

BOLETÍN DE VIGILANCIA TECNOLÓGICA

DPI Nº16 T1 2026

# DIGITALIZACIÓN DE LA PRODUCCIÓN INDUSTRIAL

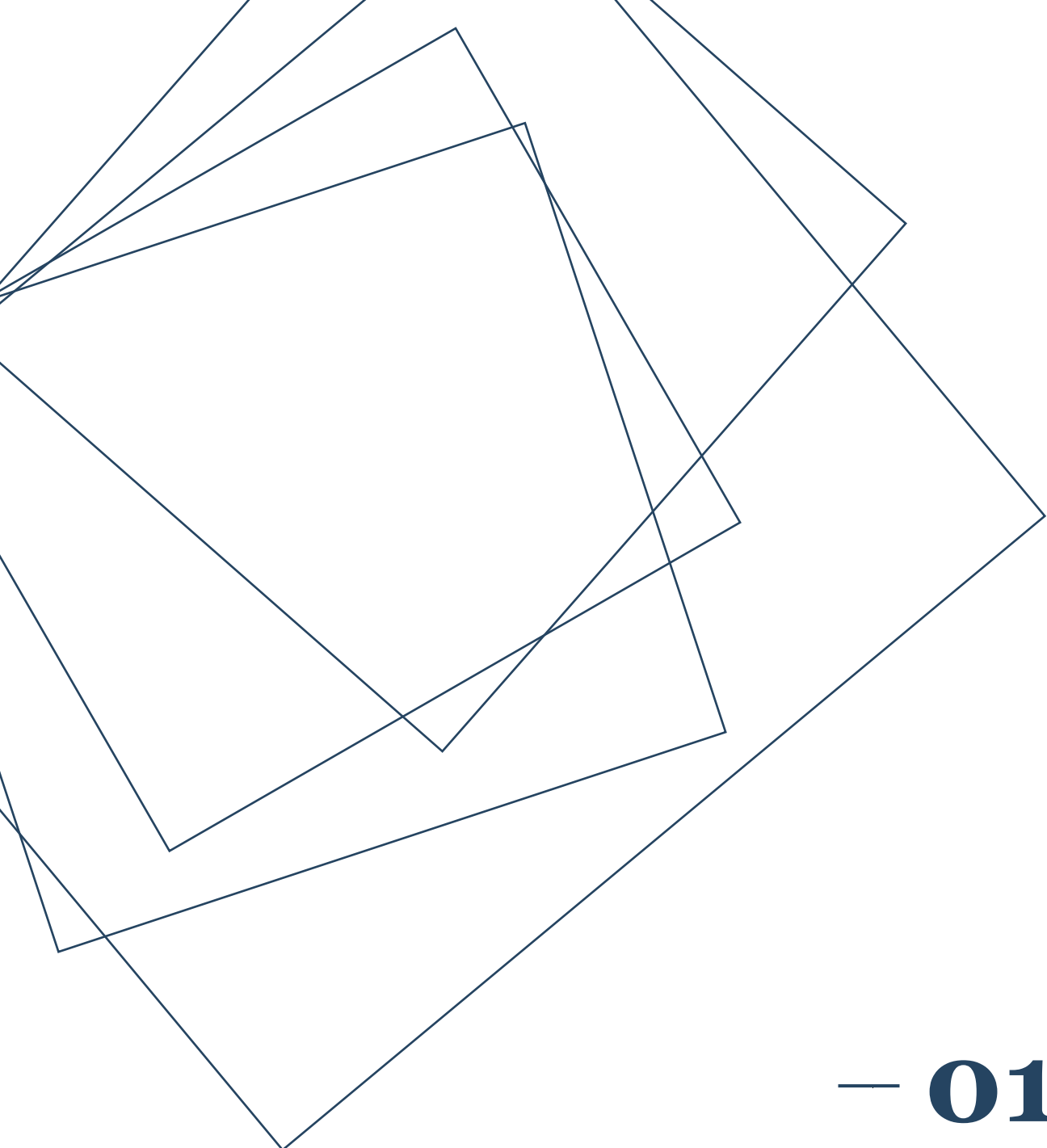


El Boletín de Vigilancia Tecnológica sobre Digitalización de la Producción Industrial es una publicación trimestral de la Escuela de Organización Industrial desarrollada en colaboración con CTIC Centro Tecnológico. Este Boletín pretende ofrecer una visión general de las tecnologías emergentes y los avances más relevantes en materia de digitalización de la producción industrial.

Esta publicación forma parte de una colección de Boletines temáticos de Vigilancia Tecnológica, a través de los cuales se busca acercar a la pyme información especializada y actualizada sobre sectores industriales estratégicos. Los Boletines seleccionan, analizan y difunden información obtenida de fuentes nacionales e internacionales, con objeto de dar a conocer los principales aspectos del estado del arte de la materia en cuestión, así como otras informaciones relevantes de la actualidad en cada uno de los campos objeto de Vigilancia Tecnológica.

# Índice

- \_04 Arquitecturas de computación  
avanzadas en la producción industrial
- \_12 Actualidad
- \_19 Tendencias tecnológicas
- \_24 Agenda
- \_34 *Just in Time*
- \_38 Cierre



# — 01

## Estado del Arte

*Estado del arte acerca de las tendencias y novedades en el campo de la digitalización de la producción industrial.*

# Arquitecturas de computación avanzadas en la producción industrial

La producción industrial ha dejado de ser un entorno dominado exclusivamente por la automatización local para convertirse en un sistema distribuido de procesamiento, datos y decisión. Durante décadas, la arquitectura clásica de planta se apoyó en una estructura relativamente estable: sensores y actuadores en campo, controladores lógicos programables (PLC, Programmable Logic Controller) para el control, sistemas de supervisión, control y adquisición de datos (SCADA, Supervisory Control and Data Acquisition) para la supervisión y, en niveles superiores, sistemas de ejecución de manufactura (MES, Manufacturing Execution System) y sistemas de planificación de recursos empresariales (ERP, Enterprise Resource Planning). Ese modelo sigue siendo esencial, pero ya no basta para responder a las exigencias actuales de flexibilidad, conectividad, trazabilidad y análisis en tiempo real.

Por eso, el primer gran cambio que conviene abordar es la [transición desde la automatización clásica a la arquitectura distribuida](#). La fábrica ya no funciona como una cadena jerárquica cerrada, sino como un entorno donde distintas capas computacionales cooperan entre sí. El cálculo se reparte entre dispositivos inteligentes, sistemas de control, nodos intermedios y plataformas más centralizadas, en función de las necesidades operativas. En este nuevo marco, una de las cuestiones decisivas ya no es solo qué sistemas participan en la producción, sino dónde se procesa la información y dónde se toman las decisiones operativas. Es precisamente ahí donde el edge computing adquiere un papel central.

## Edge computing y cloud-edge-IoT continuum

En ese nuevo escenario, uno de los elementos más importantes es el [edge computing industrial](#). En una planta moderna, cámaras, sensores, robots y máquinas generan enormes cantidades de información, pero no toda puede enviarse continuamente a la nube para ser procesada. En muchos casos, las decisiones deben tomarse en milisegundos: detectar un defecto en una pieza, identificar una vibración anómala, detener una máquina ante una condición insegura o asistir a un operario con información contextual.

El [edge computing](#) responde a esa necesidad situando capacidad de procesamiento cerca del proceso físico, junto a la máquina o a la célula de fabricación. Esto permite **reducir la latencia, disminuir el tráfico de red, mejorar la continuidad operativa y hacer viable la inferencia local de modelos de inteligencia artificial**. Así, el edge no es solo una solución técnica, sino una nueva capa funcional de la arquitectura industrial.

A partir de ahí aparece un concepto especialmente útil para entender el estado actual del sector: el [cloud-edge-IoT continuum](#). Este enfoque plantea que la computación industrial ya no debe dividirse de forma rígida entre “lo local” y “la nube”, sino entenderse como un continuo de recursos distribuidos que va desde los dispositivos de campo hasta las plataformas cloud, pasando por nodos edge y sistemas de planta. Dentro de ese continuo, cada nivel cumple una función distinta: los dispositivos captan datos o ejecutan acciones sobre el proceso físico; el edge procesa información y responde localmente; la planta coordina, contextualiza e integra operaciones; y la nube agrega información, entrena modelos y optimiza a mayor escala. El valor de esta aproximación reside en que permite diseñar arquitecturas más flexibles, en las que la información y las aplicaciones pueden moverse o repartirse según criterios de latencia, criticidad, coste, seguridad o disponibilidad.

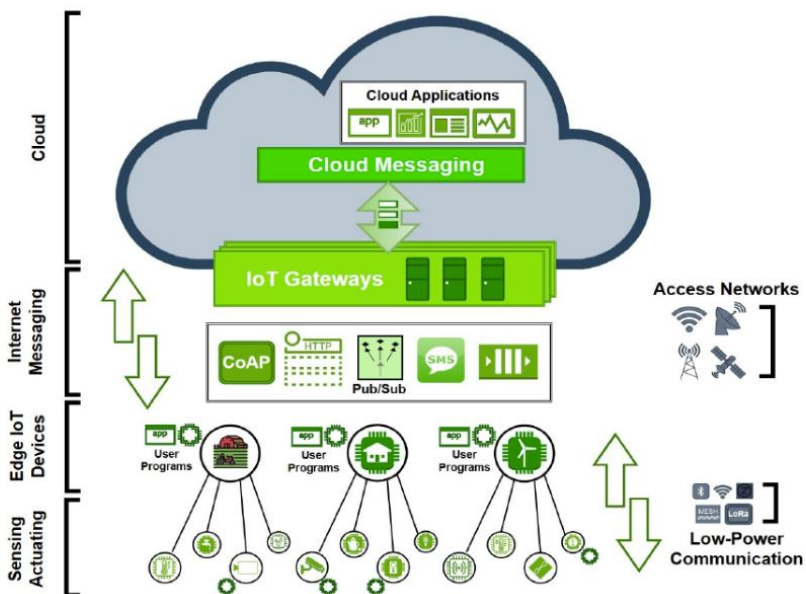


Figura 1: Esquema del cloud-Edge-IoT continuum que muestra varios ámbitos de aplicación del IoT junto con dispositivos edge programables. Fuente: [Transformative Reconfigurability For Edge IoT Devices In Small-Scale IoT Systems](#).

Sin embargo, el verdadero desafío no consiste solo en conectar dispositivos, sino en armonizar recursos distribuidos. En este punto resulta útil distinguir entre [tres planos del sistema](#):

- **Plano de datos:** engloba la red, el cómputo y el almacenamiento necesarios para manejar la información de aplicación.
- **Plano de control:** toma decisiones en tiempo de ejecución sobre cómo se procesa esa información y cómo se actúa sobre ella.
- **Plano de gestión:** supervisa, configura y mantiene el estado de los recursos y servicios distribuidos.

En una arquitectura industrial avanzada, estos tres planos ya no se concentran en un único nivel, sino que se reparten a lo largo del cloud-edge-IoT continuum. Esta visión ayuda a explicar por qué la producción moderna no es solo una cuestión de automatización, sino también de coordinación entre flujos de datos, decisiones operativas y gestión del ciclo de vida de la infraestructura digital.

El reparto funcional entre edge y nube debe entenderse como parte de un continuo computacional. El edge es clave para tareas que exigen baja latencia, proximidad al activo y resiliencia; la nube, para almacenar históricos, entrenar modelos de IA y coordinar operaciones a gran escala. Así, **la arquitectura industrial más avanzada no es ni totalmente local ni centralizada, sino híbrida y distribuida**. Pero esta distribución solo funciona si todos los niveles intercambian datos y contexto de forma coherente, segura e independiente del fabricante. En ese punto, estándares como OPC UA resultan estratégicos.

### **OPC UA: interoperabilidad para la fábrica distribuida**

[OPC UA](#) (Open Platform Communications Unified Architecture) se ha consolidado como uno de los [estándares](#) más relevantes para resolver un problema histórico de la automatización: la interoperabilidad entre sistemas, dispositivos y aplicaciones de distintos fabricantes. Su importancia radica en que no se limita a transportar datos, sino que **proporciona una base común para que equipos heterogéneos puedan intercambiar información con significado operativo**.

Esa capacidad resulta especialmente valiosa en la industria actual, donde conviven PLC, robots, sensores inteligentes, sistemas SCADA, plataformas MES, aplicaciones analíticas y servicios cloud. En un entorno así, el problema no es solo conectar activos, sino lograr que la información circule de forma coherente entre el nivel de campo, la planta y los sistemas corporativos. OPC UA aporta precisamente ese puente entre OT e IT porque combina comunicaciones estandarizadas con un modelo de información que permite describir datos, relaciones, estados, eventos y objetos industriales de forma estructurada. Por eso se ha convertido en [una pieza clave de la integración vertical](#), desde el dispositivo hasta la nube, y de la creación de arquitecturas industriales más abiertas y menos dependientes de integraciones propietarias (Figura 2).

Además de su papel como estándar de interoperabilidad, OPC UA destaca por [varias ventajas que explican su creciente adopción](#): **interoperabilidad, seguridad, escalabilidad y flexibilidad**. Su diseño neutral respecto al fabricante permite la comunicación fluida entre dispositivos y sistemas de distintos proveedores, algo especialmente importante en entornos industriales heterogéneos.

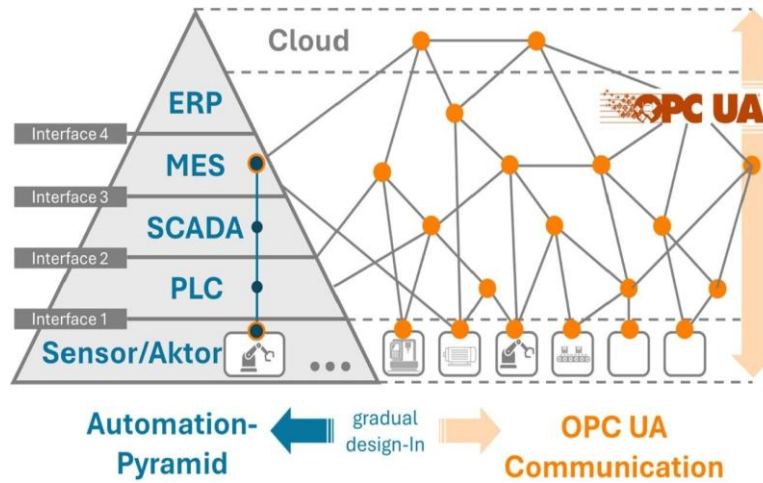


Figura 2. Comparativa entre el uso de una comunicación basada en diferentes interfaces y una comunicación basada en OPC UA. Fuente: [Exploring the Integration of cloud manufacturing and cyber-physical systems in the era of industry 4.0 – An OPC UA approach.](#)

En definitiva, OPC UA puede cubrir prácticamente todos los componentes de un sistema de automatización, desde sensores y dispositivos de campo hasta sistemas de nivel superior como SCADA, MES y ERP. Su alcance no se limita a la comunicación básica, sino que ha sido diseñado para el modelado avanzado de datos, el intercambio de información estructurada y la integración entre distintos protocolos y capas tecnológicas. En los últimos años, además, el desarrollo de [OPC UA FX](#) (Field eXchange) ha ampliado el alcance del estándar hacia el nivel de campo, con el objetivo de extender la interoperabilidad también a las comunicaciones más cercanas al proceso (Figura 3).

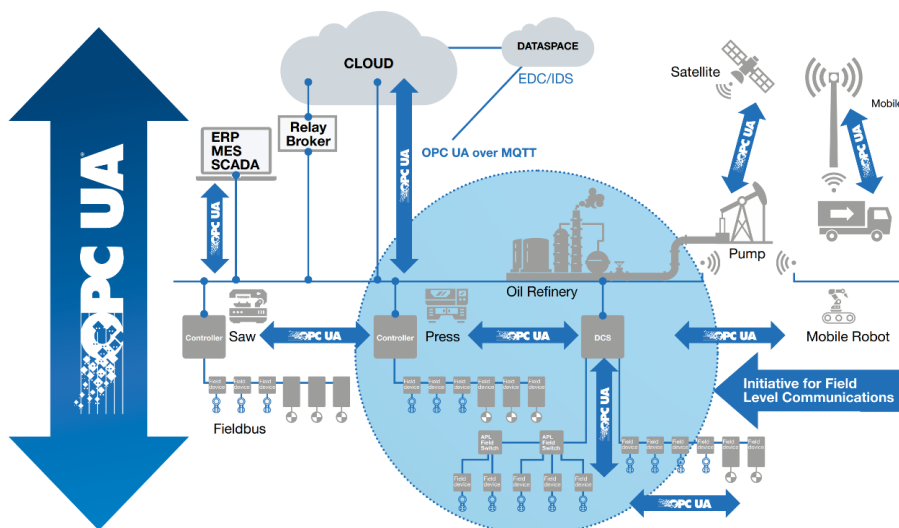


Figura 3. Casos de uso de conectividad con OPC UA FX. Fuente: [OPC UA FX solution.](#)

No obstante, la interoperabilidad por sí sola no basta para sostener la nueva complejidad de la producción industrial. Una vez que los datos y servicios pueden intercambiarse de forma coherente entre capas, el siguiente reto consiste en decidir cómo desplegar, escalar y gobernar esa capacidad computacional distribuida. Es aquí donde las arquitecturas híbridas y multinube adquieren relevancia, al ofrecer modelos de infraestructura capaces de combinar proximidad operativa, elasticidad y resiliencia a escala corporativa.

### Arquitecturas Híbridas

La nube híbrida es un modelo de infraestructura de TI que combina y unifica entornos locales, de nube privada y de nube pública en una solución única y flexible. Este enfoque permite a las organizaciones ejecutar cargas de trabajo críticas con mayor portabilidad y eficiencia, adaptándose a las necesidades cambiantes del negocio.

Una de las principales ventajas es la agilidad y escalabilidad. Este modelo permite el aprovisionamiento rápido de recursos, facilitando que las fábricas respondan a picos inesperados de tráfico de manera económica y automática, además de ofrecer un mayor control y flexibilidad en la asignación de recursos. Por otra parte, la empresa industrial podría mantener datos altamente sensibles (como propiedad intelectual o información crítica de producción), en una nube privada bajo control estricto, mientras utiliza la nube pública para tareas que consumen muchos recursos, como la analítica avanzada, el entrenamiento de modelos de IA o la explotación centralizada de datos históricos.

Desde el punto de vista financiero, la nube híbrida favorece la optimización de costes al reducir la necesidad de invertir capital en hardware físico y aprovechar el modelo de pago por uso de las nubes públicas.

Además, mejora la resiliencia y continuidad del negocio, ya que permite realizar copias de seguridad redundantes e integradas entre el almacenamiento local y la nube, acelerando la recuperación ante desastres. También puede actuar como motor de innovación, facilitando la modernización de aplicaciones heredadas y el despliegue de nuevas capacidades digitales en planta.

Sin embargo, su **implementación puede ser compleja y costosa**. Integrar y sincronizar datos entre distintos entornos y herramientas exige un esfuerzo elevado, al tiempo que dificulta la visibilidad global de la infraestructura y puede generar silos de información. A ello se suma la falta de perfiles capaces de operar múltiples plataformas y la dificultad de mantener una gobernanza unificada del dato, los accesos y la ciberseguridad.

### Arquitecturas multinube

La [arquitectura multinube](#) es una estrategia que integra servicios de dos o más proveedores de nube, ya sean públicas o privadas, para satisfacer las necesidades específicas de una organización. A diferencia de la nube híbrida, que se centra en la combinación de un entorno local con una nube pública principal, el enfoque multinube busca aprovechar las fortalezas individuales de múltiples plataformas independientes.

Uno de los [beneficios más significativos](#) es **evitar la dependencia de un solo proveedor**, lo que otorga a las empresas mayor libertad para elegir y probar nuevos servicios según su evolución. Esto permite una selección optimizada de funciones, donde los arquitectos de TI pueden escoger herramientas de primer nivel de diferentes proveedores, como usar una plataforma por su potencia de cómputo y otra por sus capacidades avanzadas de inteligencia artificial.

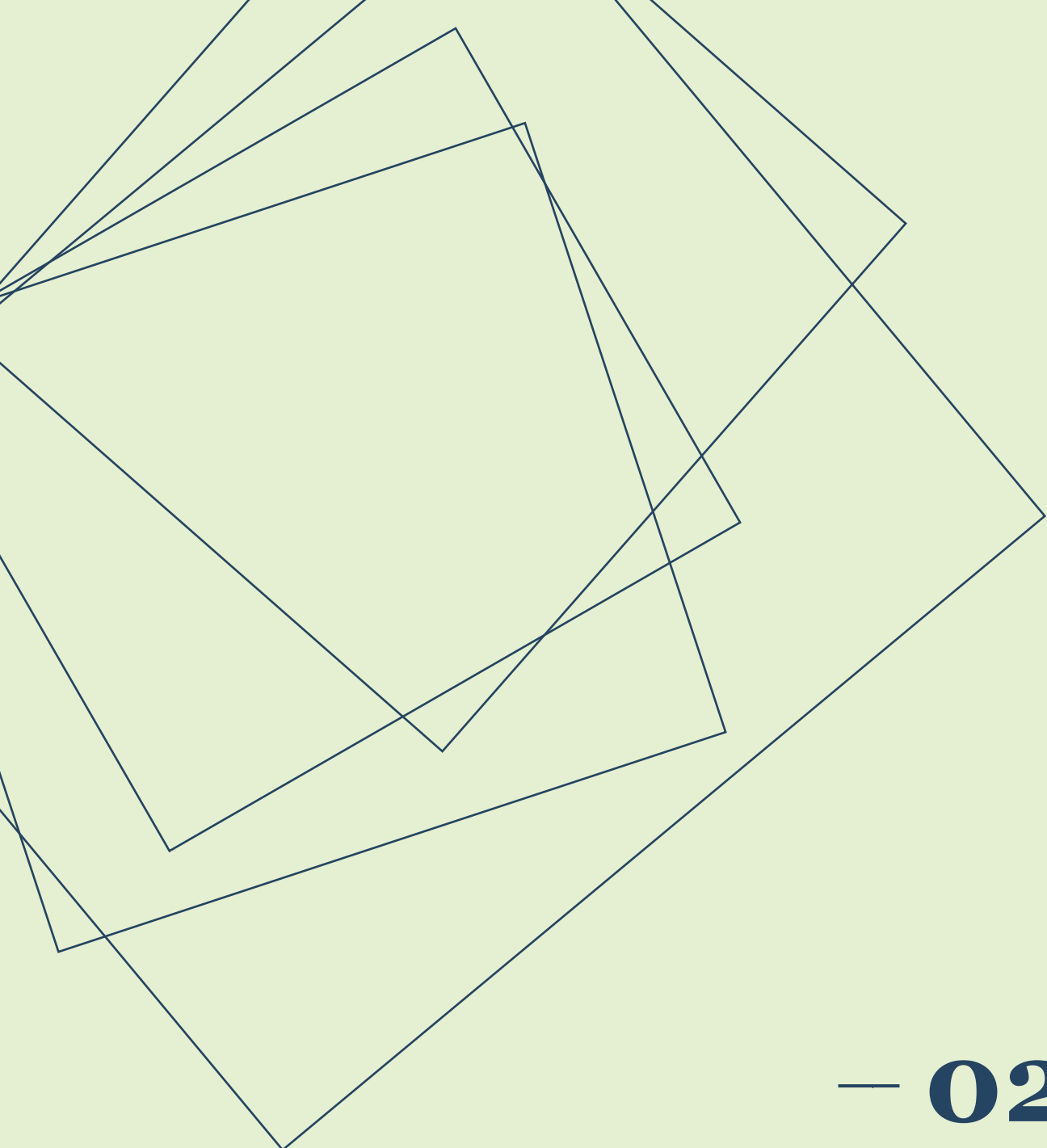
En términos de resiliencia y recuperación ante desastres, este modelo es superior, ya que permite **distribuir las cargas de trabajo** en distintas geografías y proveedores, eliminando puntos únicos de falla y garantizando la alta disponibilidad. Además, favorece la optimización de costes, puesto que las organizaciones pueden comparar precios y seleccionar la opción más económica para cada tarea específica. También puede facilitar el cumplimiento normativo y la residencia de datos, permitiendo que la información se almacene en regiones geográficas específicas para cumplir con leyes locales de privacidad.

A pesar de sus bondades, la multinube introduce una **gestión operativa compleja**, debido a que cada proveedor tiene sus propias API, portales de administración y herramientas de automatización. Esta disparidad puede generar una falta de visibilidad centralizada, dificultando que los equipos de TI tengan una visión completa de la postura de seguridad y el rendimiento de toda la red. La seguridad y el cumplimiento representan un reto constante, ya que lograr políticas consistentes en entornos heterogéneos es difícil y puede exponer a la empresa a nuevos riesgos. A esto se suma la brecha de habilidades, pues es escaso el personal con experiencia técnica agnóstica capaz de operar múltiples nubes simultáneamente. Otros obstáculos incluyen problemas de interoperabilidad y los costes asociados al movimiento de datos entre nubes (tarifas de salida), así como posibles problemas de latencia que afecten el rendimiento de las aplicaciones si la integración no está bien diseñada. Para mitigar estos retos, las organizaciones deben invertir en herramientas de orquestación y monitoreo que unifiquen la administración y estandaricen los flujos de trabajo en todas las plataformas.

## Conclusión

En definitiva, las arquitecturas de computación avanzadas en la producción industrial evolucionan hacia modelos cada vez más distribuidos, interoperables y adaptativos, en los que el valor no reside en una tecnología aislada, sino en la combinación coherente de edge computing, cloud-edge-IoT continuum, estándares como OPC UA y despliegues híbridos o multinube. El futuro de estas arquitecturas apunta a entornos capaces de reconfigurarse dinámicamente según la criticidad del proceso, la disponibilidad de recursos, los requisitos de ciberseguridad o las necesidades de negocio, incorporando además inteligencia artificial operativa, gemelos digitales y orquestación automática de servicios entre planta y nube. Más que una simple modernización de la automatización, se trata de una transformación profunda de la infraestructura digital industrial, donde la flexibilidad arquitectónica será un factor decisivo para la competitividad, la resiliencia y la sostenibilidad de las fábricas.





# — 02

## Actualidad

*Recopilación de las noticias más relevantes de la actualidad nacional e internacional en materia de digitalización de la producción industrial.*

## Adjudicada la ampliación del superordenador MareNostrum 5 para impulsar la Factoría de IA del Barcelona Supercomputing Center

La Factoría de Inteligencia Artificial del Barcelona Supercomputing Center–Centro Nacional de Supercomputación (BSC-CNS) se prepara para impulsar sus capacidades de IA con la ampliación del superordenador MareNostrum 5. La European High Performance Computing Joint Undertaking (EuroHPC JU), la empresa conjunta de supercomputación de la Unión Europea ha firmado el contrato de adquisición del proyecto MareNostrum 5 AI Upgrade con el consorcio liderado por Fsas Technologies, la rama especializada en HPC (High-Performance Computing) e IA de Fujitsu, y Telefónica, lanzado en una convocatoria el pasado julio.

Esta ampliación del superordenador MareNostrum 5 tiene como finalidad impulsar la infraestructura de la Factoría de IA ubicada en el BSC-CNS, una de las siete primeras aprobadas por la Comisión Europea en diciembre de 2024. El objetivo es democratizar el acceso a la infraestructura de supercomputación avanzada, ofreciendo capacidad de cómputo y almacenamiento a pymes y startups de toda Europa, así como a la Administración Pública, para entrenar modelos de IA y para el desarrollo de sistemas innovadores en esta tecnología, lo cual supone un paso adelante para fortalecer las capacidades europeas de supercomputación.

Con un presupuesto aproximado de 129 millones de euros, el proyecto está cofinanciado al 50 % por EuroHPC y el otro 50 % por España, Portugal y Turquía. Del porcentaje correspondiente a España, que asciende a un total de 60 millones de euros, la financiación procede del Gobierno de España, a través del Ministerio para la Transformación Digital y de la Función Pública y el Ministerio de Ciencia, Innovación y Universidades, y de la Generalitat de Catalunya.

La ampliación contará con la instalación de dos nuevas particiones de cómputo, una para entrenar modelos de lenguaje (LLMs) y otra para aplicarlos (inferencia), una mejora de las capacidades de almacenamiento con un nuevo sistema de ficheros de alto rendimiento por IA y nuevas tecnologías, así como un conjunto de software especializado.

La máquina, que se instalará durante el primer semestre de 2026, usará dos espacios del BSC-CNS interconectados adecuadamente -el centro de datos de la sede del BSC, el mismo que MareNostrum 5, y la capilla de Torre Girona- y contará con tecnologías de Supermicro (hardware), IBM (almacenamiento y software), VAST (almacenamiento) y NVIDIA (software y hardware).

Con esta iniciativa de crear Fábricas de IA, EuroHPC y el BSC-CNS impulsan las capacidades de supercomputación de IA de Europa, y facilitan la adopción y el uso de estas tecnologías por parte de la industria, con especial énfasis en las pymes, las startups y la Administración Pública de los países participantes de la red de Fábricas de IA. España es, junto a Alemania y Polonia, uno de los tres únicos países europeos que cuentan con dos de estas infraestructuras, tras la reciente aprobación, por parte de la Comisión Europea, de una segunda factoría en el Centro de Supercomputación de Galicia (CESGA).

## La industria española centra el foco de los ciberataques con tres incidentes graves al día

La industria española se ha posicionado como el blanco principal de los ciberataques, sufriendo una media de tres incidentes graves al día impulsados por motivaciones económicas. Esta situación consolida al país como uno de los entornos más expuestos, con 605 sucesos significativos registrados en el segundo semestre de 2025, según recoge el equipo de **Cyber Threat Intelligence** de NTT Data en su informe [Tendencias y ciberamenazas](#), donde se analiza el impacto global de estos riesgos en el tejido empresarial nacional.

La investigación destaca que los sectores que más sufren los ciberataques en España no siguen los mismos patrones que en el resto del mundo, siendo la **industria** local uno de los focos prioritarios para los actores criminales. El sector manufacturero español, por ejemplo, ha experimentado intrusiones contra los sistemas que automatizan y monitorean sus operaciones. Esto ha generado en el segundo semestre numerosos casos en los que las empresas se han visto obligadas a detener líneas de producción para evitar la propagación de los ataques.

Otros sectores vitales para la economía, como la alimentación, la logística o el turismo, también han sufrido accesos no autorizados a sus portales operativos, aunque la mayoría de ellos no han trascendido públicamente. La amenaza también afecta a servicios esenciales, y la administración pública vuelve a situarse entre los sectores más castigados. La heterogeneidad tecnológica y la coexistencia de múltiples niveles administrativos incrementan su superficie de exposición.

Los servicios sanitarios, donde también se incluyen clínicas privadas y centros regionales, también se posicionan entre los sectores más afectados por los ciberincidentes, con un impacto concreto en los pacientes debido a los retrasos en las consultas y procedimientos médicos.

“Los ataques registrados en estos meses no solo confirman la sofisticación de los atacantes, sino el imperativo ineludible de blindar la resiliencia en áreas donde el impacto tendría consecuencias operativas, económicas y sociales críticas”, afirma Sandra Somastre Gonzalez, investigadora del equipo de Ciberamenazas de NTT Data España. “El país se sitúa ya como un objetivo crítico, lo que exige acelerar la transición hacia un marco de ciberseguridad más robusto, cohesionado y, sobre todo, preventivo”.

La mayor parte de los ataques registrados responden a campañas de *ransomware* (secuestro de datos). Esta tendencia se explica por el elevado grado de digitalización del país, la relevancia económica de determinados sectores y la presencia de un tejido empresarial compuesto mayoritariamente por **pymes** con niveles de protección desiguales. A nivel europeo se destaca Alemania, que ha sufrido más de 856 ataques en el segundo semestre de 2025, lo que lo posiciona como el principal objetivo europeo.

El informe destaca también la intensificación sostenida de la dimensión híbrida de la guerra entre Rusia y Ucrania, con ataques no solo a objetivos ucranianos, sino también de instituciones y empresas europeas. El cibercrimen ha confirmado en 2025 su papel como riesgo sistémico para las organizaciones, y su impacto económico anual supera por primera vez la barrera de los 10 billones de dólares anuales (alrededor de 8,5 billones de euros, según el tipo de cambio actual).

Una de las explicaciones de este aumento se encuentra en el uso de la [inteligencia artificial \(IA\)](#), que deja de ser una tendencia emergente para convertirse en un acelerador táctico, integrado ya en las distintas fases de los ataques. Su uso permite acelerar tareas concretas, como la generación de contenido y la adaptación lingüística y cultural, así como la modificación de herramientas maliciosas.

La investigación también señala que la IA no sustituye a los operadores humanos, sino que reduce el coste cognitivo y operativo de cada evento. La expectativa es que su uso continúe expandiéndose, no tanto mediante técnicas disruptivas, sino como acelerador de procesos ya existentes: automatización del reconocimiento, personalización avanzada de ingeniería social y optimización de la selección de objetivos.

Los ataques de *ransomware*, el incidente más frecuente, supone un coste promedio total superior a los cinco millones de dólares, al incluir los períodos de interrupción y recuperación. En materia de brecha de datos, donde el coste medio supera los 4 millones de dólares, el informe destaca la importancia de los marcos regulatorios europeos de protección de datos, que permiten una mayor estandarización de los procesos de respuesta para las firmas.

Pese a los altos costes de cada incidente, las estimaciones de mercado publicadas durante 2025 han situado el gasto mundial en seguridad de la información y gestión de riesgos en torno a los 213.000 millones de dólares, lo que representaría un crecimiento interanual cercano al 14 por ciento.

De cara al nuevo año, el informe destaca un aumento sostenido de campañas basadas en persistencia silenciosa (aquellas que buscan mantener acceso, operar o influir sin ser detectados en el largo plazo), abuso de identidades y explotación de relaciones de confianza, tanto humanas como técnicas. Estas tendencias, así como la evolución en el uso de la inteligencia artificial, reducirán aún más las barreras de entrada al cibercrimen y ampliarán la base de actores capaces de ejecutar ataques complejos.

Fuente: [Red Seguridad](#)

24/02/2026

## Hoja de ruta para acelerar la soberanía digital en España

El Consejo de Ministros, a propuesta del Ministerio para la Transformación Digital y de la Función Pública, presentó el pasado mes de febrero la **Hoja de Ruta para acelerar la Soberanía Digital en España**, un documento que reordena, conceptualiza y proyecta la siguiente fase de la revolución digital española.

“Esta hoja de ruta no es un plan a futuro, es una sistematización de todo lo que está haciendo este Gobierno. Este es el informe que, por cierto, también vamos a compartir con la Comisión Europea. Tiene la máxima importancia porque después de todo lo que está pasando en el contexto geopolítico internacional, Europa ha decidido reforzar su soberanía digital y España también, en coherencia con las medidas que está planteando la Comisión Europea. Hemos destinado una parte muy importante de los fondos europeos a reforzar esa soberanía digital y vamos a darle continuidad con el fondo llamado España Crece, que una de sus prioridades es seguir invirtiendo en reforzar esta soberanía digital”, ha explicado el ministro Óscar López en la rueda de prensa posterior al Consejo de Ministros.

El documento contiene diez propuestas de acción, entre las que destacan reforzar y conectar la Infraestructura Pública Digital española a la europea, con ejemplos como el sistema Cl@ve, el DNI electrónico o la Nube Sara, y potenciar el uso de Código Abierto, OpenDesk y Software Libre en las Administraciones Públicas, como con ALIA, la familia de modelos de lenguaje de IA entrenada en español y lenguas cooficiales.

Aboga también por acelerar un sistema europeo de pagos transfronterizo, seguro, ágil e interoperable, como el que defiende la Alianza EuroPA que integra las soluciones de pago Bizum, MBWay y Bancomat. Y considera imprescindible mantener el ritmo de inversiones en tecnologías críticas como con los semiconductores en el caso de Imec, la cuántica en el caso de Nu Quantum, la industria satelital en el caso de Sateliot.

Además, el análisis destaca que España es polo inversor gracias a sus recursos energéticos y a su conectividad, lo que, según indica, ofrece la oportunidad de que nuestro país lidere la aprobación de una norma de Centros de Datos sostenibles que combine eficiencia energética y crecimiento económico.

Asimismo, pone el acento en el buen posicionamiento en materia de gigafactorías de inteligencia artificial contando con empresas punteras en construcción, telecomunicaciones, refrigeración y compresión de modelos. “Estoy hablando de algo que es esencial para el presente y, sobre todo, para el futuro de nuestro país y que estamos poniendo en marcha con el impulso de los fondos europeos, que va a tener continuidad con ese fondo llamado España Crece y que está transformando nuestro país y no está al margen de todo lo bueno que está pasando en la economía de nuestro país”, ha afirmado el ministro.

Fuente: [MTDFP](#)

3/03/2026

## La Comisión anuncia el proyecto EURO-3C para construir una infraestructura federada de telecomunicaciones, borde y nube para la soberanía digital

EURO-3C, es un proyecto de 75 millones de euros para desarrollar la primera infraestructura federada a gran escala de telecomunicaciones, borde y nube de Europa, con el apoyo de Horizonte Europa.

Este proyecto emblemático demostrará la capacidad de Europa para ofrecer servicios digitales de vanguardia íntegramente a través de su propia infraestructura de conectividad, reduciendo así la dependencia de proveedores de terceros países. Telco-edge-cloud combina redes de telecomunicaciones, computación perimetral e infraestructura en la nube en una única plataforma integrada, acercando la potencia informática segura y de alta velocidad a los usuarios finales.

En consonancia directa con los objetivos de la propuesta [Ley de Redes Digitales](#), el proyecto abre la puerta a nuevas oportunidades que fortalecerán el mercado único de telecomunicaciones europeo e incrementarán la soberanía tecnológica. Al impulsar la innovación europea en 6G, IA, ciberseguridad y telecomunicaciones, numerosos sectores de la economía podrán beneficiarse de las soluciones que desarrollará EURO-3C.

Algunas de las empresas y organizaciones líderes de Europa se están uniendo para construir EURO-3C: operadores de telecomunicaciones, proveedores de servicios en la nube, desarrolladores de software, fabricantes de equipos, instituciones de investigación y una amplia red de especialistas en integración.

Con un total de 87 miembros del consorcio, el proyecto también se alinea con las prioridades estratégicas más amplias de la UE y con el trabajo de organizaciones como IPCEI-CIS, la [Empresa Común de Redes y Servicios Inteligentes \(SNS JU\)](#) y [EuroHPC](#), apoyando la competitividad industrial europea.

Fuente: [Comisión Europea](#)

19/03/2026

## La ciberseguridad en España supera los 6.351 millones de euros de facturación y se consolida como cuarto mercado europeo

El Instituto Nacional de Ciberseguridad (Incibe), junto a la Confederación Española de Empresas de Tecnología de la Información, Comunicaciones y Electrónica (Conetic), han presentado las conclusiones del *Estudio sobre la industria de la ciberseguridad en España 2025*, que revela que la ciberseguridad se ha consolidado como uno de los grandes motores del sector tecnológico en España, superando los **6.351 millones de euros de facturación** y situando a España como cuarto mercado europeo.

La ciberseguridad es ya uno de los sectores con más **empuje de la economía digital española**. Concretamente, los datos del estudio muestran con claridad ese salto: más empleo, más facturación, más empresas y una previsión de crecimiento que mantiene al sector en plena expansión.

A día de hoy, la ciberseguridad da **empleo a 164.761 personas** en España y ya representa el 25,55 por ciento del empleo del sector de las Tecnologías de la Información y la Comunicación (TIC). La tendencia, además, apunta claramente al alza. Las previsiones del estudio señalan que entre 2026 y 2029 el sector crecerá a un **ritmo anual del 14,25 por ciento**, lo que permitiría alcanzar los 282.157 empleos al final de ese periodo.

No se trata de una subida puntual. Entre 2021 y 2025, el número de personas empleadas en este ámbito aumentó un 35,14 por ciento, al pasar de 122.284 a 165.256 profesionales. Es decir, la ciberseguridad no solo gana importancia por la necesidad de proteger entornos digitales, sino también por su capacidad real de crear **actividad económica** y empleo cualificado.

Ese crecimiento también se refleja en la facturación. En 2024, la industria alcanzó el 4,65 por ciento de toda la facturación del sector TIC. En paralelo, España cuenta con 3.431 empresas de ciberseguridad, equivalentes al 4,47 por ciento del total de compañías tecnológicas del país.

Por otro lado, la imagen internacional también deja una posición destacada para España. El estudio sitúa al país como **cuarto mercado europeo de ciberseguridad**, con un 12 por ciento de la facturación europea y un 2,8 por ciento de la mundial. Las empresas españolas tienen una presencia especialmente destacada en Portugal, Colombia, Alemania, Brasil y Chile, lo que confirma una proyección exterior cada vez mayor.

El sector se apoya en una base muy atomizada. El 45 por ciento de las empresas son microempresas, un ocho por ciento son autónomos y solo el cinco por ciento son grandes compañías. En otras palabras, la ciberseguridad española crece sobre una red de pequeñas firmas y proyectos empresariales que, poco a poco, van ganando tamaño y relevancia.

El estudio también aborda la evolución de la **presencia femenina**. Las mujeres representan ya el 20 por ciento del empleo en ciberseguridad, un porcentaje ligeramente superior al del conjunto del sector TIC, que se sitúa en el 19,57 por ciento. Aunque la distancia sigue existiendo, hay señales de mejora, de hecho, Euskadi y Castilla-La Mancha aparecen como las comunidades donde más se ha reducido la brecha, con porcentajes de empleo femenino por encima del 35 por ciento.

### **Impulso a la industria de la ciberseguridad**

Otro de los ejes que recoge el informe es el **impulso al emprendimiento** con programas como Incibe Emprende. En este marco, se han firmado 35 convenios con incubadoras y aceleradoras, con prioridad para las provincias con menor presencia de empresas del sector. A ello se suman 2.068 charlas, 652 talleres y 261 eventos, además de iniciativas de incubación para 796 proyectos, aceleración para 244 *startups* y programas exprés para 419 pymes.

La conexión entre el ecosistema empresarial y los servicios de apoyo también va en aumento. Un 42 por ciento de las empresas asegura recibir avisos del servicio de Alerta Temprana de Incibe, mientras que un 31 por ciento figura en el catálogo de empresas de ciberseguridad de Incibe.

Por otra parte, en la presentación de las conclusiones del estudio, se ha celebrado la mesa '**Presente y futuro de la ciberseguridad en España**', moderada por Gloria Díaz, gerente de Conetic. En ella han participado Patricia Alonso, gerente de Incibe-CERT; M<sup>a</sup> Pilar de Cos, responsable de Promoción Empresarial y Desarrollo de Negocio de Incibe; Xabier Mitxelena, presidente de CyberLur; Pablo Lisaso, manager de Operaciones de Infraestructuras y Ciberseguridad del Grupo CIC Consulting Informático; y Jorge Herráez, cofundador y CEO de ClickDefense, quienes han destacado los retos y desafíos en la industria de la ciberseguridad, desde el punto de vista de las instituciones, del emprendimiento, del desarrollo de negocio y también desde las pequeñas y grandes empresas.

También se ha destacado cómo la IA y el cumplimiento normativo de la NIS2 son fundamentales en el avance del sector y cómo se está abordando actualmente desde los distintos eslabones de la cadena y el apoyo del sector público.

En conjunto, las conclusiones del estudio y la mesa de expertos han dejado una idea clara: la ciberseguridad es una industria con peso propio, capacidad de arrastre y un **papel cada vez más relevante en la economía española**. Su crecimiento, tanto en empleo como en facturación, apunta a que seguirá siendo una de las áreas con más recorrido en los próximos años.

Fuente: [Red de Seguridad](#)



## Apunte de interés

### Las pymes industriales españolas lideran la transformación digital en Europa

Un estudio de [Forterro](#) elaborado en cinco países europeos, revela que el 49 % de las empresas industriales españolas califica su transformación digital de los últimos tres años como buena o excelente, superando en 14 puntos la media europea. Además, el 57 % ya tiene una hoja de ruta clara, alineada con el promedio continental.

El 35 % usa ERP en la nube y el 40 % modelos híbridos, con un 79 % planeando migrar en el futuro. Sin embargo, el 60 % ve la nube como una oportunidad sin explotar, el porcentaje más alto de Europa, limitando el potencial de la IA y GenAI.

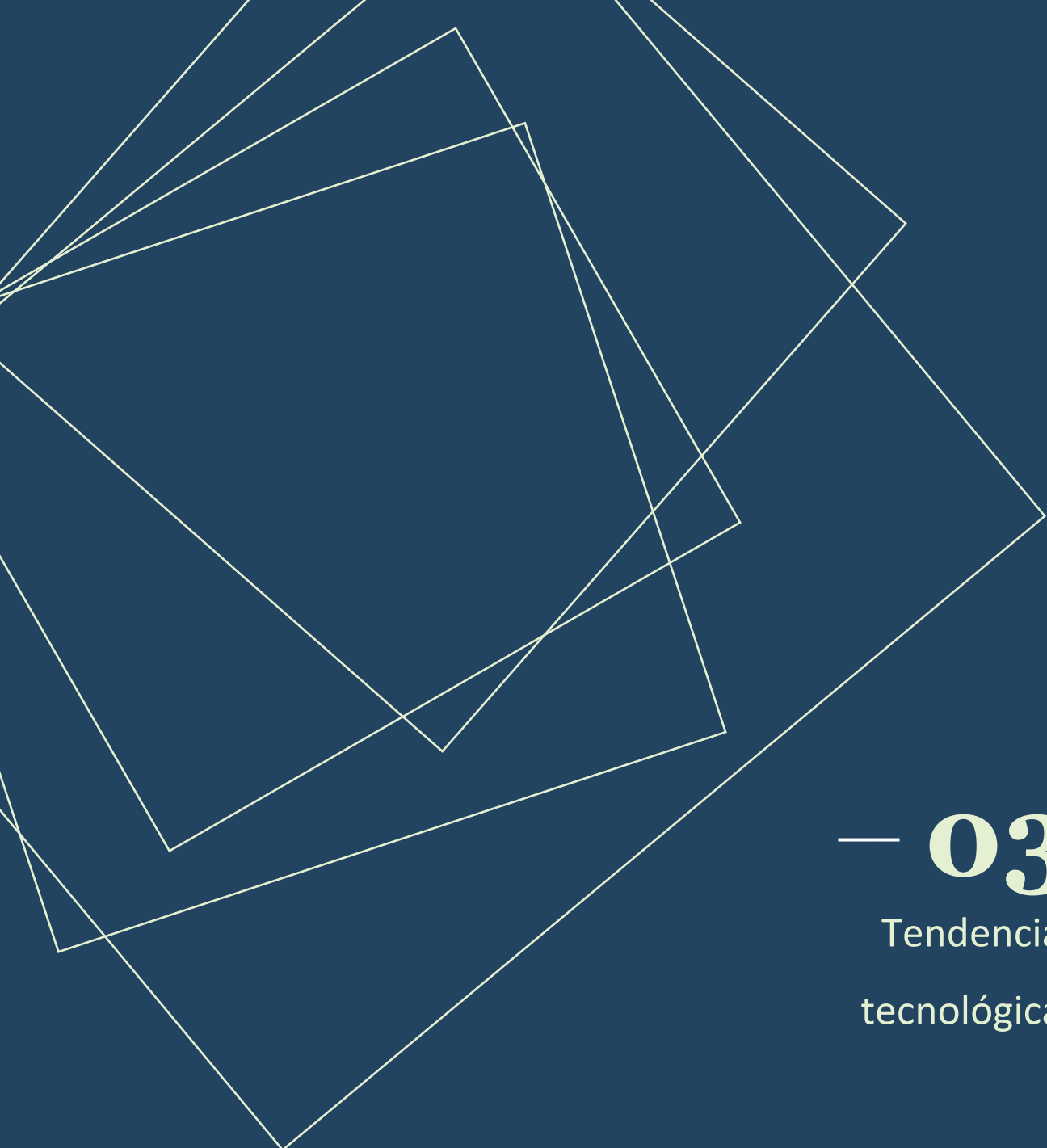
El 48 % prioriza la GenAI, liderando el ranking europeo, pero el 34 % cita restricciones financieras como principal obstáculo.

El 78 % confía en contratar expertos digitales (21 puntos sobre la media UE), pese a que el 60 % admite que las carencias ya frenan proyectos. Departamentos como producción y finanzas muestran más reticencia al cambio.

España parte con ventaja en actitud digital, pero debe resolver presupuestos, alineación directiva y capacitación para capitalizar su potencial frente a competidores europeos.



[Acceso para descargar el estudio completo.](#)



— **03**  
Tendencias  
tecnológicas

*Nuevas patentes, prototipos y resultados de investigación.*

Nº de Publicación: EP3995909B1  
Fecha: 28/01/2026

## Configuración de plantas industriales modulares

La [invención](#) describe un método informático que sirve de herramienta de ingeniería para configurar una planta industrial modular. También abarca el dispositivo informático que ejecuta el método y el programa (software) que contiene las instrucciones necesarias para llevarlo a cabo. En este enfoque, la planta se construye a partir de módulos, y cada módulo incluye al menos un “módulo de función” con el software de control de la planta. La herramienta de ingeniería de módulos crea primero un archivo de configuración “marcador de posición” para ese módulo de función. Después, la persona ingeniera edita este archivo para adaptarlo a la planta industrial modular concreta.

Al modificar el archivo de configuración, la herramienta actualiza automáticamente la representación del módulo de función dentro del entorno de ingeniería de planta, de forma que refleja todos los cambios realizados. Por último, la herramienta de ingeniería se encarga de asignar los módulos de función ya configurados a la planta industrial modular.

Nº de Publicación: EP4703928A1  
Fecha: 4/03/2026

## Método para la creación de pruebas de certificación para un dispositivo industrial

La atestación remota es un mecanismo de seguridad que se utiliza para verificar la integridad y confiabilidad de los sistemas y dispositivos informáticos. En entornos de automatización industrial, donde la confiabilidad y la seguridad de los dispositivos son primordiales, la atestación remota desempeña un papel crucial para garantizar la autenticidad e integridad del software y las configuraciones de los dispositivos.

En el campo de la automatización industrial y la ciberseguridad, se reconoce cada vez más la necesidad de técnicas de certificación más avanzadas para abordar estos desafíos. La mejora de los métodos para crear y mantener certificaciones que permitan registrar el estado actual de los dispositivos industriales, incluso tras largos periodos de funcionamiento, reforzaría considerablemente la seguridad de los sistemas industriales.

La presente [invención](#) se refiere a métodos para crear evidencia de atestación para dispositivos industriales y, en particular, a sistemas y técnicas para recrear y mantener atestaciones después del arranque del dispositivo para mejorar la seguridad y la confianza en entornos de automatización industrial.

### FLF-RCNN: Una red neuronal rápida y ligera optimizada para la inspección de calidad industrial precisa y eficiente

Heuermann A, Ghrairi Z, Zitnikov A, Al Noman A y Thoben KD (2025) Un enfoque para la agrupación no supervisada de interacciones en el trabajo colaborativo humano-robot mediante redes neuronales convolucionales gráficas espaciotemporales. *Front. Robot. AI* 12:1545712. doi: 10.3389/frobt.2025.1545712

La inspección de calidad industrial (IQI) desempeña un papel fundamental para garantizar la consistencia del producto, mejorar la eficiencia de la producción y reducir los índices de desperdicio. A medida que la industria manufacturera avanza hacia la alta precisión y la automatización, se requieren sistemas de inspección que alcancen una alta exactitud, robustez y eficiencia computacional. Los métodos basados en aprendizaje profundo han atraído una atención creciente por su excelente capacidad de extracción de características, superando a los enfoques de detección tradicionales. Sin embargo, los métodos existentes aún presentan problemas de eficiencia insuficiente y escasa transferibilidad. Por lo tanto, mejorar la eficiencia de inferencia y la eficiencia de implementación, manteniendo al mismo tiempo el rendimiento de detección, se ha convertido en un desafío clave de la investigación.

Este [artículo](#) propone un marco de trabajo FLF-RCNN (Fine-tuned Lightweight Faster RCNN) diseñado para abordar los principales desafíos de la IQI, incluyendo el equilibrio entre precisión y eficiencia computacional, y la insuficiente adaptabilidad de las proporciones de cajas de anclaje preestablecidas.

### Revisión de modelos de lenguaje federados de gran tamaño para la Industria 4.0

ing F, Zhang Y, Gao M, Zhang X, Zhou H. Una revisión de los modelos de lenguaje federados a gran escala para la Industria 4.0. *Sensors* 2026; 26(4):1116. <https://doi.org/10.3390/s26041116>

La Industria 4.0 prevé un ecosistema de fabricación autónomo y altamente interconectado, impulsado por el Internet industrial de las cosas, los sistemas ciberfísicos y la inteligencia artificial. La aparición de modelos de lenguaje a gran escala introduce nuevas capacidades para la toma de decisiones con conciencia semántica, la integración de conocimiento entre dominios y la automatización inteligente.

Esta [revisión](#) examina sistemáticamente la integración de LLM y FL en la Industria 4.0, abarcando fundamentos arquitectónicos, técnicas habilitadoras y escenarios de aplicación representativos. Si bien nuestro análisis incorpora avances recientes tanto desde perspectivas académicas como industriales, cabe señalar que el panorama de Fed-LLM está evolucionando rápidamente y podrían surgir nuevos métodos más allá del alcance temporal de esta revisión. Además, al centrarnos en la integración de LLM, FL e Industria 4.0, es posible que ciertos temas adyacentes, como la inteligencia perimetral independiente o los modelos de fundamentos industriales centralizados, no se hayan tratado con la misma profundidad. Estos factores deben tenerse en cuenta al interpretar las conclusiones de este trabajo.

## Proyecto MetaFacturing

[MetaFacturing](#) desarrolla Proyecto una cadena de herramientas digitalizada para la producción de piezas metálicas. Esto permitirá un proceso de producción más resiliente en cuanto a las materias primas utilizadas reducirá el esfuerzo y los costes del operario, y reducirá los desechos debidos a piezas fuera de especificación.

Se ha centrado en la creación de un marco de configuración y control de procesos basado en Gemelos Digitales de amplia aplicación, que satisfaga los requisitos de los fabricantes de piezas a escala industrial (con especial atención a las piezas metálicas), cuyo principal obstáculo es el uso eficaz de los datos disponibles sobre piezas y procesos para optimizar el tiempo de comercialización y la calidad del producto.

El consorcio está formado por 12 entidades coordinados por la Universidad Katholieke de Lovanas de Bélgica. El proyecto iniciado en enero de 2023 finalizó en diciembre de 2025.



**metaFacturing**

## Proyecto Digi4Circular

El proyecto [Digi4Circularv](#), financiado con fondos europeos, tiene como objetivo crear un flujo de trabajo digital para el desarrollo de productos circulares. Centrado en la fundición de aluminio en el sector automotriz, el proyecto permitirá la generación automatizada de diseños de productos circulares al tiempo que evalúa los impactos ambientales en varios escenarios de fin de vida útil. Empleará métodos innovadores para diseñar aleaciones circulares y realizará evaluaciones rápidas del ciclo de vida y análisis de costos.

El proyecto Digi4Circular aborda estos desafíos mediante la creación de un sólido flujo de trabajo digital para el desarrollo de productos circulares. Facilita la generación de diseños de productos circulares y posibilidades de fabricación, en función de las evaluaciones de impacto ambiental para diferentes escenarios de fin de vida útil. El flujo de trabajo conecta todas las herramientas de software necesarias y los datos generados a lo largo de la cadena de valor en un espacio de información dedicado, mientras que los datos del ciclo de vida de cada producto se almacenan sistemáticamente en un Pasaporte Digital del Producto, accesible para todos los desarrolladores de la cadena de valor.

Su consorcio está formado por 11 entidades. Iniciado en 2024 tiene previsto finalizar en abril de 2028.



## Proyecto Radiance

[RADIANCE](#) es un proyecto de Horizonte Europa que desarrolla un conjunto integrado de tecnologías robóticas, digitales y basadas en IA para respaldar el proceso completo de renovación, desde la inspección y el diagnóstico hasta la reparación, la seguridad, la planificación y la evaluación de la sostenibilidad.

A través de tres escenarios de validación reales en edificios europeos, el proyecto tiene como objetivo acelerar los flujos de trabajo de renovación, apoyar a los trabajadores con herramientas avanzadas, mejorar la seguridad y reducir la huella ambiental de las actividades de construcción.

Su consorcio coordinado por la Universidad de Vigo reúne a 12 organizaciones líderes de 7 países europeos que combinan experiencia en robótica, automatización, IA, construcción, digitalización y sostenibilidad.

El proyecto se inició en septiembre de 2025 y tiene prevista su finalización en agosto de 2029.



## Proyecto HEDGE-IoT

El proyecto [HEDGE-IoT](#) presenta un innovador marco digital que conecta la nube con el borde de la red e introduce aplicaciones federadas gestionadas por soluciones avanzadas de orquestación computacional. Este marco mejorará la resiliencia de la red, liberará un potencial de flexibilidad sin explotar y creará nuevas oportunidades de mercado.

Su enfoque multidimensional abarca pilares como la facilitación tecnológica, la interoperabilidad, la estandarización y la habilitación del ecosistema energético digital, lo que garantiza una comunicación fluida, un intercambio de datos estandarizado y la creación de un ecosistema resiliente para una mayor integración de las fuentes de energía renovables.

El proyecto se inició en enero de 2024 y tiene previsto finalizar en junio de 2027. Cuarenta y seis entidades forman el consorcio, coordinados por Dinámica Europea Luxemburgo SA.





— **04**  
Agenda

*Congresos, ayudas, modificaciones normativas y otros hitos relevantes  
del calendario del sector industrial en materia de digitalización.*

¿Qué ha ocurrido?

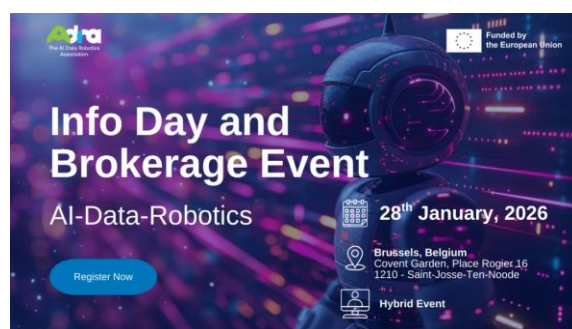
## Info Day and Brokerage Event AI–Data–Robotics 2026

Bruselas y online, 28/01/2026

La Comisión Europea, junto con ADRA y la red de Puntos Nacionales de Contacto (PNC), organizó una [Jornada Informativa](#) y un evento de Intermediación dedicados a las próximas convocatorias de 2026 en las áreas de Inteligencia Artificial, Datos y Robótica, en el marco del Clúster 4 de Horizonte Europa (Digital, Industria y Espacio) y el Programa Europa Digital.

El evento presentó el contexto político y las principales características de los temas relevantes, y apoyó la formación de consorcios mediante actividades de presentación de proyectos y de intermediación, incluyendo reuniones bilaterales organizadas a través de la plataforma de intermediación de los PNC.

Desde la página del [evento](#) se pueden descargar todas las presentaciones y/o ver la grabación de la reunión.



## Jornadas informativas de Horizont Europa – Clúster 4: Digital, Industria y Espacio

Madrid, 29-30/01/2026

Las [jornadas](#) informativas trataron las oportunidades de financiación para la investigación y la innovación para desarrollar una industria competitiva, digital, baja en carbono y circular. Incluyeron información sobre tecnologías digitales clave, tecnologías cuánticas, tecnologías habilitadoras emergentes, inteligencia artificial y robótica, Internet de próxima generación, informática avanzada y Big Data.

Ponentes de la Comisión Europea presentaron información detallada sobre los temas de la convocatoria, así como sobre los procedimientos de evaluación y adjudicación.

Desde la página del [evento](#) se puede acceder a las grabaciones.



¿Qué ha ocurrido?

## Fusion HPC Workshop

Online, 24-25/02/2026

El [evento](#) internacional está centrado en el uso de la supercomputación, la inteligencia artificial y las tecnologías de datos para abordar retos de gran complejidad industriales, científicos y sociales.

Se abordarán casos de uso y avances en áreas como ciencia computacional, ingeniería avanzada, salud y biociencias, modelización climática, energía, industria digital y gemelos digitales, poniendo el foco en la transición desde la investigación hacia aplicaciones reales con impacto económico y social.



## Transfiere

Málaga, 24-26/02/2026

[Transfiere](#), el foro europeo de I+D+i celebró su 15ª edición entorno a nueve ejes temáticos y su aplicación directa en el tejido productivo generando un espacio donde convergen el potencial investigador, la iniciativa empresarial y el compromiso institucional.

Más de 4.700 visitantes profesionales; más de 600 entidades; empresas y administraciones públicas; 430 ponentes expertos; 101 paneles temáticos; 65 universidades y 36 países representados son algunas de las cifras del éxito de esta nueva edición de Transfiere.



**Transfiere**  
15º European Meeting on Science,  
Technology and Innovation

**MÁLAGA**  
**24-26**  
**FEB 2026**

*¿Qué ha ocurrido?*



## ICUR

Madrid, 24-27/02/2026

Se celebró la 25ª edición del [Salón Internacional de la Seguridad](#) reuniendo, como cada dos años, a empresas, asociaciones, profesionales y usuarios de la seguridad global en los ámbitos públicos y privados.

La innovación y el desarrollo tecnológico fueron los ejes del evento que aborda la seguridad integral desde cuatro grandes áreas (Security, ciberseguridad, seguridad contras incendios y emergencias, seguridad laboral).



## BIEMH

Bilbao, 2-6/03/2026

Una nueva edición de la [Bienal Internacional de Máquina-Herramienta](#) se dio cita en Bilbao con más de 2.500 productos innovadores y exposiciones de 29 países con demostraciones en vivo para la innovación, la automatización y la digitalización de la industria.

Durante el evento se dieron a conocer los ganadores de los Premios de Innovación Avanzada que reconocen a las empresas que destacan por sus aportaciones tecnológicas, capacidad de transformación industrial y visión de futuro.



*Próximamente*

## Hannover Messe

Hannover, 20-24/04/2026

[Hannover Messe](#) reúne a expertos internacionales, responsables de la toma de decisiones de inversión y usuarios. Con visitantes de más de 150 países, la feria ofrece la mayor plataforma para la transformación industrial.

Este evento líder mundial en tecnología industrial presenta las últimas tecnologías que impulsan la transformación digital.

Esta edición contará con un pabellón centrado en hidrógeno verde, automatización y digitalización industrial, dirigido a presentar la oferta tecnológica española en el ámbito de la energía con especial foco en el hidrógeno verde y la descarbonización y en el ámbito de la automatización y la digitalización industrial.



## Advanced Factories

Barcelona, 5-7/05/2026

[Advanced Factories](#) presentará as últimas soluciones en automatización, robótica, sistemas integrados de la producción, inteligencia artificial, machine learning, gemelo digital, visión artificial, VR/AR, ciberseguridad, IIoT, analítica de datos y cloud computing para impulsar la competitividad, productividad y sostenibilidad de las fábricas y centros de producción.

Más de 400 expertos internacionales de primer nivel compartirán sus experiencias industriales en automatización, robotización, integración de sistemas e implementación de nuevas tecnologías 4.0. Analizarán el **impacto de tecnologías** como la inteligencia artificial, la ciberseguridad, el cloud industrial o el gemelo digital, y desvelarán las tendencias y **aplicaciones de futuro** en el sector industrial.



*Próximamente*



## South Summit Madrid

Madrid, 3-5/06/2026

South Summit Madrid conecta a startups, inversores y corporaciones para generar oportunidades de negocio e innovación tecnológica.

El [evento](#) busca reunir a las mejores startups del mundo, de todas las industrias y sectores, al nivel más avanzado posible, para responder a las necesidades de las corporaciones. Se espera seguir la tendencia de crecimiento y superar los datos de 2025.

# SOUTH SUMMIT

## SIL Barcelona 2026

Barcelona, 3-5/06/2026

El [Salón de la Logística](#) de Barcelona celebrará su vigesimosexta edición con el foco en la innovación. Una de las principales novedades serán los nuevos espacios dedicados a la innovación, la digitalización y el talento como el SIL Lab, o el IA Corner.

Estará representada toda la cadena de suministro, con la participación de empresas que ofrecen: servicios de transporte, logística y distribución; tecnología e IT; infraestructuras; inmologística; talento; intralogística; industria 4.0; última milla y entrega en el ecommerce y sostenibilidad.

# SIL

## Barcelona

3 - 5 junio 2026

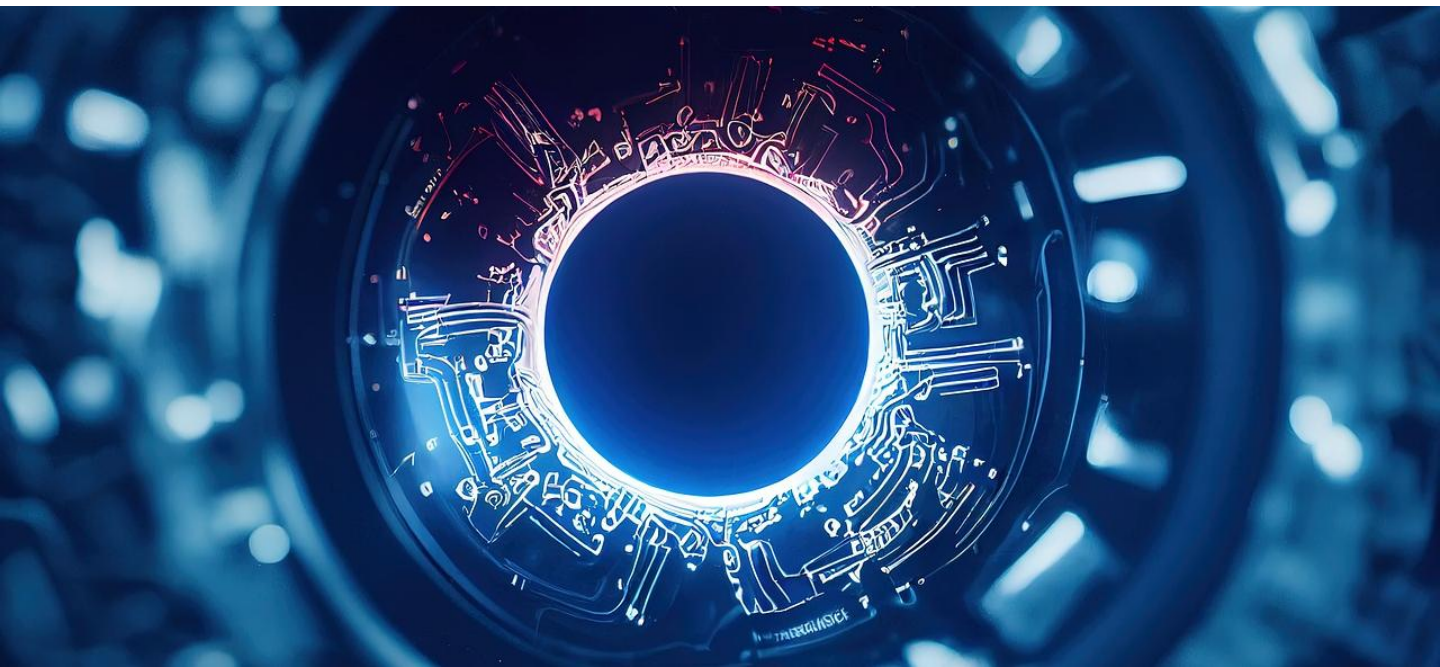
*Próximamente*

# Digital Enterprise Show

Málaga, 9-11/06/2026

[DES](#) es el evento B2B internacional en IA y tecnologías exponenciales para la transformación empresarial y las estrategias de crecimiento.

Se presentarán más de 700 innovaciones, soluciones y servicios en inteligencia artificial, datos, ciberseguridad, nube, IoT, computación cuántica, tecnología para el comercio minorista, marketing, startups y negocios digitales, impulsando la transformación, la competitividad y el crecimiento de 15.000 profesionales de alto nivel a industrial.



## Convocatorias de Chips cofinanciadas por la AEI

Chips JU es una iniciativa internacional orientada a reforzar la investigación, la innovación y la capacidad de fabricación en semiconductores, con la ambición de posicionar a Europa como referente global, mejorar su autonomía digital y contribuir a objetivos estratégicos como la sostenibilidad y la competitividad tecnológica. En este contexto, la AEI participa apoyando la financiación de proyectos competitivos dentro de la empresa.

Los topics actualmente abiertos son HORIZON-JU-CHIPS-2026-1-IA y HORIZON-JU-CHIPS-2026-1-RIA, orientados a reforzar la base tecnológica europea en semiconductores y microelectrónica avanzada. Estas acciones de investigación e innovación abordan, respectivamente, el desarrollo de tecnologías y arquitecturas vinculadas a Inteligencia Artificial, así como el avance de procesos, materiales, diseño, integración y validación de dispositivos y sistemas electrónicos.

Las convocatorias se dirigen a centros de investigación, universidades y entidades sin ánimo de lucro que participen en consorcios internacionales, y se alinean con las prioridades estratégicas del ecosistema europeo de componentes y sistemas electrónicos, incluyendo tecnologías fundamentales, tecnologías transversales como HPC, IA y ciberseguridad, y aplicaciones en ámbitos como movilidad, energía, industria digital, salud y transformación digital.

[Más información](#)

## Línea de Ayudas a Infraestructuras de Ensayo y Experimentación

El CDTI Innovación ha puesto en marcha la Línea de Ayudas a Infraestructuras de Ensayo y Experimentación, una iniciativa destinada a financiar proyectos de inversión orientados a la construcción y/o mejora de infraestructuras científico-tecnológicas que permitan prestar servicios de apoyo a la innovación empresarial.

El objetivo de esta actuación es reforzar la capacidad de los agentes de interfaz del ecosistema de innovación —como Centros Tecnológicos y de Apoyo a la Innovación, Parques Científicos-Tecnológicos, Incubadoras u Oficinas de Transferencia de Conocimiento— para facilitar el desarrollo tecnológico, la investigación aplicada y la transferencia de tecnología hacia el tejido empresarial.

Estas infraestructuras permitirán a las empresas, especialmente a las pymes, validar, probar o demostrar tecnologías en entornos avanzados —como bancos de pruebas, líneas piloto, demostradores, instalaciones de ensayo o laboratorios vivos— antes de su entrada en el mercado, favoreciendo el desarrollo de nuevos productos, procesos y servicios y contribuyendo al fortalecimiento de los ecosistemas de innovación.

Podrán beneficiarse de esta línea de ayudas centros tecnológicos y centros de apoyo a la innovación tecnológica, tanto de ámbito estatal como territorial, así como asociaciones, fundaciones y empresas que desarrollen actividad económica y dispongan de personalidad jurídica propia y domicilio fiscal en España.

Las ayudas financiarán proyectos de inversión destinados a la adquisición de activos fijos nuevos, tanto materiales como inmateriales, necesarios para la construcción y/o mejora de estas infraestructuras tecnológicas. Los proyectos deberán tener una duración mínima de nueve meses y máxima de veinticuatro meses.

La línea se instrumenta mediante Ayudas Parcialmente Reembolsables (APR) financiadas con fondos del CDTI Innovación, con un tipo de interés fijo referenciado al Euríbor a un año.

Todos los detalles de la convocatoria [aquí](#).

El plazo de presentación de solicitudes se abrió el 16 de marzo y permanecerá abierto durante todo el año a través de la [sede electrónica del CDTI Innovación](#).



## La UE retrasa hasta 2027 la entrada en vigor de las normas sobre IA

La Comisión propuso ampliar el plazo de aplicación de las normas sobre sistemas de IA de alto riesgo hasta en 16 meses, de modo que dichas normas entren en vigor una vez que la Comisión confirme la disponibilidad de las normas y herramientas necesarias.

Asimismo, propuso modificaciones específicas a la Ley de IA que extenderían ciertas exenciones reglamentarias concedidas a las pymes también a las pequeñas y medianas empresas (PYME), reducirían los requisitos en un número muy limitado de casos, ampliarían la posibilidad de procesar datos personales sensibles para la detección y mitigación de sesgos, reforzarían las competencias de la Oficina de IA y reducirían la fragmentación de la gobernanza.

Entre los cambios planteados figura el ajuste del calendario de aplicación de las obligaciones para los sistemas de IA de alto riesgo. La propuesta contempla un aplazamiento de hasta 16 meses para que estas normas empiecen a aplicarse una vez que estén disponibles los estándares y herramientas necesarios, entrando en vigor el 2 de diciembre de 2027 para los sistemas de IA de alto riesgo independientes y 2 de agosto de 2028 para los sistemas de alto riesgo integrados en productos. También se retrasa hasta el 2 de diciembre de 2027 el plazo para establecer los sandboxes regulatorios de IA a escala nacional y clarifica las competencias de la Oficina Europea de IA en la supervisión.

Esto se enmarca en el objetivo más amplio de la UE de reducir cargas administrativas y regulatorias para las empresas, especialmente para pymes, y de reforzar a la vez la seguridad jurídica y la aplicación armonizada del Reglamento de IA.

La iniciativa forma parte del llamado Digital Omnibus, orientado a facilitar la aplicación del marco digital europeo y, en particular, de las reglas armonizadas vinculadas al Reglamento de IA.

[Más información](#)





*Just in Time*

## **Digitalización como palanca de la autonomía estratégica**

Avances a lo largo de 2025

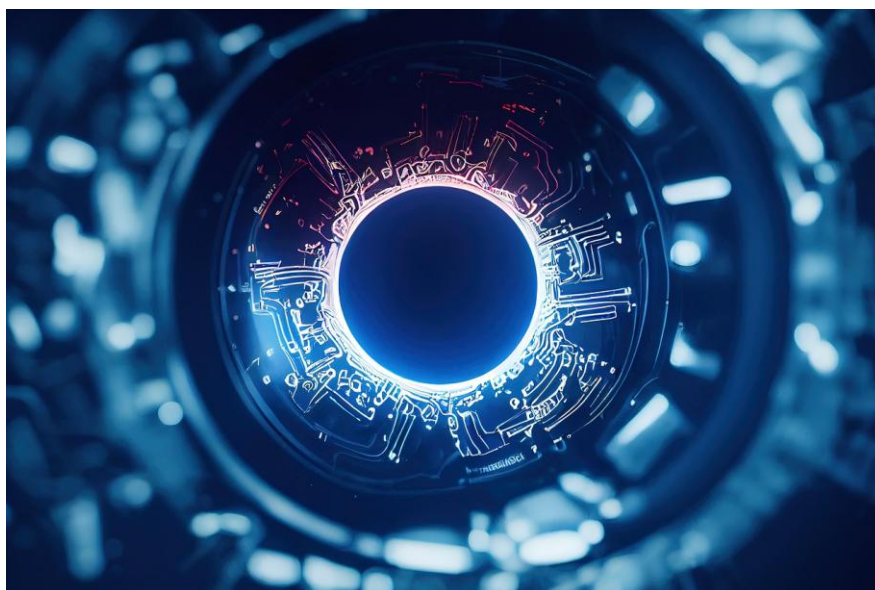
La transformación digital en Europa está experimentando una aceleración sin precedentes, impulsada por la necesidad de **infraestructuras digitales más resilientes, sostenibles y estratégicamente autónomas**. En este contexto, las infraestructuras de conectividad integrada y los servicios de informática colaborativa constituyen los pilares fundamentales para garantizar la competitividad industrial, la cohesión territorial y la soberanía tecnológica de la Unión Europea (UE).

2025 ha supuesto un año de avance posicionando la digitalización no solo como herramienta de eficiencia, sino como medio para reducir dependencias tecnológicas, fortalecer la soberanía en datos, IA y semiconductores, y potenciar la competitividad industrial.

### Iniciativas europeas clave

La UE aceleró infraestructuras digitales resilientes, con énfasis en conectividad de alta capacidad y computación distribuida como edge, cloud federado y fog computing.

- **Continente de IA:** en abril de 2025 la Comisión fijó el rumbo hacia el liderazgo de Europa en Inteligencia Artificial con su ambicioso plan de acción. Transformó industrias tradicionales en motores de innovación mediante Factorías de IA para reforzar la infraestructura computacional europea.
- **Estrategia de datos:** una iniciativa integral con el objetivo salvaguardar la soberanía de los datos de la UE y **fortalecer su posición global** mediante su enfoque estratégico creó un mercado interior de datos seguro, promoviendo flujos transfronterizos con socios de confianza para expandir soluciones de IA.
- **InvestAI:** Movilizó 200.000 millones de euros en infraestructuras y modelos avanzados de IA, un hito para la transformación digital.
- **Apply AI:** a finales de 2025 la estrategia sectorial Impulsó adopción industrial de IA en sectores clave, con centros de innovación digital y gigafábricas de IA.



El **Informe Década Digital 2025** publicado por la Comisión Europea destacó avances en IA, nube y big data, pero alertó sobre dependencias en semiconductores, datos y ciberseguridad, agravadas por la demanda energética de la IA. En concreto el informe señala:

- **El futuro digital de la UE depende cada vez más de una producción energética estable.** La creciente demanda de energía, vinculada, entre otros factores, al uso cada vez mayor de la IA, está superando rápidamente el desarrollo de un suministro energético limpio y fiable y la capacidad de la red eléctrica en toda la UE. Esta discrepancia se perfila como un obstáculo importante para la expansión de tecnologías digitales clave y retrasa la capacidad de la UE para aprovechar plenamente la IA y la innovación basada en datos en aras de la competitividad económica.
- **La adopción de la inteligencia artificial (IA), la nube y el big data por parte de las empresas** ha mejorado, pero necesita acelerarse. La UE sigue **dependiendo de proveedores externos para los servicios de IA y nube**, así como para la producción de semiconductores y componentes de infraestructura cuántica.

Precisamente en relación a la dependencia histórica de nubes hiperscalares extranjeras, antes vista como una eficiencia de costes, y que hoy se identifica como un riesgo crítico emerge, el **"Edge Continuum" europeo** no solo como una solución técnica, sino como una frontera de seguridad donde los datos industriales se procesan y mueren dentro de la jurisdicción de la propia planta. Esta iniciativa conjunta hace avanzar a Europa hacia la soberanía digital.

## Avances en España

La autonomía estratégica en tecnologías avanzadas, especialmente en el ámbito de los chips y semiconductores también ha sido protagonista en 2025. Los semiconductores sustentan la transformación digital, son esenciales para todas las industrias. España alineó su agenda con la UE mediante el **PERTE Chip**, el Proyecto Estratégico de Microelectrónica y Semiconductores alcanzando su madurez técnica este año y superando los 330 millones de euros en inversión, movilizándolo 12.000 millones totales.

En esta misma línea y enmarcado como proyecto estratégico en el PERTE Chip, se aprobó un centro de desarrollo de semiconductores de última generación que estará alojado en Cataluña, financiado con fondos procedentes del plan Next Generation de la UE.

- **Ley de Industria y Autonomía Estratégica:** proyecto de Ley en tramitación, impulsado por el Ministerio de Industria y Turismo estableció las bases de ordenación del sector industrial con el objetivo de impulsar una nueva estrategia industrial para incrementar el peso de la industria, mejorar su competitividad y resiliencia y hacer posible su contribución a los objetivos de descarbonización de la economía y de **transformación digital**.
- **Plan Industrial y Tecnológico para Seguridad y Defensa (junio 2025):** una iniciativa para fortalecer capacidades, reducir dependencias estratégicas y consolidar la industria española como referente europeo en seguridad y defensa.
- **Espacios de datos sectoriales:** España destaca en el desarrollo de grandes espacios de datos en sectores estratégicos como salud, turismo y agroalimentación.
- **Estrategia Nacional de Tecnologías Cuánticas (2025-2030):** busca fortalecer la soberanía digital, impulsar la competitividad y promover un desarrollo sostenible, ético y regulado. Así, España participa activamente en la creación de una red europea de infraestructuras cuánticas acelerando la industrialización de las tecnologías cuánticas, salvaguardando nuestra autonomía estratégica.



La **ciberseguridad** se ha convertido en un componente central de la soberanía digital de España porque la capacidad de proteger infraestructuras críticas, datos, cadenas de suministro y sistemas industriales condiciona directamente la autonomía estratégica del país.

En 2025 la ciberseguridad deja de ser un asunto técnico para convertirse en un pilar de **competitividad, soberanía digital y resiliencia nacional**. Así, se refleja en el **Informe de situación Ciberseguridad en España 2025**.

La creación del **Centro Nacional de Ciberseguridad** aparece como una medida clave para coordinar la defensa, mejorar la respuesta ante incidentes y reforzar la protección de infraestructuras críticas.

La presión regulatoria europea, especialmente **NIS2**, obliga a España a elevar el nivel de gobernanza, notificación y gestión del riesgo, lo que fortalece la capacidad estatal de control y reacción ante amenazas.

En mayo de 2025 se aprobó un plan de inversión pública de **1.157 millones de euros** en ciberseguridad y ciberdefensa, con objeto de reforzar refuerza la capacidad nacional para desarrollar infraestructura, talento y soluciones propias.

A pesar de progresos, España destaca en 5G y e-salud, pero necesita acelerar la adopción de IA en empresas y estándares de Internet. El informe Década Digital señala una dependencia externa superior al 80 % en productos digitales, un déficit de 300.000 especialistas en ciberseguridad y brecha energética para IA.

# Ley de Aceleración Industrial: acelerar la digitalización para competir globalmente

La Comisión Europea impulsa la **Ley de Aceleración Industrial** (IAA, por sus siglas en inglés) para fortalecer la industria y generar empleo en Europa. Esta propuesta busca agilizar la transición digital y verde mediante procesos administrativos simplificados.

La Comisión Europea presentó el 4 de marzo de 2026 la propuesta de Ley de Aceleración Industrial, un marco legislativo diseñado para revitalizar la competitividad industrial europea frente a competidores globales como China y EE.UU. El objetivo central es reducir los plazos de obtención de permisos para proyectos industriales clave, pasando de años a meses, mediante ventanillas únicas digitales que integran evaluaciones ambientales y autorizaciones sectoriales.

Esta iniciativa responde al informe Draghi sobre la competitividad europea y al Pacto Verde, priorizando sectores como el acero, cemento, baterías, renovables y semiconductores.

## Medidas clave para la digitalización

- **Ventanilla Única Digital:** Un portal centralizado para todas las autorizaciones, con plazos máximos de 6-12 meses para proyectos "de interés estratégico", incorporando herramientas de IA para acelerar evaluaciones.
- **Priorización de Proyectos Net-Zero:** Incentivos para inversiones en tecnologías limpias y digitales, como automatización y eficiencia energética, con exenciones regulatorias temporales para pruebas piloto.
- **Apoyo a la Reindustrialización:** Creación de "Zonas Industriales Estratégicas" con trámites acelerados y financiación del programa InvestEU, estimando la generación de 500.000 empleos directos hasta 2030.

Para la industria española, esta ley representa una oportunidad clave en la digitalización, alineándose con la **Estrategia España Digital 2026** y el **PERTE de Industrias Estratégicas**. Las empresas podrán acceder a fondos europeos para modernizar plantas con gemelos digitales y robótica, reduciendo emisiones en un 30 % según proyecciones de la CE.

Esta reforma posiciona a Europa como líder en industria inteligente y sostenible, pero requiere implementación rápida por los Estados miembros para maximizar su efecto multiplicador en la cadena de valor.

El Reglamento propuesto será negociado por el Parlamento Europeo y el Consejo de la Unión Europea antes de su adopción y entrada en vigor.

# Créditos

---

## DIRECCIÓN:

EOI Escuela de Organización Industrial  
Fundación EOI F.S.P.  
C/ Gregorio del Amo, 6  
28040 Madrid  
Tel: 91 349 56 00  
[www.eoi.es](http://www.eoi.es)



Esta publicación está bajo licencia *Creative Commons* Reconocimiento, No comercial, Compartirigual, (by-nc-sa). Usted puede usar, copiar y difundir este documento o parte del mismo siempre y cuando se mencione su origen, no se use de forma comercial y no se modifique su licencia.

Más información:

<http://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

---

## ELABORADO POR:

Fundación CTIC  
Centro Tecnológico para el desarrollo en Asturias de  
las Tecnologías de la Información y la Comunicación  
[www.fundacionctic.org](http://www.fundacionctic.org)





Boletines

DE

Vigilancia  
Tecnológica

**CEPI** Centro de  
Estrategia y  
Prospectiva  
Industrial