BYTIC MEDIA

NÚMERO 43 | ENERO 2025

Las AAPP españolas, bajo asedio constante

ENTREVISTA

Estrella Martín, Directora General de Emprendimiento del Ayuntamiento de Madrid

TENDENCIAS

En 2026 habrá un aumento de ataques basados en la identidad digital

sdg GROUP

Somos una consultora especializada en **IA, Data & Analytics.**

Ayudamos a nuestros clientes a transformar
sus datos en activos estratégicos
para tomar las mejores decisiones de negocio.

WE ARE RECOGNIZED BY:

Gartner® PENTEO Analytics Insight Everest Group®

Are you ready
to go **beyond**?

TABLA DE CONTENIDOS

Sobre NOSOTROS

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

BYTIC MEDIA

Nuestra misión

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

Nuestra visión

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

contacto@bytic.es
www.bytic.es

COMITÉ DE EXPERTOS

Carmen García Roger

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

Ángel Luis Sánchez García

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

Montaña Merchán Arribas

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

Pedro M. Galdón Conejo

CIO & CISO de EMASA

Ildefonso Vera Gómez

Director Innovación, Procesos y Transformación Digital. ISDEFE

Andrés Prado Domínguez

Director del Área TIC UCLM

Concepción García Diéguez

Sistemas de Información Madrid Digital

Lucía Quiroga Rey

Asesora Técnica Delegación del Gobierno. Junta de Andalucía

Nacho Santillana Montal

exDirector de sistemas de la información del Ayuntamiento de Barcelona

Concepción Campos Acuña

Presidenta de la asociación de mujeres en el Sector Público

Sebastian Puig Soler

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

María Luisa Ulgar

Coordinadora Iniciativa WomANDigital en Junta de Andalucía

BYTIC MEDIA

Forma parte de la comunidad ByTIC

Comunidad de innovación y tecnología exclusiva para la Administración Pública

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

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

adjudicaciones y licitaciones TIC | powered by byte TI

El Gobierno lanza las ayudas RedCyTI por valor de 89 millones de euros

El Gobierno de España pone en marcha el nuevo programa RedCyTI para potenciar la digitalización de entidades locales y comunidades autónomas uniprovinciales. Ya se ha publicado en el BOE la orden de bases de esta línea de ayudas, dotada con un total de 89 millones de euros, que gestiona Red.es, entidad adscrita al Ministerio para la Transformación Digital y de la Función Pública a través de la Secretaría de Estado de Inteligencia Artificial y Digitalización. Próximamente estará abierto el plazo de solicitud de esta convocatoria, cuya finalidad es reforzar el impulso a las ciudades y territorios inteligentes poniendo el foco, en esta ocasión, en el "fomento del desarrollo económico y productivo".

Según la Comisión Europea, "una ciudad o territorio inteligente tiene como objetivo mejorar el bienestar de sus habitantes, empresas, visitantes, organizaciones y administradores mediante la prestación de servicios digitales que contribuyan a una mejor calidad de vida". Las actuaciones pueden darse en seis dimensiones: Living (asociada a la calidad de vida), People (participación ciudadana), Environment (sostenibilidad), Mobility (movilidad), Economy (desarrollo económico) y Governance (gobernanza de la ciudad o territorio).

La dimensión de ciudad inteligente denominada 'smart economy', en la que se centra esta nueva convocatoria, se entiende como la intersección entre ciudad y economía, y contempla todas aquellas iniciativas que, promovidas desde las ciudades y territorios, se orientan a potenciar la digitalización al servicio de la actividad económica, el empleo y el emprendimiento.

Apoyo a entidades locales y CC.AA. uniprovinciales

Red.es, sumando fondos propios y Fondo Europeo de

Desarrollo Regional (FEDER), aportará entre el 40 y el 85% de cada iniciativa seleccionada, que habrá de tener un presupuesto total de entre 1.5 y 6 millones de euros. El porcentaje varía según la comunidad autónoma desde la que se presente. Las entidades que pueden solicitar estas ayudas son entidades locales (ayuntamientos, diputaciones, cabildos insulares, consejos insulares y comarcas) y comunidades autónomas uniprovinciales.

Los proyectos han de conllevar actuaciones destinadas a crear o reforzar infraestructuras tecnológicas y las soluciones y servicios asociados, a disposición de sectores estratégicos de actividad económica, con el propósito de probar y desarrollar tecnologías de aplicación sectorial. Asimismo, se apoyará la creación o mejora de espacios destinados al fomento de la innovación y el fortalecimiento del ecosistema sectorial, a fin de impulsar el desarrollo de la economía y el empleo, tanto a nivel local como regional y estatal.

Ejemplos de estas actuaciones serían la creación de espacios de prueba o sandboxes para el sector de la movilidad y transporte (vehículos conectados y autónomos, drones...), la creación de laboratorios urbanos de innovación, o la dotación de las infraestructuras necesarias para la prueba y desarrollo de tecnologías de aplicación a sectores como la agricultura, la pesca, la ganadería, o la energía, entre otros.

Las entidades que deseen solicitar estas ayudas habrán de presentar sus proyectos en la sede electrónica de Red.es, una vez publicada la convocatoria, tal y como se indica en el extracto de la convocatoria publicado en el Boletín Oficial de Estado. Los criterios de otorgamiento valorarán aspectos como el grado de madurez digital, el impacto de la iniciativa en el desarrollo económico local y su sostenibilidad. Aquellos proyectos que sean seleccionados recibirán una ayuda en régimen de concurrencia competitiva, que será licitada y ejecutada por Red.es.

Compromiso con las ciudades y territorios inteligentes

Desde la aprobación del Plan Nacional de Ciudades Inteligentes en 2015, el Gobierno de España ha realizado cinco convocatorias en las que Red.es ha desempeñado un papel impulsor protagonista. En total, se ha destinado más de 200 millones de euros -cofinanciados por el Fondo Europeo de Desarrollo Regional (FEDER)- a 59 iniciativas repartidas por todo el territorio nacional: 25 ciudades, 24 destinos turísticos, 7 edificios y 3 islas. Además, Red.es, colabora de manera continua con la Red Española de Ciudades Inteligentes (RECI) y la Federación Española de Municipios y Provincias (FEMP) para impulsar el desarrollo de ciudades y territorios inteligentes.

Editorial

La Administración pública es uno de los objetivos prioritarios de los ciberdelincuentes. Incluso, algunas voces empiezan a alertar de que los ciberataques van a ser cada vez más numerosos y van a superar a los registrados por los tradicionales objetivos: la banca o el transporte.

Presentado recientemente, el informe ENISA THREAT LANDSCAPE, de la Agencia Europea de Ciberseguridad explica el por qué de este aumento. Lejos de lo que sucede en otros ámbitos, en los que el dinero o la obtención de datos son las motivaciones principales, en el caso de las Administraciones Públicas, 8 de cada 10 ataques dirigidos contra entidades públicas en Europa (el 79,4 %, concretamente) obedecen a razones de carácter ideológico.

Estamos en un contexto cada vez más polarizado, con crisis institucionales en buena parte de Europa, Gobiernos ineficientes o directamente secuestrados como ocurre en el caso español, y que se abonan con crisis de vivienda, salarios cada vez más bajos, corrupción política, etc. Todo esta siendo aprovechado por los ciberdelincuentes para lanzar todo tipo de ataques. A lo tradicionales phishing, o DDoS, los ataques preferidos contra las AAPP ahora se suman las fake news o los deep fakes para, beneficiandose de las diferentes crisis, tener éxito en los ataques.

LAs AAPP españolas deben estar atentas. No podemos permitirnos una crisis más en estos tiempos.

El presupuesto hará de 2026 el año de la inteligencia artificial en el Principado de Asturias

El presupuesto autonómico permitirá que la Administración del Principado avance en 2026 en la simplificación administrativa gracias al apoyo de la inteligencia artificial (IA), con el objetivo de reducir trámites, acortar tiempos de espera y mejorar la atención a la ciudadanía y a las empresas.

La vicepresidenta del Principado, Gimena Llamedo, ha anunciado hoy esta meta durante la presentación en la Junta General de las cuentas de la Consejería de Presidencia, Reto Demográfico, Igualdad y Turismo para 2026, que ascienden a 221,57 millones.

Llamedo ha asegurado que la modernización administrativa constituye una política sostenida del Gobierno de Asturias para mejorar los servicios públicos y la relación con la ciudadanía. Con este propósito ya se han dado pasos como la Ley Simplifica, el despliegue de la aplicación miPrincipado o la creación de la Oficina Económica de la Presidencia para facilitar proyectos empresariales.

El uso de la inteligencia artificial también contribuirá a alcanzar este objetivo. La vicepresidenta ha desgranado varias iniciativas relacionadas con la IA. Así, ha anunciado que el próximo año se extenderá a otras áreas un plan piloto aplicado este ejercicio a las ayudas de natalidad, que utiliza inteligencia artificial para la lectura de documentación y permite agilizar de manera significativa los plazos de resolución.

Con esta ambición, la transformación digital seguirá siendo uno de los ejes del presupuesto, con 95,29 millones, de los que 42,7 se destinan a inversión. "Cada euro invertido es una lucha contra la burocracia", ha afirmado Llamedo. Entre los proyectos más destacados figuran el desarrollo de una superapp que integrará los servicios digitales del Principado, las mejoras en miPrincipado, el uso de la IA como apoyo a la tramitación administrativa y a los servicios públicos, el refuerzo de la ciberseguridad y nuevas actuaciones para garantizar la fiabilidad de los sistemas digitales.

Las cuentas consolidan además a Asturias como territorio de referencia en el desarrollo responsable de la inteligencia

artificial, con la puesta en marcha de una factoría de IA y un sandbox (una especie de campo virtual de pruebas) regulatorio. La factoría permitirá desarrollar y aplicar soluciones concretas para simplificar trámites y mejorar la gestión pública, mientras que el sandbox funcionará como un entorno controlado para probar nuevos usos de la IA con seguridad jurídica, supervisión humana y garantías éticas.

El presupuesto destina también casi tres millones a la modernización de infraestructuras críticas para la gestión de emergencias, con el objetivo de reforzar la capacidad de respuesta del Principado ante situaciones extremas.

La vicepresidenta ha destacado igualmente la apuesta por la formación en inteligencia artificial del personal público, con programas específicos tanto para perfiles directivos como para el conjunto de la plantilla. Estos programas serán impulsados por la Dirección General de Estrategia Digital e Inteligencia Artificial y el Instituto Asturiano de Administración Pública.

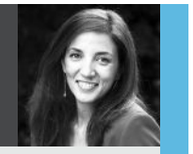
"El objetivo es que la Administración gane tiempo para las personas y para las empresas, utilizando la tecnología para simplificar trámites y reforzar la capacidad de respuesta de los servicios públicos", ha explicado Llamedo.

Reforzar los servicios públicos

En paralelo, el presupuesto refuerza los servicios públicos con 1.465 nuevas plazas, concentradas en servicios públicos esenciales. El grueso del incremento corresponde a sanidad, con 206 profesionales médicos y sanitarios, y educación, con 1.158 nuevas plazas, la mayoría para docentes (938) y técnicas de educación infantil (167). La vicepresidenta ha subrayado que la mayor parte del personal de la Administración se concentra en los pilares del Estado del bienestar: cerca del 40% de la plantilla corresponde a sanidad y alrededor del 30%, a educación.

"En política, hay dos modelos: reforzar los servicios públicos o debilitarlos. Este gobierno apuesta sin ambigüedades por servicios públicos de calidad, frente a las políticas de recortes y privatización aplicadas en otras comunidades autónomas, como Madrid, cuyas consecuencias ya son visibles para la ciudadanía", ha concluido.

La opinión de Arantxa Herranz



Históricamente, la hegemonía tecnológica ha tenido un marcado acento norteamericano. Desde las costas del Pacífico que bañan el emblemático Silicon Valley, han fluido hacia el resto del mundo la gran mayoría de las herramientas digitales e innovaciones disruptivas que definen nuestra cotidianidad actual. Sin embargo, este liderazgo convive con una fragilidad institucional que emerge cuando el famoso «sueño americano» se transforma en una parálisis burocrática conocida como el cierre de la administración. Este fenómeno de bloqueo político, que detiene el engranaje público y deja incluso a los funcionarios sin percibir su nómina, resulta absolutamente ajeno y casi cinematográfico para la mentalidad europea. En el Viejo Continente, quizá por un exceso de garantismo o un arraigado espíritu legalista, hemos diseñado sistemas capaces de seguir operando incluso ante la ausencia de presupuestos aprobados.

Ejemplos notables como el de Bélgica, que logró funcionar durante periodos récord de 541 y 591 días sin un ejecutivo formal, demuestran que la maquinaria estatal puede mantenerse en marcha gracias a la estabilidad de sus normas. ¿Es este modelo mejor o peor que el estadounidense?Contar con reglas claras y respetarlas parece ser el seguro de vida necesario para que la sociedad nunca deje de funcionar.

Arrancan las obras del nuevo Centro de Datos de la Junta de Andalucía, con 35 millones de inversión

El consejero de Industria, Energía y Minas y presidente de la Agencia Digital de Andalucía, Jorge Paradela, ha participado en el acto simbólico de colocación de la primera piedra del nuevo Centro de Proceso de Datos (CPD) de la Junta de Andalucía que se levantará en la Isla de la Cartuja de Sevilla, en el recinto de Sevilla TechPark. Una infraestructura estratégica en el proceso de transformación digital de la región, con una inversión de 35 millones de euros y concebida para convertirse en el "cerebro tecnológico" de la Administración andaluza.

Jorge Paradela ha destacado que el nuevo centro es "una actuación emblemática de la infraestructura digital de la Junta de Andalucía" y se convertirá en "un referente nacional en sostenibilidad, fiabilidad y eficiencia, y representa un paso decisivo en la estrategia del Gobierno andaluz para consolidar a Andalucía como líder de la transformación digital en España". Ha precisado, además, que "será el único CPD de España con un sistema de autoconsumo fotovoltaico de más de 20.000 metros cuadrados, que permitirá cubrir al menos el 50% de su demanda energética con fuentes renovables", ha subrayado el consejero.

Esta infraestructura, impulsada por la Agencia Digital de Andalucía (ADA) de la Junta de Andalucía, ocupará una superficie de 5.150 metros cuadrados con una edificabilidad de 6.240 metros cuadrados, y estará diseñado bajo criterios de fiabilidad, modularidad y eficiencia energética.

En el acto de primera piedra, en el que ha participado el alcalde de Sevilla, José Luis Sanz, y el subdelegado del Gobierno, Francisco Toscano, el consejero ha explicado que el nuevo CPD contará con "un innovador sistema de refrigeración por gas que sustituye al tradicional uso de agua, lo que constituye una medida pionera que refuerza el compromiso con la sostenibilidad y la gestión responsable de los recursos hídricos, especialmente relevante en el contexto de sequía estructural de la región". De hecho, gracias a estas innovaciones, "el CPD reducirá un 75% las emisiones de CO respecto a los centros actuales".

El consejero Paradela en su intervención en el acto con el que arrancan las obras del nuevo 'cerebro' tecnológico de la Junta.

Jorge Paradela en su intervención en el acto con el que arrancan las obras del nuevo 'cerebro' tecnológico de la Junta.

El consejero ha incidido en que el proyecto no solo busca eficiencia energética y sostenibilidad ambiental, sino también reforzar la seguridad y disponibilidad de los servicios digitales de la Junta de Andalucía. Para ello, "integrará tecnologías de nube híbrida, inteligencia artificial, big data y computación cuántica para optimizar la gestión de los sistemas públicos y garantizar una administración más inteligente, accesible y cercana al ciudadano", ha abundado.

El Centro de Proceso de Datos de Sevilla se suma a la red de infraestructuras tecnológicas impulsadas por la Junta en los últimos años junto al Centro de Ciberseguridad de Andalucía (CIAN), con sede en Málaga y ya consolidado como referente en el sur de Europa y ANIA, el Centro de Inteligencia Artificial de Andalucía, inaugurado el mes pasado en Granada como polo de talento e innovación en inteligencia artificial y tecnologías exponenciales.

Esa apuesta por las infraestructuras se verá reforzada con el primer Plan de Impulso a las infraestructuras digitales en Andalucía, con el fin de favorecer el desarrollo de un ecosistema de infraestructuras digitales que disponga de enlaces de comunicaciones troncales y centros de datos de gran capacidad.

Además, la Junta de Andalucía continúa impulsando la transformación digital de la administración pública andaluza mediante el uso de infraestructuras en la nube, que aportarán beneficios como flexibilidad en el uso de recursos informáticos, mayor capacidad del procesamiento y almacenamiento de datos, mejora en la gestión de la seguridad y la privacidad de la información, una mayor velocidad y agilidad en la entrega de nuevos servicios TI y reducción de costes en infraestructuras y sistemas informáticos.

La futura nube híbrida de la Junta de Andalucía es una de las piezas clave de las acciones que marca la Estrategia Cloud de Andalucía 2030, aprobada el pasado mes de abril por el Consejo de Gobierno.

Mayor inversión de la historia

"Todas estas actuaciones forman parte de la mayor inversión en digitalización de la historia de Andalucía, con más de 1.400 millones de euros entre 2021 y 2024, y una previsión de 2.600 millones adicionales hasta 2030, con el objetivo de convertir a Andalucía en líder nacional en digitalización", ha concluido Paradela.

El consejero de Industria, Energía y Minas y presidente de la Agencia Digital de Andalucía, Jorge Paradela, el alcalde de Sevilla, José Luis Sanz, y el subdelegado del Gobierno, Francisco Toscano, en el acto de la primera piedra del CPD.

El consejero de Industria, Energía y Minas y presidente de la Agencia Digital de Andalucía, Jorge Paradela, el alcalde de Sevilla, José Luis Sanz, y el subdelegado del Gobierno, Francisco Toscano, en el acto de la primera piedra del CPD.

Hirugarrena, nuevo espacio para el emprendimiento tecnológico y la innovación en Navarra

El consejero de Industria y de Transición Ecológica y Digital Empresarial, Mikel Irujo; el rector de la Universidad Pública de Navarra (UPNA), Ramón Gonzalo; y la directora gerente de CEIN, Uxue Itoiz; han visitado las obras de Hirugarrena, el nuevo espacio para el emprendimiento y la innovación que se ubica en la tercera planta del edificio de El Sario de la UPNA.

Este novedoso espacio va a facilitar equipamiento y servicios para el impulso del emprendimiento científico-tecnológico y digital innovador en nuestra comunidad. El objetivo es que en sus instalaciones puedan desarrollar sus proyectos tanto personas emprendedoras, como startups, la comunidad universitaria y el resto de agentes del ecosistema emprendedor. Hirugarrena, que ha sido remodelado por la UPNA con fondos europeos y del departamento de Industria, será gestionado de forma compartida por CEIN y la UPNA y estará en funcionamiento a inicios de 2026.

Según ha destacado el consejero Irujo, "Hirugarrena va a ser el punto neurálgico para la creación de empresas tecnológicas y de alto impacto y para el escalado de startups de la mano de CEIN, referente en estos ámbitos en nuestro territorio. Además, va contar con los servicios del Polo IRIS de Innovación Digital de Navarra que se ubica justo encima, y con la colaboración de la UPNA. Vamos a crear sinergias muy valiosas, sin duda".

Por su parte, el rector Gonzalo ha subrayado que "dentro de la estrategia de emprendimiento de la UPNA se hacía necesario contar con un espacio específico para el desarrollo de las diferentes iniciativas de creación y desarrollo de nuestras Spin-off en colaboración con el Gobierno de Navarra y CEIN. No en vano más de dos tercios de las spin-off tecnológicas nacen de las investigaciones que se realizan en las universidades y la UPNA es la 19 universidad, en valor absoluto, que más empresas de base tecnológica ha creado en los últimos años"

Por último, Itoiz ha destacado que "este equipamiento se suma al resto de programas e instalaciones que CEIN ofrece a la ciudadanía con el objetivo de fomentar todo tipo de emprendimiento". "Actualmente contamos con 46 empresas instaladas que generan cerca de 250 empleos en nuestros viveros de Noáin y Tudela y esperamos que con estas nuevas instalaciones esta cifra crezca de forma significativa", ha concluido.

Las personas emprendedoras con proyectos vinculados a la ciencia, tecnología y

digitalización tendrán a su disposición itinerarios formativos, servicios de asesoramiento para la creación de empresas, asistencia para analizar el potencial de mercado de sus desarrollos y programas de pre-aceleración y aceleración empresarial para convertirlos en nuevas empresas.

Las startups o spin off científico-tecnológicas y digitales podrán acceder igualmente a servicios de asesoramiento y apoyo especializados y formación vinculados al escalado. Además, se diseñarán espacios de encuentro y eventos para favorecer el networking con agentes del ecosistema emprendedor, así como programas de innovación abierta con empresas consolidadas y tractoras y herramientas para facilitar la transferencia tecnológica. El colectivo universitario (alumnado, profesorado, personal investigador), por su parte, contará con acompañamiento para la creación de empresas y también para la realización de trabajos fin de grado (TFG) o fin de máster (TFM) vinculados a la creación de empresas. Del mismo modo se ofrecerá formación práctica a los estudiantes a través de las startups, así como programas de emprendimiento en doctorado, máster y cátedras.

El Ayuntamiento de Salamanca despliega con Liferay un chatbot con IA

Liferay ha anunciado que el Ayuntamiento de Salamanca ha desplegado la plataforma de experiencias digitales Liferay DXP para poner en marcha su estrategia de gobierno abierto y participación ciudadana. Más concretamente, ha desplegado un chatbot llamado Vega.

Se trata de una solución que ha transformado la relación digital con la ciudadanía y empresas, logrando una mayor interacción y consolidando un modelo de administración más cercano, eficiente e inteligente.

El Ayuntamiento de Salamanca, consciente de la necesidad de modernizar su administración y acercarla a la ciudadanía, inició en 2015 una estrategia de transformación digital que se consolidó en 2017 con el Plan de Administración Electrónica. Como parte de este plan, el consistorio buscaba poner solución a un ecosistema digital fragmentado y ofrecer una administración más eficiente y disponible 24/7, que facilitara la gestión de trámites y fomentara la participación, adaptándose a las expectativas de una sociedad cada vez más digitalizada.

Para materializar esta visión, el Ayuntamiento desplegó Liferay DXP en la nube en modalidad PaaS (Platform as a Service). Liferay DXP proporcionó la base tecnológica para "Salamanca Núcleo Tecnológico y Funcional", integrando capacidades avanzadas como inteligencia artificial, búsqueda semántica avanzada (sobre Elastic Search) y personalización de contenidos. El socio tecnológico Ayesa lideró el desarrollo, construyendo un ecosistema moderno y centrado en el ciudadano.

El ecosistema resultante se ha articulado en torno a varios pilares estratégicos. Para ello, se ha diseñado una nueva experiencia digital omnicanal, moderna y accesible desde cualquier dispositivo, que se apoya en una arquitectura de información estructurada por temáticas y un buscador potenciado por IA para ofrecer respuestas precisas. En este nuevo modelo de atención destaca el chat semántico 'Vega', un asistente virtual con IA capaz de comprender el lenguaje natural para resolver dudas de manera inmediata e ininterrumpida.

Toda esta base tecnológica ha permitido, a su vez, el desarrollo de ejes estratégicos de servicios orientados al ciudadano como 'Salamanca Comunica' para la gestión de contenidos, 'Salamanca Abierta' para fomentar la transparencia y la participación, y 'Salamanca Funciona' para centralizar trámites y servicios digitales, con información personalizada y segmentación inteligente.

"La implementación de Liferay DXP ha sido un hito fundamental en nuestra estrategia de transformación digital. Hemos logrado construir un puente digital más sólido y eficiente con nuestros ciudadanos y empresas, haciendo realidad nuestra visión de un gobierno abierto y participativo. La tecnología nos permite ser más transparentes, accesibles y proactivos, y el impacto cuantificable, como el crecimiento de visitas y el éxito de Vega, valida nuestro compromiso con la innovación al servicio de Salamanca", explica Sergio Bravo Martín, Jefe de Servicio, Departamento de Tecnologías de la Información y Comunicaciones del Ayuntamiento de Salamanca.

El impacto de esta transformación se refleja en resultados medibles y significativos. En poco más de un año, la interacción ciudadana se ha disparado, cuadruplicando las visitas al ecosistema web de 500.000 a 2 millones anuales, con 300.000 usuarios únicos. Este crecimiento ha estado impulsado por la consolidación del uso del móvil, que ya representa más del 60% de los accesos. El asistente virtual 'Vega' se ha consolidado como una pieza clave, gestionando alrededor de 21.000 conversaciones, un volumen que ya equivale al 50% del servicio telefónico 010.

ENTREVISTA

Estrella Martín,

Directora General de Emprendimiento del Ayuntamiento de Madrid

“Las AAPP no pueden depender únicamente de los proveedores tradicionales”

María Estrella Martín Martín es la Directora General de Emprendimiento del Ayuntamiento de Madrid, puesto que ocupa desde julio de 2023 dentro del Área de Gobierno de Economía, Innovación y Hacienda del Consistorio madrileño. Economista de formación, está especializada en economía de la empresa y ha desarrollado la mayor parte de su trayectoria en el ámbito de la función pública y la gestión económico-financiera. Ingresó en 1989 en el Cuerpo Superior de Intervención y Contabilidad de la Seguridad Social. Desde entonces ha desempeñado diversos puestos de responsabilidad, entre ellos jefa de Departamento de Seguimiento y Desarrollo Presupuestario, jefa de Servicio de Coordinación Económico-Administrativa y responsable de control financiero permanente en diferentes administraciones. En esta charla con ByTIC, Martín desgrana cómo conviven dos sectores tan opuestos como las startups y las administraciones públicas.

Desde su experiencia como funcionaria de carrera al frente de la Dirección General de Emprendimiento, ¿cómo ha evolucionado la relación entre las administraciones públicas (como el Ayuntamiento de Madrid) y las startups?

La relación entre las administraciones públicas y las startups ha vivido una transformación importante en los últimos años. Ya no somos una administración rígida, centrada únicamente en velar por el cumplimiento normativo, con procesos muy burocráticos y lentos, hoy somos una administración mucho más abierta y flexible, que entiende

que el emprendimiento y la innovación son motores reales para el desarrollo económico de la ciudad de Madrid.

Hace veinte años tomamos una decisión estratégica, convertirnos en un socio del ecosistema emprendedor. Apostamos por un modelo en el que el Ayuntamiento de Madrid no pone trabas, sino que ayuda; no complica, sino que facilita; y no se limita a observar, sino que acompaña a las startups en sus primeros pasos.

Y este cambio no fue algo fortuito, fue una apuesta decidida para atraer el talento y mejorar la competitividad y el futuro económico de nuestra ciudad. Porque cuando las startups crecen, Madrid crece con ellas.

Empezamos creando la red de viveros de empresas, espacios donde las startups pueden desarrollar sus ideas y crecer con recursos como asesoramiento, formación y, lo más importante, contar con una comunidad emprendedora para no emprender en soledad.

Después pusimos en marcha la Ventanilla Única de Emprendimiento, donde ofrecemos asesoramiento integral a personas emprendedoras y pymes y realizamos la constitución telemática de las empresas como Punto de Apoyo al Emprendimiento (PAE) que somos. El próximo año incorporaremos un nuevo servicio gratuito para apoyar a startups que se encuentren en dificultades o que quieran escalar su negocio.

También dimos un paso más facilitando a las startups el acceso al capital privado a través de los Foros de Inversión de Madrid Emprende, que arrancaron en 2019, y facilitando el acceso a la red de mentores de Madrid Emprende, con más de 270 mentores comprometidos con el emprendimiento, y que quieren compartir el conocimiento y la experiencia que han adquirido durante su carrera profesional con las personas que ahora empiezan a emprender.

En cuanto a una petición que siempre han hecho las startups relativa a facilitar el acceso a las licitaciones públicas, la Ley de Contratos del Sector Público (LCSP) ha supuesto un cambio importante. Ahora los procedimientos son más ágiles y flexibles: se dividen contratos en lotes funcionales, se reducen requisitos de solvencia y se facilita la subcontratación. Todo esto ha abierto la puerta a que las startups participen en proyectos que antes eran inaccesibles.

El reto ahora es seguir avanzando para que Madrid se consolide como un referente europeo en emprendimiento, porque tenemos talento, energía y una ciudad que cree en la innovación.

¿Qué es lo más fácil y lo más difícil de esta relación entre dos sectores tan opuestos y diferentes (sobre el papel)?

Lo más fácil es la parte humana, la ilusión que genera ayudar a las startups a hacer crecer y consolidar sus empresas; es algo muy gratificante.

Además, las startups aportan frescura, creatividad, tecnología y una visión muy práctica que nos puede ayudar a mejorar e innovar en procesos en los que, a veces, nos quedamos atrás las administraciones públicas. Tenemos mucho que ganar trabajando con startups.

Lo más difícil es ajustar los tiempos y las formas de trabajar. Las administraciones públicas estamos obligadas a respetar los procedimientos establecidos en la normativa vigente, que no siempre encajan con la rapidez y la flexibilidad que caracteriza a las startups. Ellas esperan respuestas inmediatas y nosotros necesitamos tiempo para asegurar transparencia y cumplimiento de la legalidad. El reto está en encontrar el equilibrio, porque las startups se mueven con gran rapidez y la administración, por su naturaleza, debe ser garantista y asegurar igualdad de oportunidades.

Por eso, creo que el camino está en buscar fórmulas más flexibles para contratar con las startups. Si logramos esto, no solo modernizaremos la administración, sino que también impulsaremos el ecosistema emprendedor.

¿Qué lecciones clave pueden extraer las AAPP de las startups, especialmente en un contexto de transformación digital?

Las administraciones públicas podemos aprender mucho de las startups, especialmente en un contexto de transformación digital ya que es un reto que han asumido como parte de su crecimiento orgánico. Por ello, la primera lección que podemos aprender es adoptar una mentalidad ágil inspirada en la forma de trabajar de las startups, fomentando equipos colaborativos y metodologías flexibles que permitan innovar con rapidez y adaptarnos rápidamente a los cambios; esa mentalidad es esencial para que las AAPP podamos responder con mayor eficacia y eficiencia a las necesidades ciudadanas.

La segunda lección es la orientación al usuario. Las startups siempre ponen al cliente en el centro de su estrategia, y las AAPP debemos hacer lo mismo con el ciudadano, por lo que debemos diseñar servicios públicos que sean digitales, pero intuitivos, accesibles y realmente útiles para ser usados por nuestros usuarios, y apoyarnos en el uso ético e inteligente de los datos para anticipar necesidades y tomar decisiones basadas en la evidencia.

Creo que la tercera lección para que una administración sea realmente pragmática es apostar por una cultura de innovación y aprendizaje continuo. Las startups nos enseñan algo muy valioso: no tienen miedo de experimentar, equivocarse y mejorar. En la administración deberíamos adoptar esa misma actitud probando nuevos servicios, lanzando programas piloto, explorando tecnologías que se adapten mejor a las necesidades de la gente, cada vez más personalizadas y, sobre todo, aprendiendo de cada experiencia para escalar lo que funciona. No se trata de innovar por innovar,

sino de hacerlo con propósito y con datos que respalden las decisiones.
En definitiva, las startups nos enseñan que la transformación digital no es solo cuestión de tecnología, sino de cultura organizativa y visión estratégica. Y esa es la gran lección que estamos incorporando en el Ayuntamiento de Madrid.

¿Qué rol juegan las AAPP como "clientes iniciales" para validar soluciones innovadoras de startups en sectores como la agroalimentación, salud digital o IA?

En 2021 la Dirección General de Emprendimiento, bajo la marca Madrid Emprende, puso en funcionamiento un nuevo vivero de empresas, Madrid Food Innovation Hub, el primer centro de fomento del emprendimiento, innovación y tecnología en la cadena de valor agroalimentaria de la ciudad de Madrid.
Queríamos crear un espacio donde las ideas se transformaran en proyectos reales, y lo hemos conseguido: en estos cuatro años hemos apoyado a más de 214 startups con programas gratuitos de incubación y aceleración y hemos formado a más de 2.400 emprendedores en áreas clave como diseño alimentario, digitalización de la restauración, el desarrollo de proteínas alternativas, foodtech, la agricultura de precisión o la reducción del desperdicio alimentario. Todo esto ha convertido a Madrid en un referente internacional en innovación alimentaria y ha fortalecido nuestro ecosistema emprendedor.
Ahora queremos dar un salto hacia otro sector estratégico: la salud. Es una industria que no solo genera empleo e inversión, sino que impacta directamente en la calidad de vida de las personas. Creemos que la mejor manera de acelerar su digitalización y modernización es fomentando el emprendimiento, igual que hicimos con el sector alimentario. Por eso estamos trabajando en la creación de un vivero de empresas orientado a salud, donde ciencia, tecnología e innovación se unan para desarrollar soluciones disruptivas, atraer inversión internacional y posicionar a Madrid como un punto de referencia global en salud digital y medicina personalizada.
Para nosotros, la mejor manera de validar soluciones innovadoras en estos sectores es a través de la colaboración público-privada. Trabajamos mano a mano con empresas y entidades para formalizar acuerdos que no solo impulsan el desarrollo y consolidación de startups, sino que también les dan visibilidad y oportunidades reales de negocio. Queremos que estas empresas tengan un canal para mostrar lo que hacen, comercializar sus servicios

y darse a conocer. Algunos de estas colaboraciones son las que hemos firmado hasta ahora con Sodexo, Alimentación Varma, S.L y el Club del Atlético de Madrid.

Madrid Emprende y los viveros de empresas han impulsado a más de 150 startups; ¿qué estrategias recomienda a otras AAPP locales para replicar estos modelos de aceleración equity-free y softlanding internacional?

Madrid Emprende, la marca bajo la que opera la Dirección General de Emprendimiento del Ayuntamiento de Madrid, se ha consolidado como uno de los principales referentes del ecosistema emprendedor en España. A lo largo de más de dos décadas, su labor ha contribuido de manera decisiva a impulsar la innovación y el desarrollo económico de la ciudad, ofreciendo recursos, espacios y acompañamiento especializado para transformar ideas en proyectos empresariales reales.
Durante este tiempo, Madrid Emprende ha asesorado a más de 262.000 personas y emprendedores, tanto en los viveros de empresas municipales como en la Ventanilla Única del Emprendimiento. Este servicio integral ha permitido que miles de proyectos encuentren orientación y apoyo en sus primeras etapas, reduciendo barreras y fomentando la creación de nuevas empresas.
Además, los viveros de empresas han incubado más de 2.400 startups o pymes, que han generado 12.400 puestos de trabajo y aportado 279 millones de euros en facturación al bienestar socioeconómico de la ciudad. Estos datos reflejan el impacto real de la iniciativa en la consolidación del tejido empresarial madrileño.
Además, Madrid Emprende ha acelerado más de 700 startups mediante programas reconocidos por su excelencia en el ecosistema emprendedor.

ENTREVISTA

Julia Bernal,

directora general de Red Hat Iberia

"Hoy más que nunca, la UE necesita resguardar la resiliencia operativa de sus administraciones públicas"

Julia Bernal atesora más de 25 años de trayectoria en el sector. Responsable del negocio de Red Hat en el mercado ibérico como directora general para España y Portugal y, más recientemente, como líder de ingresos para la región mediterránea de la compañía, esta ingeniera informática por la Universidad Politécnica de Madrid ha completado su formación con distintos programas de liderazgo y gestión en escuelas de negocio europeas. En 2016 se incorporó a Red Hat y, desde 2017, dirige la filial de España y Portugal, impulsando la adopción del código abierto, la nube híbrida y las arquitecturas modernas en empresas y administraciones públicas y consolidando a Red Hat Iberia como uno de los motores de crecimiento de la región EMEA. Además, es una de las voces más visibles en defensa del modelo open source como motor de innovación y pilar de la soberanía digital europea, subrayando el papel del software abierto en la competitividad y la resiliencia de las organizaciones. De ello nos habla en esta entrevista con ByTIC.

¿Cuáles son los principales riesgos de no avanzar en soberanía digital para las administraciones públicas europeas y, en concreto, las españolas?

La soberanía digital es un objetivo estratégico para la Unión Europea y, por supuesto, para España, en el que las administraciones públicas tienen un papel esencial. No se trata de un aislamiento digital, sino de una gestión inteligente y estratégica del ecosistema tecnológico para hacer frente a los riesgos que pueden afectar la protección de nuestros datos y nuestra privacidad, la seguridad y la resiliencia de nuestras infraestructuras críticas, así como la innovación y el desarrollo económico europeo.

Se trata de asegurar un futuro digital resiliente y alineado con nuestros valores como europeos, en el que tengamos la capacidad de aplicar el marco normativo europeo, diversificar y fortalecer nuestro tejido tecnológico, y así fomentar un ecosistema tecnológico propio capaz de generar propiedad intelectual, software y soluciones de vanguardia.

En Red Hat llevamos 30 años desarrollando tecnología en el modelo de código abierto,

que funciona como el principal habilitador de esa soberanía digital, ya que proporciona transparencia, seguridad y flexibilidad, características que hacen posible responder a los riesgos que podría conllevar el hecho de no avanzar en soberanía digital.

¿Qué elementos diferencian la propuesta de Red Hat Confirmed Sovereign Support frente a otros modelos de soporte tradicionales u ofertados por proveedores de software propietario?

Es una propuesta diseñada específicamente para y desde la Unión Europea, abordando los retos de la soberanía digital. Garantizamos que en la asistencia técnica solo participen ciudadanos de la UE, acreditados y que operan exclusivamente desde dentro de los 27 estados miembros, asegurando una total alineación con el contexto regulatorio y cultural europeo. Este control operativo localizado, gestionado y supervisado desde la Unión Europea y disponible 24/7 en la región, reduce la dependencia de dinámicas externas y refuerza la resiliencia operativa de las administraciones públicas y de las organizaciones. Este enfoque de Red Hat se amplifica gracias a su sólido ecosistema de más de 500 socios de nube de la UE, muchos de los cuales ya ofrecen nubes soberanas. Esta potente red ayuda a reducir estratégicamente la dependencia de los hiperescalares no comunitarios, proporcionando a los clientes alternativas robustas y locales que se alinean directamente con las políticas regulatorias regionales y las prioridades económicas. Es un soporte que permite a las organizaciones desplegar, ejecutar y mantener sus infraestructuras de TI actuales y futuras de forma independiente en cualquier entorno de nube soberana.

¿Por qué la soberanía digital se ha convertido en una cuestión estratégica para la UE en el contexto geopolítico y regulatorio actual?

En el contexto geopolítico actual, marcado por una mayor interconexión, inestabilidad política y riesgo de dependencias tecnológicas, la UE busca asegurar su autonomía estratégica. Esta autonomía implica fortalecer su capacidad de decisión y acción sobre su propia infraestructura digital, el tratamiento de sus datos y la seguridad de sus infraestructuras más críticas. Hoy más que nunca, la Unión Europea necesita resguardar la resiliencia operativa de sus administraciones públicas y empresas frente a cualquier disrupción externa, garantizando la continuidad y la integridad de sus servicios esenciales. La UE tiene un firme compromiso con la protección de los derechos digitales y la privacidad de sus ciudadanos, lo que le ha llevado a desarrollar un marco regulatorio que muestra el camino hacia una implementación tecnológica más responsable y alineada con los valores europeos. La soberanía digital es la materialización de la aspiración de que estos valores y principios se apliquen de forma consistente y efectiva en todo el ecosistema digital, sin importar dónde se generen, procesen o almacenen los datos. Busca asegurar un control jurisdiccional pleno y la capacidad de auditoría sobre las soluciones tecnológicas, fomentando un entorno de confianza y transparencia. Este enfoque no solo impulsa la creación de un mercado único digital con bases sólidas y equitativas, sino que también promueve la innovación local y el desarrollo de tecnologías que estén intrínsecamente alineadas con los valores y la visión a largo plazo de una Europa digitalmente independiente.

¿De qué forma la base de open source constituye la única "ruta confiable hacia la soberanía digital", como afirma Red Hat? ¿Qué rol tienen la transparencia y la auditabilidad en ese modelo?

La soberanía digital es la capacidad de una nación o una organización para controlar su propio destino tecnológico, garantizando que sus datos, infraestructuras y procesos no estén sujetos a la influencia o el control de actores externos. Y para controlar ese destino, la transparencia total y la capacidad de auditoría son necesarias. Precisamente por eso, el open source es un habilitador de la soberanía digital, ya que ofrece transparencia y seguridad gracias a la comunidad global que lo sustenta, y que tiene la capacidad de auditarlo. Esta forma de trabajo comunitario fomenta la innovación colaborativa, y facilita la identificación rápida de vulnerabilidades. Además, actúa como un catalizador, permitiendo que un ecosistema de empresas innove y construya soluciones propias sobre una base tecnológica abierta y verificable.

La flexibilidad que proporciona el código abierto es la que habilita la arquitectura que mejor materializa este concepto: la nube híbrida. Al adoptar una estrategia de nube híbrida abierta, las empresas y las administraciones públicas recuperan la capacidad de decidir estratégicamente dónde y cómo gestionar sus cargas de trabajo. Pueden mantener los datos más sensibles en sus propias instalaciones o en nubes privadas, mientras aprovechan la escala y la agilidad de las nubes públicas para servicios menos críticos. Este enfoque les devuelve el control total sobre sus datos, sus infraestructuras, sus tecnologías y sus procesos, que es, en esencia, el principal objetivo de la soberanía digital.

A medida que el sector público busca autonomía en nube e IA, ¿cómo afronta Red Hat la demanda de soluciones que permitan desplegar infraestructuras TI sin depender de grandes "hiperescaladores" internacionales?

Entendemos perfectamente esta demanda. De hecho, está en el centro de nuestra propuesta de valor, porque la soberanía digital para el sector público no se trata de rechazar la innovación, sino de tener el control estratégico sobre sus infraestructuras y datos. Nuestra propuesta se basa en tres pilares fundamentales. Por un lado, ofrecemos tecnología habilitadora, que funciona como una capa de abstracción consistente que

permite a las administraciones desplegar y gestionar sus aplicaciones en cualquier entorno que elijan, eliminando la dependencia de un hiperescalar específico y garantizando que sus datos no queden "bloqueados" en una arquitectura propietaria. Esta abstracción sirve para las cargas de trabajo de IA. Con Red Hat AI 3, ofrecemos capacidades como la inferencia distribuida inteligente con llm-d, que permite ejecutar modelos de lenguaje de gran tamaño (LLM) de forma eficiente en la propia infraestructura de la organización, optimizando el uso de su hardware y reduciendo costes. Además, ofrecemos las capacidades de Modelo como Servicio (MaaS), que permite a los equipos de TI del sector público actuar como sus propios proveedores de MaaS, sirviendo modelos comunes de forma centralizada y ofreciendo acceso bajo demanda tanto para desarrolladores de IA como para aplicaciones de IA. Esto no solo garantiza la soberanía del dato y el cumplimiento de la regulación europea al evitar la exposición a servicios públicos, sino que ofrece la libertad de ejecutar 'cualquier modelo, en cualquier acelerador y en cualquier nube', eliminando la dependencia de arquitecturas propietarias.

Red Hat destaca el soporte técnico gestionado exclusivamente por ciudadanos de la UE. Más allá de la localización del personal, ¿qué ventajas prácticas se derivan para las administraciones públicas a la hora de garantizar la protección de datos, la seguridad y el cumplimiento normativo?

Esta propuesta supone una serie de ventajas. Por un lado, asegura que toda la operación de soporte está bajo la jurisdicción de la UE, protegiendo a las administraciones de leyes extraterritoriales que podrían obligar a un proveedor a compartir datos. Además, el personal que accede, aunque sea para soporte, a sistemas potencialmente críticos, tiene una acreditación y un vínculo legal con la UE. Y, por último, fomenta el talento tecnológico local, creando un círculo virtuoso de experiencia y conocimiento dentro de Europa. En la práctica, asegura que los datos y las operaciones se gestionan de acuerdo con las normativas y los valores europeos en todo momento.

Dado que el ecosistema de socios locales es clave en esta propuesta, ¿cómo trabaja Red Hat para fortalecer ese tejido y reducir la dependencia de tecnologías y servicios no comunitarios?

Para nosotros la soberanía digital se construye en comunidad. Entendemos que la tecnología es la base, pero que la soberanía digital se construye a través de un ecosistema fuerte y colaborativo de socios locales . Por ello, nuestro papel va más allá de ser un proveedor de software. Actuamos como un catalizador y orquestador de este ecosistema, asegurando que las organizaciones europeas tengan acceso a

soluciones y talento de proximidad.

En la práctica, esto significa que trabajamos activamente con una red diversa de socios locales para cubrir todas las dimensiones de la soberanía. Colaboramos con integradores de sistemas que certifican la seguridad y el cumplimiento normativo, con proveedores de nube regionales que proporcionan la soberanía operativa y del dato, y con consultores que validan los procesos. Esta colaboración, sobre una base de código abierto, es la que hace posible el desarrollo de soluciones soberanas que son auditables, confiables y adaptadas a las necesidades específicas de cada entidad pública o privada.

La soberanía digital debe ser el motor para fomentar un ecosistema tecnológico propio, capaz de generar propiedad intelectual, software y soluciones de vanguardia. A través de la inversión en el talento y en las tecnologías abiertas podremos impulsar una verdadera innovación y generar empleo de alta cualificación que definirá nuestra competitividad futura. Al hacerlo, no solo aceleramos el camino de nuestros clientes hacia la soberanía digital, sino que también creamos un círculo virtuoso que fortalece el tejido tecnológico, fomenta el talento y aumenta la competitividad industrial de toda Europa.

Retos de la resiliencia digital en el sector público: Talento, burocracia y legacy

En un reciente encuentro ejecutivo de la Comunidad ByTIC, patrocinado esta vez por Lenovo y Veeam Software, representantes de diversas entidades públicas analizaron los retos de la resiliencia digital a los que se enfrentan en sus organizaciones. La transformación digital del sector público español tiene ante sí una encrucijada marcada por la escasez de talento cualificado, la rigidez de los procesos de contratación y la complejidad de modernizar sistemas tecnológicos heredados, según se desprende de los comentarios realizados por estos altos responsables de entidades clave como Grupo Tragsa, Renfe, AENA, Correos, la Agencia Tributaria, la Oficina Española de Patentes y Marcas y la Casa Real. Unas barreras comunes que dificultan garantizar servicios públicos resilientes y sostenibles en un entorno cada vez más exigente.

De nuevo el talento

La falta de personal vuelve a aparecer como el principal obstáculo, un problema que trasciende las limitaciones presupuestarias del pasado. Cristóbal Rodríguez, subdirector de sistemas en Grupo Tragsa, fue contundente al describir la situación. "Básicamente, la falta de medios por la dificultad de tenerlos", afirmó, para luego precisar: "La falta de recursos de personas. Hemos llegado a una situación, iba a decir absurda, pero no podemos gastar todos los medios económicos que tenemos por falta de recursos". Rodríguez detalló las dificultades inherentes a su condición de empresa pública, con "limitaciones de contratación inmensas", contratos temporales de solo seis meses y "tablas salariales absolutamente fuera de mercado".

Esta visión es compartida en Correos, donde la búsqueda de talento es una lucha constante. Verónica Crespo, jefa de área en la Dirección de Tecnología, señaló que "para nosotros también es el principal problema, no encontrar personal cualificado, poderlo contratar internamente". Aunque recurren a la externalización, Crespo subrayó la necesidad de equipos internos para "retener ese conocimiento". Su compañero, Jon Sarasola, responsable de explotación de infraestructuras, añadió otro desafío crítico: "el tema de legacy, la obsolescencia tecnológica también es uno de los retos con lo que estamos luchando constantemente".

En Renfe, el problema es una combinación de factores. Pedro Galián, responsable de seguridad, explicó que la estrategia de la compañía ha sido externalizar el área técnica a través de una filial, creando centros tecnológicos en la llamada "España vaciada". Sin embargo, la retención del talento sigue siendo un hándicap. "El personal que está en Madrid cuesta mucho, y es la misma empresa", comentó Galián, reconociendo que, si bien han reducido la rotación, esta "empieza otra vez" si las condiciones económicas no son competitivas. Además, la agilidad para adoptar nuevas tecnologías se ve frenada por la burocracia. "El poder ir a una cloud nos cuesta. No tenemos esa capacidad de decir 'me voy a la cloud y voy mañana'. Esa capacidad de contratación o de actualización tecnológica nos cuesta porque no contratamos directamente", lamentó.

Desde la Oficina Española de Patentes y Marcas, Ana Redondo, directora de la división de tecnología, apuntó a un reto más organizativo y cultural. Con una gran cantidad de "activos de software que tienen muchos años y que funcionan muy bien", el principal desafío es adaptar la seguridad a un paradigma en constante cambio. "El mayor reto, que es el que estamos afrontando ahora, es desde el punto de vista organizativo. Montar una

buena estructura que sea capaz de reaccionar rápido", declaró Redondo. "Culturalmente es algo que cuesta", admitió, destacando la importancia de que cada miembro interiorice su rol ante situaciones inesperadas.

Mariano Domingo, CIO de AENA, describió un panorama de cierta complejidad en el que, a pesar de ser una empresa muy atractiva, experimentan similares condicionantes. "Estamos sujetos, desde el punto de vista de contratación de personal interno, a toda la legislación pública", explicó. Una de las consecuencias es una dificultad para atraer y retener talento IT interno. En el caso de la contratación de proveedores externos, lo que si advertimos por parte de nuestros proveedores, es una alta rotación en áreas críticas como la ciberseguridad dado que son recursos altamente demandados". "En un año o dos años, los proveedores externos en este ámbito, han rotado aproximadamente un 25% de las plantillas", estimó. Mariano Domingo también introdujo otro reto mayúsculo: la gestión desde el punto de vista de ciberseguridad, de un "perímetro cada vez más amplio y más dinámico.", especialmente en la convergencia de los mundos IT y OT (Tecnología de la Operación). "Estamos llevando el ámbito de ciber al mundo OT. Como infraestructura crítica que somos, desde el punto de vista de ciberresiliencia, nos está planteando un gran reto que estamos afrontando con determinación ", afirmó, mencionando la necesidad de mejorar la protección de activos OT como sistemas del ámbito security o safety ".

Por su parte, Luis Amper, responsable de ciberseguridad en la Casa Real, identificó el presupuesto como el principal desafío histórico. "En nuestro caso, el mayor reto siempre debe ser presupuestario. Llevamos muchos años con presupuesto controlado", indicó. A esto se suma la dificultad para incorporar personal y "las propias limitaciones que impone el propio usuario a la hora de innovar", describiendo su entorno como una de las "administraciones más conservadoras".

Finalmente, José Borja Tomé, director del Departamento de Informática Tributaria de la Agencia Tributaria, añadió una variable social que impacta directamente en la contratación: la demanda de teletrabajo por parte de los nuevos profesionales. "Me sorprende. Hay gente que dice 'no, que aquí no se puede teletrabajar', pues no me interesa", relató, confirmando que esta se ha convertido en una de las primeras condiciones en las entrevistas laborales, un reflejo de cómo las nuevas expectativas del mercado laboral chocan con las estructuras tradicionales de la administración.

Inteligencia Artificial, ¿salvavidas o espejismo?

Ante esta cruda realidad de que el modelo actual de desarrollo tecnológico es insostenible, se puso sobre la mesa la opción de que la inteligencia artificial (IA) sea esa herramienta disruptiva que genera tanto esperanza como escepticismo.

La demanda de nuevas funcionalidades crece de forma exponencial, mientras que los recursos, humanos y presupuestarios, son finitos. Esta tensión obliga a una búsqueda incesante de eficiencia que, paradójicamente, puede mermar la capacidad de las organizaciones para afrontar imprevistos.

José Borja Tomé, de la Agencia Tributaria, fue contundente al diagnosticar el problema de raíz. "A mí me gusta decir que tenemos un problema básico y es que la tecnología no es sostenible, nuestra tecnología no es sostenible", afirmó. "Todo lo que hacemos lo tenemos que mantener el resto de la vida, pero cada año la sociedad, nuestros clientes, nos demandan que construyamos funcionalidades adicionales". Esta dinámica crea una presión insostenible. "Si tus recursos no son crecientes hasta el infinito y más allá, pues siempre hay un momento en el cual, por lo que quiera que sea, te vas a encontrar en una situación de estrecheces, que solamente puedes resolver de una manera que es haciéndote más eficiente", señaló.

Sin embargo, la eficiencia tiene sus límites y un coste oculto. "La eficiencia está reñida con la resiliencia, porque evidentemente cuando no tienes grasa, pues es muy difícil que puedas pasar el invierno", advirtió el directivo. "Cuando

te vienen mal dadas, resulta que ya no tienes ningún recurso adicional". Ante este panorama, la conversación giró inevitablemente hacia el papel de la IA. ¿Puede ser la solución a la falta de recursos? La visión general de los participantes muestra ciertos recelos o, al menos, cautelas. "La inteligencia artificial, como cualquier otra tecnología y en este caso disruptiva, en la medida en la que nos pueda ayudar a ser más eficientes, pues al menos durante un tiempo nos permitirá lo mismo que nos han permitido otros cambios tecnológicos", comentó Tomé. Sin embargo, advirtió sobre los costes asociados: "Hoy por hoy, si hablamos sobre todo de IA generativa, tampoco es barata. El coste del entrenamiento es muy grande y el coste de la inferencia también tiene un coste que existe".

La discusión se centró en el impacto real de la IA en el desarrollo de software. Lejos de sustituir a los programadores más cualificados, la tecnología parece, por ahora, una herramienta para potenciar su trabajo. "Tú con IA generativa puedes sustituir... ni siquiera voy a decir a un mal programador. Lo que puedes hacer es que tareas de un buen desarrollador que hasta ahora le llevaban más tiempo, puede hacerlas en menos tiempo", explicó Tomé.

Otras organizaciones, sin embargo, ya están encontrando aplicaciones prácticas. Ana Redondo, de la Oficina Española de Patentes y Marcas, reveló su uso para mejorar la calidad del software desde sus fases iniciales. "La inteligencia artificial no la usamos para desarrollar, para programar, pero sí que la utilizamos para desarrollar historias de usuario", compartió. Según explicó, la IA generativa ayuda a "recopilar todos los matices que son necesarios para realmente hacer algo que luego funcione". Además, su organización, que gestiona un volumen masivo de documentación, la emplea para optimizar procesos como las prebúsquedas del estado de la técnica para los examinadores de patentes.

Desde Grupo Tragsa, se están explorando tres vías principales. Además de buscar mejoras de eficiencia en el desarrollo, el foco está en la asistencia al usuario. "El Grupo Tragsa tiene ahora mismo 30.000 empleados y generamos cerca de 100.000 casos al año. Lo que estamos intentando es desarrollar una especie de chatbot que nos resuelva al menos el 25% de esas incidencias", detalló Cristóbal Rodríguez. La tercera línea de trabajo es la redacción de pliegos para licitaciones, aunque con ciertas reservas.

En Correos, la IA se perfila como una aliada clave para la predicción y la automatización en infraestructuras. "La IA esperamos que nos ayude precisamente a ser más predictivos, a identificar patrones, a poder reaccionar más rápidamente, incluso a la automatización, a dar una respuesta rápida ante incidentes", comentó Jon Sarasola.

La IA y la ciberseguridad

La irrupción de la IA generativa ha desatado una carrera por su adopción, generando tanto expectativas de eficiencia como una profunda preocupación por los nuevos riesgos en ciberseguridad. La dualidad de esta tecnología es clara: una herramienta poderosa para la resiliencia, pero también un arma que los ciberdelincuentes están adoptando a una velocidad alarmante.

Mariano Domingo, de AENA, admitió cierta presión inicial por adoptar estas tecnologías como la IA generativa. "Adicionalmente a iniciales medidas de seguridad y de cumplimiento del Reglamento Iact, junto con la ejecución de pilotos, una de las primeras actuaciones que hemos hecho es gestionar un poco cierta ansiedad que se genera. Parecía que, si en un año no hacías algo, se venía todo abajo", confesó. A pesar de su convicción de que la IA generativa es disruptiva y generará eficiencias, uno de los principales riesgos reside en la ciberseguridad. "Estoy convencido de que va a generar eficiencias, que va a generar impacto y valor, que nos va a ayudar, pero a la vez tenemos que ser conscientes que va a ser un riesgo que hay que gestionar. Los "malos" son más early adopters que las empresas, organismos, etc...

La conversación viró hacia el marco normativo NIS 2 y su capacidad para preparar a las organizaciones. La normativa, que obliga a reforzar la ciberseguridad en la cadena de suministro, fue vista como un avance crucial. "En ciberseguridad, no solo tienes que estar tú preparado, sino todas las empresas con las que estás relacionado y tus stakeholders, y NIS 2 aborda la cadena de suministro, que es uno de los principales riesgos en ciberseguridad", señaló Domingo, destacando la dificultad de asegurar que todos los proveedores cumplan.

Cristóbal Rodríguez, de Tragsa, reveló una dura realidad: "Nuestros incidentes de seguridad que hemos tenido este año, todos han sido por la cadena de suministro y de proveedores".

Desde la perspectiva de los fabricantes de infraestructura como Lenovo, la respuesta comienza en el nivel más fundamental. Carlos Hernández, responsable comercial de la compañía, explicó su filosofía de "arrancarla desde el silicio", detallando el exhaustivo proceso para garantizar la seguridad desde la fábrica hasta el cliente final, que incluye "tener firmados criptográficamente los firmwares para evitar corrupciones" y exigir certificaciones a todos sus proveedores.

Por su parte, empresas de software como Veeam están redefiniendo su rol. José García, responsable comercial, declaró: "No podemos escurrir el bulto de que no somos una empresa de ciberseguridad, porque el backup y la resiliencia de datos se ponen ahora mismo un activo vital". La estrategia de la compañía se centra ahora en cubrir todo el ciclo de vida del dato, lanzando soluciones para "escanear y etiquetar todos los datos que hay en una organización" y así establecer controles que garanticen un uso seguro.

ENCUENTROS BYTIC

La Administración Pública se enfrenta a la revolución de la Inteligencia Artificial

La Inteligencia Artificial (IA) promete ser una revolución en la eficiencia y la productividad, pero su éxito depende de un ingrediente fundamental: la calidad y gestión de los datos que la alimentan.

Así al menos quedó de manifiesto en un encuentro ejecutivo de la Comunidad ByTIC organizado por esta publicación que contó con el patrocinio de Ayesa y SDG Group. Dicho encuentro, que reunió a responsables de transformación digital de diversas entidades públicas, puso sobre la mesa el debate de cómo están abordando diferentes entidades públcias este desafío inicial, las dificultades encontradas en proyectos de datos compartidos y las primeras incursiones en el mundo de la IA generativa. La conclusión es clara: el camino está lleno de obstáculos, pero la voluntad de avanzar es firme, aunque no exenta de cautela y una notable tensión entre la urgencia por innovar y la necesidad de garantizar la seguridad y los derechos de los ciudadanos.

Marco normativo

Uno de los primeros puntos de fricción que se pusieron sobre la mesa fue el marco normativo actual, que limita severamente el uso explícito de la IA en resoluciones administrativas. "Desde la administración deberíamos ser muy cuidadosos cuando decimos que usamos la IA, porque ahora está la cruzada contra los algoritmos y la IA es una caja negra", advirtió Antonio Sanz Pulido, Responsable Inspección General Ministerio de Hacienda. Explicó que, ante la creciente litigiosidad, especialmente en resoluciones negativas, admitir el uso de IA "no se puede hacer bajo la normativa actual". La clave, según él, reside en decidir "hacia qué normativa queremos ir", pero reconoció que hoy por hoy "no está permitido".

Esta situación genera una paradoja, ya que la tecnología que sustenta muchos servicios públicos ya integra componentes de IA de forma casi invisible. Javier Jimeno, Head of Public Sector Business Development & Alliances SDG Group España, señaló esta contradicción:

"Hasta ahora, la tecnología estaba embebiendo esa IA de manera natural, digamos orgánica, y nadie estaba presentando ninguna queja. Y ahora de repente, porque se ha popularizado la IA generativa y se ha generado este ruido, pues todo el mundo está muy preocupado por la explicabilidad". Como ejemplo, citó el caso de la Agencia Tributaria, que, aunque oficialmente no usa IA para sus decisiones, se beneficia de ella a través de las infraestructuras que emplea. "Ha sido un gran beneficiario", afirmó, cuestionando la viabilidad de separar los procesos con y sin esta tecnología.

La gobernanza del dato, el primer paso

La gestión de los datos en organismos de gran envergadura como el Ayuntamiento de Madrid es un desafío colosal. Marta Cruz, jefa del servicio de coordinación de la transformación en la Oficina Digital, explicó cómo han tenido que poner orden en un ecosistema donde "los datos han aflorado por todas partes". Para ello, la estrategia ha sido reforzar la gobernanza y la colaboración. "Se ha creado una estructura para poder crear grupos de trabajo", detalló. "En primer lugar, se creó una estrategia de datos que sirve para aclarar ideas y poner una dirección a todo lo que se estaba haciendo". Esta estructura incluye la figura del "delegado digital" en cada área, un nexo clave entre los responsables de negocio y la Oficina Digital. El objetivo final, según Cruz, es ambicioso: "Estamos avanzando hacia lo que parece que va a ser por donde vaya Europa, que es la creación de un espacio de datos del ayuntamiento para poder poner unas reglas de compartición de los datos que ya tenemos y que además las empresas privadas con las que colaboramos (...) puedan también aportar datos".

Una experiencia diferente es la del Instituto Cervantes, que optó por integrarse en la plataforma del dato de la Administración General del Estado (AGE). Tíscar Lara, Subdirectora de Transformación y Comunicación Digital, relató un proceso marcado por los retrasos. "En un primer

momento pensamos en tener una propia, pero como estaba la de la AGE, que también debe ser así, empezamos a trabajar con ellos. Con los retrasos que también tenía porque también la estaba construyendo", admitió. La plataforma, financiada con fondos PRTR, ha sido un camino de aprendizaje. "¿Estáis satisfechos con el servicio que ha dado?", se le preguntó, a lo que respondió con sinceridad que, dados los "muchos retrasos qye ha tenido", el resultado no ha sido el de iba a ser. Pese a las dificultades, el Cervantes sigue adelante y ahora se enfoca en la siguiente fase. "Ahora el punto en el que estamos es en el de poner en marcha la oficina del dato, la gobernanza del dato, toda la estructura de cómo vamos a manejar eso", afirmó, reconociendo que de momento tienen "todo un desarrollo pero en papel".

Esta experiencia con la plataforma de la AGE fue compartida por otros participantes. Antonio Sanz Pulido, responsable de la Inspección General del Ministerio de Hacienda, reveló que su organismo decidió abandonar el proyecto. "Nosotros fuimos pioneros y nos salimos", declaró. La razón fue la falta de avances tangibles: "Nos habían vendido que el entorno de pre iba a estar en tres meses, nos salimos del proyecto después de un año y no había entorno". Sanz Pulido aclaró que, aunque el proyecto no fue un éxito, "sí que nos ayudó a ver muchos temas, que teníamos muchos datos heterogéneos". Esta experiencia les ha permitido ahora "empezar a explorar proyectos de IA, pero digamos más compartimentalizados".

Las primeras incursiones en la Inteligencia Artificial

Respecto a la inteligencia artificial, Antonio Sanz Pulido reconoció que están en una fase incipiente, arrastrados por lo que la consultora Gartner denomina "la ola que te arrastra". "No puedes planificar nada porque empiezan a usarlo los usuarios,

entonces ya tienes que ir corriendo a hacer unas directrices", comentó. Por su parte, Renfe ha optado por un enfoque estructurado para no dejarse llevar por esa misma ola. Sara Guillén, jefa del área de transformación tecnológica, explicó que han replicado el modelo de gobierno del dato para la IA. "Hemos definido un framework (...) para no solo gestionar la parte metodológica, sino también la parte regulatoria y compliance que nos aprieta a todos mucho", señaló. Para identificar los casos de uso más valiosos, implicaron a toda la organización, "desde los maquinistas hasta gente de taller".

Finalmente, Pedro Hernández, subdirector general de Tecnologías de la Información y Comunicaciones del Ministerio de Trabajo y Economía Social, compartió la visión de su departamento, donde el primer objetivo es claro: "el incremento de la productividad de los empleados". Para ello, han adoptado una política abierta y pragmática sobre el uso de herramientas de IA generativa como ChatGPT, Copilot o Gemini. "Hemos optado por una política bastante laxa, es decir, ten cuidado con lo que metes, o sea, puedes usar cualquier herramienta, pero no metas datos sensibles y revisa lo que te devuelva", explicó. La filosofía es no intentar "poner puertas al campo" y permitir que los empleados exploren las posibilidades, siempre bajo unas directrices básicas de seguridad.

Responsables de tecnología y datos de diferentes áreas de la administración debatieron también sobre el estado actual de la implantación, compartiendo experiencias y preocupaciones comunes.

Una de las primeras decisiones a las que se han enfrentado es el grado de libertad que se debe otorgar a los funcionarios para usar estas nuevas herramientas. Víctor Balbás, Dirección de Sistemas y TIC MITECO, explica que han optado por una política flexible, pero con un claro aviso sobre la responsabilidad individual. "Hemos avisado de la responsabilidad de que tu información a través de aquí y al mismo tiempo de los resultados que te devuelve, permanece inalterable en el funcionario", advierte. "Si un funcionario que utiliza la inteligencia artificial crea una alucinación, se la come y da una respuesta inválida, pues veremos a ver las consecuencias que tiene eso".

La lógica detrás de esta política es pragmática: prohibir su uso podría ser contraproducente. "Hemos pensado que lo van a hacer igual el que lo quiera hacer, salvo que lo capes y que entonces es posible que lo que hagan es, eso es, se conectan por el móvil para resolver las dudas y encima, además de generar una dificultad a él, le estás teniendo la brecha de seguridad igual", argumenta Víctor Balbás. "Por ahí sí que hemos preferido tener una política mucho más laxa y mucho más de concienciación".

Asimetría ante el ciudadano y el reto de la soberanía

Esta nueva realidad introduce una dinámica inédita en la relación entre la administración y el ciudadano. Raúl Casado , Responsable de AI-DATA y Digital Experience para AAPP Ayesa, reflexionó sobre una "situación ahora asimétrica", en la que el ciudadano dispone de herramientas para interpretar y responder a la compleja jerga administrativa. "Ahora llega la gente, le saca una foto, lo sube a ChatGPT y hace un escrito y te manda el escrito", describió. Esto podría llevar a que el ciudadano "empiece a, digamos, a atacarle", empoderado por una comprensión que antes no tenía. La administración, por tanto, "acaba de perder la conversación".

Esta nueva realidad, sin embargo, también fue vista como una oportunidad. Antonio Sanz argumentó que, lejos de ser un arma, la IA podría eliminar barreras: "Si me lo simplifican el lenguaje, yo no tengo que referir a ella. A mí me parece que eso acerca al ciudadano de la administración".

La capacidad de la IA para procesar y traducir la ingente documentación burocrática se perfila como su mayor valor. "Gran parte de los proyectos que se hacen con IA de más productividad están en torno a la gestión documental", se afirmó.

La lenta maquinaria pública frente a la velocidad tecnológica

El debate se trasladó al contraste entre el sector público y el privado a la hora de adoptar estas innovaciones. Javier Jimeno, Head of Public Sector Business Development & Alliances SDG Group España, fue claro al señalar que "es un tema que marca la diferencia es la agilidad en la elección y en la contratación". Explicó que mientras una empresa privada puede tomar decisiones rápidas, "en la empresa pública tienes que pasar por un proceso de licitación que son meses en el mejor de los casos". Este ritmo más lento choca con una tecnología cuyo retorno de inversión (ROI) es muy claro, especialmente en áreas como la atención al cliente.

La velocidad del cambio tecnológico choca frontalmente con la inercia administrativa. Durante el debate, algunas voces plantearon que, aunque se quieran adoptar determinadas herramientas, mientras se produce esa adopción ya está habiendo un cambio mientras la estás adaptando. Además, el requerimiento de la aprobación por parte de instancias superiores abre otro frente, "Desde arriba no pueden y no tienen agilidad, pero si se pudieran tenerla sería lo ideal: tener un grupo de gente que estuviera tope probándolo todo y dándonos esa tranquilidad de 'por aquí sí, por aquí no, esto es bueno'".

La ausencia de directrices claras es una queja recurrente. Se menciona la necesidad de "una política de uso de la inteligencia artificial a nivel AGE". Un ejemplo concreto ilustra la lentitud: "Nosotros hemos sacado una resolución con estas cosas un año y medio después de que saliera ChatGPT, o casi dos años, y todavía no hay una política. Ya no es la agencia, más bien la Secretaría de Estado de Función Pública".

A pesar del optimismo sobre el potencial de la tecnología, sobrevoló un sentimiento de pesimismo sobre la capacidad de la administración para capitalizar esta oportunidad.

TEMA DE PORTADA

Las AAPP españolas, bajo asedio constante

La ciberseguridad en las administraciones públicas españolas atraviesa una fase de exposición máxima: el volumen y la sofisticación de los ataques crecen más rápido que la capacidad operativa para contenerlos, pero la inversión en marcos como el ENS, la Estrategia España Digital 2026 y el Plan Nacional de Ciberseguridad empieza a consolidar una base más madura.

Por eso, no es de extrañar que los responsables tecnológicos del sector público se muevan en una tensión permanente entre resiliencia, cumplimiento regulatorio, escasez de talento y presión presupuestaria, mientras los atacantes convierten a la administración en uno de sus objetivos preferentes.

Un sector en el centro del tablero

En pocos años, la administración pública ha pasado de ser un objetivo secundario a situarse en el foco de la ciberdelincuencia en Europa y en España. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) estima que cerca del 38% de los ciberincidentes registrados en 2024 en la UE afectaron a organismos públicos, y el Centro Criptológico Nacional (CCN-CERT) sitúa en torno al 34% la proporción de ataques dirigidos al sector público en España, con más de 100.000 incidentes anuales y crecimientos de casi el 190% respecto al año anterior.

Esta presión se traduce en una sucesión de

incidentes visibles que han dejado al descubierto debilidades estructurales: desde campañas coordinadas de denegación de servicio contra diputaciones y ayuntamientos hasta ataques de ransomware que han paralizado durante días consistorios como Badajoz, Melilla o otros municipios de tamaño medio, obligando a suspender trámites, cerrar sedes electrónicas y limitar la atención ciudadana.

"Lo primero que debería asumir la Administración Pública es que, en algún momento, sí o sí, se dará una circunstancia en la que la seguridad se verá amenazada por un ataque de ransomware o por cualquier otra incidencia", subraya Alejandro Rebolledo, Consulting Solutions Engineer de NetApp para España y Portugal. La administración se ha dotado en paralelo de un armazón regulatorio singularmente exigente: el Esquema Nacional de Seguridad (ENS), actualizado por el Real Decreto 311/2022, ya incorpora muchos de los requisitos de la Directiva NIS2 y obliga no solo a las administraciones de todos los niveles, sino también a sus proveedores tecnológicos. Sin embargo, en palabras de Eduardo Montero Remesal, Fortinet System Engineer Manager para Sector Público, "creer que basta con cumplir la normativa mediante un check puntual, sin tener sólidos protocolos de prevención y respuesta, y alimentar, configurar y operar adecuadamente los productos y servicios desplegados, conduce inevitablemente a problemas de seguridad"

Del "check" normativo a la resiliencia operacional

Los expertos coinciden en que el gran salto pendiente no es tanto regulatorio como operacional.

Es cierto que el sector público español ha avanzado en marcos, guías y certificaciones, pero sigue arrastrando un déficit de capacidad real para detectar, contener y recuperarse de los incidentes con la rapidez que exige el entorno actual. "En la actualidad, la principal brecha no es tecnológica, sino de capacidad operativa", advierte Rebolledo, que apunta a un exceso de tareas manuales, herramientas aisladas y falta de centralización que sobrecarga a unos equipos de seguridad limitados y fragmenta la visión sobre el dato.

Montero incide en esa idea desde otra perspectiva: el problema no es la falta de soluciones, sino de gestión y de talento capaz de sacarles partido. "En el momento actual, la principal brecha en la ciberseguridad de las Administraciones Públicas españolas se encuentra en el talento especializado, más que en la tecnología disponible", sostiene, reclamando una formación técnica sostenida para los funcionarios que gestionan entornos híbridos y una gobernanza más estratégica del ecosistema tecnológico para evitar solapamientos y herramientas infrautilizadas.

La visión de César Deza, director de Desarrollo de Negocio para Sector Público en Palo Alto Networks España, es que "las organizaciones del sector público afrontan el doble desafío de asegurar la protección y, a la vez, de mejorar la eficiencia en un contexto de crecientes ciberamenazas" y, para ello, "necesitan dejar atrás la fragmentación tecnológica y apostar por la plataformización". Frente a modelos basados en decenas de soluciones inconexas, Deza defiende arquitecturas unificadas capaces de reducir el "ruido" operativo, simplificar la

gestión y cerrar los puntos ciegos que hoy explotan los atacantes.

Riesgos en aumento: del ransomware a la superficie de ataque extendida

La estadística y los casos recientes muestran una combinación de riesgos donde el ransomware actúa como vector estrella, pero no el único. Ayuntamientos y diputaciones han sufrido cifrados masivos de sistemas que han afectado a la tramitación de expedientes, al registro electrónico y a la recaudación, mientras proliferan las campañas de denegación de servicio distribuida (DDoS) lanzadas por grupos hacktivistas, en ocasiones vinculados a conflictos geopolíticos.

De hecho, El sector gubernamental ha concentrado gran parte de los incidentes, con especial protagonismo de los ataques de denegación de servicio lanzados por el grupo de hacktivistas prorruso NoName057 al menos durante la primera mitad de 2025, que también detalla ataques de ransomware a ayuntamientos como Melilla o la Vila Joiosa.

A esta presión se suma la ampliación de la superficie de ataque asociada a la digitalización acelerada de los servicios públicos, la extensión del trabajo híbrido y la adopción de infraestructuras en la nube. Los sistemas legacy conviven con entornos multicloud y aplicaciones SaaS, lo que complica la aplicación homogénea de controles de seguridad y multiplica los posibles vectores de entrada.

Deza insiste en que "una de las principales brechas en la seguridad en el Sector Público está representada por la falta de agilidad en la detección y la respuesta a incidentes, debido a que muchos de estos organismos siguen añadiendo tecnologías de seguridad sobre infraestructuras tecnológicas legacy", y reclama facilitar la seguridad nativa en la nube y capacidades de inspección del tráfico cifrado en tiempo real.

El dato, mientras tanto, se ha convertido en el auténtico campo de batalla. La irrupción de la inteligencia artificial, tanto en manos defensivas como ofensivas, agrava el riesgo de filtraciones, manipulación de información y explotación de datos sensibles. "Otra brecha importante para la seguridad en la Administración es la gobernanza del dato", alerta Rebolledo, que apunta a la necesidad de mapear, clasificar y contextualizar la información (incluyendo datos personales identificables) con apoyo de IA, machine learning y procesamiento de lenguaje natural para evitar la "gobernanza a ciegas" y dar respuesta a obligaciones regulatorias como GDPR o ENS.

El reto de coordinar un escudo distribuido

La respuesta del Estado y de las comunidades autónomas ha incluido la puesta en marcha de un Centro de Operaciones de Ciberseguridad (SOC) para la Administración General del Estado, así como la creación de SOC autonómicos y la Red Nacional de SOC pilotada por el CCN-CERT. Este entramado pretende coordinar la defensa de un mosaico de miles de organismos, desde ministerios hasta pequeños ayuntamientos, pasando por entes instrumentales y empresas públicas.

Montero considera que "el impulso del Centro de Operaciones de Ciberseguridad de la Administración General del Estado, junto con los SOC autonómicos y locales, es un acierto estratégico, especialmente en la medida en que la AGE asume un papel de liderazgo y coordinación del conjunto del ecosistema". Propone un modelo escalonado en el que las entidades locales dispongan, al menos, de un "SOC de Nivel 1" capaz de monitorizar, detectar anomalías y escalar incidentes cualificados a los SOC nacionales, que aportarían inteligencia avanzada y coordinación.

Deza, por su parte, ve margen para profundizar esa coordinación con una aproximación "API-first y en tiempo real", donde la detección de una amenaza en cualquier punto del "escudo cibernético español" se traduzca en una distribución automática y casi instantánea de esa inteligencia al resto de la red, actualizando políticas en milisegundos. "Ya existe una Red Nacional de SOC impulsada por el CCN-CERT para interconectar la ciberdefensa del sector público, y el sector privado puede complementar esos esfuerzos con sus capacidades operativas y tecnología innovadora", sostiene.

En este esquema, la colaboración público–privada deja de ser un eslogan para convertirse en una necesidad operativa. "Las AAPP presentan grandes dificultades para enfrentarse solas a un entorno de amenazas tan dinámico, por lo que la colaboración público–privada es fundamental", afirma Deza, que aboga por considerar a los proveedores como "aliados estratégicos y habilitadores de tecnología e inteligencia", con modelos de cogestión y equipos mixtos que permitan la transferencia continuada de conocimiento. Montero coincide en que "el modelo más eficaz es aquel en el que la AGE lidera y coordina, los SOC autonómicos y locales participan activamente y las empresas privadas acompañan, refuerzan y especializan, construyendo juntos un sistema progresivo, realista y sostenible".

Talento, gobernanza y cultura siguen siendo los principales desafíos

Más allá de las soluciones tecnológicas, los especialistas consultados sitúan el talento, la gobernanza y la cultura organizativa como los grandes ejes de transformación pendientes.

La Estrategia Nacional de Ciberseguridad plantea un incremento notable del número de expertos, pero la brecha entre oferta y demanda se mantiene, especialmente en el sector público, donde los esquemas retributivos y de carrera compiten en desventaja frente a la empresa privada.

Por eso, "resulta fundamental reforzar la formación técnica de los funcionarios, especialmente de aquellos que tienen responsabilidades de coordinación y gestión de entornos híbridos", insiste Montero, que subraya la importancia de modelos híbridos donde perfiles especializados trabajen desde el sector privado en proyectos públicos de forma estable y alineada con los objetivos de la Administración. Deza va más allá y recuerda que "los profesionales en ciberseguridad jóvenes quieren trabajar con las mejores herramientas y las tecnologías más punteras, en un entorno que no está planteado para el mantenimiento sino para innovar y aportar valor", lo que obliga a transformar los SOC públicos en "hubs de innovación" si se quiere atraer y retener talento.

La gobernanza del dato y de las propias relaciones con los proveedores aparece como otro punto crítico. La combinación de marcos como GDPR, ENS, NIS2 o el secreto administrativo, junto con una cierta aversión al riesgo y a la exposición reputacional, tiende a generar silos tecnológicos y organizativos que dificultan la compartición de información sobre amenazas.

"En realidad, se trata de una combinación de barreras normativas, contractuales, técnicas y culturales, que se refuerzan entre sí", señala Montero, que defiende modelos de transparencia responsable y colaboración con investigadores, consultores y otros proveedores para romper esas

inercias.

Deza coincide en que "los marcos contractuales deben dejar de penalizar la transparencia" y plantea avanzar hacia esquemas de responsabilidad compartida donde el intercambio ágil de información sobre una brecha activa se entienda como parte de la defensa colectiva, no como una admisión de culpa. Rebolledo añade un elemento clave: sin una clasificación adecuada del dato y sin herramientas que permitan generar informes de riesgo y cumplimiento, compartir indicadores sin exponer información sensible se vuelve extremadamente complejo, lo que alimenta aún más la cultura del silencio.

Tecnologías prioritarias y hoja de ruta hasta 2026

En cuanto a las tecnologías prioritarias que deberían guiar las licitaciones públicas en los próximos años, las posiciones convergen en torno a algunos pilares: Zero Trust, segmentación, detección y respuesta avanzadas, cifrado robusto y capacidades de orquestación y automatización impulsadas por IA.

Desde la óptica del dato, Rebolledo propone "priorizar un modelo zero trust centrado en los datos y en las cargas de trabajo, además de dotarse de cifrado y de una resiliencia probada con capacidades para la recuperación de datos rápida y repetible", incluyendo detección de anomalías, snapshots y entornos de recuperación aislados para hacer frente al ransomware.

Fortinet introduce un matiz de orden y secuencia en esa adopción. "Más que identificar tecnologías prioritarias de forma aislada, el verdadero reto para las licitaciones públicas de 2026 es definir un orden lógico y operativo de adopción", explica Montero, que sitúa la segmentación de red, tanto en entornos IT como OT, como primer paso para limitar el movimiento lateral de los atacantes. Sobre esa base, propone avanzar hacia un modelo Zero Trust centrado en la identidad de usuarios, dispositivos y servicios, y desplegar

plataformas XDR que integren EDR, NDR y la automatización de SIEM y SOAR, reservando al cifrado avanzado (incluida la preparación post-cuántica) un papel de mejora continua.

Deza, por su parte, destaca la evolución hacia XDR y XSIAM como enfoque que va "más allá del esquema XDR tradicional", correlacionando telemetría de endpoints, red, nube e identidad, y subraya la importancia de la microsegmentación basada en identidad para evitar que la compromisión de una oficina municipal se convierta en una puerta de entrada al resto de la red regional o estatal. Para manejar el volumen creciente de amenazas, aboga por "impulsar la automatización de los SOCs con la ayuda de la inteligencia artificial" y cita casos en los que se ha logrado automatizar hasta el 90% de las tareas de los analistas de nivel 1 y 2, liberando al personal especializado para funciones de mayor valor.

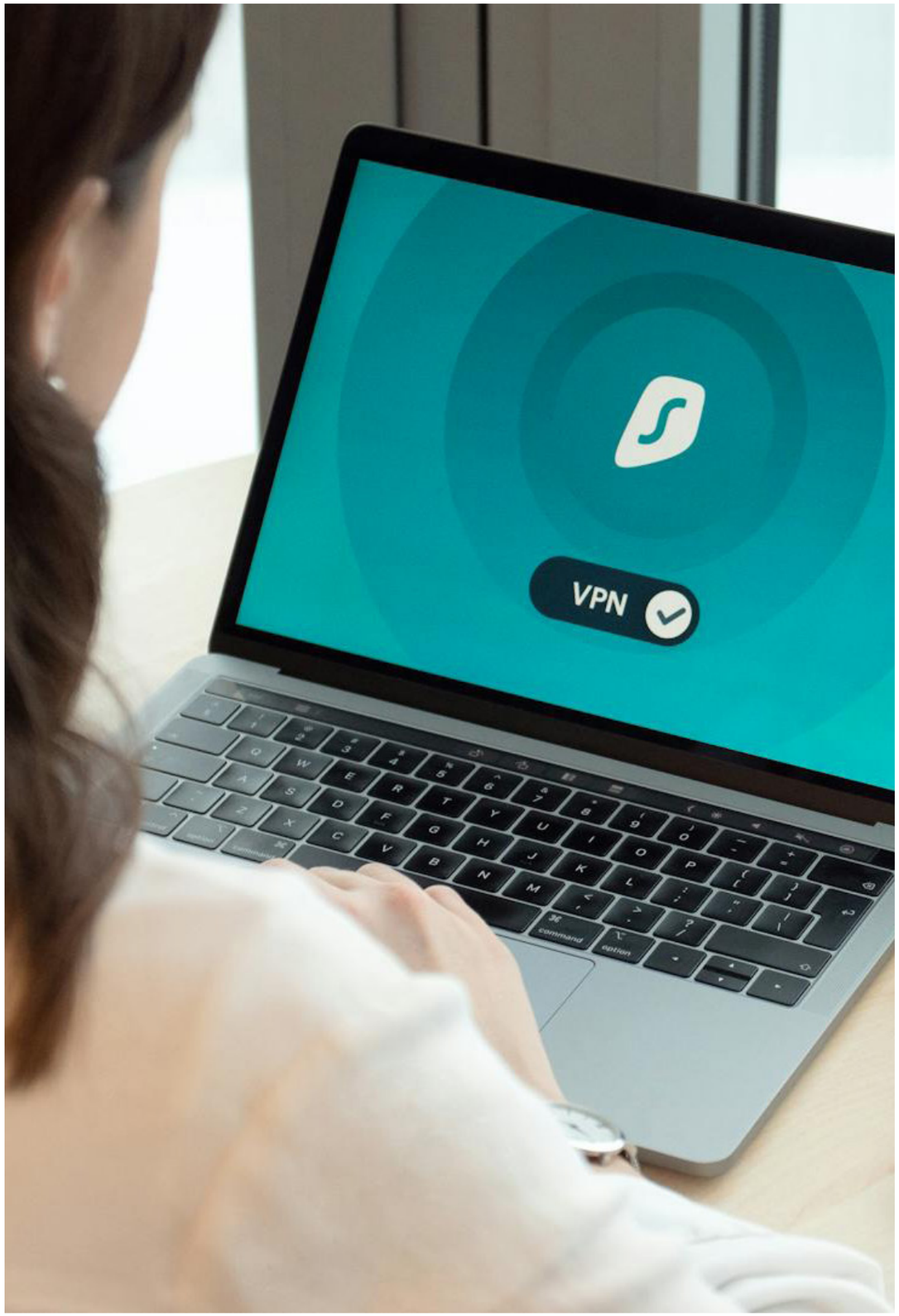
En el marco de España Digital 2026 y del Plan Nacional de Ciberseguridad, estas propuestas encajan con la apuesta institucional por reforzar la capacidad operacional del Estado en ciberseguridad, impulsar la Red Nacional de SOC y consolidar a España como hub europeo en este ámbito. El Esquema Nacional de Seguridad, alineado con NIS2, marca el listón normativo, mientras la futura Ley NIS2 en España reforzará mecanismos de coordinación como el Centro Nacional de Ciberseguridad y los CSIRT nacionales.

Comparación con la empresa privada y con otros países

Aunque las comparaciones siempre son odiosas, podemos decir que, en términos de nivel de madurez, las administraciones públicas españolas se encuentran en una situación ambivalente frente al sector privado y frente a otros países europeos.

Por un lado, cuentan con un marco regulatorio más exigente que muchas empresas, con el ENS obligando a aplicar controles avanzados de seguridad a cualquier organismo público y a sus proveedores, y con estructuras como el CCN-CERT y la Red Nacional de SOC que no siempre tienen equivalentes directos en otros estados. Por otro, sufren con más intensidad las limitaciones presupuestarias, la rigidez de los procesos de compra, la dependencia de sistemas legacy y el déficit de perfiles especializados, lo que dilata la ejecución de proyectos y complica la adopción rápida de nuevas tecnologías.

Los informes públicos subrayan que, mientras algunos sectores privados



TEMA DE PORTADA

[como el financiero o partes del sanitario] se sitúan entre los más avanzados en ciberseguridad y han acelerado sus inversiones en respuesta al aumento del ransomware, buena parte del tejido empresarial español sigue en niveles de madurez medios o bajos, especialmente entre pymes. La administración, en cambio, se ve obligada a mantener un estándar mínimo homogéneo por mandato legal, lo que la coloca en una posición relativamente más robusta en ciertos ámbitos de cumplimiento, pero más expuesta mediáticamente cuando se producen fallos.

A nivel europeo, la participación de España en iniciativas de ciberdefensa en el marco de la OTAN y la UE está abriendo oportunidades tanto para las administraciones como para las empresas que trabajan con ellas. "La creciente implicación de España en los marcos de ciberdefensa de la OTAN y de la UE representa una gran oportunidad para las empresas que ya trabajamos con la Administración española", afirma Deza, que destaca cómo estos proyectos elevan el nivel de exigencia, impulsan arquitecturas alineadas con estándares internacionales y abren la puerta a consorcios europeos. Montero coincide en que "el ecosistema español de AAPP actúa hoy como entorno de validación y madurez para soluciones que, cuando están bien diseñadas y operadas, pueden escalar hacia marcos comunitarios, de defensa y de resiliencia, tanto en el contexto europeo como en el internacional".

En ese sentido, informes gubernamentales recientes describen a España como un candidato a hub de ciberseguridad europeo, apoyado en la combinación de capacidades de INCIBE, CCN-CERT, la red de SOC, el tejido empresarial especializado y el empuje de la regulación. Sin embargo, también advierten de que la brecha de talento y la necesidad de mayores inversiones en resiliencia [especialmente en el ámbito local y en infraestructuras críticas] siguen siendo factores de riesgo que pueden lastrar esa aspiración si no se abordan con rapidez y continuidad.

En conjunto, la fotografía de la seguridad en las administraciones públicas españolas muestra un ecosistema sometido a una presión de amenazas creciente, con una arquitectura institucional avanzada y un tejido tecnológico potente, pero que aún necesita traducir el cumplimiento normativo en capacidades operativas homogéneas en todos los niveles de la Administración. Las administraciones se ven empujadas a madurar al mismo ritmo que se digitalizan los servicios y se multiplica la exposición, y el sector privado se consolida como socio imprescindible para cerrar la brecha entre lo que exige la norma y lo que permite la operación diaria en la trinchera

TENDENCIAS

El año 2026 promete un aumento de ataques basados en la identidad digital

Álvaro Fraile, director de Ciberseguridad de Ayesa

Ayesa Digital ha publicado el informe 'Ciberseguridad 2026: predicciones y tendencias clave', en el que analiza la evolución del riesgo digital y las principales tendencias que marcarán la protección de sistemas, datos e infraestructuras críticas en los próximos años.

El documento incide en el papel creciente de la inteligencia artificial, el aumento de los ataques basados en la identidad digital y la necesidad de fortalecer la resiliencia ante amenazas cada vez más sofisticadas.

Tal y como se explica en el análisis se considera que, en el recién estrenado año 2026, la ciberseguridad dejará de ser percibida como un elemento técnico para consolidarse como un recurso estructural comparable a suministros esenciales.

El estudio de Ayesa destaca, asimismo, que la dependencia de sistemas digitales en ámbitos como la industria, la administración pública o los servicios ciudadanos hace que cualquier incidencia pueda tener efectos directos en el tejido económico y social.

Conclusiones

Entre las principales conclusiones del informe, Ayesa identifica un incremento de amenazas avanzadas, especialmente aquellas potenciadas por la inteligencia artificial. Los ataques serán más creíbles, personalizados y difíciles de detectar, utilizando técnicas capaces de replicar voces reales, generar comunicaciones sin errores y explotar la urgencia y el estrés para inducir respuestas precipitadas. A su vez, la IA se posicionará como aliado fundamental en detección y respuesta temprana, siempre que exista supervisión humana y criterios de uso responsable.

Evolución del ransomware

El informe también subraya la evolución del ransomware, que dejará de centrarse exclusivamente en el secuestro de dispositivos para orientarse al chantaje basado en reputación, exposición pública de datos y presión a terceros. Esta tendencia refuerza la necesidad de estrategias de resiliencia, continuidad de negocio y recuperación ágil como prioridades críticas para el sector empresarial.

Asimismo, Ayesa advierte del impacto de los ciberataques en infraestructuras físicas, señalando que la interconexión entre lo digital y lo físico convierte servicios esenciales como energía, transporte, sanidad o producción industrial en objetivos de alto riesgo. La protección ya no se limita al dato, sino al funcionamiento de sistemas que

sostienen la vida cotidiana.

El estudio identifica la identidad digital como la superficie de ataque más relevante, con un crecimiento notable de fraudes basados en suplantación, ingeniería social avanzada, manipulación audiovisual y deepfakes. En este sentido, el enfoque Zero Trust se consolidará como paradigma: verificar siempre y asumir que la confianza no puede darse por defecto. En opinión de Álvaro Fraile, director de Ciberseguridad de Ayesa, "estamos entrando en una etapa donde la ciberseguridad trasciende lo puramente técnico. La pregunta ya no es si una organización puede ser atacada, sino si está preparada para mantener su actividad, proteger su reputación y recuperarse con rapidez. El reto para 2026 será construir sistemas resilientes, integrar inteligencia artificial con supervisión humana y asumir que la seguridad es una responsabilidad compartida entre empresas, instituciones y ciudadanos."

Recomendaciones estratégicas

El informe establece líneas prioritarias para reforzar la seguridad en 2026:

- Inversiones orientadas a resiliencia y continuidad operativa más allá del cumplimiento.
- Integración de IA en detección y respuesta, con controles éticos y humanos.
- Refuerzo de identidades digitales y autenticación avanzada.
- Políticas Zero Trust y segmentación de redes en entornos cloud e IoT.
- Formación y concienciación como eje central del factor humano.

Estas recomendaciones son especialmente relevantes para administraciones públicas, compañías industriales, entidades financieras y sectores críticos, que deberán anticiparse al impacto combinado de amenazas híbridas sobre entornos físicos y digitales.

GRACIAS

contacto@bytic.es | www.bytic.es