí, de la mano de una transformación digital. Y en ello los empleados públicos de todas las administraciones e instituciones van a jugar un papel clave.

¿Qué rol juega la colaboración público-privada en los proyectos de modernización tecnológica?
Con carácter general, cualquier contrato de prestación de servicios informáticos licitado por la Administración Pública es una forma de colaboración público-privada. Si la Administración decide contratar un bien o un servicio con una empresa, está solicitando de esta su colaboración en la consecución, directa o indirecta, de una finalidad pública.
En este sentido la colaboración entre el sector público y el privado es necesaria y, me atrevería a decir, que imprescindible.
En un sentido más estricto, la figura de contratación de "colaboración público-privada" es una vía más de contratación de la administración, que en determinadas ocasiones resulta ser la más adecuada para cubrir determinados proyectos de modernización tecnológica que por sus características no encajan con una contratación "tradicional".

ENTREVISTA

Lucas Ferrera Hernández,

gestor de proyectos TIC en el Cabildo de Gran Canaria

"Estamos perdiendo la oportunidad de fomentar el acceso al servicio público directamente en las universidades"

Lucas Ferrera Hernández es un referente en la gestión de proyectos TIC vinculados a la administración pública en Canarias, con una trayectoria consolidada en el Cabildo de Gran Canaria y el Gobierno de Canarias.

Funcionario de carrera, Ferrera ocupa la categoría de Técnico Superior de Informática (A1), desempeñando funciones de gestión y coordinación de proyectos tecnológicos en la administración pública insular y autonómica. Entre sus cargos más destacados figuran el de jefe de sección IT en el Gobierno de Canarias y Project Manager TIC en el Cabildo de Gran Canaria desde 2018 hasta 2022.

¿Cuáles son los principales retos tecnológicos que enfrenta el Cabildo de Gran Canaria en su transformación digital?

El Cabildo de Gran Canaria siento decir que, tecnológicamente, hemos perdido muchos años en los que no se le ha dado la importancia debida a este área, de ahí que nuestro margen de mejora sea brutal. Temas como la implantación de un gestor de expediente electrónico único, la atención omnicanal a la ciudadanía o la gestión del dato son algunos de los muchos retos tecnológicos a los que nos estamos enfrentando. A ellos se unen otros proyectos, igual no tan visibles, pero también fundamentales como la implantación de un sistema de dirección por objetivos, la adopción gradual de la Inteligencia Artificial o una apuesta clara por la ciberseguridad.

¿Cómo los aborda?

Hemos trazado una hoja de ruta que se plasma en el Plan Estratégico de Gobernanza e Innovación Pública (PEGIP), un plan que comenzó en 2021 y que fue redefinido a principios de 2025 para ir adaptándolo a las circunstancias del momento. Como ocurre muchas veces, los planes plurianuales sufren cambios, aparecen otras prioridades y cambian algunos proyectos. En realidad este es el primer plan estratégico de este tipo que aborda el Cabildo de Gran Canaria en este sentido, que, no solo aborda proyectos

estrictamente tecnológicos, sino también algunos algunos relacionados con la interacción con la ciudadanía, la formación y la gestión de recursos humanos. El PEGIP está impulsado desde el puesto directivo de Coordinación Insular del Área de Gobierno de Presidencia, Modernización e Innovación Administrativa y coordinado desde el Servicio de Coordinación, Modernización e Innovación Administrativa. Dispone de técnicos dedicados a su seguimiento y cuenta también con el apoyo de una oficina técnica externa.

¿Qué supone liderar proyectos TIC en una administración insular respecto a otras entidades públicas, en términos de coordinación y alcance?

Haber trabajado en administraciones distintas como el Gobierno de Canarias (en Justicia y en Hacienda), el Ayuntamiento de Las Palmas de Gran Canaria, uno de los 10 más poblados de España (en proyectos de modernización) y en el propio Cabildo de Gran Canaria (en áreas como tecnología, administración electrónica, microinformática, comunicaciones, transparencia o protección de datos) me da una buena visión del panorama TIC de las islas. Una administración insular como un Cabildo, que no tiene, ni de lejos, la cercanía con la ciudadanía como puede tener un ayuntamiento, tiene puntos en común con las administraciones de los otros niveles. Todas debemos contar con los mismos sistemas e infraestructuras, pero el Cabildo, por su naturaleza, debe ser un referente y un apoyo para los ayuntamientos de la isla Si bien, hasta ahora ese apoyo se traducía en la mera concesión de subvenciones para que los ayuntamientos adquieran servicios o productos tecnológicos, ahora mismo estamos inmersos en un interesante proyecto que aborda la depuración de datos del padrón de habitantes que tiene en Instituto Nacional de Estadística. Este proyecto implica la coordinación con 19 de los 21 municipios de la isla, con el INE, el Catastro y el organismo autónomo insular encargado de la gestión tributaria. Es el primer proyecto puramente tecnológico e interadministrativo que estamos abordando y está siendo todo un reto. En cualquier caso, también debo reconocer que el Cabildo de Tenerife, nuestra isla hermana, está mucho más avanzada en este aspecto y es capaz de prestar un apoyo técnico directo a los distintos ayuntamientos, por eso es bueno ver cómo lo están haciendo otras administraciones y, por supuesto, tomar nota y aprovecharnos de ese buen hacer. Afortunadamente, en las islas tenemos buena comunicación y entendimiento con los equipos TIC de los distintos Cabildos y Ayuntamientos.

¿Cuál es el mayor reto al que se enfrenta en estos momentos?

Pues creo que el mayor reto al que nos enfrentamos no es tecnológico, sino cultural y de organización. El manido "siempre se ha hecho así" aún sigue presente en algunas áreas. La descoordinación en algunas épocas entre departamentos TIC (tenemos dos) también ha supuesto un freno evidente al desarrollo tecnológico y la innovación. Lo bueno es que estamos en el camino para que todo esto cambie. Por un lado disponemos de liderazgo directivo a alto nivel, por otro, el área se ha reforzado con un departamento dedicado exclusivamente a la coordinación, modernización e innovación administrativa (que incluye áreas como la atención ciudadana o la gestión de archivo y documental). Este nuevo departamento supone la amalgama perfecta para los departamentos TIC, hasta ahora más centrados en el día a día, para que puedan disponer y verse reforzados de una gestión de proyectos y una visión estratégica de las TIC.

¿Cómo influyen los ciclos político-administrativos en la planificación tecnológica a largo plazo en el Cabildo y qué estrategias utiliza para minimizar el impacto de estos cambios?

Como comenté antes, nuestra planificación tecnológica realmente no existía antes de la puesta en marcha del PEGIP. Sin embargo, este plan estratégico ya ha superado, y con éxito, la transición entre dos ciclos políticos (aunque es cierto que del mismo signo). Yo creo que una vez iniciada esta senda, estos planes han venido para quedarse. Podrán tener una u otra denominación, pero dudo que hoy en día haya algún político que no entienda que el apoyo a la transformación digital y la innovación es algo imprescindible. Estos planes a largo plazo son difícilmente cancelables, no apoyarlos sería darse un tiro en el pie que haga que la organización retroceda o simplemente se quede atrás con la velocidad a la que se mueve el mundo. Los departamentos TIC ya no son aquellos que ponían ordenadores, creaban webs o instalaban aplicaciones para que los usuarios trabajaran. Hoy en día, la TIC forman parte del ADN de cualquier administración pública y deben contar con el apoyo adecuado, tanto en medios económicos como de personal y, por supuesto, con un apoyo y liderazgo directivo profesional, que esté al más alto nivel y en conexión directa con los máximos responsables.

¿Cómo aborda la falta de recursos y la necesaria profesionalización del personal responsable de la transformación digital en el Cabildo de Gran Canaria?

Si hablamos de recursos económicos, efectivamente todos los años es una lucha constante para conseguir fondos. Muchos proyectos, sobre todo los relacionados con infraestructuras tienen un coste elevado y no son proyectos "vendibles" porque no se suelen ver, aunque sean cruciales para el buen funcionamiento de la administración. Además, muchas veces no se entiende que la mayoría de los proyectos no es que tengan un coste inicial y ya, sino que prácticamente todos tienen un mantenimiento

posterior que hay que contemplar si no quieres dejar morir el proyecto.
Si hablamos de personas, efectivamente el Cabildo, y en general, todas las administraciones tienen un grave problema en cuanto a dotación de personas. Sin ir más lejos, el Cabildo de Gran Canaria apenas ha aumentado su personal TIC en los últimos 15 años, pero ¿cuánto ha cambiado la tecnología en este tiempo? Tenemos un gap que urge cubrir. Además, respecto a la transformación digital también se hace imprescindible esa profesionalización, sobre todo de los grupos altos de la administración (A1). Se deben incentivar formaciones específicas en gestión de proyectos, en habilidades blandas, en comunicación, en IA, en planificación, aunque a veces sigamos viendo planes de formación que incluyen cursos de Word, Excel o Photoshop (así no). Lamentablemente, la formación siempre es opcional y puede ocurrir que tengas compañeros de trabajo que nunca más se formen y en cambio otros puedan hacer cuatro o cinco cursos al año. Por último, también es imprescindible contar con personal con funciones directivas en el área TIC que impulsen esa visión 360 que necesitan las administraciones en la transformación digital.

La falta de talento, ¿es más acusada en las islas o es más fácil atraer personal?

Por nuestra condición insular sí considero que atraer personal es más acusado en nuestro territorio. Ya ni siquiera hablo de talento, hablo simplemente de que profesionales TIC se acerquen al mundo de la administración pública. Es muy poco frecuente que recién graduados en áreas TIC se interesen por la administración pública, a menos que vivas o hayas vivido de cerca a otras personas que se muevan en ese entorno. En eso igual las administraciones estamos perdiendo la oportunidad de fomentar el acceso al servicio público directamente en las universidades, en los últimos cursos de grados o ingeniería en informática, matemáticas o telecomunicaciones. He observado una circunstancia curiosa y es que, en los últimos años, el personal que se incorpora a departamentos TIC lo hacen con edades superiores a los 35 años, y suelen ser personas que han pasado antes por la empresa privada en la que muchas de esas personas trabajaban para la propia administración pública. Al estar en contacto directo con la administración pública, aunque sea como proveedor, puedes llegar a ver y conocer dinámicas que pueden ser atractivas desde fuera, aunque al final la realidad no sea tan bonita. Si bien los empleados públicos solemos contar con ventajas como la flexibilidad horaria y la estabilidad económica, los sueldos en los puestos más altos no son tan atractivos como en el sector privado. Si a eso le unes ambientes poco dados a la innovación, jefes y jefas que siguen anclados en el año 2000 o una falta de visión y recursos, traer talento se hace una verdadera misión imposible. Además, cuanto más pequeña es la administración para la que trabajes (en el área TIC), mayores son las responsabilidades y menor el apoyo. No es lo mismo trabajar en tecnología en un ayuntamiento de 10.000 habitantes que en un gobierno autonómico, pero las exigencias legales y tecnológicas suelen ser prácticamente las mismas.

Para usted, ¿cuál es el avance tecnológico que más potencial tiene para mejorar la vida de los ciudadanos isleños en los próximos años?

En la época que estamos pasando, seguramente la opción fácil sería nombrar a la Inteligencia Artificial (IA). El panorama de los últimos dos años ha cambiado de tal manera que lo que parecía algo curioso ahora "da miedo" (pero del bueno). Una cosa está clara, los ciudadanos lo que necesitan es que los trámites que se ven obligados a hacer con la administración sean sencillos, accesibles y en un lenguaje claro. Estamos acostumbrados a formularios infumables, accesos imposibles con el uso de tecnologías complicadas, un lenguaje administrativo que abusa de "palabros" arcaicos o que remiten a articulos y leyes que la ciudadanía no conoce. Dicen que el mejor trámite con la administración es el que no existe, es decir, una administración proactiva que es capaz de darte la solución (o el servicio) incluso antes de que tengas que pedirlo, pero para llegar a eso aún quedan unos cuantos años. La IA seguro que va a acelerar todo ese proceso, pero aún nos quedan retos importantes como es que las miles de administraciones españolas sean capaces de entenderse entre ellas y no tenga que estar el ciudadano yendo de una ventanilla a otra buscando papeles que podrían compartirse las administraciones, estamos en el camino y cada vez vamos más rápido, pero esto es una carrera de fondo.

Sostenibilidad y eficiencia de procesos en la Administración Pública

ByTIC, en colaboración con HCLSoftware, realizó un almuerzo informativo en el que se trató la importancia de la eficiencia en los procesos de las administraciones públicas. El encuentro contó con la participación de Luis Samper, responsable de ciberseguridad en Casa de SM el Rey; Daniel Olmo, Public Sector en HCLSoftware; Maite Cuesta, Jefa de TIC del Ayuntamiento de Las Rozas; José Arbués, director del Centro de Inteligencia de la UCM y Javier Cobas, subdirector adjunto en Hospital La Paz.

En un contexto en el que la eficiencia, la sostenibilidad y la ciberseguridad se presentan como pilares fundamentales, quedó patente que, aunque se han realizado progresos en la adopción de tecnologías emergentes como la inteligencia artificial, aún hay obstáculos importantes que superar, especialmente en formación y cultura digital, así como en la integración efectiva de sistemas que interactúan con el ciudadano. Javier Cobas, subdirector adjunto TIC en el Hospital La Paz, reflejó la fragmentación existente en los sistemas de salud al afirmar que "cada hospital hace la guerra por su cuenta". Explicó cómo esta situación limita el seguimiento integral del paciente, ya que no se logra una conexión efectiva con atención primaria y las soluciones desarrolladas como la plataforma Horus solo permiten un registro parcial de información. Cobas añadió que la resistencia interna al cambio es un gran freno, pues muchos empleados públicos con empleo de por vida se resisten a la formación necesaria para adaptarse a nuevas herramientas digitales: "¿Para qué voy a aprender ahora con 50 años?".

La irrupción de la IA

En el ámbito tecnológico, Daniel Olmo, responsable del sector público en

HCLSoftware, señaló que "la inteligencia artificial se está implantando poco a poco en la administración, con una incursión significativa a través de chatbots que asesoran a los ciudadanos en sus trámites. Es una herramienta muy importante que ya empieza a dar muy buenos resultados". No obstante Olmo reconoció que "la IA aún se encuentra en una fase de puro marketing en muchos casos y debe ser domesticada para integrarse plenamente en los procesos. Esto abre una puerta para la hiperautomatización, que puede mejorar la planificación y reducir el consumo de recursos".

Maite Cuesta, Jefa de TIC del Ayuntamiento de Las Rozas, coincidió en que "la inteligencia artificial ya está presente y bien desarrollada. Por ejemplo, en el caso de los chatbots dotados con IA ya están muy bien entrenados". Sin embargo, puso en evidencia la complejidad normativa y las precauciones que deben adoptarse en cada paso, debido a la supervisión constante de la Oficina de Protección de Datos y la Oficina de Ciberseguridad, que en su caso están externalizadas. Cuesta relativizó la velocidad del avance tecnológico, explicando que "voy muchísimo más lenta de lo que quisiera, porque a los usuarios les cuesta aprender y el cambio cultural es muy difícil".

Por su parte, Luis Samper, responsable de ciberseguridad en Casa de Su Majestad el Rey, abordó la problemática desde la perspectiva de la seguridad y las sanciones internas. Indicó que la capacidad de castigo frente a incumplimientos en el caso de los empleados públicos es limitada. "Abrir un expediente es casi imposible, cuesta horrores y además la capacidad sancionadora es pequeña", explicó, señalando que la opción más factible es dejar de premiar comportamientos inadecuados. Samper señaló, además, que "en

nuestro caso trabajamos con datos altamente sensibles por lo que resulta imprescindible cumplir con el Esquema Nacional de Seguridad, aunque este objetivo todavía no está plenamente maduro en todas las administraciones".

La importancia de la formación

Uno de los elementos en los que más incidieron los participantes es en la importancia del papel de la formación. En este sentido, José Arbués, director del Centro de Inteligencia de la Universidad Complutense de Madrid, destacó las importantes barreras formativas que frenan el avance digital. A modo de ejemplo, recordó que "en nuestro caso, cuando implementamos Office 365, una gran parte de los empleados seguía sin entenderlo tres años después". El portavoz de la UCM insistió en que la formación debe ir más allá de lo técnico para generar una auténtica concienciación respecto a los riesgos relacionados con la ciberseguridad. Además, advirtió sobre la complejidad interna de la inteligencia artificial actual, la cual depende de grandes repositorios de datos y algoritmos poco transparentes, lo que añade un nivel de incertidumbre tecnológica que debe gestionarse con cautela.

Otra cuestión de gran relevancia es la brecha digital que aún afecta tanto a usuarios como a trabajadores públicos. Maite Cuesta detalló que no basta con ofrecer servicios digitalizados si parte de la población no puede acceder o utilizarlos de manera eficiente: "No todos saben hacer los trámites porque su cultura digital no llega a





eso. Por eso mantenemos el registro presencial y la atención telefónica, además de la digital". Para llegar a los sectores más vulnerables, se han implementado iniciativas como la oficina móvil para facilitar la realización de trámites presenciales.
En el área sanitaria, Javier Cobas subrayó la complejidad añadida de las estrictas medidas de protección de datos, que ralentizan la integración de nuevas aplicaciones en hospitales. Explicó que, "a menudo, debemos trabajar con sistemas paralelos e incluso valoramos la creación de una oficina propia de seguridad para facilitar trámites especialmente en investigación. Dejó claro que el nivel de formación del personal debe ser elevado, no solo en materia de seguridad, sino también en manejo y análisis de grandes volúmenes de datos. Esto es fundamental para aprovechar tecnologías que ya están disponibles, pero que requieren un uso adecuado para maximizar sus beneficios.
El portavoz de HCLSoftware, Daniel Olmo, añadió otra problemática que es que "muchos responsables públicos no pueden decidir qué comprar o implementar debido a la rapidez del cambio tecnológico y la incertidumbre sobre regulaciones y la aceptación por parte de usuarios. Por eso es necesario que cuenten con asesoramiento experto para afrontar esa complejidad y evitar que las herramientas se queden sin utilizar". Olmo ofreció una visión estratégica sobre la evolución tecnológica y de mercado en el sector público, recalcando la relevancia de la inteligencia artificial, la sostenibilidad y la colaboración como claves para el futuro.

La importancia de la ciberseguridad

En relación a la seguridad digital, Luis Samper detalló proyectos concretos como la deshabilitación gradual de puertos USB y la incorporación de gestores seguros de contraseñas, que pretenden limitar los riesgos de brechas. Aun así, reconoció que "la implantación es lenta, principalmente debido a la inercia cultural y a la falta de hábitos digitales adecuados en el entorno público.Por eso estamos apostando por brindar formación práctica acompañando directamente al usuario en el uso de estas herramientas".
Otra línea de progreso es la colaboración interinstitucional, donde José Arbués describió iniciativas que promueven la estandarización y apertura de datos públicos, que permiten a universidades y entidades públicas compartir información en formato uniforme para optimizar el uso y el análisis. En su opinión, "la sostenibilidad de estos proyectos depende de mantener su presencia en la agenda política, pues la desaparición del interés institucional suele conllevar el abandono de iniciativas valiosas".
En cuanto al impacto general de la digitalización, las estadísticas de 2025 ofrecen un panorama alentador pero con desafíos por resolver. Por ejemplo, el plan España Digital 2025 marca metas claras para mejorar la conectividad total con 5G, impulsar la formación en competencias digitales hasta alcanzar un 80% de la población con habilidades básicas y aumentar considerablemente el número de especialistas en ciberseguridad. También se busca que la mitad de los servicios públicos estén disponibles a través de aplicaciones móviles y que las pymes incrementen su participación en comercio electrónico y el uso de inteligencia artificial.
No obstante, las brechas persisten y por eso, los participantes en el encuentro coincidieron en que la administración pública ya no puede limitarse a la simple incorporación de tecnologías, sino que debe transformar radicalmente sus procesos y mentalidades para sacar provecho real de la digitalización. Esta transformación "requiere desde luego recursos económicos y tecnológicos, pero también un compromiso institucional para promover la formación y la colaboración efectiva entre niveles de administración", como afirmó José Arbués.
Así, la digitalización se vislumbra como un motor para hacer la administración más eficiente, responsable y cercana al ciudadano, pero con un camino todavía largo por recorrer. Como concluyó José Arbus, "estamos en pañales, pero la inteligencia artificial y las tecnologías emergentes serán las que lideren esta revolución, siempre y cuando se cuide la formación y la sostenibilidad".

TEMA DE PORTADA

La revolución de la hiperconvergencia en las AAPP

En los últimos cinco años, la Administración Pública española ha vivido una profunda transformación tecnológica. Quizá no tan intensa como muchos querrían, pero es evidente que se han hecho muchas y grandes cosas en este terreno. Pero el proceso no es homogéneo. Como en toda transformación de gran escala, la madurez tecnológica y el ritmo de adopción difieren de forma sustancial entre comunidades autónomas, ayuntamientos y organismos centrales, pero existe algo más profundo que conecta estos avances: la consolidación de infraestructuras hiperconvergentes como soporte estructural del nuevo modelo público.

El Plan de Digitalización de las Administraciones Públicas 2021-2025, eje esencial de la estrategia España Digital 2025 y articulado sobre el Fondo de Recuperación Next Generation EU, marca el compromiso estatal no solo con la incorporación de tecnología, sino con la reingeniería de procesos, garantías legales y acceso sostenible a recursos críticos. Las inversiones públicas en hardware, plataformas de almacenamiento y centros de datos hiperconvergentes han cerrado el año 2024 en máximos históricos, superando en algunos casos los 400 millones de euros y confirmando que la digitalización se ha convertido en una prioridad de Estado.

El auge de la hiperconvergencia responde tanto a necesidades operativas como estratégicas. "Yo creo que existe un grado importante de madurez y una clara apuesta por la transformación digital. La verdad es que cada vez son más las instituciones que adoptan infraestructuras hiperconvergentes para ganar agilidad y simplificar su TI", asegura Jorge Vázquez, director general de Nutanix Iberia, insistiendo en que los hitos deben leerse como parte de un proceso evolutivo, no un destino estático. "La digitalización, en especial en las administraciones públicas, es un proceso continuo, que no termina con una única inversión sino

que exige adaptación constante".

De la complejidad al entorno único

La hiperconvergencia ha dejado de ser un concepto restrictivo, asociado a grandes despliegues en compañías privadas o centros de datos de organismos internacionales.

De hecho, su valor identificativo radica hoy en permitir a instituciones públicas operar con un entorno único que integra almacenamiento, computación, red y virtualización, consolidando legados y nuevas aplicaciones bajo una misma arquitectura. El bloque de inversión pública más destacado es el de sistemas de almacenamiento, que representa el 26% de los recursos destinados por la Administración y que busca soluciones seguras y eficientes para millones de expedientes y archivos críticos.

"Las comunidades autónomas lideran esta transformación. Casi la mitad de las licitaciones, un 43%, proceden de los gobiernos regionales, con Madrid y Cataluña a la cabeza. Les sigue la Administración General del Estado, con cerca de 70 millones de euros invertidos, y los ayuntamientos que, aunque manejan presupuestos menores, aportan la capilaridad necesaria para que la digitalización llegue a todo el territorio", destaca Vázquez, invitando a leer el mapa de la modernización como una trama de áreas con necesidades particulares y desafíos propios.

La hiperconvergencia es, hoy, una pieza central en los grandes planes de modernización de infraestructuras administrativas de muchas entidades públcias. Su valor diferencial trasciende la eficiencia operativa. "La hiperconvergencia es una pieza clave dentro de los planes de modernización de las administraciones porque permite reducir la complejidad, unificar la gestión y preparar el terreno para una adopción segura de entornos híbridos y multicloud", argumenta Vázquez, desde la experiencia de haber liderado proyectos con decenas de organismos estatales

El reto no es únicamente técnico sino funcional. El directivo recuerda que Nutanix "facilita la digitalización ofreciendo soluciones de nube híbrida y multicloud que aportan flexibilidad, escalabilidad y seguridad. Esto permite a las administraciones mantener el control de sus datos, optimizar costes y avanzar hacia modelos de servicio más ágiles. Además, la simplicidad de uso de la plataforma de Nutanix permite que, incluso personas con pocos conocimientos técnicos puedan gestionarla, reduciendo la dependencia de recursos técnicos especializados y permitiendo que el personal se enfoque en tareas más productivas con impacto directo en la calidad de los servicios públicos".

Avances desiguales, transformación asimétrica

Analizar el papel de la hiperconvergencia exige perder el miedo a la asimetría, puesto que, como puede resultar evidente, no todas las administraciones han marchado al mismo ritmo. "Sí, existen diferencias en el ritmo de adopción, pero no tanto a nivel administrativo sino por el tipo de organismo y su nivel de madurez tecnológica. Hay sectores, como la educación o la sanidad, que han avanzado más rápidamente, mientras que otros están aún en fase de transición", enfatiza Vázquez, que observa un objetivo común incluso en los casos más rezagados: "modernizar su infraestructura y ofrecer servicios más digitales y accesibles".

Este enfoque ha permitido adaptar recursos a realidades muy diversas. En la sanidad pública, por ejemplo, Castilla-La Mancha y Andalucía han apostado por infraestructuras hiperconvergentes para gestionar miles de puestos de trabajo y centros médicos, mientras que en el ámbito educativo, los grandes municipios han empezado a migrar los sistemas de registro y evaluación a plataformas unificadas.

En cualquier caso, migrar hacia arquitecturas hiperconvergentes implica desafíos que se repiten, sea cual sea el tamaño, como puedan ser la especialización o el presupuesto del organismo implicado. "Los retos más habituales tienen que ver con la falta de talento especializado, la complejidad de los sistemas heredados y la gestión de presupuestos y proveedores. Además, hay que tener en cuenta el crecimiento exponencial del dato. El volumen de información que manejan las administraciones se duplica cada año y disponer de los medios de almacenamiento necesarios puede llegar a ser algo cada vez más complejo", señala el directivo de Nutanix. La gestión de la licitación pública añade, además, una capa de incertidumbre a este proceso. Los pliegos y adjudicaciones suelen incluir requisitos técnicos muy avanzados, pero el camino hasta su firma se complica por la rigidez presupuestaria y la falta de talento TI propio, obligando en ocasiones a recurrir a esquemas externalizados y a la industria privada como soporte estratégico.

"Trabajar con las administraciones públicas en España también implica enfrentarse a procesos

de licitación largos y complejos, y a la necesidad de cumplir con normativas muy estrictas, como el Esquema Nacional de Seguridad ENS. Por eso debemos ser nosotros quienes nos adaptemos a sus particularidades, ofreciendo soluciones que cumplan con los estándares regulatorios más exigentes, simplifiquen la gestión de infraestructuras y ofrezcan una experiencia de uso intuitiva. En este caso la modernización tecnológica no es solo un reto técnico, sino también una oportunidad para mejorar la calidad de los servicios públicos", reivindica Vázquez.

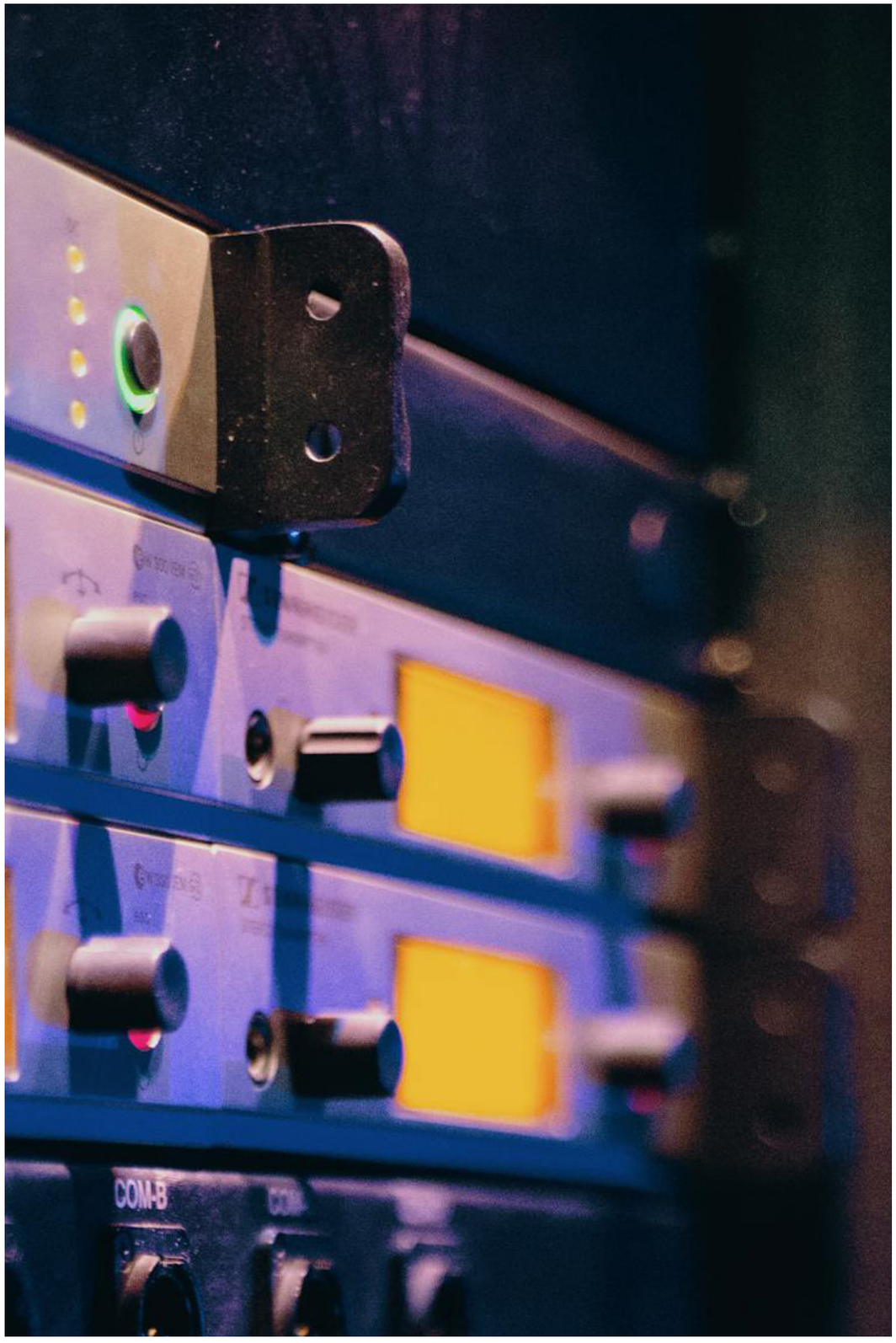
Normativa y contratación: ¿freno o catalizador?

El debate sobre la normativa pública y los procesos de contratación está presente en cada etapa de evolución tecnológica.

"Es cierto que los exigentes criterios propios de la contratación pública y las cuestiones presupuestarias pueden ralentizar la adopción de nuevas tecnologías, especialmente cuando los proyectos no están incluidos en la planificación inicial. Pero también es verdad que en aquellos casos donde el grado de digitalización es muy bajo, la necesidad de adaptarse a una nueva normativa actúa como catalizador", valora Vázquez, que defiende la regulación como garante de la "protección y soberanía de los datos públicos".

La flexibilidad de los modelos de contratación y el impulso de políticas públicas orientadas a resultados se ven como claves para acelerar el paso. "En términos generales yo diría que estamos viendo una evolución positiva, cada vez más administraciones incluyen la modernización tecnológica como parte estratégica de su transformación digital, pero también es necesario que las políticas públicas acompañen esta evolución con modelos de contratación más flexibles y orientados a resultados".

No hay que olvidar, además, que la protección de los datos públicos y la soberanía digital figuran entre los temas más sensibles para responsables y proveedores tecnológicos. Vázquez asegura, en este sentido, que la soberanía y la seguridad del dato son "prioridades absolutas para nosotros. Nuestras soluciones están diseñadas para que las administraciones mantengan el control total de sus datos, tanto si están en sus instalaciones como en la nube. Las principales preocupaciones del sector público, independientemente de su nivel, son similares a las del resto de organizaciones, la ciberseguridad y la soberanía de los datos. Con nuestra plataforma, las políticas de gestión y protección se aplican de forma consistente en todos los entornos, lo que aporta confianza y cumplimiento normativo".



Las obligaciones del Esquema Nacional de Seguridad, el Reglamento Europeo de Protección de Datos y la Ley de Administración Electrónica marcan el estándar operativo y técnico, obligando a mantener sistemas redundantes y monitorización avanzada en todos los puntos de la cadena. "Nos adaptamos a las particularidades de cada administración con soluciones que cumplen los estándares regulatorios más exigentes y que garantizan la soberanía del dato", concluye Vázquez, quien insiste en que "la seguridad no debe ser un freno, sino un facilitador de la transformación digital".

Tecnología al servicio de la ciudadanía

El impacto real de la modernización digital no puede limitarse a métricas operativas o reducción de costes. La hiperconvergencia tiene efectos directos en la vida de los ciudadanos y en la capacidad de las administraciones para prestar servicios cada vez más ágiles, personalizados y seguros.

"La hiperconvergencia simplifica enormemente la gestión y reduce costes al integrar en una misma plataforma computación, almacenamiento, red y virtualización. Nuestros modelos de nube híbrida están pensados para facilitar la implementación, mejorar el control de los costes y optimizar la eficiencia energética, algo especialmente relevante en un momento en que las administraciones deben ser más sostenibles", expone Vázquez.

El ejemplo del teletrabajo en la Gerencia de Informática de la Seguridad Social, habilitado en apenas dos semanas mediante plataforma Nutanix para garantizar la atención ciudadana durante la pandemia, ilustra la capacidad de adaptación de la tecnología. "En el ámbito sanitario, tanto el SESCAM como el SAS han apostado por infraestructuras hiperconvergentes que simplifican la gestión de miles de puestos de trabajo y centros médicos, ofreciendo una atención más coordinada y eficaz. Estos ejemplos muestran cómo la hiperconvergencia puede adaptarse a necesidades muy distintas, desde administración y sanidad hasta defensa, siempre con un mismo propósito, ayudar a construir una Administración más ágil, moderna y cercana al ciudadano".

Los ayuntamientos medianos y pequeños también han experimentado mejoras notables. Casos como el de Girona o la Diputación de Granada ejemplifican cómo el despliegue de infraestructuras hiperconvergentes ha redundado en un servicio más próximo y eficiente, generando canales digitales de atención que reducen esperas y permiten mayor capacidad de resolución para el ciudadano.

El sector público como laboratorio social

La adopción de la hiperconvergencia en la Administración española no es únicamente un proceso de ingeniería de sistemas. Actúa como laboratorio transversal de nuevas formas de prestación de servicios, colaboración público-privada y economía sostenible.

"La hiperconvergencia permite a las administraciones responder más rápido, adaptarse a nuevas necesidades y ofrecer servicios digitales más accesibles y seguros. Las tecnologías en la nube son fundamentales para transformar las operaciones y prepararse para la economía digital del futuro", sostiene el responsable de Nutanix Iberia.

La suma de factores, desde la eficiencia energética exigida por las nuevas licitaciones hasta el desarrollo de competencias digitales en todo el personal público, configura un entorno donde la gestión del recurso tecnológico se orienta por igual al ahorro de costes y a la sostenibilidad, según determina la Agenda España Digital 2025 y la orientación directa de la Comisión Europea.

Casos emblemáticos y proyección europea

En el terreno ejecutivo, el sector público español muestra una vitalidad creciente que no pasa desapercibida para actores internacionales. Instituciones como la Gerencia de Informática de la Seguridad Social, los Servicios de Salud de Castilla-La Mancha y Andalucía, el Senado, la Diputación de Granada, el Centro de Pruebas y Validación del Ejército de

TEMA DE PORTADA

Tierra y la Fundación Progreso y Salud figuran en la lista de organismos que han apostado por la hiperconvergencia para garantizar la continuidad y seguridad de servicios críticos.

El denominador común es la adaptabilidad a necesidades especializadas. En palabras de Vázquez, "cada uno de estos proyectos refleja cómo la tecnología de Nutanix ayuda a mejorar la eficiencia, la seguridad y la continuidad del servicio público. En el caso de la GISS, por ejemplo, nuestra plataforma permitió habilitar en apenas dos semanas una solución de teletrabajo segura para garantizar la atención al ciudadano durante la pandemia. En el ámbito sanitario, tanto el SESCAM como el SAS han apostado por infraestructuras hiperconvergentes que simplifican la gestión de miles de puestos de trabajo y centros médicos, ofreciendo una atención más coordinada y eficaz".

La cooperación internacional empieza a replicar modelos españoles en otras administraciones europeas, especialmente en lo relativo a la gestión descentralizada y la protección multiplataforma. "Estos ejemplos muestran cómo la hiperconvergencia puede adaptarse a necesidades muy distintas, desde administración y sanidad hasta defensa, siempre con un mismo propósito, ayudar a construir una Administración más ágil, moderna y cercana al ciudadano", concluye el experto.

Un nuevo escenario para la gestión pública

Hablar hoy de hiperconvergencia en las Administraciones Públicas es referirse a una revolución invisible pero decisiva que afecta no sólo a la arquitectura TI, sino al modelo completo de prestación de servicios, definición de políticas públicas y desarrollo de competencias. El Plan de Digitalización estatal, las nuevas normativas y los fondos europeos han permitido multiplicar la inversión, repensar procesos y explotar sinergias hasta hace poco inimaginables.

España se encuentra, pues, en pleno impulso de una estrategia digital que no solo busca eficiencia interna, sino competitividad internacional y cohesión territorial. "Nuestro objetivo es construir una Administración más ágil, moderna y cercana al ciudadano. En definitiva, se trata de una tecnología que libera a los equipos técnicos de tareas repetitivas para que puedan centrarse en proyectos de mayor impacto para el ciudadano", concluye Jorge Vázquez, condensando el sentido profundo que recorre este proceso silencioso pero irreversible.

n la ciudad de Barcelona y su área metropolitana operan tres empresas municipales de transporte público: Ferrocarril Metropolità de Barcelona, S.A., responsable de la gestión del Metro de Barcelona; Transports de Barcelona, S.A., encargada de gestionar los servicios de autobús urbano de Barcelona y otros transportes; y Projectes i serveis de mobilitat, S.A., propiedad del Área Metropolitana de Barcelona. Todas ellas forman parte de una marca comercial y una unidad gestora llamada Transports Metropolitans de Barcelona (TMB).

El desafío

Transports Metropolitans de Barcelona se enfrentaba al desafío de ampliar su infraestructura en AWS para alojar una serie de nuevos portales que debían soportar un volumen constante y muy elevado de visitas. Ante la creciente demanda de tráfico web, era esencial contar con una plataforma que no solo ofreciera alta disponibilidad, sino que también fuera capaz de adaptarse dinámicamente al número de visitas en tiempo real, asegurando así un rendimiento óptimo en todo momento.

La solución debía garantizar que los portales permanecieran operativos y accesibles incluso durante los picos de tráfico más intensos, evitando caídas y tiempos de inactividad que podrían afectar negativamente la experiencia del usuario. Además, la infraestructura debía ser lo suficientemente flexible para escalar automáticamente según las necesidades, permitiendo que los recursos se ajustaran eficientemente, tanto para manejar incrementos

CASO PRÁCTICO

repentinos en la demanda como para optimizar costos durante períodos de menor actividad.

La solución

Para satisfacer las necesidades de Transports Metropolitans de Barcelona, ACKstorm diseñó e implementó una plataforma innovadora basada en contenedores, utilizando Docker como la tecnología central para la gestión de las aplicaciones. Esta elección estratégica permitió que las aplicaciones fueran altamente portables, ligeras y autosuficientes, lo que facilitó su despliegue en distintos entornos sin depender de la infraestructura subyacente.

La portabilidad proporcionada por Docker no solo simplifica la administración y el despliegue de las aplicaciones, sino que también garantiza una mayor consistencia en el comportamiento de estas, independientemente del entorno en el que se ejecuten. Esto es especialmente crucial en un escenario de alta demanda como el de Transports Metropolitans de Barcelona, donde la fiabilidad y la rapidez en el despliegue de nuevas versiones son factores clave para mantener un servicio continuo y de alta calidad.

Para asegurar que la plataforma pudiera manejar el creciente volumen de tráfico de usuarios, ACKstorm implementó un procedimiento de Auto Scaling. Esta funcionalidad permitió que la capacidad de los componentes de la arquitectura escalara de manera automática y dinámica, en respuesta directa al número de peticiones de usuarios en cualquier momento. Así, se logró una plataforma altamente resiliente y adaptable, capaz de enfrentar picos de tráfico sin comprometer el rendimiento ni la disponibilidad del servicio.

Además, el uso de Auto Scaling no solo mejoró la capacidad de respuesta de la plataforma, sino que también optimizó la utilización de recursos, garantizando que Transports Metropolitans de Barcelona solo utilizara y pagara por los recursos necesarios en cada momento. Esto resultó en una infraestructura más eficiente y rentable, alineada con las necesidades fluctuantes del tráfico de usuarios.

El resultado obtenido

La implementación de la nueva plataforma proporcionó a Transports Metropolitans de Barcelona una infraestructura escalable y de alta

disponibilidad, diseñada específicamente para soportar los exigentes requisitos de sus nuevos portales. Esta infraestructura no solo asegura que los portales estén siempre operativos y accesibles, sino que también permite que la capacidad de la plataforma se ajuste automáticamente en respuesta a las fluctuaciones en el tráfico de usuarios, garantizando así un rendimiento óptimo en todo momento.

Además de la escalabilidad y la alta disponibilidad, se llevaron a cabo una serie de mejoras y optimizaciones en el uso de la computación.

Estas mejoras incluyeron la implementación de mecanismos avanzados para gestionar de manera más eficiente los recursos en la nube, tales como la distribución de carga, la optimización de procesos y la utilización inteligente de instancias. Como resultado, logró una significativa reducción de costes operativos, al minimizar el uso innecesario de recursos y asegurar que solo se emplearan los necesarios en cada momento.

TENDENCIAS

El apagón que señaló una brecha: replanteamiento de la ciberseguridad en el sector público español

Por Raghav Iyer S,
Senior IT Security Analyst en ManageEngine

Mientras la Unión Europea sufre un aumento de los ciberataques, España se encuentra en el centro de un panorama de amenazas cada vez mayor. Aunque el apagón de la primavera pasada en España, Portugal y parte de Francia suscitó el temor de un ciberataque a la red eléctrica, las primeras investigaciones no arrojaron pruebas de intrusión en el sistema.

No obstante, las vulnerabilidades de la infraestructura energética europea son reales, y el apagón sirve como recordatorio urgente de lo devastador que puede ser su compromiso.

El aumento de las ciberamenazas en España

Según el último Índice de Economía y Sociedad Digital, España ocupa el séptimo lugar entre 27 países de la UE, en servicios públicos digitales, posicionándose como líder en gobernanza electrónica. La digitalización nacional proporciona eficiencia e innovación, pero también conlleva vulnerabilidades compartidas. Los atacantes suelen aprovechar los puntos débiles de la infraestructura digital para extraer información o datos sensibles que pueden venderse en la dark web.

Con millones de usuarios, aplicaciones como Mi Carpeta Ciudadana y el DNI Digital (MiDNI) han ayudado a España a alcanzar una puntuación de 88,75 en servicios digitales para los ciudadanos (por encima de la media europea de 82,2), según el informe Estado de la Década Digital 2025. Esto demuestra la gran cantidad de información pública sensible disponible del sector público, lo que lo convierte en un objetivo ideal para los ciberatacantes.

El Centro Criptológico Nacional informó de un aumento del 20 % en los ciberataques a entidades públicas en 2024, lo que subraya la necesidad de implementar medidas de resiliencia más sólidas.

Consciente de los riesgos asociados a la digitalización, el Gobierno español ha destinado el 2 % de su PIB a medidas de ciberseguridad y ha previsto más de 3.000 millones de euros en inversiones, que incluyen la integración de la inteligencia artificial, el análisis avanzado y la mejora de la ciberseguridad. Si bien esto demuestra la concienciación y la urgencia del Gobierno, España sigue enfrentándose a retos para garantizar la interoperabilidad entre organismos, reducir la brecha digital en las zonas rurales y proteger los servicios críticos contra ataques cada vez más sofisticados.

Un sector público bajo asedio

Las divisiones gestionadas por el gobierno, desde las redes municipales hasta los departamentos de defensa nacional, son objetivos atractivos para los ciberatacantes. Esto se debe, en gran medida, a la gran cantidad de información confidencial que poseen y a las medidas insuficientes de seguridad que la protegen.

Muchos sectores públicos siguen dependiendo de sistemas heredados con una ciberresiliencia limitada para gestionar infraestructuras críticas y datos confidenciales. Esto amplía la superficie de ataque, lo que facilita a los atacantes su explotación.

A diferencia de las violaciones de seguridad en el sector privado, el impacto de un ataque al sector público puede ser devastador debido al enorme volumen y la

naturaleza crítica de los datos involucrados. Por ejemplo, si los documentos de identidad de los ciudadanos, los registros fiscales o la información sanitaria caen en manos de un actor malintencionado, este puede utilizar esos datos para causar graves daños a las personas.

En los casos en que el objetivo es la infraestructura pública, toda la nación se ve afectada. El reciente ataque a la cadena de suministro de los aeropuertos europeos pone de relieve la creciente amenaza que se cierne sobre los servicios críticos como el transporte.

Para agravar el problema, los retos presupuestarios y los largos procesos de aprobación suelen retrasar la implementación de medidas de seguridad robustas, lo que obliga a los departamentos de TI a trabajar con herramientas obsoletas, como si se tratara de una lucha simbólica contra robots, con palos y piedras.

El impacto a largo plazo de los incidentes cibernéticos

El período posterior a un incidente cibernético es crítico. Los impactos inmediatos, como los costos del incidente, la pérdida de datos, las interrupciones del servicio y las perturbaciones públicas, son visibles y, a menudo, cuantificables.

Sin embargo, las consecuencias a largo plazo de un ciberataque, especialmente en el sector público, suelen pasarse por alto. Algunos de los efectos duraderos más comunes son:

- Erosión de la confianza pública: los incidentes cibernéticos repetidos pueden romper la confianza de los ciudadanos en las instituciones gubernamentales. Una vez que se pierde la confianza, el avance de la digitalización se vuelve mucho más difícil.
- Pérdidas económicas duraderas: más allá del coste inicial del incidente, las multas reglamentarias, los litigios prolongados y los gastos de revisión de los sistemas afectados pueden suponer una carga para el presupuesto de un país.

- Vulnerabilidades de la seguridad nacional: las violaciones persistentes de los sistemas públicos atraen nuevos intentos de actores maliciosos similares, lo que supone un grave riesgo para la seguridad nacional. Estas vulnerabilidades también pueden ser explotadas por naciones hostiles para incitar a la inestabilidad política.
- Exposición persistente de los datos: una vez que los datos se exponen y se venden en la web oscura, siguen siendo una amenaza persistente, lo que da lugar a robos de identidad o espionaje años después de la violación inicial.
- Déficit de habilidades y recursos: la dificultad del sector público para atraer y retener a profesionales de la ciberseguridad, amplía la brecha de talento. Con el tiempo, este desequilibrio permite a los adversarios seguir innovando y mantenerse varios pasos por delante.

Desarrollar la resiliencia: estrategias de ciberseguridad

Para España y otros Estados miembros de la UE, hacer frente a las crecientes amenazas cibernéticas requiere una estrategia integral y coordinada que combine modernización, colaboración y mejora continua.

El primer paso consiste en actualizar los sistemas heredados que constituyen la columna vertebral de muchas operaciones del sector público. Las infraestructuras obsoletas y las arquitecturas de seguridad fragmentadas suelen proporcionar puntos de entrada fáciles para los atacantes. La transición a entornos modernos basados en la nube y respaldados por marcos de confianza cero puede reducir significativamente estas vulnerabilidades y mejorar la resiliencia general del sistema.

Además, cabe destacar de igual forma el fomento de prácticas sólidas de higiene cibernética en todos los niveles del gobierno: las auditorías de seguridad periódicas, las evaluaciones de vulnerabilidad y las simulaciones de respuesta a incidentes deben convertirse en procedimientos estándar para garantizar que las agencias sigan siendo proactivas en lugar de reactivas. Los programas de formación y sensibilización continuos pueden capacitar a los empleados públicos para reconocer y responder rápidamente a las ciberamenazas, fomentando una cultura de responsabilidad compartida.

La colaboración también desempeñará un papel fundamental en el fortalecimiento de la postura de Europa en materia de ciberseguridad.

Dado que las ciberamenazas no respetan las fronteras nacionales, es esencial una cooperación más estrecha entre los Estados miembros de la UE. Esto incluye compartir información sobre amenazas, armonizar los protocolos de defensa y realizar ejercicios conjuntos para desarrollar la preparación colectiva.

Al mismo tiempo, deben fomentarse las asociaciones público-privadas, lo que permitirá a los gobiernos aprovechar la innovación y los conocimientos técnicos de las empresas privadas de ciberseguridad y las instituciones de investigación.

Por último, aunque es fundamental aumentar los presupuestos de ciberseguridad, la eficacia de ese gasto depende de una asignación estratégica. Los recursos deben dirigirse a las áreas más críticas, como la preparación para responder a incidentes, la infraestructura digital segura y el desarrollo de la mano de obra, en lugar de dispersarse demasiado. Combinando tecnología moderna, profesionales cualificados y marcos de colaboración, España y la UE en general no solo pueden defenderse de las ciberamenazas actuales, sino también construir una resiliencia digital a largo plazo para el futuro.

Una llamada de atención para España

El reciente apagón en España ofrece una visión de las crecientes vulnerabilidades cibernéticas de los estados modernos. La respuesta del país, en particular su compromiso de aumentar la inversión en ciberseguridad, refleja un cambio más amplio en toda Europa que reconoce la resiliencia digital como algo tan esencial como la defensa física.

Cuando las redes eléctricas, los hospitales y las bases de datos públicas están conectados a través de la misma estructura digital, el coste a largo plazo de descuidar la ciberseguridad supera con creces cualquier interrupción inmediata.

La llamada de atención a España debería servir de catalizador para que toda la UE fortalezca sus defensas, no solo para hoy, sino para las amenazas del mañana.

GRACIAS

contacto@bytic.es | www.bytic.es