

BOLETÍN DE VIGILANCIA TECNOLÓGICA

DPI Nº17 T2 2026

DIGITALIZACIÓN DE LA PRODUCCIÓN INDUSTRIAL

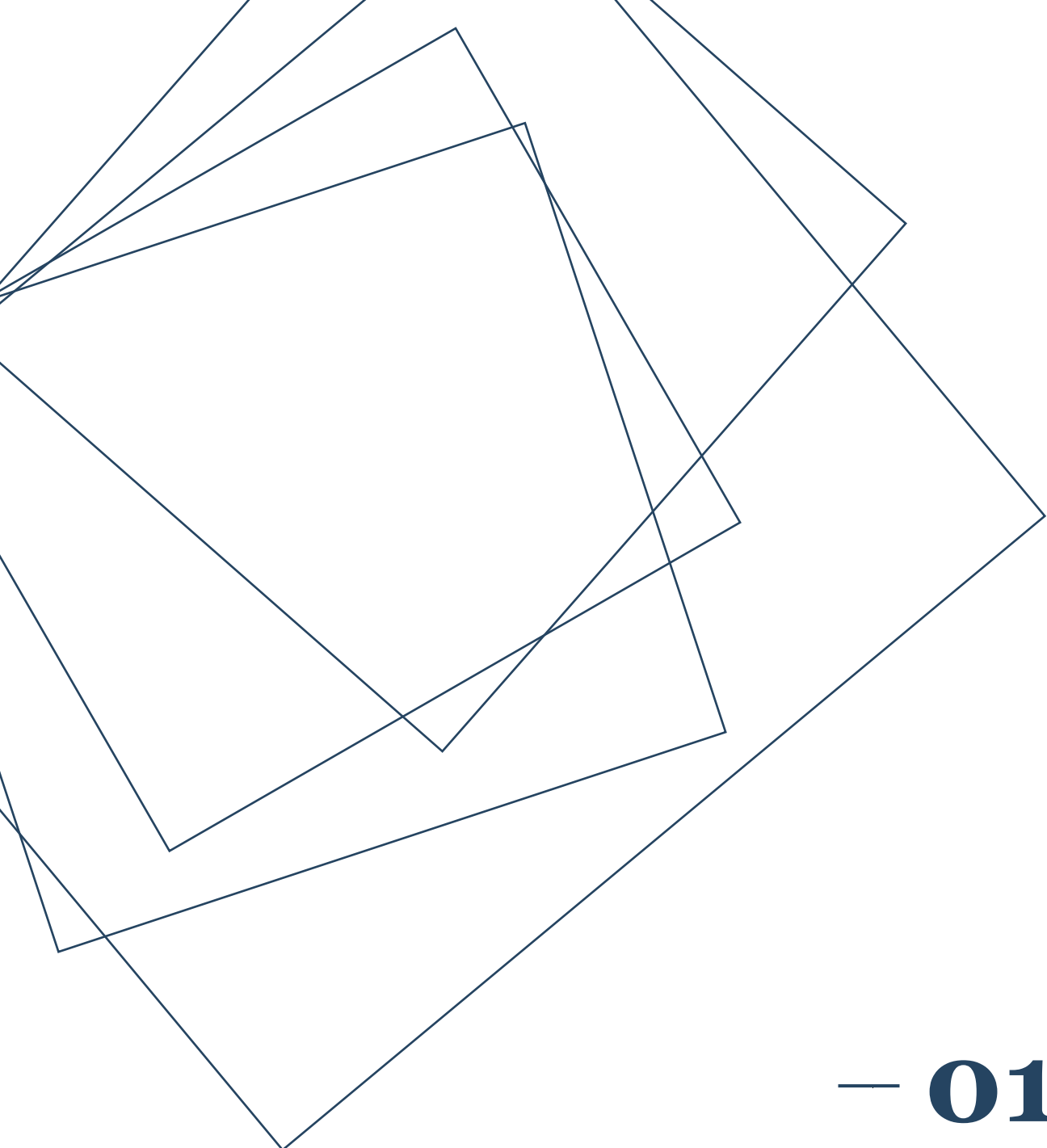


El Boletín de Vigilancia Tecnológica sobre Digitalización de la Producción Industrial es una publicación trimestral de la Escuela de Organización Industrial desarrollada en colaboración con CTIC Centro Tecnológico. Este Boletín pretende ofrecer una visión general de las tecnologías emergentes y los avances 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 Factor humano y resiliencia en la ciberseguridad industrial
- _11 Actualidad
- _20 Tendencias tecnológicas
- _25 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.

Factor humano y resiliencia en la ciberseguridad industrial

En el actual ecosistema de la **Industria 4.0**, la ciberseguridad ha dejado de ser un compartimento estanco de las tecnologías de la información (IT) para convertirse en el pilar fundamental de la continuidad del negocio. La convergencia IT/OT (Tecnologías de Operación) ha diluido las fronteras que tradicionalmente aislaban las plantas de producción, exponiendo infraestructuras críticas a amenazas globales. Según investigaciones recientes publicadas en el [Journal of Information Processing Systems](#), más del 70-80 % de los ciberataques contra sistemas industriales tienen en el comportamiento humano su punto de entrada principal.

En este escenario, el factor humano no debe entenderse meramente como una fuente de errores estadísticos, sino como la **variable estratégica definitiva**. Es la capacidad de discernimiento, adaptabilidad y formación del personal lo que marca la diferencia entre una operación ininterrumpida y un desastre de proporciones físicas, ambientales y legales.

Estudios recientes, como el publicado en [Information](#) (MDPI, 2025), refuerzan que las organizaciones con culturas de seguridad maduras registran tiempos de recuperación significativamente menores ante incidentes. Este análisis sostiene que la resiliencia industrial moderna depende de transformar el rol del operador: de ser el vector de entrada involuntario a convertirse en el **sensor inteligente** más avanzado de la organización.

El factor humano como origen de riesgos en la ciberseguridad industrial

La vulnerabilidad humana en el entorno industrial no es un fenómeno aislado, sino el catalizador que permite a un atacante completar la **Cyber Kill Chain** (Cadena de Ataque). Mientras que las defensas técnicas pueden bloquear ataques automatizados, la ingeniería social y la negligencia operativa facilitan las fases de Entrega, Instalación y Acciones sobre objetivos. En el entorno OT, un comportamiento inadecuado trasciende la pérdida de datos; compromete la Safety (seguridad operativa), afectando la integridad de bienes y personas. El eBook de Cisco sobre [Ciberseguridad Industrial](#) ilustra con detalle cómo los vectores de amenaza específicos del mundo OT difieren radicalmente de los entornos IT convencionales.

Vectores de ataque conductual

El atacante moderno sabe que es más sencillo engañar a un humano que romper un cifrado de grado militar. Los tres vectores críticos donde la acción humana define el riesgo son:

- **Uso de dispositivos extraíbles (USBs):** A pesar de las políticas restrictivas, la práctica de utilizar llaves USB para transferir diagnósticos, actualizaciones de firmware o archivos de configuración sigue siendo habitual. Este acto introduce malware directamente en el núcleo del sistema de control, saltándose los firewalls perimetrales. El malware, una vez dentro, inicia un "desplazamiento lateral" hacia estaciones críticas.
- **Ingeniería social y Spear Phishing:** Mediante el spear phishing, un atacante puede, por ejemplo, comprometer una estación de ingeniería. Estas estaciones contienen la lógica de programación de los PLC (Controladores Lógicos Programables). Un solo clic erróneo de un operario puede permitir exfiltrar programas de PLC, modificar variables de proceso o alterar setpoints, resultando en sabotajes indetectables a corto plazo. Investigaciones recientes en el campo de la [ciber-criminología](#) documentan cómo estos ataques aprovechan sesgos cognitivos como la urgencia y la autoridad percibida.
- **Accesos remotos y terceros:** La necesidad de mantenimiento preventivo ha generalizado las conexiones VPN y ADSL. El riesgo es la suplantación de accesos autorizados de personal subcontratado. Si las credenciales de un tercero son comprometidas, el atacante obtiene un punto de entrada de "alta calidad" al núcleo de la instalación.

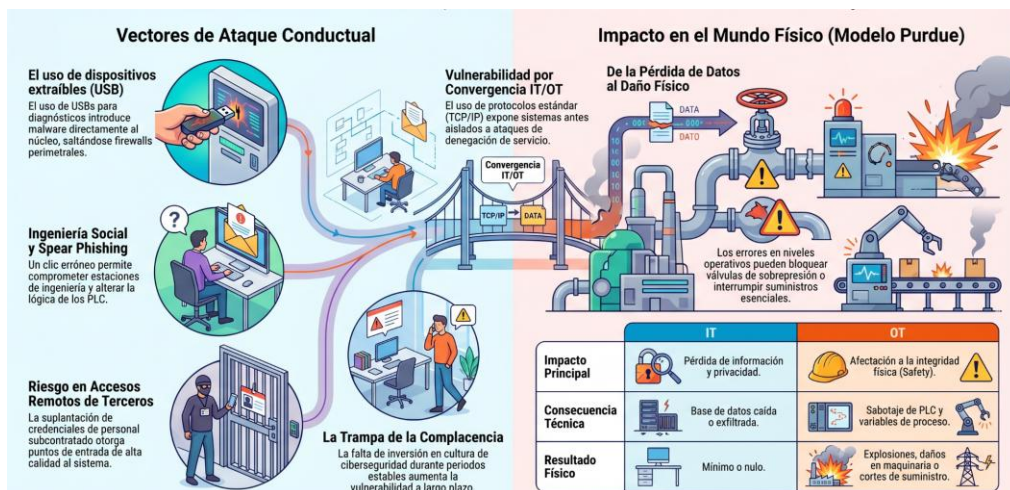


Figura 1: El factor humano: vector de ataque e impacto. Fuente: Elaboración propia.

La jerarquía del riesgo: el Modelo Purdue

Es vital comprender por qué el riesgo humano en OT es cualitativamente distinto al de IT. Según el **Modelo Purdue**, los niveles 0-1 (campo/proceso y control) contienen sensores, actuadores y PLCs que interactúan directamente con el mundo físico; el nivel 2 (supervisión) agrupa las estaciones SCADA y HMI donde los humanos visualizan el proceso; y el nivel 3 (operaciones) engloba sistemas MES y LIMS. Un error humano en estos niveles no resulta en una base de datos caída; puede provocar una válvula de sobrepresión bloqueada, una centrifuga a velocidades críticas o la interrupción de suministros esenciales como agua o gas.

La convergencia IT/OT ha permitido que tecnologías estándar (Windows, TCP/IP) penetren en estos niveles, exponiendo sistemas que antes estaban «aislados por aire» a vulnerabilidades típicas de entornos de oficina, pero con el agravante de que una denegación de servicio (DoS) puede causar consecuencias físicas graves. Aunque la [segmentación de redes](#) OT sigue siendo una salvaguarda necesaria, ninguna arquitectura técnica elimina la dependencia del criterio humano en estos niveles: es el operador quien, en última instancia, interpreta si un evento en el nivel 2 (SCADA/HMI) responde a la lógica del proceso o a una intrusión en curso.



Figura 2: Esquema Modelo Purdue. Fuente: Elaboración propia.

Presión operativa y complacencia: amplificadores del riesgo humano

El error humano rara vez nace de la incompetencia; suele ser el producto de condiciones de trabajo adversas. La fatiga, la sobrecarga cognitiva y la presión por mantener la producción degradan la capacidad de atención del operador y aumentan la probabilidad de un clic erróneo o de que se omita un control. Reconocer estos condicionantes (turnos, carga de trabajo y claridad de los procedimientos) como variables de ciberseguridad es el primer paso para reducir el riesgo. El informe [SANS 2025 State of ICS Security](#) insiste en que la resiliencia industrial depende tanto de las personas como de la tecnología, y que la preparación del personal de planta es uno de sus factores determinantes.

A ese riesgo se suma la trampa de la complacencia: la ausencia de inversión en cultura de ciberseguridad durante los periodos de estabilidad operativa es, en sí misma, una vulnerabilidad que los atacantes aprovechan. Como muestran los estudios sobre [riesgos del factor humano en ciberseguridad](#), la percepción del riesgo dentro de la organización condiciona directamente las prioridades de inversión: cuando el incidente parece lejano, la formación y los simulacros son lo primero que se recorta, justo lo que más se echa en falta cuando el ataque llega.

El factor humano como elemento de resiliencia

El cambio de paradigma es radical: debemos dejar de ver al humano como el "eslabón débil" para posicionarlo como un "sensor inteligente". Las soluciones de detección basadas únicamente en firmas o listas negras fallan ante ataques que utilizan comandos legítimos con fines maliciosos. Aquí es donde el juicio humano y el conocimiento contextual del proceso se vuelven insustituibles. Los factores humanos en ciberseguridad abarcan tanto las vulnerabilidades como las capacidades de defensa activa del personal.

Defensa activa y detección de anomalías contextuales

En una red industrial, un comando "DETENER" enviado a un PLC es sintácticamente correcto. El software de seguridad tradicional no lo bloqueará porque es un comando estándar. Sin embargo, un operador formado puede identificar que ese comando es anómalo si se produce fuera de una ventana de mantenimiento. La [guía técnica de Cisco Cyber Vision](#) documenta exactamente este tipo de eventos operativos que, sin contexto humano, son invisibles para los sistemas automáticos.

La resiliencia se construye sobre la capacidad del personal para monitorizar propiedades críticas que el software a menudo ignora:

- **Identificación de activos:** Validar direcciones MAC, nombres de PLC y puertos TCP/UDP.
- **Inventario profundo:** Supervisar versiones de firmware, números de serie de hardware y versiones de proyectos de PLC.
- **Detección de manipulaciones:** Alertar sobre cambios en el reloj del controlador, borrado de memoria o cambios al modo de diagnóstico.
- **Indicadores de Compromiso (IoC):** Identificar consultas DNS inusuales de estaciones industriales hacia servidores de mando y control (C2) externos, un patrón que señala la presencia de malware activo.

Solo el conocimiento operativo permite discernir si una variación en la temperatura de una caldera responde a una lógica de producción o a un atacante "cebando" la supervisión SCADA con información falsa para ocultar un sabotaje físico. Investigaciones recientes sobre [comportamiento humano en sistemas de control](#) destacan que el operador experto actúa como un sistema de detección de anomalías distribuido y adaptativo, capacidad que ningún algoritmo ha logrado replicar completamente.

Cultura y formación como activo estratégico

La resiliencia industrial es un constructo social. La formación continua reduce drásticamente la probabilidad de incidentes por «desplazamiento lateral». El enfoque Human-Centric implica coordinar mantenimiento, operaciones y seguridad. Esta sinergia crea una red de defensa que permite: detección temprana antes de la fase de explotación; respuesta ágil con capacidad de pasar a modos de operación manual ante una denegación de servicio; y recuperación rápida minimizando el Recovery Time Objective (RTO) mediante simulacros y procedimientos ensayados.

Los datos respaldan este enfoque: según el [informe SANS 2025 sobre seguridad ICS](#), las organizaciones que incorporan a técnicos de campo y operadores en sus ejercicios de simulación (tabletop) declaran niveles de preparación 1,7 veces superiores, y las que se sienten plenamente preparadas tienen siete veces más probabilidades de implicar a ese personal en los entrenamientos.

El enfoque interdisciplinar es clave: la ausencia de colaboración entre ingeniería, criminología y psicología en los equipos de seguridad genera productos y procedimientos que no contemplan las necesidades cognitivas y emocionales del operador. Como señala la investigación de [Nobles & Burrell \(2024\)](#), la falta de especialistas en factores humanos en los equipos de ciberseguridad intensifica la brecha de conocimiento y las vulnerabilidades resultantes. Los programas de concienciación deben abordar específicamente los vectores OT, no simplemente adaptar materiales de formación corporativa genérica, para que el personal identifique amenazas en su contexto real de trabajo.

Sinergia con tecnologías de apoyo (IA y Digitalización)

La digitalización y el Big Data no sustituyen al experto humano; lo potencian. La Inteligencia Artificial debe servir para filtrar el ruido y permitir que el operador concentre su atención en los indicadores de riesgo (IoC). Según las investigaciones recientes sobre [IA en ciberseguridad industrial](#) (MDPI, 2025), los modelos de aprendizaje automático alcanzan su máximo potencial cuando trabajan de forma sinérgica con operadores humanos formados, combinando la capacidad de procesamiento masivo de la máquina con el juicio contextual del experto. Esta sinergia es especialmente crítica ante los protocolos propietarios de los ICS (Siemens, Schneider, ABB, Rockwell), que carecen de especificaciones públicas: las técnicas automáticas de cumplimiento de protocolo solo son parcialmente aplicables, de modo que la interpretación humana de los eventos de red sigue siendo imprescindible para distinguir una operación legítima de un sabotaje encubierto.

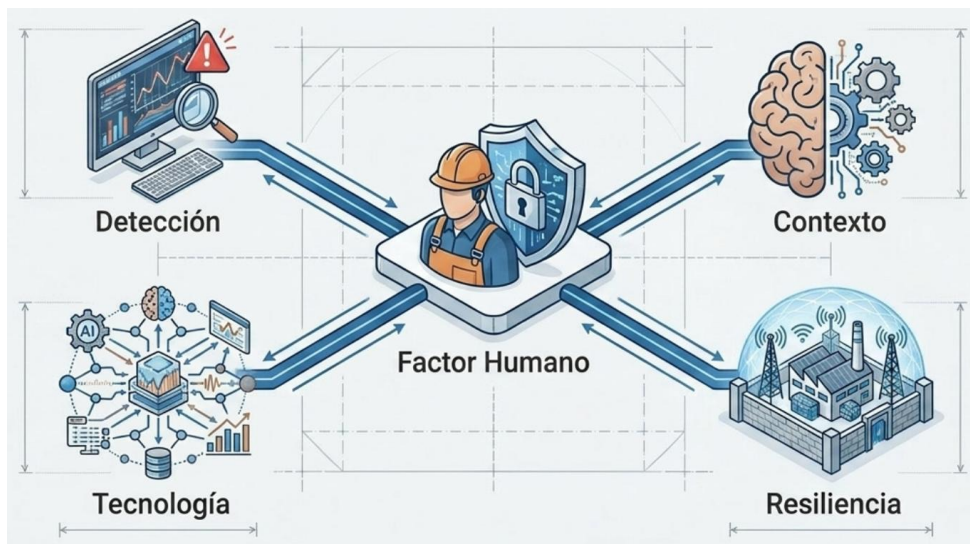


Figura 3: Factor humano como centro de la ciberseguridad. Fuente: Elaboración propia.

Impacto en la competitividad

La resiliencia no es evitar el ataque, sino asegurar la supervivencia de la empresa tras el mismo. Un personal capacitado para detectar una anomalía en el firmware de un PLC antes de que el atacante active su carga destructiva ahorra millones en paradas no planificadas y daños.

Conclusión

La ciberseguridad industrial es, ante todo, un problema humano.

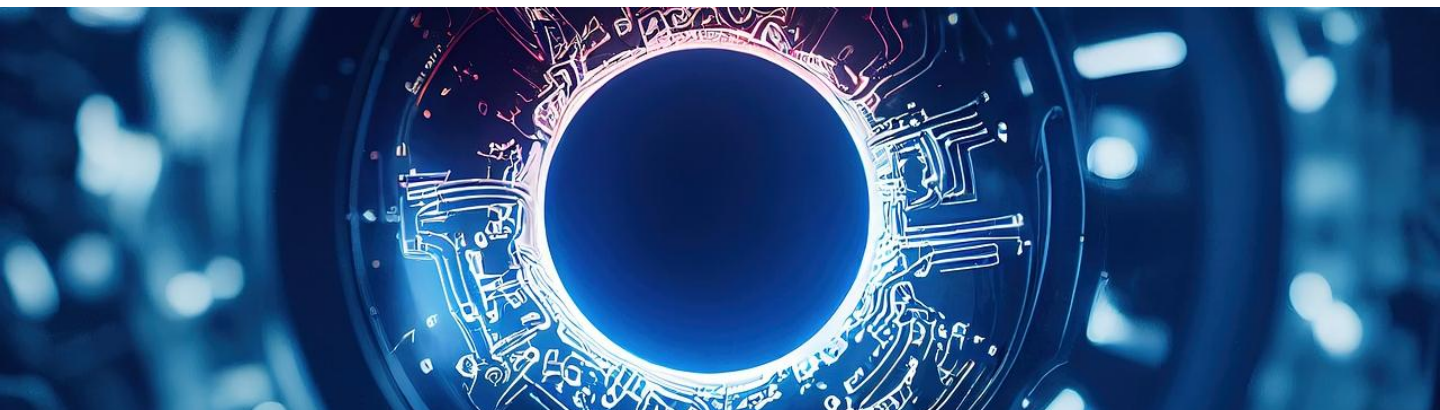
Como punto de partida, los datos son contundentes: entre el 70 y el 80 % de los ciberataques contra entornos industriales tienen su origen en el comportamiento humano. No en fallos de hardware, no en vulnerabilidades de firmware sin parchear, sino en decisiones, a menudo rutinarias y bien intencionadas, de personas que trabajan bajo presión, con herramientas diseñadas sin tener en cuenta sus necesidades cognitivas.

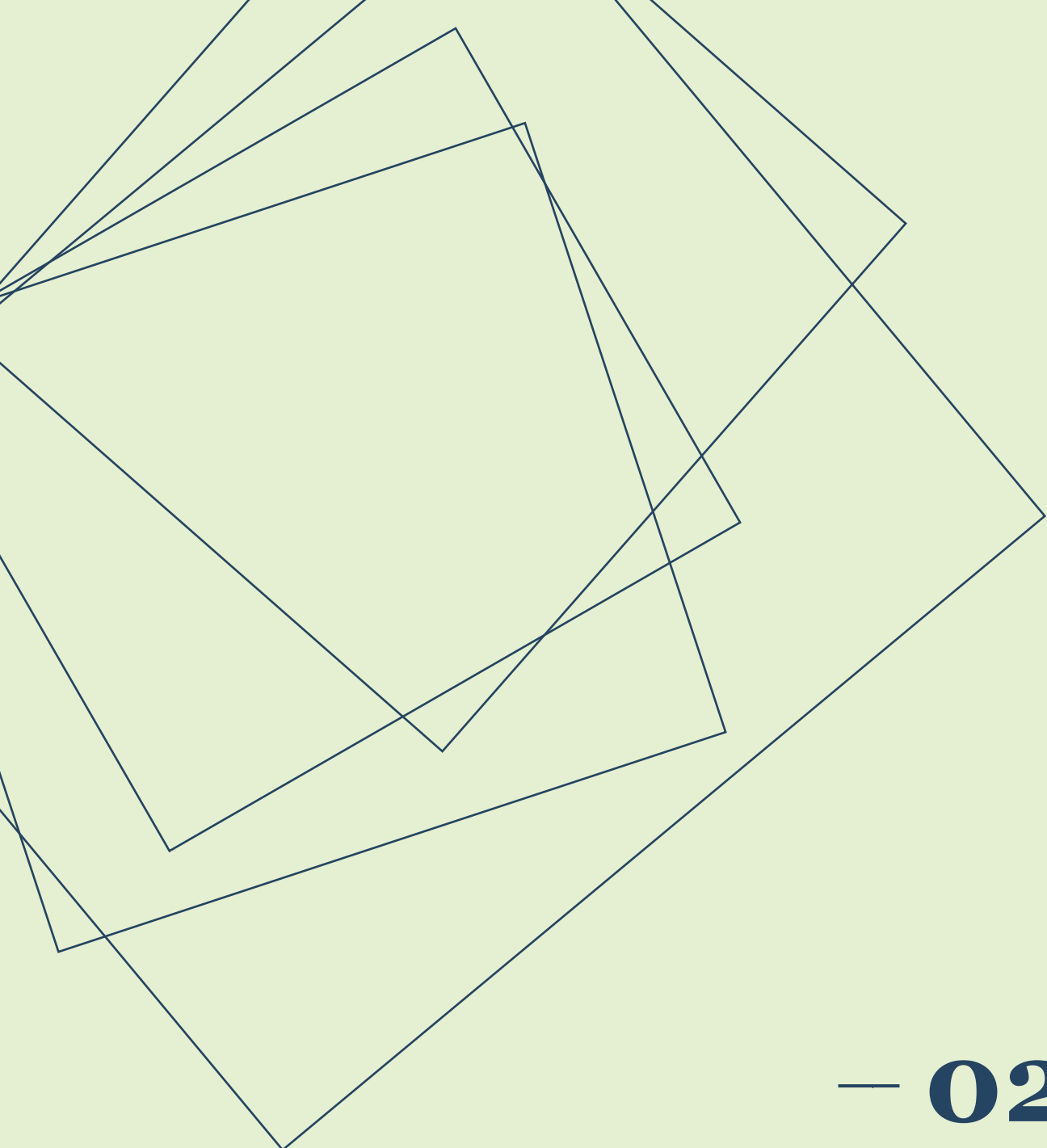
El sector lleva décadas invirtiendo en capas tecnológicas de protección mientras dejaba en segundo plano la variable que más influye en el resultado final. La convergencia IT/OT ha acelerado esa contradicción: sistemas que durante años operaron aislados ahora están expuestos a las mismas amenazas que el correo corporativo, pero con consecuencias que van mucho más allá de una base de datos comprometida.

El cambio de enfoque que propone la investigación más reciente, tratar al operador como un **sensor inteligente** en lugar de como un eslabón débil, no es solo una cuestión semántica. Implica rediseñar los programas de formación, los procedimientos de respuesta y las propias herramientas de supervisión para que se adapten a cómo las personas perciben, deciden y actúan en entornos de alta exigencia.

La tecnología seguirá evolucionando. Los protocolos propietarios irán abriéndose. La inteligencia artificial mejorará la detección de anomalías. Pero ningún algoritmo reemplazará al técnico que reconoce, por experiencia, que una variación en la temperatura de una caldera a las 3 de la madrugada no cuadra con el plan de producción. Esa capacidad de contextualización es el activo más difícil de replicar y el que más merece ser cultivado.

El futuro de la industria es digital, pero su seguridad seguirá siendo profundamente humana.





— 02

Actualidad

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

Plan de Acción del Continente de IA

El objetivo del Plan de Acción «Continente de IA» que se ha puesto en marcha es ocupar la posición de líder mundial en inteligencia artificial (IA). Según lo expuesto por la presidenta Von der Leyen en la Cumbre para la Acción sobre la IA celebrada en París en febrero de 2025, la finalidad de esta ambiciosa iniciativa es transformar las grandes industrias tradicionales europeas y sus excepcionales activos de talento en poderosos motores de innovación y aceleración de la IA.

Aún quedan muchas vueltas en la carrera hacia el liderazgo en IA. Desde unos modelos fundacionales punteros hasta unas aplicaciones de IA especializadas, el panorama de la inteligencia artificial en la UE se presenta dinámico. Lo impulsan la investigación, las tecnologías nacientes y un fértil ecosistema de empresas emergentes y en expansión. El Plan de Acción «**Continente de IA**» potenciará las capacidades de innovación de la Unión Europea en materia de IA mediante acciones y políticas articuladas en torno a cinco pilares fundamentales:

- **Construcción de una infraestructura informática y de datos de IA a gran escala.** La Comisión reforzará la infraestructura europea de inteligencia artificial y supercomputación con una red de Factorías de IA. Trece de estas factorías o fábricas están implantándose ya en torno a los superordenadores de vanguardia de Europa. Apoyarán a las empresas emergentes de IA, a la industria del sector y a los investigadores de la UE en el desarrollo de modelos y aplicaciones de IA.
- **Aumento del acceso a grandes volúmenes de datos de alta calidad.** Potenciar la innovación en IA requiere también el acceso a grandes volúmenes de datos de alta calidad. Un importante elemento del Plan de Acción es la creación de laboratorios de datos en los que se reúnan y preserven grandes volúmenes de datos de alta calidad procedentes de diferentes fuentes en las factorías de IA. En 2025 se pondrá en marcha una estrategia de datos de la Unión, iniciativa integral para crear un auténtico mercado interior de datos que permita expandir las soluciones de IA.
- **Desarrollo de algoritmos y fomento de la adopción de la IA en sectores estratégicos de la UE.** Pese al potencial de la IA, tan solo el 13,5 % de las empresas de la UE la ha incorporado. Con el fin de desarrollar soluciones de IA adaptadas a los distintos usos e impulsar su utilización industrial y su plena adopción en los sectores público y privado estratégicos de la UE, la Comisión pondrá en marcha en los próximos meses la estrategia de uso de la IA. Desempeñará un importante papel en esta estrategia la infraestructura europea de innovación en IA, en particular las factorías de IA y los centros europeos de innovación digital.
- **Refuerzo de las capacidades y el talento en materia de IA.** Para satisfacer la creciente demanda de talento en materia de IA, la Comisión facilitará la contratación internacional de expertos e investigadores altamente cualificados en IA a través de iniciativas como la Reserva de Talentos, la acción Marie Skłodowska-Curie «MSCA Choose Europe» y los programas de becas sobre IA que ofrecerá la Academia de Capacidades en IA de próxima creación. Estas iniciativas contribuirán a la apertura de vías de migración legal para los trabajadores altamente cualificados de terceros países en el sector de la IA y atraerán hacia Europa a los mejores investigadores y expertos europeos en inteligencia artificial. Además, la Comisión desarrollará programas educativos y formativos sobre IA e IA generativa en sectores clave, preparando con ello la próxima generación de especialistas en IA y favoreciendo el reciclaje y el perfeccionamiento profesional de la mano de obra.

- **Simplificación regulatoria.** El Reglamento de Inteligencia Artificial aumenta la confianza de los ciudadanos en la tecnología y proporciona a los inversores y empresarios la seguridad jurídica que necesitan para expandir su actividad e implantar la IA en toda Europa. Además, la Comisión pondrá en marcha un servicio de asistencia sobre el Reglamento de Inteligencia Artificial que ayudará a las empresas a cumplirlo. Servirá de punto central de contacto y ventanilla de información y orientación sobre este Reglamento.

Fuente: [Comisión Europea](#)

20/05/2026

Foro de Alto Nivel de la Industria Española

El Ministerio de Industria y Turismo ha aprobado la Orden Ministerial que recoge la nueva regulación del **Foro de Alto Nivel**, un órgano asesor que refuerza la política industrial española. La norma sustituye la regulación vigente desde 2020 y responde a los nuevos retos del tejido industrial.

Como principal novedad, se crea el **Comité de Diálogo Industrial**, un órgano ejecutivo permanente que permitirá dotar de mayor agilidad, continuidad y eficacia a los trabajos del Foro y reforzar la colaboración público-privada.

La nueva regulación amplía las funciones del Foro, ampliando su papel en el diseño, evaluación y seguimiento de las políticas industriales, con el objetivo de impulsar la productividad, la competitividad y la sostenibilidad de la industria española. Asimismo, se mejora la representatividad del tejido industrial, con mayor flexibilidad para incorporar nuevos actores y con un firme compromiso con la igualdad de género.

Con esta medida, el Ministerio de Industria y Turismo apuesta por un modelo de gobernanza industrial más sólido, transparente y participativo, que fortalece el diálogo social e industrial y permite anticipar grandes retos estratégicos, como la transición verde, la digitalización y la autonomía estratégica de la economía española.

El pasado 20 de mayo el ministro de Industria y Turismo, Jordi Hereu presidió la constitución del Foro de Alto Nivel de la Industria Española, acompañado de grupos de trabajo temáticos, con el objetivo de anticipar retos, acelerar decisiones y reforzar la colaboración público-privada.

El ministro ha destacado que España quiere desempeñar un papel protagonista en la nueva etapa industrial europea, apoyándose en su base productiva, su talento y su potencial tecnológico en ámbitos como la inteligencia artificial, el hidrógeno verde o la microelectrónica.

Fuente: [MINTUR](#)

La industria española avanza en automatización, pero solo un 3,3 % cuenta con fábricas inteligentes totalmente digitalizadas

La industria española avanza hacia modelos de producción más automatizados, conectados y basados en datos, aunque todavía se encuentra lejos de alcanzar un escenario de fábrica plenamente digitalizada. Así se desprende del **III Barómetro de la digitalización y automatización industrial en España**, elaborado por **Advanced Factories 2026**, que analiza el estado actual de la automatización, la robotización y la digitalización en el ámbito manufacturero a partir de la opinión de más de 500 directivos y profesionales procedentes de sectores como el automovilístico, metalúrgico, químico y farmacéutico, bienes de equipo, electrónico, alimentación y bebidas, energético, packaging, logístico, textil, construcción, aeronáutico, ferroviario, armamento y defensa o naval, entre otros.

El estudio refleja que la transformación digital de la industria española avanza de forma progresiva, pero todavía con un amplio margen de desarrollo. De hecho, el 32 % de los profesionales encuestados define el nivel de automatización y digitalización de sus fábricas como moderado, mientras que solo un 3,3 % asegura contar con fábricas inteligentes totalmente digitalizadas. Esta brecha evidencia que la fábrica autónoma, conectada y basada en datos en tiempo real sigue siendo todavía una aspiración para la mayoría del tejido industrial.

La integración de sistemas, el gran reto pendiente. Aunque muchas compañías han incorporado tecnologías digitales en sus plantas, la conexión real entre sistemas sigue siendo limitada. Según el barómetro, el 55,6% de los profesionales reconoce que su empresa cuenta con una integración parcial entre plataformas como ERP, MES, SCADA o PLM. Solo un 22,4 % afirma disponer de una integración completa, mientras que un 16,6 % asegura que no existe integración entre sistemas.

Este escenario pone de manifiesto una de las grandes paradojas de la digitalización industrial: las fábricas cuentan cada vez con más tecnología, pero no siempre con una arquitectura conectada que permita aprovechar todo su potencial. Sin una integración sólida, los datos permanecen fragmentados, los procesos pierden visibilidad y la toma de decisiones sigue dependiendo, en muchos casos, de sistemas aislados.

La inteligencia artificial avanza entre pilotos y aplicaciones concretas. La inteligencia artificial se ha convertido en una de las tecnologías con mayor capacidad transformadora para la industria, aunque su implementación todavía se encuentra en una fase inicial para muchas compañías. El 49,4 de los encuestados afirma estar realizando pruebas piloto con IA, mientras que un 22,8 % ya la utiliza en algunos procesos y un 21,2 % reconoce que aún no la emplea.

Estos datos muestran que la IA está entrando en la industria de forma gradual, a través de proyectos concretos, validaciones internas y casos de uso específicos antes de avanzar hacia una implantación más amplia. Entre las principales barreras para su implementación destaca la falta de talento, señalada por el 42,7 % de los profesionales, seguida de la resistencia al cambio organizacional, mencionada por el 32 %, y la falta de claridad sobre el retorno de la inversión, apuntada por el 30,2 %.

Pese a estas dificultades, las compañías que ya aplican inteligencia artificial están encontrando oportunidades en áreas clave de la actividad industrial. El 56,3 % de los encuestados que emplean IA en su organización la utiliza en labores de diseño asistido y simulación, lo que permite validar diseños, anticipar comportamientos y reducir errores antes de llevar una solución a planta. Asimismo, un 50 % aplica la IA en el control de calidad y otro 50 % en la optimización de procesos productivos, ámbitos donde esta tecnología empieza a ofrecer resultados tangibles en términos de productividad, precisión y eficiencia.

IA física, automatización inteligente y robótica marcarán la competitividad industrial. De cara a los próximos tres años, la IA física e industrial se sitúa como la principal tendencia tecnológica para la competitividad industrial en Europa, según la mayoría de los encuestados. Esta tecnología abre la puerta a sistemas productivos más autónomos, robots capaces de aprender en entornos simulados antes de operar en planta, gemelos digitales más precisos y procesos que combinan percepción, decisión y acción en tiempo real.

La automatización inteligente ocupa el segundo lugar entre las tendencias clave, según el 48,1 % de los encuestados, lo que confirma que la industria seguirá avanzando hacia sistemas capaces de optimizar tareas, coordinar procesos y mejorar la eficiencia operativa con un mayor grado de autonomía. Por su parte, la robótica, señalada por el 41,1 %, continuará siendo esencial para transformar las plantas de producción, especialmente en ámbitos como la fabricación flexible, la logística interna, el ensamblaje o la inspección de calidad.

Fuente: [El Economista](#)



España pide acelerar y reforzar la política industrial europea ante el Consejo de Competitividad de la Unión Europea

España ha defendido hoy en el Consejo de Competitividad de la Unión Europea la necesidad de acelerar y reforzar la política industrial europea, subrayando que la autonomía estratégica europea debe ser abierta, con industrias fuertes, resilientes y competitivas.

En el segundo y último Consejo bajo la Presidencia chipriota, el secretario de Estado de Industria, Jordi García Brustenga, ha trasladado el compromiso de España con una agenda industrial europea más ambiciosa, centrada en la agilidad en la toma de decisiones y en el apoyo efectivo a sectores estratégicos. Durante la reunión, el secretario de Estado ha puesto el foco en la necesidad urgente de actuar en sectores clave como el acero, el aluminio y la industria química, esenciales para garantizar la autonomía industrial, el empleo de calidad y el desarrollo de la transición verde y digital.

En este sentido, España ha defendido que la competitividad industrial debe situarse en el centro de la agenda europea, reforzando la resiliencia de las cadenas de suministro y reduciendo dependencias estratégicas, con un enfoque equilibrado, basado en el valor añadido, la apertura económica y la garantía de unas cadenas de suministro seguras, diversificadas y resilientes.

Uno de los ejes clave del Consejo ha sido el avance del Industrial Accelerator Act (IAA), propuesta presentada por la Comisión Europea en marzo de 2026, cuyo objetivo es reforzar la base industrial, acelerar la descarbonización y mejorar la competitividad de los sectores estratégicos.

El secretario de Estado ha resaltado que España trabaja activamente en la construcción de una posición sólida y equilibrada sobre este reglamento que prevé medidas como el fomento de productos bajos en carbono, el impulso a la cadena de valor europea, la creación de áreas de aceleración industrial, y el apoyo a la industria electrointensiva y tecnologías de cero emisiones.

España defiende un enfoque equilibrado de la propuesta, centrado en la contribución industrial efectiva y las actividades de alto valor añadido que refuercen la competitividad europea. Para el secretario de Estado de Industria, Europa debe seguir siendo un lugar atractivo para las inversiones de terceros países, pero bajo premisas y reglas de juego europeas.

El secretario de Estado ha pedido también que medidas como el IAA vengán también acompañadas de un esfuerzo inversor de la Unión Europea sostenido en el tiempo para nuestra industria.

El Consejo ha abordado también los avances sobre el Fondo Europeo de Competitividad y, durante el almuerzo, se ha producido un debate sobre la industria química, en el que España ha transmitido la urgencia de implementar medidas efectivas para el sector en Europa.

España considera que la reindustrialización es una oportunidad clave para generar empleo, atraer inversión y reforzar la posición de España y Europa en la economía global.

El secretario de Estado de Industria ha reiterado la voluntad de nuestro país de ejercer un papel activo en la definición del nuevo marco industrial europeo.

Nuevo ordenador cuántico EuroQCS-Spain

El Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC-CNS) ha presentado hoy el tercer ordenador dedicado a la computación cuántica, el EuroQCS-Spain, cofinanciado con una inversión de 9,8 millones de euros por la Comisión Europea y el Gobierno de España, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), que aporta 4,8 millones de euros. Gracias a una codificación analógica de la información, el nuevo sistema aporta una tecnología cuántica complementaria a la previamente instalada en el centro y estará disponible para el personal investigador de toda Europa.

Con esta incorporación, instalada en la remodelada capilla de Torre Girona, MareNostrum 5 se convierte en uno de los primeros superordenadores de todo el mundo en combinar computación clásica (con las particiones de propósito general y la acelerada) y computación cuántica digital y analógica (con los dos ordenadores cuánticos instalados por el proyecto Quantum Spain y la SEDIA y este último, respectivamente). Para ello, de la inversión total, 8,5 millones de euros corresponden a la instalación de las máquinas -con una cofinanciación al 50% entre EuroHPC y el Gobierno de España- y el resto, a la integración, es decir, la combinación de la máquina cuántica con la infraestructura clásica.

Este nuevo sistema cuántico formará parte de la red europea de ordenadores cuánticos interconectados en la infraestructura de la European High Performance Computing Joint Undertaking (EuroHPC JU) que, hasta la fecha, ha adquirido seis ordenadores cuánticos ubicados por toda Europa, tres de los cuales (Polonia, Chequia y Alemania) ya han sido inaugurados. Estas tecnologías son clave en la Estrategia de la Europa Cuántica, que busca hacer de Europa un líder mundial en este ámbito de aquí a 2030 y consolidar la soberanía tecnológica, la competitividad industrial y la seguridad de Europa.

El secretario de Estado de Ciencia, Innovación y Universidades, Juan Cruz Cigudosa, ha asegurado que “el Euro QCS-Spain refuerza el mensaje de que España está preparada para liderar, innovar y ser protagonista del futuro tecnológico de Europa”. “Es la prueba de que cuando hay voluntad política, coordinación institucional y excelencia científica, los proyectos se materializan. Proyectos con tecnología 100% europea y que contribuyen a nuestra autonomía estratégica”, ha señalado.

Por su parte, la secretaria de Estado, María González Veracruz, ha destacado que “este ordenador cuántico ha sido diseñado y desarrollado en Europa, principalmente en España, y nos sitúa en una posición inimaginable hace tan solo cinco años: ya no importamos tecnología, sino que la creamos”. También ha señalado que es una iniciativa que “forma parte de un plan más amplio, tejido conjuntamente entre ministerios, Administraciones, universidad y Comisión Europea, y es lo que realmente hace que sea exitosa esta estrategia de país”. Además, ha resaltado que esta infraestructura “es de acceso abierto para la comunidad investigadora europea, es una soberanía que trasciende lo digital y marca la diferencia tejiendo alianzas: avanzar de forma conjunta nos hace ser más fuertes”.

Este nuevo ordenador alcanza así un hito para el ecosistema tecnológico español y europeo, y supone un paso más en el camino de la soberanía tecnológica europea que siguen EuroHPC y el BSC, alineándose con la estrategia de la Comisión Europea para reducir la dependencia de infraestructuras clave de terceros países.

Fuente: [Ministerio Ciencia, Innovación y Universidades](#)

Paquete de medidas de soberanía tecnológica para reforzar la autonomía y la resiliencia digital de Europea

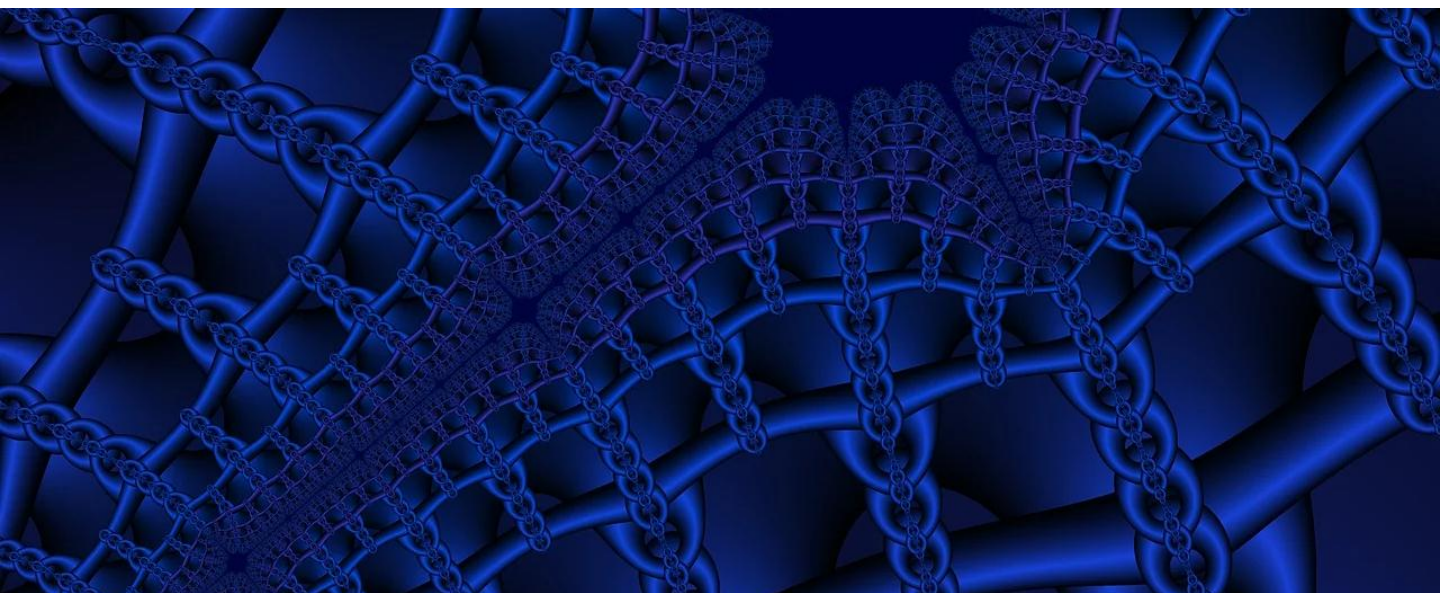
La Comisión Europea ha presentado el **Paquete de Soberanía Tecnológica Europea**, un conjunto de medidas para reforzar la capacidad de Europa en semiconductores, inteligencia artificial (IA), computación en la nube y código abierto.

El paquete incluye dos propuestas legislativas: la Ley de Chips 2.0 y la Ley de Desarrollo de la Nube y la IA , así como la Estrategia de Código Abierto y una Hoja de Ruta Estratégica para la Digitalización y la IA en el Sector Energético .

En conjunto, estas medidas respaldan la ambición de Europa de convertirse en un continente líder en inteligencia artificial, fortalecen su autonomía digital y contribuyen a construir un futuro digital más sostenible. Asimismo, ayudarán a ampliar las opciones en tecnologías clave para las empresas, los ciudadanos y las administraciones públicas de la UE.

Esta medida se produce en un momento en que Europa sigue dependiendo en gran medida de proveedores externos a la Unión Europea para tecnologías digitales esenciales y ante el fuerte aumento de la demanda de capacidad informática debido a la expansión de la IA. Su objetivo es reducir las dependencias estructurales y garantizar que Europa pueda desarrollar, implementar y proteger las tecnologías de las que dependen los europeos. Representa un cambio significativo en el enfoque de la UE hacia la tecnología.

Fuente: [Comisión Europea](#)



Apunte de interés

Informe de Tendencias en Robótica y Automatización

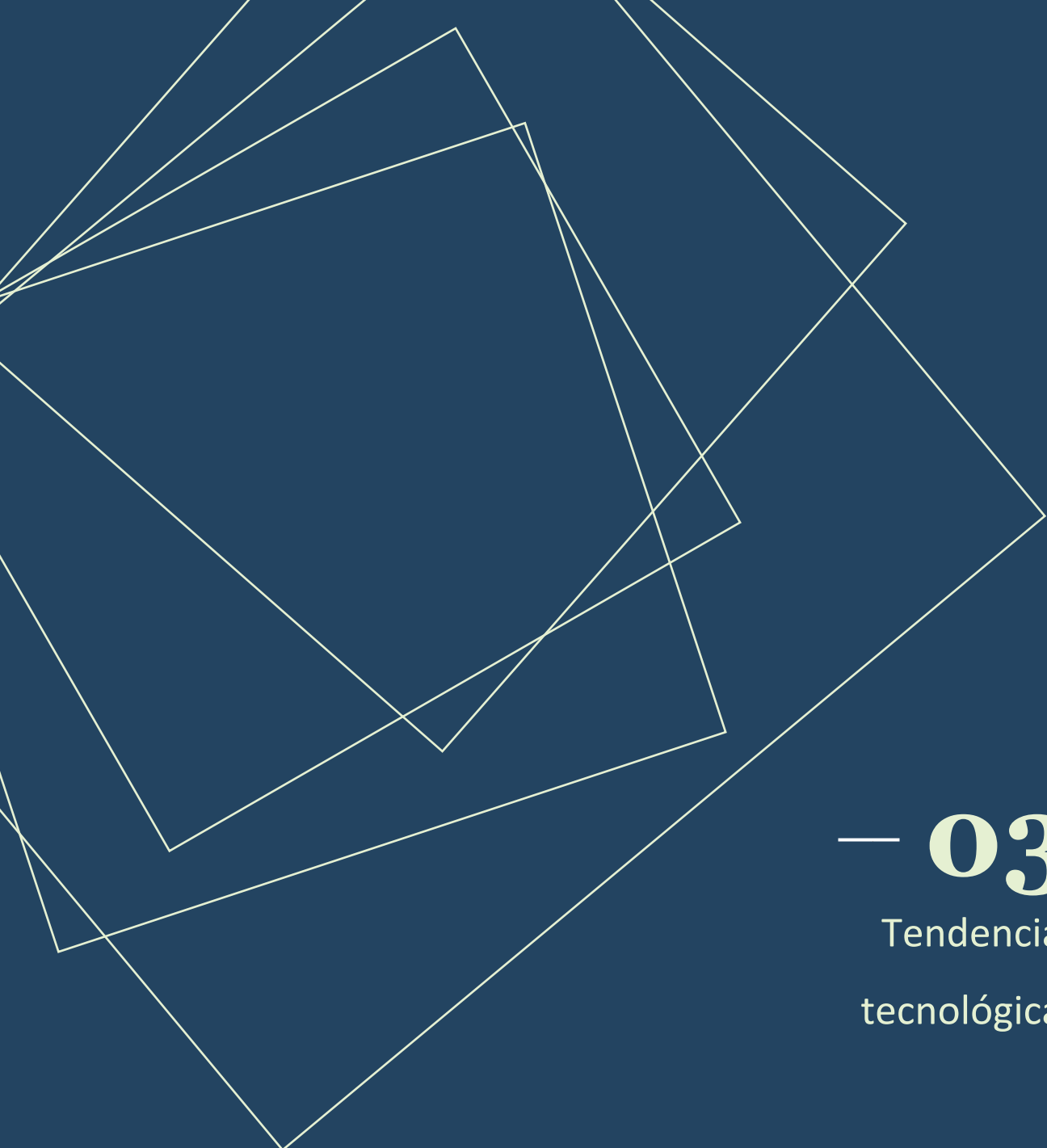
La **Asociación Española de Robótica y Automatización** ha presentado este mes de junio su primer [Informe de Tendencias en Robótica y Automatización](#), una publicación que aspira a convertirse en una referencia para entender la evolución reciente del sector y sus principales líneas de desarrollo. Ofrece una visión panorámica del estado de la robótica en España y en el entorno internacional, con especial atención a los ámbitos donde la automatización está teniendo un impacto más visible: industria, logística, salud, servicios avanzados y nuevas aplicaciones vinculadas a la inteligencia artificial.

El informe subraya que la robótica ya no puede entenderse solo como una herramienta de sustitución de tareas, sino como un factor estratégico para mejorar la productividad, la flexibilidad y la competitividad empresarial. Entre las tendencias más destacadas aparecen la integración con sistemas de IA, la colaboración entre personas y robots en entornos compartidos, el avance de la robótica móvil y autónoma, y la incorporación de soluciones más adaptables a procesos complejos. También se insiste en el papel de la automatización como palanca para afrontar retos como la escasez de mano de obra en determinados sectores, el envejecimiento poblacional y la necesidad de modernizar el tejido productivo.

Uno de los ejes del documento es la **creciente convergencia entre robótica, datos e inteligencia artificial**. Esta combinación permite desarrollar sistemas más precisos, capaces de aprender de su entorno, tomar decisiones en tiempo real y operar con mayor autonomía. El informe destaca que esta evolución está impulsando **nuevas oportunidades** para la industria española, especialmente en sectores que requieren altos niveles de eficiencia, trazabilidad y seguridad, como la automoción, la alimentación, la farmacia o la energía.



La publicación también pone el foco en los **desafíos pendientes**. Entre ellos figuran la necesidad de reforzar la formación técnica, aumentar la inversión en innovación, mejorar la transferencia tecnológica y facilitar la adopción de estas soluciones por parte de pequeñas y medianas empresas. En este sentido, la Asociación Española de Robótica y Automatización insiste en que el futuro del sector dependerá no solo del avance tecnológico, sino también de la capacidad para crear un ecosistema colaborativo que conecte empresas, centros de investigación, administraciones y talento especializado.



— 03

Tendencias tecnológicas

Nuevas patentes, prototipos y resultados de investigación.

Nº de Publicación: EP4749506A1
Fecha: 27/05/2026

Sistema y método para el despliegue automático de gemelos digitales

En la industria moderna (Industria 4.0 e Industria 5.0), la aplicación de Gemelos Digitales (GD) representa un nuevo enfoque para interactuar con los activos de fabricación (recursos, procesos y productos). En concreto, un GD puede intercambiar datos bidireccionalmente con su activo correspondiente. De este modo, los usuarios pueden beneficiarse de los GD para diversas aplicaciones avanzadas, como interactuar con el GD en lugar de estar físicamente cerca del activo real para su monitorización y control, o comprobar la viabilidad de una configuración industrial antes de su puesta en marcha.

El objeto de la presente [invención](#) es un método de despliegue para proporcionar gemelos digitales a los usuarios finales de forma rápida y automática.

La invención puede ser de interés en el ámbito industrial, en particular:

- para los trabajadores de una fábrica que pueden usar un teléfono o un equipo industrial con una interfaz hombre-máquina (HMI) para controlar y monitorear un robot o dispositivo industrial, simplemente escaneando un código QR (o una etiqueta NFC) disponible en el cuerpo o en la pantalla del robot.
- para los trabajadores que pueden obtener fácilmente información sobre varios equipos industriales para tener sus gemelos digitales asociados, y que luego pueden iniciar la puesta en marcha virtual y la comprobación de viabilidad, es decir, comprobar en un entorno virtual directamente desde un dispositivo de usuario si esos equipos pueden funcionar juntos antes de ponerlos en marcha físicamente.

Nº de Publicación: EP4756663A1
Fecha: 10/06/2026

Método y sistema para generar representaciones digitales de diagramas de ingeniería en un entorno informático

En un entorno de automatización, se utilizan uno o más diagramas de ingeniería para representar uno o más componentes físicos, las conexiones físicas entre dichos componentes en una instalación técnica y los valores de los parámetros correspondientes de los componentes y las conexiones físicas. En muchas plantas antiguas los operadores dependen de formatos no editables y por lo tanto no se almacenan componentes e interconexiones en un formato estructurado.

El objeto de la presente [invención](#) es proporcionar un método y un sistema para generar una representación digital de uno o más diagramas de ingeniería en un entorno informático.

Resultados de investigación

Innovaciones en la industria 4.0: avances en movilidad y manipulación en robótica

Harada K and Muthusamy R (2026) Editorial: Innovations in industry 4.0: advancing mobility and manipulation in robotics. Front. Robot. AI 13:1889141. doi: 10.3389/frobt.2026.1889141

La robótica se ha convertido en un componente fundamental de las tecnologías de la Industria 4.0, con aplicaciones en la fabricación, el almacenamiento, el comercio minorista, el transporte, la logística y diversos procesos industriales.

La integración de la robótica busca mejorar la eficiencia operativa, la flexibilidad y la productividad. Con la continua transformación digital, la creciente variedad de productos y la demanda de volumen por parte de los consumidores, así como la adopción de prácticas inteligentes de fabricación y logística, existe una necesidad imperiosa de robots autónomos en las tecnologías de la Industria 4.0. Estos robots deben navegar en entornos complejos, agarrar y manipular diversos objetos en espacios desordenados, utilizar herramientas finales eficaces, integrarse sin problemas en flujos de trabajo automatizados, aprender y generalizar habilidades, y colaborar de forma segura con los humanos. En los últimos tiempos, la manipulación móvil ha surgido como un aspecto crucial, que conecta la manipulación estática con la navegación y amplía el alcance de las tareas realizables en diversos entornos.

Este tema de [investigación](#) se dedica a explorar y mostrar las últimas innovaciones en movilidad, manipulación y manipulación móvil de robots, específicamente diseñadas para permitir la automatización flexible y colaborativa en diversos sectores industriales.

Interacción humano-robot en la hostelería sostenible: cómo el tipo de robot influye en las emociones del cliente, las percepciones ecológicas y la fidelización al servicio

Ng KM and Bayakhmetova A (2026) Human-robot interaction in sustainable hospitality: how robot type shapes customer emotions, green perceptions, and service loyalty. Front. Robot. AI 13:1845884. doi: 10.3389/frobt.2026.1845884

La creciente adopción de robots de servicio en la hostelería ha transformado la prestación de servicios y creado nuevas oportunidades para mejorar la eficiencia operativa y las prácticas de servicio sostenibles. Sin embargo, la investigación sobre cómo los diferentes tipos de robots de servicio influyen en las emociones de los clientes y cómo estas respuestas emocionales dan forma a las percepciones de sostenibilidad y al comportamiento posterior al consumo es limitada.

Este [estudio](#) proporciona información importante sobre cómo el tipo de robot influye en las emociones de los clientes, la sostenibilidad percibida y el comportamiento posterior al consumo en entornos de servicios hoteleros.

Proyecto AMALTEA

La necesidad de soluciones más inteligentes y adaptables se vuelve cada vez más urgente, ya que el sector de la construcción se enfrenta a exigencias de sostenibilidad, eficiencia y seguridad, al tiempo que lidia con el creciente consumo energético, el agotamiento de los recursos y la generación de residuos. En este contexto el proyecto [AMALTEA](#) tiene como objetivo integrar la robótica, la inteligencia artificial y los datos en el sector de la construcción para reducir el consumo de energía, el uso de recursos y los residuos en los edificios.

El proyecto se centra en mejorar la seguridad, aumentar la fiabilidad de los procesos y elevar la calidad del producto para responder a las necesidades cambiantes de los usuarios finales y apoyar los objetivos del Pacto Verde.

Cuatro entidades forman su consorcio coordinado por Tecnalía. AMALTEA se inició en enero de 2025 y tiene prevista su finalización en diciembre de 2028.



Proyecto 6GINTENSE

El proyecto [6GINTENSE](#) propone una nueva arquitectura de sistema para futuras redes inteligentes 6G, caracterizada por su alto rendimiento y eficiencia energética, que facilita aplicaciones avanzadas de internet.

Entre sus objetivos clave se encuentran impulsar una revolución industrial, fomentar la transformación digital y construir sociedades inteligentes con una mejor calidad de vida mediante funcionalidades como sistemas autónomos, comunicación háptica y atención médica inteligente.

El proyecto enfatiza nuevas estrategias para el diseño de infraestructuras de telecomunicaciones, promoviendo ecosistemas multiactor que incluyan a operadores de redes móviles y propietarios de recursos. El concepto de «red de redes» en 6G plantea desafíos de gestión, estos desafíos se abordan proponiendo un enfoque de orquestación inteligente *Gestión y Orquestación Distribuida Basada en la Intención (DIMO)* que simplifica los recursos computacionales y de comunicación mediante la abstracción y la federación.

Su consorcio está formado por 11 entidades. Iniciado en 2024 tiene previsto finalizar en diciembre de 2026.



Proyecto COLLECTiEF

[COLLECTiEF](#) desarrolla paquetes de software y hardware para una gestión de la demanda basada en inteligencia colectiva (CI-DSM) que aumenta la seguridad de los datos, la flexibilidad energética y la resiliencia climática de los edificios existentes, al tiempo que reduce el coste de instalación, la transferencia de datos y la potencia de cálculo.

COLLECTiEF Implementa, prueba y certifica un sistema de gestión energética interoperable y escalable, basado en inteligencia colectiva, un enfoque de inteligencia distribuida que lleva las soluciones de computación y sensores directamente al nivel del edificio (borde).

El sistema de COLLECTiEF facilita la conexión de equipos heredados a redes colaborativas entre edificios y sistemas energéticos urbanos. Ayuda a reducir los costes de instalación, minimizar la transferencia de datos y las exigencias computacionales, mejora la seguridad de los datos y aumenta la flexibilidad energética y la resiliencia climática.

14 entidades forman su consorcio, coordinados por Norges Teknisk-Naturvitenskapelige Universitet NTNU.



Proyecto AI4SWEG

[AI4SWEng](#) tiene como objetivo brindar soporte impulsado por IA a los desarrolladores de software para ayudar a reducir el estrés laboral más allá de los puntos débiles en los flujos de desarrollo de software ágiles y aumentar la productividad, lo que mejora la satisfacción laboral y la creatividad.

Desarrollará, entregará y validará, en 4 casos de uso, una plataforma que comprende un conjunto de herramientas, incluidas AISysDev y la herramienta de automatización de pruebas, para dar soporte al ciclo de vida del software de extremo a extremo para entregables funcionales y no funcionales.

15 entidades forman su consorcio, coordinados por AISEC OU.

El proyecto se inició en diciembre de 2024 y tiene previsto finalizar en noviembre de 2028.





— **04**
Agenda

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

¿Qué ha ocurrido?

VII Cybersecurity & Data Innovation Summit 2026

Madrid, 28/04/2026

Se celebró la séptima edición de [CyberSummit26](#) con el objetivo de difundir, presentar, descubrir y evaluar las soluciones y las tendencias de la industria. Un evento que solo estuvo abierto a profesionales de la industria de la ciberseguridad como punto de encuentro y divulgación tecnológica de referencia para el sector dicho sector.

Además de las ponencias se celebraron talleres prácticos y se contó con una zona expositiva para la presentación de productos y servicios tecnológicos.



GrindingHub 2026

Madrid, 5-8/05/2026

La [feria](#) internacional de tecnología de rectificado se desarrolló con más de 11.000 visitantes y 462 expositores que de 28 países que presentaron soluciones, productos y tecnologías que abarcan toda la cadena de procesos de rectificado: desde máquinas y herramientas de rectificado hasta automatización, tecnología de medición y software, así como digitalización, periféricos de proceso y servicios.

Un punto culminante de la feria fue el recién inaugurado Grinding Solution Forum, centrado en retos industriales específicos y soluciones prácticas. El foro abordó cuestiones clave del sector, como la estabilidad de los procesos, la calidad, la automatización, los datos, la digitalización, la IA, la rentabilidad y las perspectivas de futuro de la tecnología de rectificado



¿Qué ha ocurrido?

Congreso Industria 4.0

Zaragoza y online, 7/05/2026

Se celebró la sexta edición del [Congreso](#) Industria 4.0 evento reuniendo a líderes del sector para abordar la transformación digital, la automatización y la ciberseguridad empresarial en el panorama industrial español.

Además de las ponencias se presentaron casos de éxito y aplicaciones tecnológicas prácticas.



Conferencia sobre Inteligencia Artificial

Granada, 8-10/05/2026

La [Conferencia](#) sobre Inteligencia artificial (IEEE CAI), uno de los congresos internacionales de referencia en el ámbito de la inteligencia artificial estuvo centrada en las aplicaciones de la IA y sus principales sectores que impactan en las aplicaciones e innovaciones tecnológicas industriales.

A través de paneles específicos, mesas y sesiones de debate se dieron a conocer las últimas investigaciones y avances del sector, con más de 400 artículos científicos seleccionados. Y se desarrollaron diez workshops temáticos, entre los que destacan talleres dedicados a la IA en el sector Salud y la Ciberseguridad en entornos industriales.

Sin duda, ha resultado una oportunidad para que los directivos de las empresas más disruptivas y los científicos que están desarrollando los algoritmos del mañana compartieran diálogos de interés en torno a soluciones tecnológicas reales para la industria.



¿Qué ha ocurrido?



Q-Expo

Bilbao, 18-19/05/2026

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.

Más de 500 asistentes de 32 países se dieron cita entorno a el ecosistema cuántico global.

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).



VIII Aerospace & Defense Meetings-ADM 2026

Sevilla, 19-21/05/2026

Se celebró el [evento](#) de networking B2B líder en España para las industrias aeroespacial y de defensa, que conecta a fabricantes de equipos originales (OEM), proveedores de nivel 1 y 2, fabricantes y proveedores de servicios a través de reuniones individuales previamente programadas.

El programa se cerró con 21 conferencias y talleres centradas en innovación, aviación sostenible, espacio, defensa y ciberdefensa.

El talento, la digitalización y la seguridad tecnológica fueron otras de las temáticas desarrolladas.



CIBITEC26

Madrid, 3-4/06/2026

Bajo el lema “Reindustrialización, competitividad y autonomía estratégica”, se celebró la octava edición del [Congreso](#) Iberoamericano de Ingeniería y Tecnología reuniendo representantes de empresas industriales, instituciones públicas, centros tecnológicos y expertos.

El congreso abordará las claves para construir una industria fuerte, innovadora y sostenible, enfocándose en aspectos como la Ley de Industria y visión 2030, la electrificación de procesos productivos, la oportunidad del biometano y el hidrógeno, o la IA generativa y computación cuántica, entre otros.



II Encuentro Nacional de la Economía del Dato

Madrid y online, 24/06/2026

Esta segunda [jornada](#) técnica organizada por la Dirección General del Dato, a través del Centro de Referencia de Espacios de Datos (CRED) y dirigida a empresas, centros tecnológicos y entidades del sector tuvo como principal objetivo dar a conocer como el dato está impulsando nuevos modelos, servicios y oportunidades en diferentes sectores.



Próximamente



BNEW

Barcelona y online, 5-7/10/2026

Barcelona New Economy Week – BNEW es un evento B2B físico y digital que reúne eventos singulares de los sectores de Aviación, Industria Digital, Movilidad, Sostenibilidad, Talento, Salud y Experiencia. Todos ellos comparten un denominador común: Nueva Economía.

La propuesta de valor de este evento es su formato híbrido, con una parte presencial y otra digital, que se complementan y crean sinergias entre agentes de diferentes sectores desde cualquier parte del mundo.

Estos son los 3 aspectos fundamentales: sesiones de contenido en formato televisivo con speakers de primer nivel; Una potente plataforma digital propia para hacer networking y acceso a toda la innovación y últimas tendencias de cada sector.



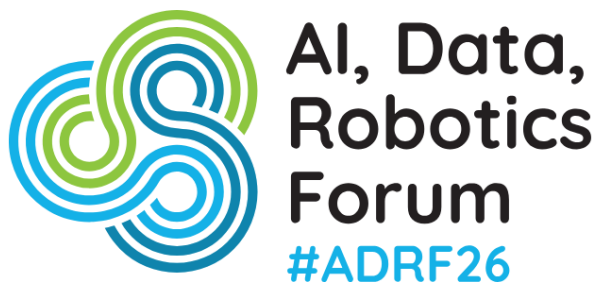
Foro de IA, Datos y Robótica

Oporto, 13-14/10/2026

Bajo el lema “Innovando en el futuro: IA, datos y robótica para una Europa resiliente, estratégicamente autónoma y globalmente competitiva se celebrará el [ADR26](#). Líderes de la industria, investigadores y responsables políticos que abordarán temas industriales y sociales cruciales.

Diversos talleres explorarán cómo las tecnologías ADR pueden fortalecer la infraestructura crítica, mejorar la ciberseguridad y respaldar los marcos regulatorios para garantizar la independencia tecnológica de Europa. Se debatirá y analizará cómo la convergencia de ADR puede impulsar la innovación, la competitividad y el crecimiento económico en las industrias europeas.

La transferencia y adopción de tecnología, centrada en las mejores prácticas para integrar soluciones ADR en la industria y el sector público, así como estrategias para reducir las barreras regulatorias y fomentar la colaboración entre el mundo académico y las empresas, serán otras temáticas presentes en el foro.



Próximamente

Congreso de IA Barcelona

Barcelona, 20-22/10/2026

El [Congreso](#) de IA presentará las tendencias y mejores prácticas de empresas pioneras, los nuevos desarrollos tecnológicos y sus aplicaciones, así como historias de éxito inspiradoras. El evento brindará la oportunidad de descubrir las últimas novedades tecnológicas basadas en IA y disfrutar de un entorno propicio para establecer contactos. Y, en todo momento, con el negocio como eje central.

AI Congress es el punto de encuentro para profesionales, proveedores y empresas que desarrollan proyectos en el campo de la IA, ofreciendo oportunidades de networking especializadas.

Está dirigido a profesionales de la tecnología, proveedores de tecnología, empresas usuarias, emprendedores y startups que trabajan en el contexto de la IA y la economía basada en datos.



Conferencia sobre Big Data en Europa 2026

Barcelona, 24-27/10/2026

La [Big Data Conference Europe](#) es un evento de cuatro días centrado en debates técnicos sobre Big Data, alta carga de trabajo, ciencia de datos, aprendizaje automático e inteligencia artificial.

La conferencia incluye una serie de talleres y sesiones que reúnen a desarrolladores, profesionales de TI y usuarios para compartir experiencias, analizar buenas prácticas, describir casos de uso y aplicaciones empresariales basadas en sus éxitos.



Convocatoria INNOGLOBAL 2026

La convocatoria **INNOGLOBAL 2026** se encuadra en el programa transversal sobre "Internacionalización" del PEICTI, que tiene como objetivo impulsar la financiación de proyectos de I+D de carácter internacional para potenciar la presencia de España en la I+D+I internacional, en particular su protagonismo en el Espacio Europeo de Investigación, facilitando la colaboración con socios extranjeros.

Se dirige específicamente, a pymes y empresas de mediana capitalización (con menos de 499 empleados) que desarrollen su actividad en alguna de las once comunidades y ciudades autónomas elegibles para los fondos FEDER.

Se financiará la actividad de empresas españolas que participen en consorcios internacionales de I+D en el marco de los programas de cooperación tecnológica internacional y la cooperación internacional para Big Science.

Los proyectos seleccionados deberán contar con un presupuesto mínimo de 175.000 euros y podrán recibir intensidades de ayuda de hasta el 80 % para pequeñas empresas.

Entre las principales modalidades de cooperación incluidas destacan:

- **Programas multilaterales y bilaterales:** participación en la iniciativa Eureka (proyectos de Red y Clústers), proyectos Iberoeka y el programa PRIMA, además de acuerdos bilaterales con países como Alemania, Japón, Corea, China, India, Marruecos o Brasil.
- **Proyectos unilaterales:** colaboración con socios de más de 50 países, elegibles bajo esta modalidad.
- **Big Science:** proyectos orientados a satisfacer necesidades tecnológicas de infraestructuras científicas internacionales como el CERN, ITER, ESRF, ESS o IFMIF-DONES, entre otros.

El plazo de presentación es del 17 de junio al 16 de julio de 2026, a las 12:00 horas del mediodía, hora peninsular.

Más información: [CDTI](#)

Convocatoria Horizon-JU-SNS-2026-FEM

La Empresa Común de Redes y Servicios Inteligentes (SNS JU) anuncia la apertura de su **séptima convocatoria** de propuestas, la segunda de 2026, centrada en el Módulo Front-End (FEM), una iniciativa estratégica orientada a reforzar la soberanía europea en el hardware 6G.

Con una dotación de 14 millones de euros por parte de la UE, esta convocatoria responde a la necesidad de desarrollar **microelectrónica** de diseño europeo para el FEM, un componente esencial de los sistemas avanzados de radio 6G. Su objetivo es reducir la dependencia de tecnologías de semiconductores ajenas a Europa que sustentan las redes de nueva generación.

La microelectrónica constituye la base de la 6G, ya que permite el funcionamiento de todos los elementos de la red, desde los dispositivos de usuario hasta las estaciones base y los aceleradores de inteligencia artificial. Aunque Europa ya cuenta con posiciones de liderazgo en ámbitos clave, la desalineación entre los plazos de desarrollo de los semiconductores y la duración habitual de los proyectos podría retrasar su preparación para la 6G. Esta convocatoria busca cerrar esa brecha mediante la colaboración entre los sectores de telecomunicaciones y microelectrónica, impulsando un ecosistema europeo capaz de reforzar la resiliencia de la cadena de suministro y alinearse con los objetivos de la Ley de Chips de la UE.

Además, esta iniciativa complementa la convocatoria de la Empresa Común de Chips, que aborda las tecnologías fundamentales del FEM, su integración, encapsulado y transferencia a las líneas piloto correspondientes. También incorpora las recomendaciones más recientes del Grupo de Política del Espectro Radioeléctrico y los avances en estandarización, al tiempo que apoya la estrategia europea de implantación de la inteligencia artificial y las capacidades de IA en el borde de las redes 6G.

Los proyectos seleccionados desarrollarán soluciones avanzadas para el FEM, contribuirán a la estandarización europea y ayudarán a consolidar un ecosistema continental de microelectrónica para telecomunicaciones. Integrarán tecnologías digitales, de radiofrecuencia y de encapsulado avanzado para crear front-ends 6G reconfigurables y multifrecuencia, con capacidad para gestionar espectro prioritario, mitigar interferencias y facilitar su futura transferencia a las líneas piloto de Chips JU. En conjunto, esta convocatoria refuerza la posición de Europa en la microelectrónica para 6G y apoya al mismo tiempo las transiciones digital y verde, reduciendo vulnerabilidades geopolíticas.

Plazo abierto hasta el 3 de septiembre de 2026 a las 17:00 CEST.

Más información: [Comisión Europea](#)

The top right corner of the page features a series of overlapping, thin, dark blue lines that form a complex, abstract geometric pattern. These lines create several irregular, overlapping shapes, resembling a stylized architectural or technical drawing. The lines are thin and consistent in color, set against a plain white background.

Just in Time

La Estrategia Nacional Deep Tech

Una oportunidad para acelerar la digitalización
de la industria española.

En abril de 2026, el Gobierno de España presentó la nueva **Estrategia Nacional Deep Tech**, un plan de país con el que prevé movilizar 8.000 millones de euros hasta 2030 para impulsar tecnologías avanzadas basadas en ciencia y con alto potencial de transformación económica e industrial. La iniciativa, coordinada por el Ministerio de Ciencia, Innovación y Universidades junto con el Ministerio para la Transformación Digital y de la Función Pública y otros once ministerios, aspira a convertir el conocimiento científico generado en España en liderazgo tecnológico, capacidad productiva y empleo de alto valor.

La estrategia pone el acento en **la transferencia real al mercado**, la industrialización de soluciones y la creación de un ecosistema capaz de escalar tecnologías complejas. Según lo anunciado, más del 70 % de los fondos se destinará directamente al tejido productivo para acompañar el crecimiento de proyectos, su paso a producción y su salida a mercados internacionales.

La Estrategia Deep Tech parte de una idea sencilla pero ambiciosa: España dispone de talento científico, capacidad investigadora y empresas innovadoras, pero necesita reforzar el puente entre laboratorio y mercado. Este es uno de los grandes desafíos de la innovación profunda, conocida como deep tech, que engloba tecnologías como la inteligencia artificial avanzada, la computación cuántica, la biotecnología, la robótica avanzada, los nuevos materiales, los semiconductores y las energías limpias.

Estas tecnologías no siguen la lógica de los desarrollos digitales más rápidos o de bajo coste. Requieren tiempo, inversión intensiva, equipos altamente cualificados y validación industrial antes de alcanzar el mercado. Por eso, uno de los objetivos centrales de la estrategia es evitar el llamado “valle de la muerte”, la fase en la que muchos proyectos prometedores se quedan sin financiación o sin capacidad de escalar.

La digitalización de la industria ya no depende solo de adoptar software, sensores o automatización básica, sino de integrar capacidades avanzadas que permitan fabricar mejor, diseñar con mayor precisión, optimizar procesos complejos y reducir costes y emisiones. En ese contexto, la deep tech se convierte en una palanca para una digitalización más profunda, estratégica y competitiva.

La estrategia se articula en **tres grandes ejes**:

- Reforzar las capacidades científicas y tecnológicas.
- Fortalecer el tejido empresarial desde la investigación hasta el mercado.
- Construir un ecosistema coordinado entre administraciones, centros de investigación y empresas.

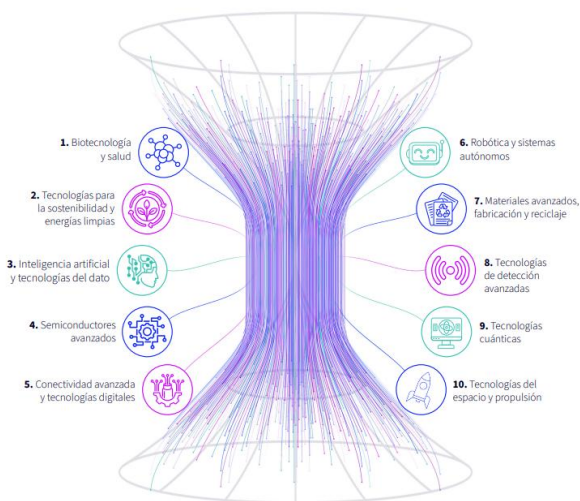


Esta estructura tiene una lectura muy concreta para el mundo industrial, no basta con generar conocimiento, hace falta crear condiciones para que ese conocimiento se transforme en productos, procesos y cadenas de valor.

El **primer eje**, centrado en capacidades científicas y tecnológicas, es clave para acelerar la base digital de la industria. Sin una infraestructura científica sólida, las empresas tienen más dificultades para incorporar tecnologías de frontera, probar soluciones avanzadas o desarrollar gemelos digitales, sistemas autónomos o materiales inteligentes.

El **segundo eje**, orientado al tejido empresarial, apunta a un reto habitual en España: el escalado. Muchas innovaciones nacen en universidades o centros de investigación, pero necesitan acompañamiento, inversión y capacidades industriales para convertirse en soluciones comerciales.

El **tercer eje**, la coordinación del ecosistema, también es decisivo. La digitalización industrial no avanza solo por la acción de una empresa aislada; necesita conexión entre políticas públicas, centros tecnológicos, universidades, startups, grandes compañías y pymes. Esa coordinación facilita entornos de prueba, compras públicas innovadoras, transferencia tecnológica y colaboración intersectorial.



Uno de los aspectos más interesantes de la estrategia es la selección de **ámbitos prioritarios**.

Biotecnología y salud; Tecnologías para la sostenibilidad y energías limpias; Inteligencia artificial y tecnologías del dato; Semiconductores avanzados; Conectividad avanzada y tecnologías digitales; Robótica y sistemas autónomos; Materiales avanzados, fabricación y reciclaje; Tecnologías de detección avanzadas; Tecnologías cuánticas y Tecnologías del espacio y propulsión.

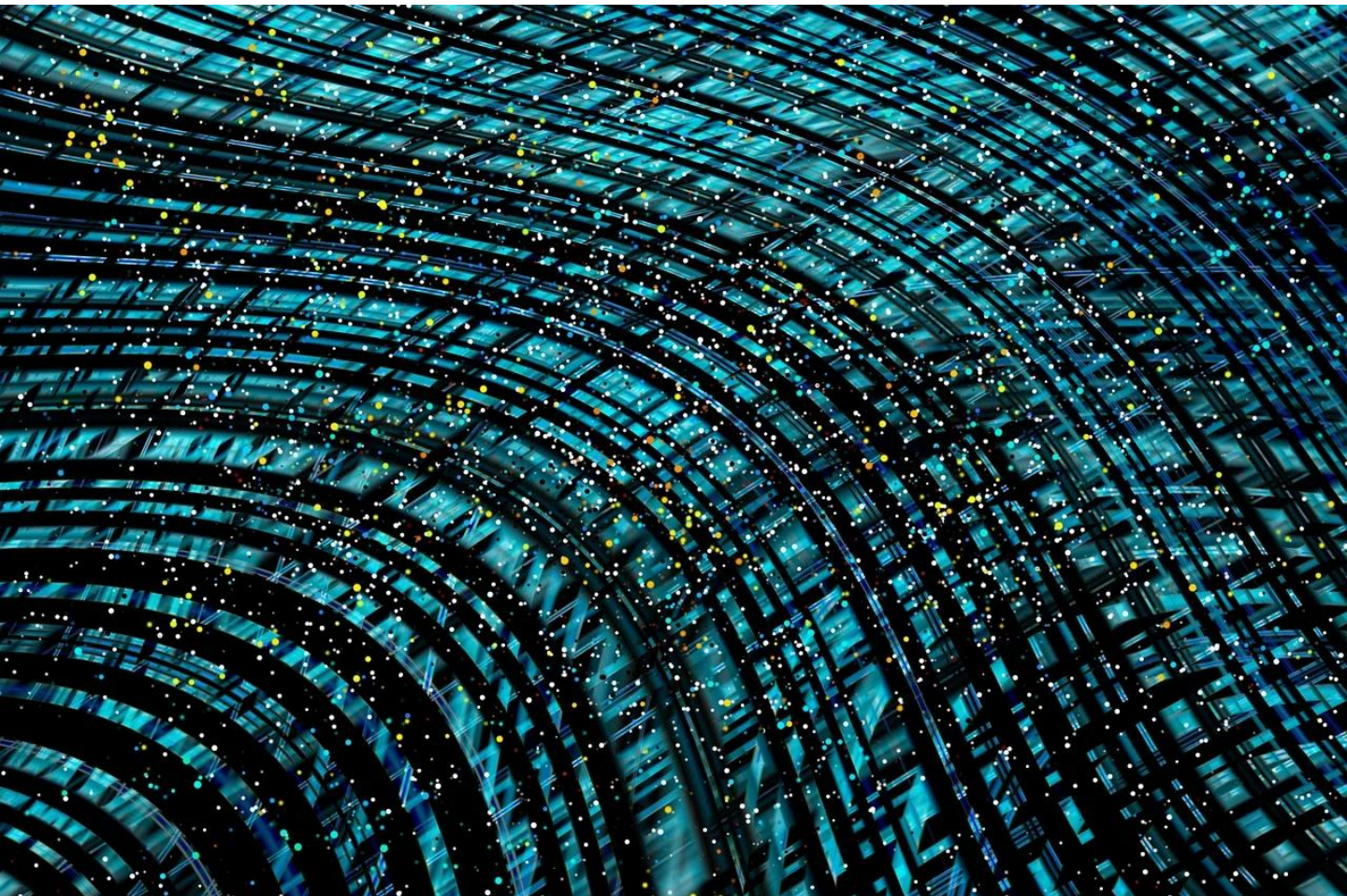
Figura 4: Áreas científico-tecnológicas prioritarias. Fuente: Estrategia Nacional Deep Tech.

En la industria manufacturera, la inteligencia artificial puede mejorar el control de calidad, el mantenimiento predictivo y la planificación de la producción. La robótica avanzada permite automatizar tareas complejas y trabajar en entornos peligrosos o de alta precisión. Los semiconductores son esenciales para la sensorización, el control industrial y la conectividad de equipos y sistemas. Por su parte, la computación cuántica abre perspectivas para optimizar procesos de gran complejidad, como la simulación de materiales o la gestión avanzada de redes.

La biotecnología y las energías limpias también tienen una fuerte conexión con la digitalización industrial. En sectores como química, alimentación, farmacia o energía, la integración de datos, modelos avanzados y tecnologías de laboratorio automatizado puede acelerar la innovación, mejorar la trazabilidad y apoyar la transición hacia modelos productivos más sostenibles. La industria, en este sentido, deja de ser un espacio exclusivamente físico para convertirse en un entorno donde convergen ciencia, datos, software y fabricación.

La estrategia presentada, sin duda, mejorará el acceso a tecnologías de alto impacto que hoy suelen desarrollarse fuera del país o a gran distancia del tejido productivo local. En segundo lugar, favorecerá la creación de más proyectos de colaboración entre empresas, universidades y centros tecnológicos, algo imprescindible para innovar en sectores intensivos en capital y conocimiento. Además, la estrategia puede contribuir a reforzar la **soberanía tecnológica**, un concepto cada vez más presente en Europa. Disponer de capacidades propias en semiconductores, IA, ciberseguridad o energía avanzada no es solo una cuestión de competitividad, sino también de resiliencia industrial y autonomía estratégica.

La Estrategia Nacional Deep Tech no debe entenderse únicamente como un plan de innovación, sino como una política industrial de nueva generación. Su apuesta por la ciencia aplicada, la transferencia tecnológica y la industrialización conecta directamente con los retos de la digitalización: productividad, sostenibilidad, escalabilidad y competitividad internacional.



719 millones de euros para desarrollar una Gigafactoría de IA

Las **gigafactorías de IA** son infraestructuras tecnológicas e industriales de gran escala, concebidas para alojar cientos de miles de GPU y proporcionar la enorme capacidad de cálculo necesaria para entrenar y operar grandes modelos de inteligencia artificial, como los grandes modelos de lenguaje o los sistemas avanzados de visión artificial. A diferencia de los centros de datos convencionales, orientados a servicios cloud generalistas y almacenamiento, estas instalaciones se diseñan específicamente para cargas de trabajo intensivas en cómputo, convirtiéndose en piezas críticas de la nueva economía de la IA. En un contexto global dominado por hiperescaladores estadounidenses y un ecosistema muy concentrado en China, la apuesta europea —y española— por este tipo de infraestructuras busca reducir la dependencia externa y avanzar hacia una mayor **soberanía tecnológica**.

El pasado martes el Consejo de Ministros autorizó una **inversión de 719 millones de euros** del Ministerio para la Transformación Digital y de la Función Pública, canalizada a través de la Sociedad Española para la Transformación Tecnológica (SETT), para desarrollar una Gigafactoría avanzada de Inteligencia Artificial.

Esta operación se articula mediante la facilidad Next Tech, con fondos del Plan de Recuperación, Transformación y Resiliencia, y permitirá a la SETT incorporarse al accionariado del consorcio público-privado que desarrollará la infraestructura y optará a la convocatoria que lanzará próximamente la Comisión Europea. La propuesta española se presentará como una candidatura multisede, con ubicaciones en Móra la Nova (Tarragona) y San Fernando de Henares (Madrid), reforzando el carácter estratégico y territorial del proyecto.

La futura gigafactoría tendrá un enfoque claro en sostenibilidad y eficiencia energética, alineado con los objetivos de descarbonización y con la estrategia europea de infraestructuras digitales verdes. La nueva instalación se integrará en el ecosistema ya existente de capacidades de cómputo avanzado, en el que España cuenta con dos AI Factories vinculadas a la red EuroHPC: el Barcelona Supercomputing Center y el Centro de Supercomputación de Galicia (CESGA), ambos financiados con fondos públicos. Esta red de infraestructuras permitirá a startups, pymes, grandes empresas, universidades, centros de investigación y administraciones públicas entrenar, probar y desplegar modelos de IA avanzados sin depender en exclusiva de proveedores extranjeros, abriendo la puerta a nuevos servicios, aplicaciones y proyectos científico-tecnológicos.

La operación se estructurará a través de un consorcio público-privado cuya composición se está ultimando, con el objetivo de combinar liderazgo institucional, músculo industrial, financiación y capacidades tecnológicas en una misma iniciativa. La participación de la SETT garantiza la dirección estratégica pública y la coordinación de inversiones, en línea con su papel como instrumento para acelerar proyectos tecnológicos de alto impacto. Más allá de la dimensión tecnológica, el Ejecutivo destaca el potencial de arrastre industrial y de empleo cualificado que supone la gigafactoría, tanto en las regiones que albergarán las sedes como en el conjunto de la economía española, posicionando al país en la primera línea europea de la inteligencia artificial y reforzando su autonomía en infraestructuras de cómputo de alto rendimiento.

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



Esta publicación está bajo licencia *Creative Commons* Reconocimiento, No comercial, Compartir igual, (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





Boletines

DE

Vigilancia
Tecnológica

CEPI Centro de
Estrategia y
Prospectiva
Industrial