CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Informe de tendencias y reglamento

Abril 2026

Financiado pola Unión Europea
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Edita: Xunta de Galicia

Agencia para la Modernización Tecnológica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Año: 2026

Índice

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

1 Introducción

Este informe forma parte del **Observatorio de Ciberseguridad Industrial**. Se integra en el marco del **Laboratorio y Centro Demostrador de Ciberseguridad en Productos con Elementos Digitales y Ciberseguridad Industrial**, perteneciente a la **Red de Laboratorios y Centros Demostradores de Ciberseguridad de la Xunta de Galicia**. La iniciativa forma parte del **Programa de Redes Territoriales de Especialización Tecnológica (RETECH)**, impulsado por la Secretaría de Estado de Digitalización e Inteligencia Artificial.

El proyecto está financiado por la **Unión Europea a través de NextGenerationEU** en el **marco del Plan de Recuperación, Transformación y Resiliencia (PRTR)**, y se desarrolla conforme a los requisitos establecidos por el **Instituto Nacional de Ciberseguridad (INCIBE).**

El Observatorio constituye un **eje estratégico dentro de esta estructura transversal, orientado al análisis de tendencias, amenazas y necesidades del ecosistema de ciberseguridad industrial gallego**, así como a la dinamización y fortalecimiento del tejido empresarial y tecnológico de nuestra tierra.

--

En el actual escenario de transformación digital, los sistemas industriales —incluyendo entornos **ICS/OT (@Systems / Operational Technology)**— están experimentando una progresiva convergencia con infraestructuras digitales, redes corporativas y servicios conectados. Esta evolución introduce **nuevas oportunidades de eficiencia, automatización y optimización operativa, pero también amplía la superficie de exposición** a riesgos cibernéticos, dependencias tecnológicas e interacciones complejas entre sistemas físicos y digitales.

En este contexto, la capacidad de **anticipar tendencias tecnológicas, reglamentarias y de mercado** se convierte en un elemento clave para reforzar la resiliencia de las organizaciones y de las infraestructuras críticas. La identificación temprana de cambios en el ecosistema tecnológico permite comprender mejor **cómo pueden evolucionar las amenazas, que nuevos requisitos de gobernanza o cumplimiento pueden subsanar y que adaptaciones estratégicas pueden resultar necesarias en el medio plazo**.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

Este informe tiene como finalidad ofrecer una **visión estructurada de las principales tendencias con potencial impacto en la ciberseguridad industrial**, así como una aproximación inicial a los **principales vectores reglamentarios que podrán influir en la evolución del sector en los próximos años**. El análisis es de aplicación directa para el **ecosistema industrial e institucional gallego**, teniendo en cuenta la creciente importancia de la protección de los sistemas que soportan procesos productivos, servicios esenciales e infraestructuras críticas.

La diferencia de otras publicaciones centradas exclusivamente en el análisis de amenazas o incidentes, este documento adopta una aproximación de **vigilancia estratégica**, orientada a identificar señales de cambio que puedan condicionar la seguridad y la resiliencia de los sistemas industriales en el horizonte próximo. El informe combina así el análisis de **tendencias tecnológicas emergentes** con una aproximación sintética al **contexto normativo europeo y nacional**.

El documento se estructura en dos partes principales. En primer lugar, se presenta un análisis de las **tendencias con potencial impacto en los entornos ICS/OT**, clasificadas según su grado de prioridad u horizonte de atención. En segundo lugar, se introduce una **visión inicial del contexto normativo relevante para ciberseguridad industrial**, identificando los principales marcos y evoluciones que deberán ser monitorizadas en los próximos años.

Con esta aproximación, el informe pretende contribuir a **mejorar la capacidad de antelación y preparación de las organizaciones gallegas**, facilitando una lectura contextualizada de las transformaciones tecnológicas y normativas que están redefiniendo el panorama de la **ciberseguridad industrial**.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

2 Resumen ejecutivo

La **ciberseguridad industrial** está experimentando una transformación profunda como consecuencia de la convergencia entre **digitalización, automatización, conectividad y presión reglamentaria**. Los entornos **ICS/OT**, tradicionalmente más estables, cerrados y orientados a la continuidad operativa, se están integrando progresivamente con infraestructuras digitales, plataformas cloud, servicios remotos, herramientas basadas en datos y sistemas de inteligencia artificial. Esta evolución aporta oportunidades relevantes en términos de eficiencia, visibilidad y optimización, pero también introduce nuevas **superficies de exposición, dependencias tecnológicas y riesgos ciberfísicos**.

En este contexto, el presente informe ofrece una lectura estructurada de dos dimensiones que condicionarán de forma creciente la resiliencia de las organizaciones industriales y de las administraciones con activos críticos en Galicia:

- por una banda, las **tendencias tecnológicas y organizativas con potencial impacto en ICS/OT**;
- por otra, los **principales vectores reglamentarios y de estandarización** que deberán ser monitorizados en los próximos años.

En el plano tecnológico, el informe identifica un conjunto de tendencias, que ya están influyendo —o lo harán a corto y medio plazo— en la arquitectura, operación y gobernanza de la ciberseguridad industrial. Entre las de mayor prioridad destacan la **convergencia IT/OT**, la **conectividad remota en entornos industriales**, la expansión de una **fuerza laboral conectada y aumentada**, **la integración transversal de la inteligencia artificial**, el uso creciente de **agentes de IA**, la necesidad de **gestión de vulnerabilidades orientada a riesgo en OT,** el refuerzo de la **segmentación de redes industriales**, la atención a la **cadena de suministro tecnológico**, la evolución hacia **arquitecturas OT defendibles,** la **"cloudización",** los **sistemas digitales inmunes,** la importancia creciente de la **cripto-agilidad** ante futuras transiciones criptográficas, o la **soberanía tecnológica** en un mundo cada vez más inestable.

Junto a estas tendencias de atención inmediata, el informe recoge otras de **materialidad moderada**, como la **computación confidencial**, el **cifrado homomórfico**, **la seguridad frente a la desinformación**, **la geopatriación**, **la simulación inteligente**,

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

la computación espacial o la progresiva incorporación de **IA encarnada e IA física** a procesos industriales y entornos automatizados.

A ellas se suman tendencias de **vigilancia estratégica**, entre las que figuran la posible evolución hacia la **inteligencia artificial general (AGI)**, la **meta-computación**, los **comerciantes máquina**, el **aprovisionamiento autónomo**, los **compañeros cibernéticos**, la **descarga cognitiva**, el **conocimiento fluido**, **las interfaces cerebro-máquina** o la **transformación del modelo tradicional de experiencia de usuario**.

Todas las anteriores e incluso más, hasta llegar a una totalidad de **45 tendencias extraídas principalmente de fuentes como informes de Gartner (de tecnologías emergentes y tendencias estratégicas), o el propio Informe de Riesgos Tecnológicos desde Observatorio**, se presentan en fichas homogéneas y concisas con cada uno descripción, relevancia y consideraciones adicionales.

El conjunto de estas tendencias evidencia que la ciberseguridad industrial ya no puede analizarse únicamente desde la lógica clásica de la protección perimetral. La realidad actual exige una aproximación más amplia, en la que la exposición viene determinada también por la **interoperabilidad entre sistemas**, por la dependencia de **terceros y proveedores**, por la creciente presencia de **software y servicios conectados**, por la automatización de procesos cognitivos y por la necesidad de mantener la **seguridad funcional y la continuidad operativa** en entornos con impacto físico.

En el plano reglamentario, el informe señala que la ciberseguridad industrial entra en una nueva **fase marcada por la consolidación del marco europeo de ciberseguridad y resiliencia**. En este escenario sobresalen tres piezas fundamentales: la **Directiva NIS2**, que refuerza las obligaciones de gestión de riesgos, reporte y gobernanza; la **Directiva CER**, que amplía el foco hacia la resiliencia integral de las entidades críticas; **y el Cyber Resilience Act (CRA)**, que introduce requisitos obligatorios de seguridad para productos con elementos digitales y tendrá un impacto relevante sobre la compra, integración y operación de tecnología en los entornos industriales.

A este marco europeo se suma su **aterrizaje práctico en el ordenamiento español**, especialmente a través de los procesos de transposición de NIS2 y CER, así como la evolución de otras iniciativas que afectarán a la gobernanza, a la evidencia de cumplimiento y a la relación con proveedores. El informe destaca también tres frentes adicionales que deberán ser seguidas con atención: el avance de exigencias en torno a la **cadena de suministro y el SBOM** (*Software Bill of Materials o* Listado de Materiales de Software), la progresiva incorporación de la **criptografía post-cuántica** y de la **cripto-**

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

agilidad a las hojas de ruta europeas, y la creciente relevancia de las **certificaciones europeas de ciberseguridad, los estándares armonizados y los requisitos de seguridad por diseño**.

Para Galicia, la conclusión principal es que el impacto de estas transformaciones no será sólo tecnológico ni sólo normativo: será también **operativo, organizativo y estratégico**. Las organizaciones tendrán que reforzar su capacidad para **inventariar activos**, **comprender dependencias, mejorar la gobernanza TI-OT, controlar el acceso de terceros, gestionar vulnerabilidades con enfoque realista, proteger cadenas de suministro y generar evidencias de cumplimiento y madurez**. Al mismo tiempo, deberán **integrar criterios de antelación tecnológica que les permitan evaluar que innovaciones son realmente prioritarias, cuáles deben incorporarse de manera planificada y cuáles conviene mantener bajo observación.**

Este análisis muestra que la ciberseguridad industrial está evolucionando hacia un escenario en el que **tecnología, regulación, resiliencia operativa y gobernanza del riesgo** aparecen cada vez más interrelacionadas. La capacidad de Galicia para adaptarse a este nuevo contexto dependerá, en buena medida, de combinar **vigilancia estratégica, planificación técnica y criterio de priorización**, tanto en el ámbito público como en el privado.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

3 Tendencias con impacto en ICS/OT

3.1 Introducción

3.1.1 Objetivo

Esta sección tiene como finalidad **identificar y priorizar tendencias** —tecnológicas y también de naturaleza organizativa—, geopolítica o de mercado— que puedan **afectar a la ciberseguridad y a la resiliencia operativa** de los entornos **ICS/OT** (Industrial Control Systems / Operational Technology) del **tejido productivo gallego** y de las **administraciones públicas** con activos y servicios críticos.

El foco no es describir "innovación" por sí misma, **sino traducir señales de cambio** en:

- **Implicaciones de riesgo** (nuevas superficies de ataque, dependencias, modos de fallo, impactos ciberfísicos).
- **Implicaciones operativas** (disponibilidad, seguridad funcional, continuidad, mantenimiento, teleoperación).
- **Implicaciones de gobernanza** (controles necesarios, evidencias, roles y responsabilidades, coordinación TI–OT).

La lectura está orientada a la práctica: cada tendencia se recoge con **descripción ejecutiva**, **por qué importa en OT/ICS**, y una **prioridad de atención** para apoyar la toma de decisiones.

3.1.2 Fuentes de información

Para garantizar una visión equilibrada entre **prospectiva global y materialidad local**, este apartado integra información de tres piezas documentales principales.

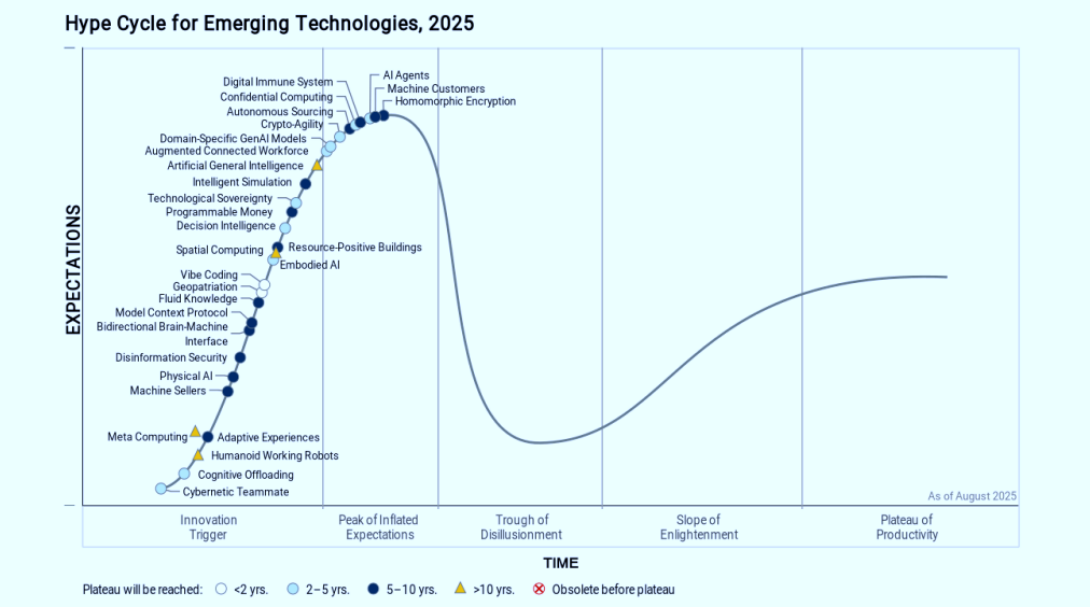
En primer lugar, o **Hype Cycle for Emerging Technologies (2025)** [1]. Documento de referencia de Gartner, empresa líder mundial en investigación y asesoramiento tecnológico, proporcionando análisis objetivos, herramientas prácticas y consultoría para mejorar el desempeño empresarial. **Condensa y clasifica tecnologías emergentes** (en un conjunto reducido de "must-know" frente a un universo mucho mayor) y las organiza según su **grado de madurez y horizonte de adopción**. Su utilidad para este informe es triple:

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

- Actúa como **radar estructurado** para identificar tecnologías con potencial transformador.
- Permite situar cada tecnología en un **horizonte temporal de adopción**, útil para anticipación.
- Incluye líneas y temas especialmente relevantes para **resiliencia y seguridad** (p.ej. fragilidad tecnológica, criptografía, protección de datos, sistemas autónomos).

Adicionalmente, el **Gartner – Signature Series: Top Strategic Predictions for 2026 and Beyond** [2]. Esta es una pieza de prospectiva estratégica sintetizada que recoge **10 predicciones de alto nivel** sobre cómo evolucionarán las organizaciones, la tecnología y el comportamiento socioeconómico en el corto y medio plazo (2026–2030). Su contribución a esta sección se trae en:

- Identificar **fuerzas motrices no estrictamente tecnológicas** (talento, gobernanza, automatización de decisiones, plataformas, cambios en la economía digital...).
- Aportar un marco de **impacto estratégico**, especialmente en ámbitos como **agentes de IA**, **automatización**, **compras a terceros**, y **gobernanza**.
- Servir como "puente" entre tecnología y **decisión ejecutiva** (riesgos, prioridades y accountability).



Gartner Hype Cycle. Fuente: Gartner (2025)

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Y como no podría ser de otro modo, el propio **Observatorio de Ciberseguridad Industrial (AMTEGA), mediante su *Informe de riesgos tecnológicos*** [3]**.** Trabajo propio del Observatorio que ofrece una visión aplicada a entornos industriales e infraestructuras críticas, incorporando:

- Una lectura del **riesgo ciberfísico** en OT/ICS (impacto económico, continuidad y seguridad funcional).
- Una identificación de **riesgos y vectores de preocupación** en Galicia en los diferentes sectores de actividad (energía, agua, automoción, alimentación, logística, manufactura, etc.), no estrictamente en el ámbito tecnológico.
- Una orientación práctica hacia medidas de **arquitectura OT**, **conectividad segura**, **gobierno** y **resiliencia**.

Esta fuente es especialmente importante porque actúa como **filtro de realidad**: permite priorizar tendencias en función de su encaje con las restricciones y dinámicas reales de operación OT y los niveles de riesgo general.

Adicionalmente, se incorporará alguna tendencia adicional no referida explícitamente pero afín, o que claramente parece que experimentará el sector industrial a corto, medio o largo plazo, según el caso.

3.1.3 Criterios de selección de tendencias

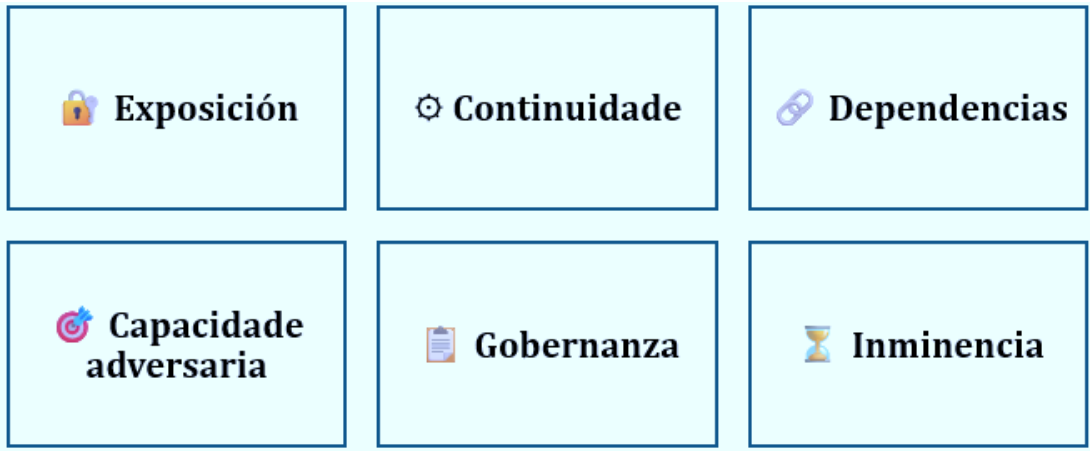
Con el objetivo de **no descartar tendencias relacionadas** (dado el carácter ejecutivo del informe y el número limitado de fuerzas), la metodología empleada no elimina elementos a priori, sino que **ordena por prioridad de atención**.

Para ello se han aplicado los siguientes **criterios de inclusión**. Una tendencia se considera "relevante" cuando contribuye de forma clara a **al menos dos de estos** criterios (aunque puede incluirse con menor prioridad cuando sólo cumple uno, se aporta contexto estratégico):

1. **Impacto en la superficie de ataque OT/ICS**: incrementa exposición, interconexión, acceso remoto, IIoT, integración con cloud/edge o dependencia de identidades.
2. **Impacto en la continuidad y en la seguridad funcional (safety)**: puede afectar disponibilidad, operación segura, tolerancia a fallos, recuperación y respuesta a incidentes con consecuencias físicas.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

3. **Incremento de complejidad y dependencia de terceros**: introduce nuevas capas (software, plataformas, proveedores, integradores), cadena de suministro y riesgos sistémicos.
4. **Efecto multiplicador en el adversario**: facilita automatización, escalabilidad, evasión, fraude o aceleración de cadenas de intrusión.
5. **Implicaciones de gobernanza y cumplimiento**: demanda nuevos controles, procedimientos, evidencias auditables, roles y coordinación TI–OT.
6. **Proximidad temporal (inminencia)**: tendencia ya observable o con adopción probable en el horizonte 2–5 años en sectores industriales.



Criterios de selección de tendencias. Fuente: elaboración propia (2026)

Adicionalmente, a fin de mantener la sección **operativa y accionable**, cada tendencia se clasifica en una de las siguientes categorías de prioridad:

Prioridad	Denominación	Definición ejecutiva	Cumplimiento de criterios
1	**Atención inmediata / Alta materialidad**	Tendencias con **alto impacto potencial en OT/ICS** y/o **alta inminencia**, que suelen implicar cambios en **arquitectura, operación o gobernanza**.	Cumplen **3 o más criterios**, incluyendo habitualmente los criterios **1 (Exposición) y 2 (Continuidad / safety)**.
2	**Atención programada /**	Tendencias con **impacto plausible**, pero más dependientes del sector, del	Cumplen **2–3 criterios**.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

	Materialidad moderada	ritmo de modernización o con un horizonte más medio. Se recomienda incorporarlas a la **planificación, evaluación de riesgo y pilotos controlados**.	
3	**Vigilancia estratégica / Horizonte largo**	Tendencias con relevancia principalmente **contextual o indirecta** para OT/ICS, o con un horizonte más largo y mayor incertidumbre. Deben mantenerse bajo **observación**, sin desplazar prioridades operativas.	Cumplen **1–2 criterios** o presentan impacto de menor intensidad.

Criterios de priorización de tendencias. Fuente: elaboración propia (2026)

A continuación, se describirán las tendencias una a una, agrupadas por estas tres prioridades.

3.2 Tendencias

Con el objetivo de facilitar un análisis claro y homogéneo de las principales tendencias que afectan a la ciberseguridad industrial, cada una de las tendencias incluidas en este informe se presentan mediante una ficha estructurada en tres apartados.

- En primer lugar, la **Descripción de la tendencia** ofrece una explicación sintética del fenómeno tecnológico, organizativo o estratégico identificado, contextualizando su aparición y los factores que impulsan su evolución.
- A continuación, el apartado **Relevancia e implicaciones** analiza el impacto potencial de la tendencia en el ámbito de la ciberseguridad industrial, considerando especialmente el contexto del tejido productivo y de las infraestructuras críticas se aplica.
- Finalmente, en **Consideraciones adicionales** se recogen elementos complementarios que permiten ampliar la comprensión de la tendencia, tales como evidencias, evolución observada, posibles riesgos asociados u oportunidades y medidas de mitigación cuando proceda.

Esta estructura pretende ofrecer una visión equilibrada entre explicación conceptual, interpretación estratégica y elementos prácticos de apoyo a la toma de decisiones.

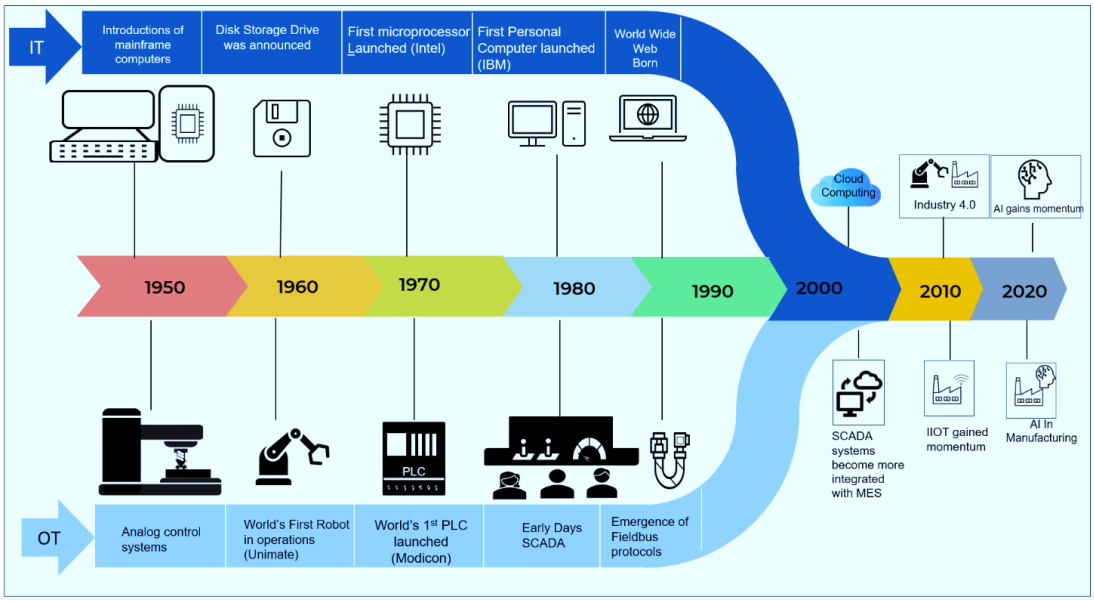
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

3.2.1 De atención inmediata (prioridad #1)

3.2.1.1 Convergencia acelerada IT/OT

Descripción de la tendencia

La **convergencia entre tecnologías de la información (IT) y tecnologías operacionales (OT)** constituye una de las transformaciones estructurales más relevantes de la industria moderna. La progresiva **digitalización de los procesos industriales**, la adopción de sistemas de **monitorización avanzada**, la integración con **plataformas de análisis de datos** y la necesidad de operaciones más eficientes están impulsando la interconexión entre sistemas tradicionalmente aislados. Como resultado, **redes industriales, sistemas de control y plataformas corporativas comparten cada vez más infraestructuras, protocolos y flujos de datos**, generando arquitecturas híbridas en las que los límites entre IT y OT son progresivamente más difusos.



Convergencia IT-OT. Fuente: Inductive Automation (2025)

Relevancia e implicaciones

Para el **tejido industrial gallego**, caracterizado por una fuerte presencia de sectores como **la automoción, la alimentación, energía o la logística portuaria**, esta convergencia supone una oportunidad para **mejorar la eficiencia operativa, la trazabilidad y la capacidad de análisis de los procesos productivos**. Con todo, también introduce **nuevos retos de ciberseguridad**, ya que la integración de sistemas OT con entornos IT ha expuestos a Internet **amplía la superficie de ataque** y facilita

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

posibles **vectores de intrusión hacia infraestructuras industriales críticas**. La protección de estas arquitecturas convergentes requiere enfoques específicos que combinen **prácticas de seguridad IT tradicionales** con medidas adaptadas a las **particularidades de los sistemas industriales**.

Consideraciones adicionales

Diversos estudios e informes especializados señalan que la **convergencia IT/OT es uno de los principales factores que están redefiniendo el panorama de riesgo en los entornos industriales modernos** [4]. La interdependencia creciente entre **sistemas corporativos y sistemas de control** hace que incidentes inicialmente limitados al ámbito IT puedan tener **repercusiones operacionales sobre procesos físicos**, especialmente en sectores industriales altamente automatizados. Al mismo tiempo, esta tendencia impulsa la adopción de nuevos modelos de seguridad basados en **visibilidad de activos industriales, segmentación de redes OT, monitorización específica de protocolos industriales e integración de la ciberseguridad en el diseño de las arquitecturas industriales**. La correcta gestión de esta convergencia se convertirá previsiblemente en un **elemento clave para la resiliencia de las organizaciones industriales en los próximos años**.

3.2.1.2 Conectividad segura en OT y acceso remoto (modernización)

Descripción de la tendencia

La modernización de las infraestructuras industriales está impulsar una adopción creciente de **mecanismos de conectividad remota en entornos OT**, destinados a facilitar operaciones como **el mantenimiento remoto, la supervisión centralizada, la gestión de activos industriales y la integración con plataformas digitales corporativas**. Históricamente, muchos sistemas industriales operaban en redes aisladas o con conectividad muy limitada; sin embargo, la necesidad de optimizar operaciones, reducir costes de desplazamiento técnico y permitir la asistencia de fabricantes está favoreciendo la introducción de **accesos remotos controlados, pasarelas seguras y soluciones de acceso específico para sistemas industriales**.

Relevancia e implicaciones

En el contexto de la **industria gallega**, donde muchas instalaciones industriales e infraestructuras críticas están distribuidas territorialmente (plantas industriales, instalaciones energéticas, puertos o instalaciones de tratamiento de agua), la conectividad remota permite **mejorar la eficiencia operativa y la capacidad de**

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

respuesta ante incidencias técnicas. No obstante, también introduce **nuevos vectores de riesgo**, ya que los accesos remotos constituyen uno de los puntos de entrada más habituales en incidentes de ciberseguridad industrial. La adopción de **arquitecturas de acceso remoto específicamente diseñadas para entornos OT**, con autenticación fuerte, control de sesiones y monitorización continua, se convierte así en un elemento clave para garantizar la seguridad de estos sistemas.

Consideraciones adicionales

El **acceso remoto no autorizado o mal configurado sigue siendo uno de los factores más frecuentes en incidentes que afectan a entornos OT** según el SANS Institute [5]. En particular, el uso de **VPN tradicionales, credenciales compartidas o accesos persistentes sin control de sesión** puede facilitar la intrusión de actores maliciosos en los sistemas industriales. Como respuesta a este escenario, están emergiendo modelos de acceso más seguros basados en **acceso remoto consciente del contexto industrial, registro y grabación de sesiones, segmentación de red e integración con modelos Zero Trust** [6]. La modernización de la conectividad en entornos OT debe ir acompañada, por lo tanto, **de un diseño de seguridad específico para sistemas industriales**, que tenga en cuenta las limitaciones operativas y los requisitos de continuidad del servicio de estos entornos.

3.2.1.3 Fuerza laboral conectada aumentada (Augmented Connected Workforce)

Descripción de la tendencia

La tendencia conocida como **Augmented Connected Workforce (ACWF)** se refiere a la incorporación de **tecnologías digitales que amplían las capacidades de los trabajadores industriales**, combinando conectividad, análisis de datos y herramientas de asistencia inteligente. Ello incluye el uso de **dispositivos móviles industriales, realidad aumentada (AR), sistemas de asistencia remota, sensores portátiles y plataformas de gestión del conocimiento**, que permiten a los operarios acceder a información contextualizada sobre procesos, equipos o incidencias en tiempo real. El objetivo principal es **mejorar la eficiencia operativa, reducir errores humanos y facilitar la transferencia de conocimiento técnico**, especialmente en un contexto de creciente complejidad tecnológica en las plantas industriales.

Relevancia e implicaciones

Esta tendencia resulta especialmente relevante en sectores intensivos en operaciones técnicas como **la automoción, la industria naval, la alimentación o la energía**. La

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

utilización de herramientas de asistencia digital permite **optimizar tareas de mantenimiento, diagnóstico de fallos y formación de personal**, reduciendo tiempos de intervención y mejorando la continuidad operativa. Sin embargo, también introduce nuevos retos de ciberseguridad, ya que la incorporación de **dispositivos conectados, aplicaciones móviles industriales y plataformas de soporte remoto** amplía la superficie de exposición de los entornos OT. La protección de estos ecosistemas requiere integrar **medidas de gestión de identidades, control de dispositivos, segmentación de red y monitorización de accesos**.

Consideraciones adicionales

La adopción de una fuerza laboral conectada está directamente relacionada con **la transformación digital de la industria y con la escasez de perfiles técnicos especializados**, factores que impulsan el desarrollo de herramientas de asistencia basadas en datos y conectividad. Diversos estudios como los de Deloitte o el Foro Económico Mundial señalan que la implementación de soluciones ACWF puede mejorar significativamente **la productividad, la seguridad laboral y la capacidad de resolución de incidencias en entornos industriales complejos** [7][8]. Con todo, también requiere abordar cuestiones como **la seguridad de los dispositivos utilizados por los operarios, la protección de la información operativa y la correcta integración de estas herramientas en las arquitecturas de ciberseguridad industrial existentes** [9].

3.2.1.4 Inteligencia Artificial en OT (integración transversal)

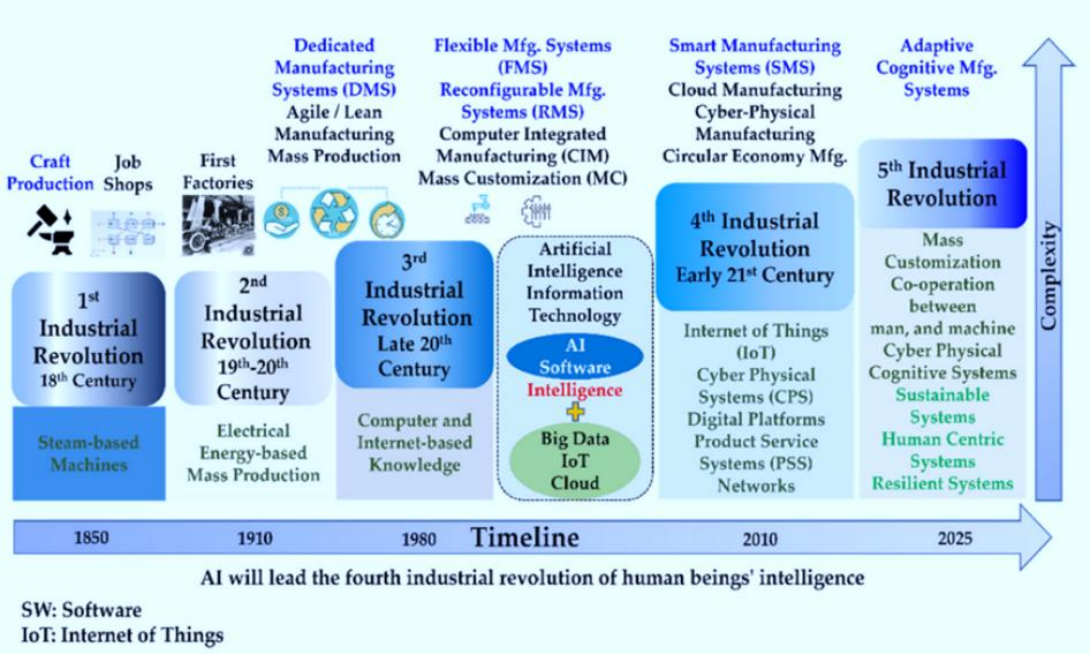
Descripción de la tendencia

La incorporación de la **inteligencia artificial (IA) en entornos de tecnología operacional (OT)** se está convirtiendo en un elemento transversal de la transformación digital industrial. A medida que las plantas industriales incorporan sensores, sistemas de monitorización y plataformas de análisis de datos, se generan una gran cantidad de información operacional susceptible de ser analizado mediante algoritmos de **aprendizaje automático, análisis predictivo y sistemas de optimización basados en IA**. Estas capacidades permiten desarrollar aplicaciones como **mantenimiento predictivo, optimización de procesos productivos, detección temprana de anomalías o mejora de la eficiencia energética**, integrando la IA directamente en los flujos operacionales de las instalaciones industriales [10].

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

Relevancia e implicaciones

En el caso de la industria **gallega**, donde sectores como la automoción, la producción alimentaria, energía o la industria marítima están avanzando hacia modelos de **industria 4.0**, la integración de IA en los sistemas industriales puede contribuir a **mejorar la eficiencia productiva, reducir costes operativos e incrementar la capacidad de análisis en tiempo real de los procesos industriales**. No obstante, la introducción de sistemas basados en IA también introduce **nuevos retos de ciberseguridad**, ya que estos sistemas dependen de grandes volúmenes de datos y de infraestructuras digitales interconectadas. La manipulación de datos, los ataques contra modelos de IA o la explotación de vulnerabilidades en las plataformas que los soportan pueden afectar directamente a la fiabilidad de los sistemas industriales.



Impacto de la IA en la evolución industrial. Fuente: Moyassar Y. Mohammed, Mirosław J. Skibniewski (2023)

Consideraciones adicionales

La creciente adopción de IA en el ámbito industrial está acompañada de un aumento del interés de los actores de amenaza por **explotar vulnerabilidades asociadas a modelos de aprendizaje automático, cadenas de datos y sistemas de decisión automatizados**. Además, la dependencia de datos operacionales hace que **la integridad y la disponibilidad de la información industrial** sean factores críticos para garantizar el correcto funcionamiento de estos sistemas. En este contexto, organismos e informes

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

internacionales subrayan la necesidad de integrar **principios de seguridad y gobernanza de la IA** en el diseño y despliegue de estas soluciones, incluyendo mecanismos de supervisión humana, convalidación de modelos y protección frente a manipulaciones de datos [11][12].

3.2.1.5 Modelos de IA generativa específicos de dominio (Domain-Specific GenAI)

Descripción de la tendencia

En los últimos años está emergiendo una nueva generación de **modelos de inteligencia artificial generativa especializados en dominios concretos**, conocidos como DomainSpecific Generative AI. La diferencia de los modelos generales de lenguaje o imagen, estos sistemas están **adiestrados con datos y conocimiento propio de un sector o de una función industrial concreta**, como operaciones de mantenimiento, procesos industriales, documentación técnica o análisis de incidentes. Esto permite desarrollar asistentes y herramientas capaces de **interpretar documentación técnica, apoyar el diagnóstico de fallos, generar procedimientos operativos o asistir a personal técnico en tiempo real**, con un nivel de precisión mayor que los modelos genéricos.

Relevancia e implicaciones

Los modelos de **IA generativa específicos de dominio pueden contribuir a mejorar la gestión del conocimiento industrial, la formación de personal y la resolución de incidencias técnicas**. Al mismo tiempo, su integración en los flujos operativos introduce nuevos retos en materia de seguridad de **la información, protección de datos industriales sensibles y control de las decisiones automatizadas**. El uso de estos sistemas requiere establecer **políticas claras de gobernanza de la IA, control del acceso a la información y convalidación de las respuestas generadas por los modelos**, especialmente cuando se aplican a procesos críticos.

Consideraciones adicionales

Estos modelos generativos especializados están siendo adoptados progresivamente en ámbitos como **el soporte técnico industrial, el análisis de documentación de ingeniería, la gestión de conocimiento corporativo o la automatización de tareas cognitivas complejas**. Con todo, diversos estudios señalan que estos sistemas pueden introducir riesgos asociados a la **filtración de información sensible, a la generación de respuestas incorrectas (alucinaciones) o a la manipulación de los modelos mediante ataques de prompt injection o envenenamiento de datos**. Por este

motivo, organismos e informes especializados destacan la necesidad de aplicar **mecanismos de gobernanza, evaluación continua de modelos y control de la calidad de los datos empleados en el adiestramiento** como parte esencial de su implantación en entornos industriales [13].

3.2.1.6 Agentes de IA (AI Agents)

Descripción de la tendencia

Los **agentes de inteligencia artificial (AI Agents)** representan una evolución de los sistemas tradicionales basados en modelos de IA hacia **entidades software capaces de ejecutar tareas de forma autónoma, interactuar con sistemas externos y tomar decisiones basadas en objetivos definidos**. La diferencia de los sistemas de análisis o recomendación convencionales, los agentes de IA pueden **interpretar información, planificar acciones, ejecutar procesos y adaptar su comportamiento en función del contexto operativo**. En el ámbito industrial, estos agentes pueden emplearse para **coordinar operaciones, gestionar flujos de datos industriales, asistir en la supervisión de procesos o automatizar tareas complejas de análisis y control**.

Relevancia e implicaciones

Para el **ecosistema industrial gallego**, la introducción de agentes de IA puede contribuir a **automatizar procesos de análisis, mejorar la gestión operativa y optimizar la toma de decisiones en entornos industriales complejos**. Estudios como el siguiente de IBM avalan esta tesis:

Encuesta de impacto de la IA agéntica en la empresa. Fuente: IBM (2025)

En sectores con operaciones distribuidas o con sistemas altamente interconectados, estos sistemas pueden apoyar tareas como **monitorización continua de activos, detección de anomalías operacionales o coordinación de respuestas ante incidencias técnicas**. No obstante, el uso de agentes autónomos también introduce **nuevos retos en materia de control, supervisión y ciberseguridad**, ya que la capacidad de estos sistemas para interactuar con múltiples componentes de la infraestructura industrial puede amplificar el impacto de posibles errores, manipulaciones o vulnerabilidades.

Consideraciones adicionales

Diversos informes tecnológicos señalan que los agentes de IA están evolucionando rápidamente hacia **arquitecturas multi-agente,** en las que diferentes sistemas cooperan para resolver tareas complejas o coordinar procesos distribuidos. Esta evolución abre oportunidades para **automatizar operaciones industriales y mejorar la eficiencia operativa**, pero también requiere establecer **mecanismos robustos de gobernanza, supervisión humana y control de las acciones ejecutadas por los agentes** [14]. Además, desde el punto de vista de la ciberseguridad, resulta esencial garantizar la **integridad de los datos utilizados por los agentes, la autenticidad de las interacciones entre sistemas y la capacidad de auditoría de las decisiones automatizadas**, especialmente cuando estos sistemas se integran en procesos industriales críticos.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

3.2.1.7 Agentes de IA que transforman procesos (AI Agents Tracend Processes)

Descripción de la tendencia

Una evolución reciente en el desarrollo de sistemas basados en inteligencia artificial es la aparición de **agentes capaces de trascender procesos individuales y coordinar cadenas completas de actividad**, conocidos como AI Agents Trascend Processes. Mientras que los primeros agentes de IA estaban orientados a tareas específicas —como análisis de datos o ejecución de acciones limitadas—, los nuevos modelos permiten **orquestar múltiples procesos, integrar información procedente de diferentes sistemas y adaptar dinámicamente los flujos de trabajo**. Estos sistemas pueden interactuar con aplicaciones empresariales, sistemas industriales o plataformas de análisis para **automatizar secuencias completas de decisión y ejecución**, convirtiéndose en un elemento clave de la próxima generación de automatización empresarial.

Relevancia e implicaciones

Esta tendencia puede tener un impacto significativo en la forma en que se gestionan **procesos productivos complejos, cadenas de suministro y operaciones distribuidas**. La capacidad de coordinar múltiples sistemas y procesos mediante agentes inteligentes puede contribuir a **optimizar flujos de producción, mejorar la respuesta ante incidencias y aumentar la eficiencia operativa**. Con todo, la introducción de estos sistemas también amplía la **dependencia de infraestructuras digitales y de decisiones automatizadas**, lo que requiere reforzar los mecanismos de **control, supervisión humana y gobernanza de la automatización** en entornos industriales.

Consideraciones adicionales

Los sistemas de agentes capaces de coordinar procesos completos están asociados al desarrollo de **arquitecturas multi-agente y plataformas de automatización inteligente,** en las que diferentes componentes cooperan para resolver tareas complejas. Esta evolución puede impulsar una nueva fase de la **automatización industrial y de la gestión basada en datos**, pero también introduce nuevos riesgos asociados a la **dependencia de decisiones automatizadas, a la manipulación de flujos de información y a la posible propagación de errores entre sistemas interconectados**. Por este motivo, los riesgos son similares a los de las tendencias previas. El enfoque es tan novedoso que apenas hay todavía literatura al respecto.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

3.2.1.8 Inteligencia para la toma de decisiones (Decision Intelligence)

Descripción de la tendencia

La **Decision Intelligence** se refiere al uso combinado de **inteligencia artificial, análisis avanzado de datos, modelos de decisión y simulación** para mejorar la calidad y la rapidez de las decisiones organizativas. Este enfoque integra técnicas de **aprendizaje automático, análisis predictivo, optimización y modelado de escenarios** para apoyar a los responsables operativos en la selección de las mejores opciones en contextos complejos. En el ámbito industrial, la Decision Intelligence permite **analizar grandes volúmenes de datos operacionales, identificar patrones relevantes y recomendar acciones basadas en evidencias**, contribuyendo a optimizar procesos productivos, gestionar riesgos y mejorar la planificación de las operaciones.

En este artículo, Roger Moser baja al terreno la definición teórica de Gartner para hacerla accionable [15].

Relevancia e implicaciones

La adopción de sistemas de Decision Intelligence puede facilitar una **mejor gestión de procesos productivos, cadenas de suministro y operaciones energéticas**, especialmente en entornos caracterizados por múltiples variables operativas. La integración de estas herramientas permite **anticipar fallos, optimizar la planificación de la producción y apoyar la toma de decisiones en tiempo real**, reforzando la competitividad de las organizaciones industriales. No obstante, también introduce retos relacionados con **la fiabilidad de los modelos, la dependencia de datos de calidad y la seguridad de las plataformas analíticas**, aspectos especialmente relevantes cuando estas decisiones tienen impacto directo sobre procesos físicos o infraestructuras críticas.

Consideraciones adicionales

La evolución hacia sistemas de Decision Intelligence está estrechamente vinculada a la creciente disponibilidad de **datos industriales, sensores IoT y plataformas de análisis avanzado**, que permiten construir modelos de decisión cada vez más sofisticados. Con todo, diversos estudios subrayan que la eficacia de estos sistemas depende en gran medida de la **calidad de los datos utilizados, de la transparencia de los algoritmos y de la capacidad de supervisión humana de las recomendaciones generadas**. Desde la perspectiva de la ciberseguridad industrial, resulta fundamental

garantizar **la integridad de los datos empleados en los procesos de análisis, la protección de las plataformas analíticas y la resiliencia de los sistemas de apoyo a la decisión**, ya que la manipulación de estos elementos podría influir directamente en la toma de decisiones operativas.

3.2.1.9 Automatización de la decisión con IA y riesgo de pérdidas catastróficas

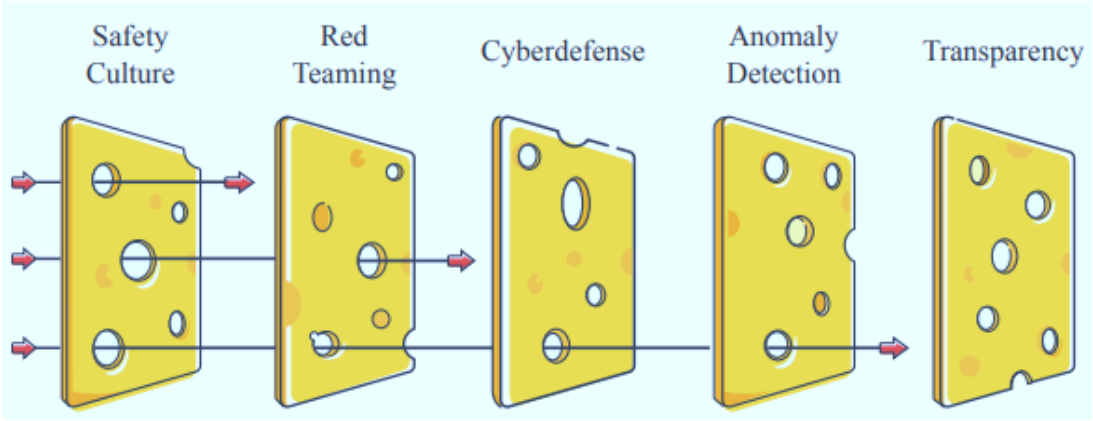
Descripción de la tendencia

La creciente integración de la **inteligencia artificial en sistemas de apoyo a la decisión** está impulsando una progresiva **automatización de decisiones operativas y estratégicas** en múltiples ámbitos empresariales e industriales. Sistemas basados en **aprendizaje automático, análisis predictivo y modelos de optimización** son capaces de ejecutar decisiones de forma autónoma o semiautónoma en áreas como planificación de la producción, gestión de inventarios, mantenimiento de activos o control de procesos industriales. Esta evolución permite **incrementar la velocidad y la eficiencia de las operaciones**, pero también introduce el riesgo de que decisiones automatizadas incorrectas o manipuladas puedan generar **impactos operacionales de gran magnitud**.

Relevancia e implicaciones

En el contexto de la **industria gallega**, donde numerosos procesos industriales dependen de **sistemas automatizados de control y supervisión** (logística, energía, etc.), la automatización de la toma de decisiones mediante IA puede contribuir a **optimizar operaciones y mejorar la capacidad de respuesta ante variaciones en la producción o en el mercado**. No obstante, también implica una mayor **dependencia de sistemas algorítmicos y de datos operacionales,** lo que puede amplificar el impacto de posibles errores de modelado, manipulación de datos o fallos en los sistemas de decisión. En entornos industriales críticos, una decisión automatizada incorrecta podría **propagar efectos adversos a lo largo de cadenas de producción o sistemas interconectados**, generando pérdidas económicas o interrupciones operativas severas.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027



Defensa en profundidad para mejorar la seguridad organizacional. Fuente: Center for AI Safety (2023)

Consideraciones adicionales

La automatización completa de decisiones en sistemas complejos puede introducir **riesgos sistémicos difíciles de anticipar**, especialmente cuando los modelos operan con poca supervisión humana o con datos incompletos. Entre los riesgos identificados se encuentran la **propagación de errores algorítmicos, la manipulación de datos utilizados por los modelos, malware, o la pérdida de capacidad o manipulación de la intervención humana en procesos críticos** [16]. Por este motivo, organismos y expertos recomiendan aplicar **principios de supervisión humana significativa, mecanismos de auditoría algorítmica y controles de seguridad en los sistemas de decisión automatizados**, especialmente cuando éstos tienen impacto directo sobre operaciones industriales o infraestructuras críticas.

3.2.1.10 Gobernanza de la IA como factor crítico organizativo

Descripción de la tendencia

La rápida adopción de sistemas basados en **inteligencia artificial (IA)** en múltiples ámbitos empresariales e industriales está impulsando la aparición de un nuevo ámbito de gestión conocido como **gobernanza de la IA**. Este concepto se refiere al conjunto de **políticas, procesos, mecanismos de control y estructuras organizativas** destinados a garantizar que el desarrollo, despliegue y uso de la IA se realice de manera **segura, transparente, responsable y conforme a las regulaciones aplicables**. La gobernanza de la IA incluye aspectos como **la gestión del riesgo algorítmico, la supervisión humana de las decisiones automatizadas, la trazabilidad de los modelos y la protección de los datos utilizados en los sistemas de IA**.

Relevancia e implicaciones

La gobernanza de la IA se convierte en un elemento cada vez más relevante a medida que las organizaciones incorporan **sistemas de análisis avanzado, automatización basada en datos y herramientas de apoyo a la decisión**. La ausencia de marcos claros de gobernanza puede provocar **dependencia excesiva de decisiones automatizadas, falta de control sobre los modelos empleados o exposición a riesgos legales y reputacionales**. Además, la progresiva aparición de **regulación específica sobre inteligencia artificial**, especialmente en el ámbito europeo, implica que las organizaciones deberán establecer **estructuras de control, evaluación de riesgos y procedimientos de supervisión** para garantizar el cumplimiento normativo y la utilización responsable de estas tecnologías.

Consideraciones adicionales

La gobernanza de la IA está consolidándose como uno de los principales ejes de la transformación digital responsable. Diversos organismos internacionales e iniciativas reguladoras subrayan que las organizaciones deben implementar **marcos de gobernanza que incluyan evaluación de riesgos, mecanismos de auditoría de los modelos, control de la calidad de los datos y supervisión humana significativa**. En este contexto, está emergiendo el concepto de **Sistemas de Gestión de la Inteligencia Artificial (SXIA)**, que buscan estructurar de forma sistemática la gobernanza de estas tecnologías dentro de las organizaciones. La norma **ISO/IEC 42001** [17], publicada recientemente, establece los requisitos para implementar un **sistema de gestión específico para la IA**, inspirado en modelos de gestión ya consolidados como **ISO 27001 para seguridad de la información** o **ISO 9001 para gestión de la calidad**.

En el contexto europeo, además, el desarrollo del **Reglamento de Inteligencia Artificial de la Unión Europea (AI Act)** [12] establece un marco normativo destinado a **regular el uso de sistemas de IA en función de su nivel de riesgo**, lo que refuerza la necesidad de que las organizaciones adopten **estructuras formales de gobernanza, evaluación de riesgos y control del ciclo de vida de los modelos de IA**.

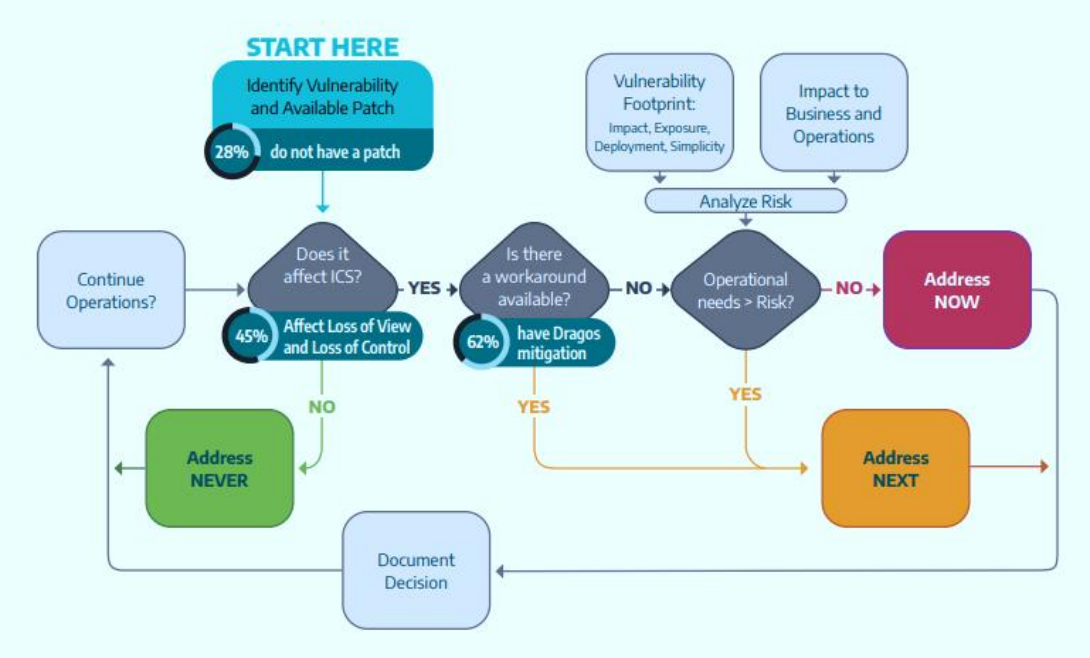
La convergencia entre regulación europea y estándares internacionales apunta a que, en los próximos años, la implantación de **SXIA (Sistemas de Gestión de la IA) basados en ISO 42001** podría convertirse en un elemento clave para demostrar **cumplimiento normativo, responsabilidad algorítmica y confianza en las soluciones basadas en IA.**

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

3.2.1.11 Gestión de vulnerabilidades y parcheo en OT orientado a riesgo

La **gestión de vulnerabilidades en entornos OT** está evolucionando desde enfoques tradicionales basados únicamente en la aplicación periódica de parches hacia modelos más avanzados de **gestión de vulnerabilidades orientada a riesgo** [18]. En los sistemas industriales, la aplicación directa de actualizaciones de software puede resultar compleja debido a factores como **la necesidad de continuidad operativa, la dependencia de fabricantes, la certificación de equipos o la antigüedad de determinados sistemas de control**.

Por este motivo, cada vez más organizaciones industriales adoptan enfoques que combinan **evaluación del riesgo, priorización de vulnerabilidades, medidas compensatorias y planificación controlada de actualizaciones**, con el objetivo de reducir la exposición sin comprometer la estabilidad de las operaciones:



Árbol de decisión de parcheo urgente del DHS americano. Fuente: Dragos (2024)

Relevancia e implicaciones

En el caso del **tejido industrial gallego y en el sector en general**, caracterizado por la presencia de **instalaciones industriales con ciclos de vida largos e infraestructuras críticas distribuidas**, la gestión de vulnerabilidades en OT representa un desafío significativo. Muchos sistemas industriales no pueden actualizarse con la misma frecuencia que los sistemas IT convencionales, lo que hace necesario adoptar **estrategias de priorización basadas en el impacto operativo, en la criticidad de los**

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

activos y en la probabilidad de explotación de las vulnerabilidades. La implementación de procesos estructurados de gestión de vulnerabilidades permite **reducir la superficie de ataque, mejorar la visibilidad de los activos industriales y fortalecer la resiliencia de las instalaciones frente a amenazas cibernéticas**.

Consideraciones adicionales

La gestión de vulnerabilidades orientada a riesgo implica combinar **diferentes medidas técnicas y organizativas** cuando la aplicación inmediata de un parche no es viable. Entre estas medidas se incluyen la **segmentación de redes industriales, la limitación de accesos remotos, la monitorización específica de protocolos OT o la implantación de controles compensatorios** que reduzcan la probabilidad de explotación.

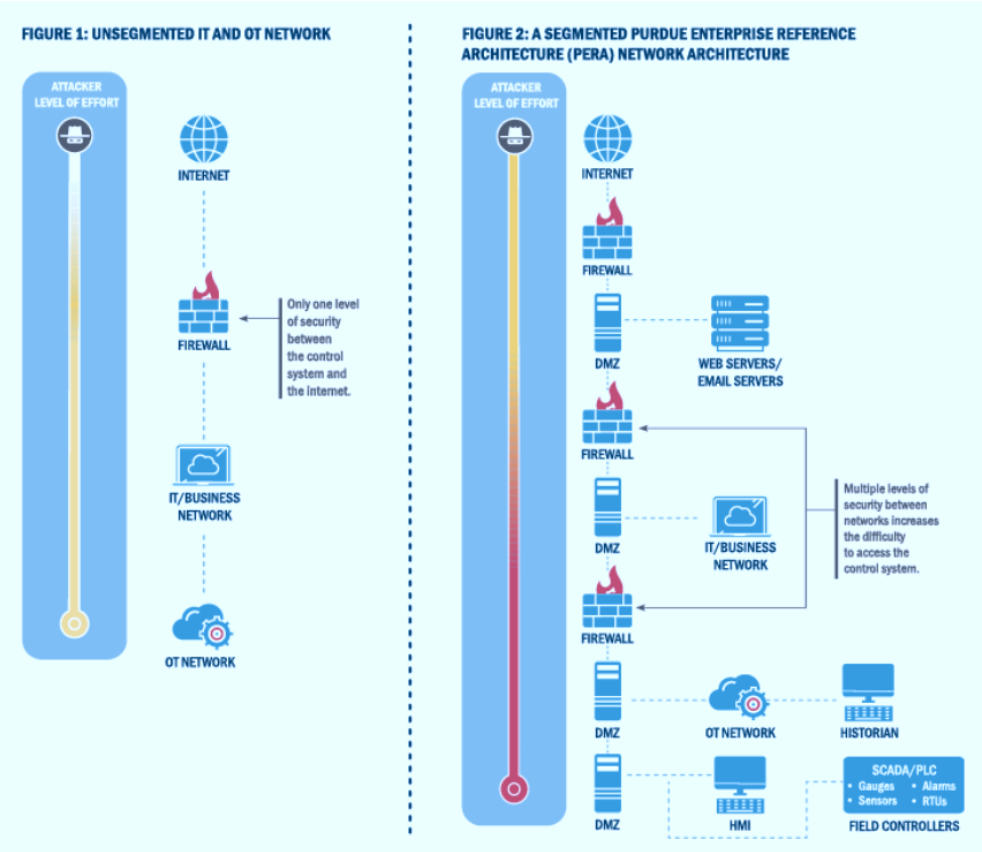
En el Informe de Ciberalertas OT II del Observatorio de Ciberseguridad Industrial de Galicia [19] se analizan precisamente **estrategias de priorización basadas en el riesgo para la gestión de vulnerabilidades**, destacando la importancia de evaluar no sólo la técnica de una vulnerabilidad, sino también **el contexto operativo en el que se encuentra el activo industrial**. Esta aproximación permite adoptar decisiones más realistas sobre cuándo y cómo aplicar actualizaciones, manteniendo el equilibrio entre **seguridad y continuidad de las operaciones industriales**.

3.2.1.12 Segmentación y segregación de redes OT

Descripción de la tendencia

La **segmentación y segregación de redes industriales** constituye uno de los principios fundamentales de la arquitectura de ciberseguridad en entornos OT. Este enfoque se basa en **dividir la infraestructura de red en zonas o segmentos con diferentes niveles de confianza**, limitando las comunicaciones entre sistemas y reduciendo la propagación de incidentes. En los entornos industriales modernos, donde conviven sistemas de control, redes corporativas y servicios conectados a Internet, la segmentación permite **establecer barreras de protección entre dominios IT y OT**, así como entre distintos niveles de la propia red industrial.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027



Arquitectura segmentada IT/OT frente a no segmentada. Fuente: CISA (2025)

Relevancia e implicaciones

La implantación de arquitecturas segmentadas es clave para **proteger procesos críticos y reducir el impacto potencial de un incidente de ciberseguridad**. La separación adecuada entre redes corporativas y sistemas industriales dificulta que un ataque iniciado en un sistema IT pueda alcanzar directamente los sistemas de control. Además, la segmentación permite **controlar y monitorizar con mayor precisión los flujos de comunicación entre equipos industriales**, facilitando la detección de comportamientos anómalos o accesos no autorizados.

Consideraciones adicionales

En la práctica, la segmentación en entornos OT adopta implementarse mediante **zonas de seguridad, conductos de comunicación controlados** (descrito con detalle en la Guía normativa de ciberseguridad industrial desde mismo Observatorio, en el apartado dedicado a ISA/IEC 62443 [20]), **firewalls industriales y políticas de acceso específicas para protocolos industriales**. Este enfoque permite establecer **capas adicionales de protección** sin interferir en la operación normal de las instalaciones. Al

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

mismo tiempo, la segmentación facilita la aplicación de otras medidas de seguridad, como la **monitorización del tráfico industrial, la gestión de accesos remotos o la aplicación de controles compensatorios cuando determinados sistemas no pueden actualizarse con frecuencia**. La adopción de arquitecturas de red basadas en zonas y conductos forma parte de las buenas prácticas de seguridad industrial y contribuye a **incrementar la resiliencia de las infraestructuras industriales frente a incidentes**.

3.2.1.13 Soberanía tecnológica (Technological Sovereignty)

Descripción de la tendencia

La **soberanía tecnológica** se refiere a la capacidad de un país, región u organización para **controlar y desarrollar las tecnologías críticas de las que dependen sus infraestructuras y actividades económicas**, reduciendo la dependencia excesiva de proveedores externos. En el ámbito industrial y digital, este concepto abarca aspectos como la **autonomía en software, hardware, infraestructuras de datos, servicios cloud, semiconductores o tecnologías de inteligencia artificial**. En los últimos años, especialmente desde la guerra entre Rusia y Ucrania, la creciente tensión geopolítica, las interrupciones en las cadenas de suministro y la importancia estratégica de las tecnologías digitales impulsaron políticas públicas orientadas a **reforzar la autonomía tecnológica y por ende la resiliencia industrial** [21][22].

Relevancia e implicaciones

El **ecosistema industrial gallego**, integrado en cadenas de valor globales y fuertemente dependiente de tecnologías digitales e industriales importadas, la cuestión de la soberanía tecnológica está directamente relacionada con la **resiliencia de las infraestructuras industriales y la seguridad de las cadenas de suministro tecnológico**. La dependencia de determinados proveedores o plataformas puede introducir riesgos **de continuidad operativa, limitaciones en la capacidad de respuesta ante incidentes o dificultades para aplicar políticas de seguridad adaptadas al contexto local**. En este sentido, reforzar la diversidad de proveedores, fomentar capacidades tecnológicas propias y adoptar estándares abiertos contribuye a **reducir vulnerabilidades estructurales y aumentar la capacidad de control sobre las infraestructuras críticas**.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

Consideraciones adicionales

La soberanía tecnológica no implica necesariamente sustituir tecnologías externas, sino **garantizar que las organizaciones mantengan capacidad de decisión y control sobre los sistemas que sustentan su actividad**. En el ámbito europeo, este enfoque está materializado en iniciativas orientadas a **reforzar la autonomía digital, promover ecosistemas industriales propios y reducir dependencias estratégicas en tecnologías críticas**. Para las organizaciones industriales, esto se traduce en prácticas como **evaluar riesgos asociados a proveedores tecnológicos, diversificar cadenas de suministro, adoptar estándares interoperables y reforzar la transparencia sobre componentes y software utilizados en los sistemas industriales**.

3.2.1.14 Cadena de suministro y dependencia de terceros en OT

Descripción de la tendencia

Los sistemas industriales dependen cada vez más de una **cadena de suministro compleja que incluye fabricantes de hardware, proveedores de software, integradores de sistemas, servicios de mantenimiento y plataformas de conectividad**. Esta realidad implica que una parte significativa de las tecnologías utilizadas en los entornos OT no es desarrollada ni controlada directamente por las organizaciones que operan las infraestructuras industriales. Como consecuencia, los riesgos asociados a la **cadena de suministro tecnológico** se han convertido en un elemento central de la ciberseguridad industrial, ya que vulnerabilidades o incidentes en un proveedor pueden afectar a múltiples organizaciones de forma simultánea.

Relevancia e implicaciones

De nuevo, para los sectores caracterizados por la integración en **cadenas de valor internacionales y por el uso intensivo de tecnología industrial especializada**, la dependencia de terceros es una realidad estructural. Fabricantes de equipos industriales, proveedores de software de control, integradores de automatización o empresas de mantenimiento remoto participan de manera directa en la operación de las infraestructuras industriales. Esto implica que la seguridad de estos sistemas no depende únicamente de las medidas internas de las organizaciones, sino también de la **madurez de ciberseguridad de los proveedores y de las condiciones de seguridad establecidas en los contratos y relaciones comerciales**, como se puede ver en este estudio de ENISA [23].

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware Infection	e.g. spyware used to steal credentials from employees.
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login.
Exploiting Software Vulnerability	e.g. SQL injection or buffer overflow exploit in an application.
Exploiting Configuration Vulnerability	e.g. taking advantage of a configuration problem.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Open-Source Intelligence (OSINT)	e.g. search online for credentials, API keys, usernames.
Counterfeiting	e.g. imitation of USB with malicious purposes.

Técnicas comunes para comprometer la cadena de suministro. Fuente: ENISA (2021)

Consideraciones adicionales

La gestión del riesgo asociado a la cadena de suministro requiere incorporar prácticas como la **evaluación de seguridad de proveedores, la definición de requisitos de ciberseguridad en contratos, la supervisión del acceso remoto de terceros y el análisis de la procedencia de los componentes tecnológicos utilizados en los sistemas industriales**. Además, la creciente complejidad de las arquitecturas industriales hace recomendable mantener **inventarios actualizados de activos y dependencias tecnológicas**, con el fin de comprender como un incidente en un proveedor podría afectar a la operación industrial. La adopción de este tipo de medidas permite **reducir la exposición a riesgos derivados de terceros y fortalecer la resiliencia de las cadenas industriales digitalizadas**.

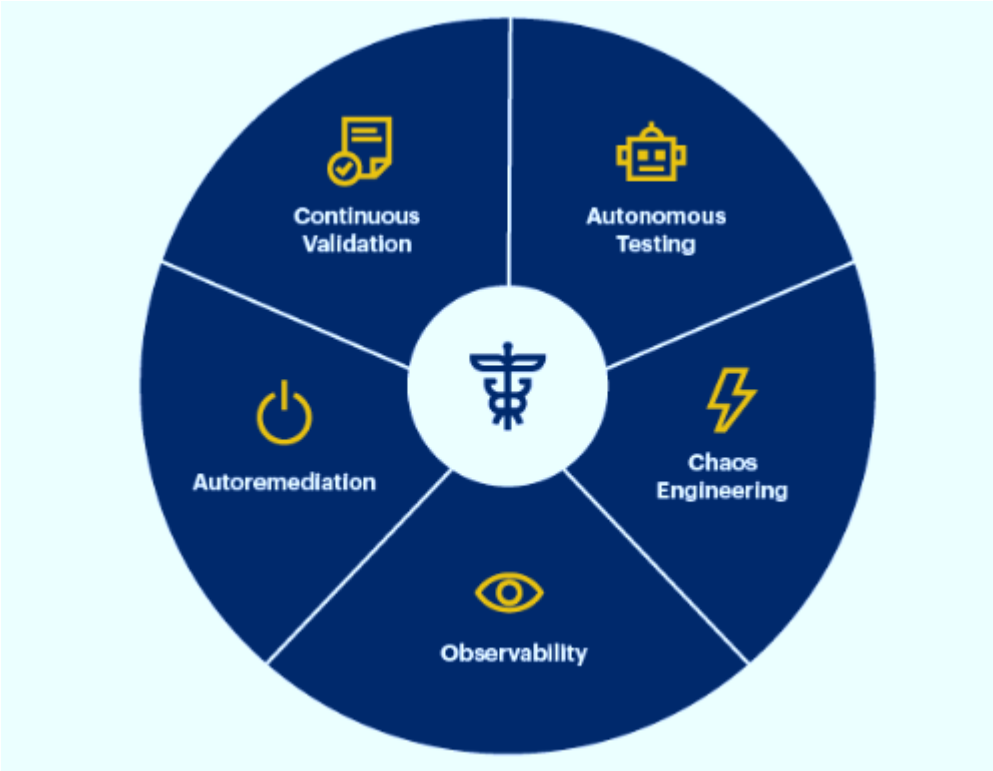
3.2.1.15 Sistema digital inmune (Digital Immune System)

Descripción de la tendencia

El concepto de **Sistema Digital Inmune (Digital Immune System)** describe un enfoque de arquitectura tecnológica orientado a **aumentar la resiliencia de los sistemas digitales mediante la detección temprana de errores, la respuesta automática a incidentes y la capacidad de recuperación continua**. Inspirado en la idea del sistema inmunitario biológico, este enfoque combina **observabilidad avanzada,**

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

automatización, inteligencia artificial, pruebas continuas y mecanismos de autorrecuperación para identificar anomalías y responder rápidamente antes de que los fallos o incidentes tengan impacto significativo en las operaciones. En el ámbito industrial, estos sistemas pueden integrarse en plataformas de monitorización, sistemas de control e infraestructuras digitales para **anticipar incidentes y mantener la continuidad operativa**. El concepto se explica con mayor profundidad en este artículo, aplicado a productos digitales [24].



Elementos de un sistema digital inmune. Fuente: Gartner (2021)

Relevancia e implicaciones

Para la **industria gallega**, donde gran parte de las instalaciones industriales dependen de **sistemas de control y supervisión que deben operar de forma continua**, la incorporación de capacidades propias de un sistema digital inmune puede contribuir a **reducir el tiempo de detección de incidentes, mejorar la capacidad de respuesta y limitar el impacto de fallos técnicos o ataques de ciberseguridad**. La integración de herramientas de observabilidad, análisis automatizado y respuesta coordinada permite **identificar anomalías en procesos industriales, detectar comportamientos anómalos en la red OT y activar mecanismos de mitigación de forma más rápida**.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

Consideraciones adicionales

La implantación de sistemas digitales inmunes adopta combinar **monitorización continua de activos, análisis de telemetría, automatización de respuesta y mecanismos de pruebas y convalidación constantes**. Este enfoque resulta especialmente relevante en entornos industriales donde los sistemas deben operar durante largos periodos sin interrupciones. La adopción de estas capacidades contribuye a **incrementar la resiliencia operativa de las infraestructuras industriales**, permitiendo detectar anomalías antes de que se conviertan en incidentes graves y facilitando la recuperación rápida de los sistemas afectados.

3.2.1.16 Cripto-axilidade (Crypto-Agility)

Descripción de la tendencia

La **cripto-agilidad** se refiere a la capacidad de un sistema tecnológico para **adaptar o sustituir rápidamente a los algoritmos criptográficos utilizados para proteger datos y comunicaciones** cuando éstos dejan de ser seguros o quedan obsoletos. En un contexto en el que evolucionan constantemente las técnicas de ataque y aparecen nuevas capacidades computacionales —como la computación cuántica—, las organizaciones necesitan infraestructuras capaces de **actualizar mecanismos de cifrado, gestión de claves y protocolos de seguridad sin interrumpir los servicios**. En los entornos industriales, esto implica diseñar sistemas y arquitecturas que permitan **modificar algoritmos criptográficos o renovar certificados y claves de forma controlada a lo largo del ciclo de vida de las instalaciones**.

Relevancia e implicaciones

En un **sector industrial** donde numerosos sistemas OT tienen ciclos de vida que pueden superar las dos décadas, la capacidad de adaptar mecanismos criptográficos se convierte en un factor clave de seguridad a largo plazo. Muchos sistemas industriales incorporan **protocolos de comunicación, dispositivos embebidos o sistemas de autenticación diseñados hay años**, lo que puede dificultar la actualización de los mecanismos de cifrado (suponiendo que disponen de ellos en primer lugar). Las arquitecturas con capacidad de evolución criptográfica permiten **proteger comunicaciones industriales, accesos remotos e intercambio de datos entre sistemas** aun cuando los algoritmos empleados inicialmente dejan de ser considerados seguros.

Consideraciones adicionales

La transición hacia modelos de cripto-agilidad está estrechamente relacionada con la preparación para **nuevos estándares criptográficos y con el desarrollo de criptografía poscuántica**. Para las organizaciones industriales, ello supone la necesidad de **inventariar algoritmos criptográficos empleados en los sistemas, establecer políticas de gestión de claves robustas y garantizar que las plataformas tecnológicas permiten actualizar mecanismos de seguridad a lo largo del tiempo**. La adopción de este enfoque reduce el riesgo de dependencia de tecnologías criptográficas obsoletas y facilita la adaptación de las infraestructuras industriales a futuros requerimientos de seguridad [25]. Según el NCSC (national Cyber Security Centre) británico, en 2035 las organizaciones deberían completar la migración de sus sistemas a algoritmos post-cuánticos [26].

3.2.1.17 SCADA en la nube y cloudización de entornos OT

Descripción de la tendencia

La progresiva digitalización de la industria está favoreciendo la **migración de determinadas funciones de los sistemas industriales hacia infraestructuras cloud**, incluyendo plataformas de supervisión, análisis de datos o integración de sistemas SCADA. Tradicionalmente, los sistemas **SCADA (Supervisory Control and Data Acquisition)** operaban en entornos locales y altamente aislados; sin embargo, la necesidad de **analizar grandes volúmenes de datos operacionales, integrar sistemas distribuidos y habilitar operaciones remotas** está impulsando modelos híbridos en los que parte de las capacidades de supervisión y análisis se ejecutan en entornos cloud o en arquitecturas combinadas de **edge computing y cloud industrial**.

Relevancia e implicaciones

Galicia no es excepción en cuanto a que existen instalaciones industriales e infraestructuras críticas distribuidas geográficamente. En este campo, la cloudización de componentes SCADA puede facilitar **una mayor visibilidad operativa, mejores capacidades de análisis de datos industriales y una gestión más centralizada de las operaciones**. La integración con plataformas cloud también permite **aprovechar herramientas avanzadas de análisis, inteligencia artificial o mantenimiento predictivo**. No obstante, esta evolución introduce nuevos retos en materia de seguridad de **la conectividad, protección de datos industriales y control de las comunicaciones entre sistemas OT y plataformas externas**, por lo que resulta esencial diseñar arquitecturas que mantengan **zonas de seguridad claramente**

definidas y mecanismos de protección para las comunicaciones industriales en base a buenas prácticas [27].

Consideraciones adicionales

La adopción de modelos híbridos –cloud requiere abordar cuestiones como **la seguridad de las pasarelas de comunicación, la autenticación de los dispositivos industriales, la protección de las API utilizadas para integrar sistemas y la visibilidad del tráfico entre entornos industriales y plataformas cloud**. Además, la separación adecuada entre **funciones críticas de control y servicios de análisis o supervisión en la nube** resulta fundamental para evitar que incidentes en un entorno externo afecten directamente a los procesos físicos. Un diseño adecuado de estas arquitecturas permite **aprovechar las ventajas de la computación cloud manteniendo los requisitos de seguridad y continuidad operativa propios de los sistemas industriales**.

3.2.1.18 Arquitectura OT "defendible" (resiliente por diseño)

Descripción de la tendencia

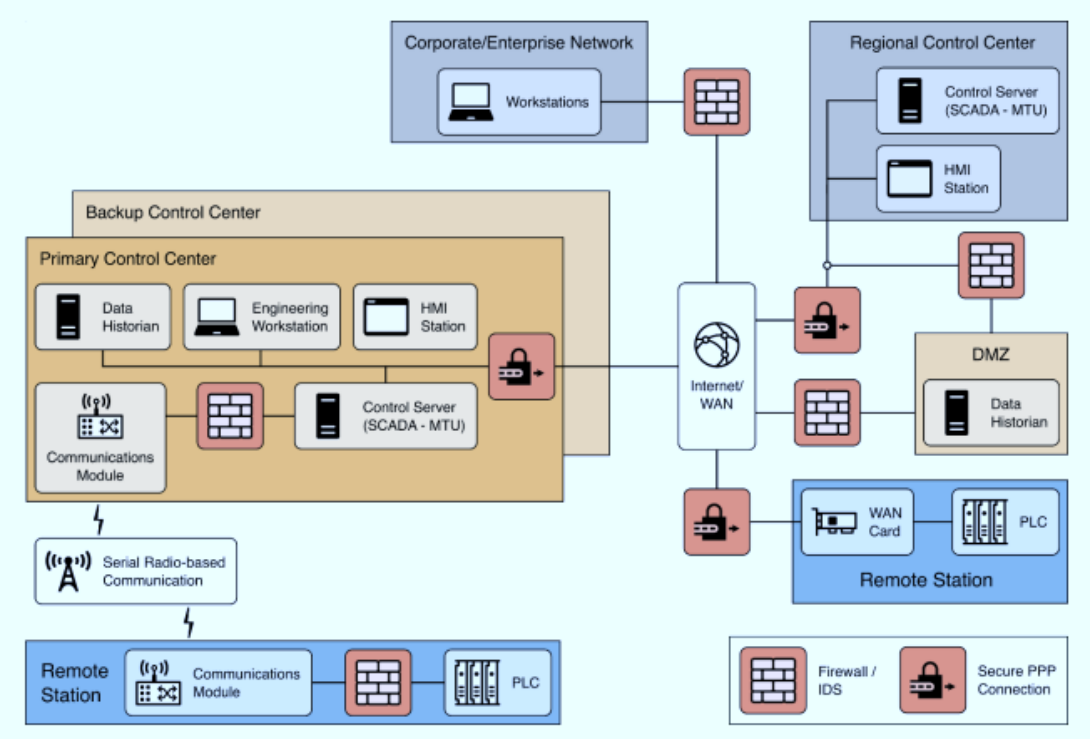
El concepto de **arquitectura OT defendible se** refiere al diseño de infraestructuras industriales en las que la **seguridad y la resiliencia se incorporan desde la propia arquitectura de los sistemas,** y no únicamente mediante medidas adicionales aplicadas posteriormente. Este enfoque implica estructurar las redes y los sistemas industriales de manera que **un incidente o intrusión no pueda propagarse fácilmente ni comprometer la totalidad de la operación**. Para ello se combinan entre otros, principios como **segmentación por zonas, control estricto de las comunicaciones, monitorización continua, autenticación robusta y mecanismos de respuesta ante incidentes**, integrados en el propio diseño de la infraestructura.

Relevancia e implicaciones

En el contexto regional, donde muchas instalaciones industriales combinan sistemas modernos con equipos heredados y ciclos de vida tecnológicos largos, el diseño de una arquitectura defendible resulta fundamental para **limitar el impacto potencial de incidentes de ciberseguridad**. Una infraestructura diseñada con estos principios permite **contener intrusiones, proteger los sistemas de control críticos y mantener la continuidad operativa incluso ante incidentes que afecten a partes de la red industrial**. Además, facilita la integración progresiva de nuevas tecnologías —como conectividad remota, análisis de datos o plataformas cloud— manteniendo **entornos**

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

claramente delimitados y controlados. En el informe **Guía normativa del Observatorio** se recopilan algunos de los controles más habituales empleados en entornos ICS/OT [20].



Ejemplo de arquitectura de seguridad para un sistema SCADA. Fuente: NIST (2023)

Consideraciones adicionales

La construcción de arquitecturas OT defendibles han adoptado basarse en **modelos de referencia de seguridad industrial, buenas prácticas de segmentación y enfoques de defensa en profundidad,** en los que múltiples capas de protección reducen la probabilidad de compromiso completo del sistema. Este enfoque también requiere **inventariar activos industriales, comprender las dependencias entre sistemas y establecer controles específicos para los flujos de comunicación entre componentes de la infraestructura**. Aplicar estos principios permite a las organizaciones **anticipar escenarios de riesgo y diseñar infraestructuras capaces de absorber y recuperar rápidamente de incidentes**, reforzando la resiliencia de las operaciones industriales digitalizadas. Una inspiración de buenas prácticas en este campo es la guía del NIST (Instituto Nacional de Estándares y Tecnología americano) SP 800-82 [28].

3.2.2 De atención programada (prioridad #2)

3.2.2.1 Computación confidencial (Confidential Computing)

Descripción de la tendencia

La **computación confidencial** se arroja a un conjunto de tecnologías destinadas a **proteger los datos mientras están siendo procesados**, no sólo cuando están almacenados o transmitidos. Tradicionalmente, los sistemas informáticos cifran la información en reposo o en tránsito, pero durante el procesamiento los datos adoptan permanecer descifrados en la memoria. La computación confidencial introduce mecanismos basados en **enclaves seguros de hardware, entornos de ejecución confiables (TEE) y procesamiento cifrado**, que permiten ejecutar operaciones sobre datos sensibles manteniendo su protección incluso durante el cálculo.

Relevancia e implicaciones

Para organizaciones industriales que manejan **datos operacionales, información de producción o telemetría de sistemas industriales**, este enfoque abre nuevas posibilidades para **compartir y analizar información sin exponer directamente los datos sensibles**. Esto puede resultar especialmente útil en entornos en los que diferentes entidades —como operadores industriales, proveedores tecnológicos o centros de análisis— necesitan colaborar sobre datos industriales manteniendo garantías de confidencialidad. En escenarios de **integración OT–cloud o análisis avanzado de datos industriales**, la computación confidencial permite reducir los riesgos asociados a la exposición de información crítica.

Consideraciones adicionales

La adopción de estas tecnologías está estrechamente ligada a la evolución de las **arquitecturas cloud seguras y de las plataformas de análisis de datos distribuidas**. En el ámbito industrial, la computación confidencial puede facilitar modelos en los que la información operativa se analiza externamente sin revelar el contenido completo de los datos. Esto resulta relevante para casos de uso como **análisis de rendimiento industrial, detección de anomalías o colaboración entre organizaciones** que necesitan compartir información de manera controlada. El desarrollo de estándares y ecosistemas tecnológicos en torno a esta tecnología está impulsando su adopción progresiva en entornos donde **la protección de la información es un requisito esencial** [29].

3.2.2.2 Cifrado homomórfico (Homomorphic Encryption)

Descripción de la tendencia

El **cifrado homomórfico** es una técnica criptográfica que permite **realizar operaciones matemáticas sobre datos cifrados sin necesidad de descifrarlos previamente** [30][31]. Esto significa que los sistemas pueden procesar información sensible manteniendo los datos protegidos durante todo el ciclo de tratamiento, por ejemplo, en el sector salud. Aunque durante mucho tiempo ha sido considerado un enfoque teórico o con limitaciones prácticas, los avances recientes en algoritmos y capacidad computacional están haciendo posible su aplicación en determinados escenarios reales, especialmente en ámbitos en los que **la privacidad y la protección de la información son críticas**.

Relevancia e implicaciones

En el contexto industrial, el cifrado homomórfico abre la puerta a **nuevos modelos de colaboración y análisis de datos** entre organizaciones sin necesidad de revelar información sensible. Ello puede resultar útil en casos como **análisis conjunto de datos industriales, investigación colaborativa entre empresas o tratamiento de información operativa en plataformas externas**, manteniendo la confidencialidad de los datos de origen. Para el tejido industrial gallego, esta tecnología podría facilitar la **cooperación en cadenas de valor industriales o proyectos de innovación compartidos**, permitiendo analizar información agregada sin comprometer secretos industriales o datos estratégicos.

Consideraciones adicionales

A pesar de su potencial, el cifrado homomórfico sigue presentando **desafíos en términos de rendimiento y complejidad computacional**, por lo que actualmente adopta emplearse en escenarios específicos donde la protección de la información justifica el coste adicional de procesamiento. Su evolución está estrechamente vinculada al desarrollo de **plataformas de análisis segura de datos y arquitecturas cloud orientadas a la privacidad**. Con el avance de las tecnologías de procesamiento y la aparición de herramientas más eficientes, se espera que estas técnicas puedan incorporarse progresivamente a entornos en los que **la confidencialidad de los datos industriales y la colaboración segura entre organizaciones** sean requisitos prioritarios.

3.2.2.3 Seguridad frente a la desinformación (Disinformation Security)

Descripción de la tendencia

La **seguridad frente a la desinformación** se refiere al conjunto de estrategias destinadas a **detectar, analizar y mitigar campañas de manipulación informativa que pueden afectar organizaciones, infraestructuras críticas o procesos económicos**. La expansión de las redes sociales, de las plataformas digitales y de las herramientas basadas en inteligencia artificial está facilitando la creación y difusión de contenido manipulado a gran escala, incluyendo **mensajes coordinadas, contenido sintético o información falsa generada automáticamente**. Este fenómeno se ha convertido en un riesgo relevante para la estabilidad institucional, la reputación de las organizaciones y la confianza pública en los sistemas tecnológicos, por lo que incluso las instituciones están tomando cartas en el asunto [32].

Relevancia e implicaciones

Aunque la desinformación adopta asociarse a contextos políticos o sociales, también puede tener **impacto directo sobre sectores industriales e infraestructuras críticas**. La difusión de información falsa sobre incidentes industriales, interrupciones de servicios o supuestos fallos de seguridad puede **afectar a la reputación de las organizaciones, provocar reacciones en el mercado o generar alarma social**. En un contexto como el gallego, donde determinados sectores industriales tienen fuerte impacto territorial y económico, la capacidad de **monitorizar el ecosistema informativo y responder con rapidez las narrativas falsas** se convierte en un elemento adicional de la resiliencia organizativa.

Consideraciones adicionales

La gestión de este tipo de riesgos requiere combinar **capacidades de análisis de información abierta, monitorización de redes sociales, análisis de patrones de difusión y verificación de contenidos**. Además, las organizaciones deben contar con **estrategias de comunicación claras y protocolos de respuesta ante información incorrecta o manipulada**, especialmente cuando pueden afectar a la confianza pública o a la continuidad de operaciones críticas. El desarrollo de herramientas basadas en inteligencia artificial para detectar contenido manipulado e identificar campañas coordinadas está convirtiéndose en un componente relevante de las estrategias modernas de seguridad informativa.

3.2.2.4 Geopatriación (Geopatriation)

Descripción de la tendencia

La **geopatriación** describe cuyo proceso por el que **datos, infraestructuras digitales o capacidades tecnológicas son relocalizadas o mantenidas dentro de una determinada jurisdicción geográfica** por razones de seguridad, control reglamentario o autonomía tecnológica. Esta tendencia está ganando relevancia en un contexto de creciente competencia geopolítica y preocupación por la dependencia de infraestructuras tecnológicas extranjeras [33]. Como consecuencia, gobiernos y organizaciones están impulsando políticas y ayudas destinadas a **garantizar que datos críticos, sistemas digitales o servicios tecnológicos clave permanezcan bajo control territorial o jurisdiccional específico**.

Relevancia e implicaciones

La geopatriación puede influir en la forma en que las organizaciones **seleccionan proveedores tecnológicos, localizan sus datos o despliegan infraestructuras digitales**. Determinadas regulaciones europeas y nacionales están promoviendo que **datos sensibles, sistemas de control o información estratégica se almacenen o procesen dentro del espacio jurisdiccional europeo,** lo que puede afectar decisiones relacionadas con la adopción de plataformas cloud, servicios de análisis de datos o infraestructuras digitales compartidas. Esta tendencia también se relaciona con la necesidad de **evaluar riesgos asociados a la dependencia tecnológica de proveedores situados fuera del ámbito reglamentario europeo**.

Consideraciones adicionales

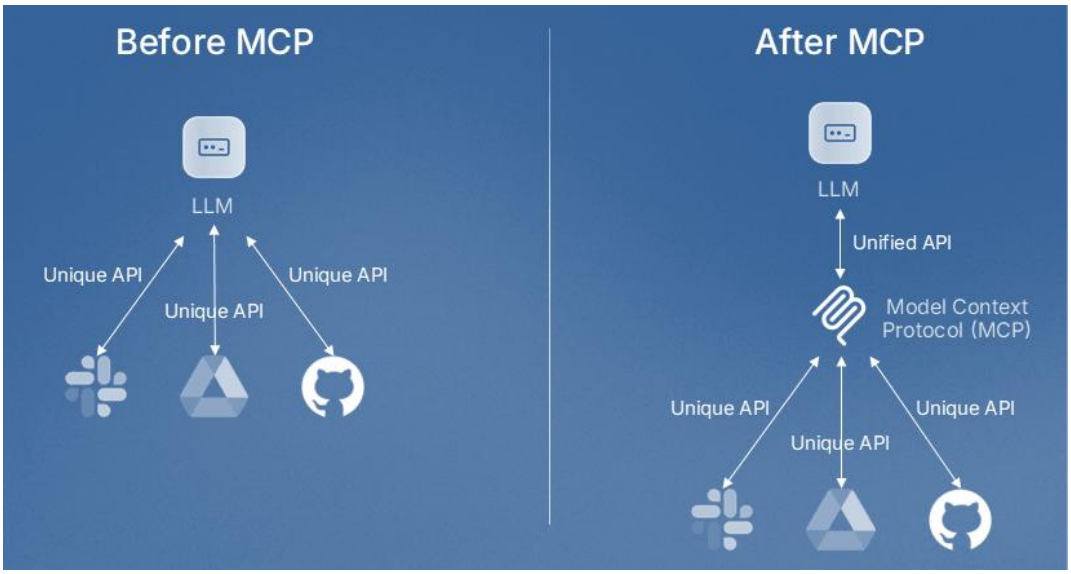
La geopatriación está estrechamente ligada a conceptos como **soberanía digital, control de las cadenas tecnológicas y resiliencia de las infraestructuras críticas**. Para las organizaciones industriales, ello puede implicar revisar la **localización de centros de datos, la procedencia de determinados servicios tecnológicos o las condiciones jurídicas aplicables al tratamiento de información industrial**. Al mismo tiempo, la evolución de las políticas europeas en materia de datos e infraestructuras digitales apunta a un escenario en el que la **ubicación y gobernanza de los datos industriales** se convertirán en un factor relevante en la planificación tecnológica de las organizaciones.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

3.2.2.5 Protocolo de contexto para modelos de IA (Model Context Protocol, MCP)

Descripción de la tendencia

El **Model Context Protocol (MCP)** es una propuesta emergente destinada a **estandarizar la forma en la que los sistemas de inteligencia artificial acceden a información, herramientas y fuentes de datos externas**. A medida que los modelos de IA pasan de funcionar como sistemas aislados a formar parte de ecosistemas más complejos —integrándose con aplicaciones empresariales, bases de datos o servicios en línea— surge la necesidad de definir **mecanismos estructurados para proporcionar contexto operativo a los modelos**.



Complejidad de integración antes y después de MCP. Fuente: Descope (2026)

El MCP propone un marco en el que aplicaciones, herramientas y modelos pueden **intercambiar información de forma controlada e interoperable**, facilitando que los sistemas de IA comprendan el entorno en el que operan y ejecuten tareas más complejas. MCP fue presentado por la empresa de IA Anthropic (creadores de Claude Code) a finales de 2024 [34].

Relevancia e implicaciones

Para organizaciones industriales que comienzan a integrar **sistemas de IA en procesos operativos, plataformas de análisis o sistemas de apoyo a la decisión**, la existencia de protocolos estandarizados para gestionar el contexto de los modelos puede facilitar la **interoperabilidad entre herramientas y la integración de IA en infraestructuras tecnológicas existentes**. En un escenario de creciente automatización basada en IA, estos protocolos pueden permitir que los modelos **accedan a datos industriales,**

documentación técnica o sistemas de monitorización de forma estructurada y controlada. Al mismo tiempo, esto requiere establecer **políticas claras de control de acceso, gestión de permisos y supervisión de las interacciones entre modelos y sistemas empresariales**.

Consideraciones adicionales

La evolución de protocolos como MCP está ligada al desarrollo de **ecosistemas de IA compuestos por múltiples modelos, agentes y servicios interconectados**. En este contexto, la forma en la que los modelos reciben contexto y acceden a datos se convierte en un elemento crítico tanto para el **rendimiento de los sistemas como para su seguridad**. Para las organizaciones industriales, ello implica prestar atención a aspectos como la **autenticación de las fuentes de datos, la trazabilidad de las interacciones de los modelos y la limitación de las capacidades de acceso de las herramientas basadas en IA**. Una implementación adecuada de estos mecanismos puede contribuir a **integrar sistemas de IA de manera más segura y controlada en las infraestructuras digitales de las organizaciones**.

3.2.2.6 Simulación inteligente (Intelligent Simulation)

Descripción de la tendencia

La **simulación inteligente** se refiere al uso combinado de **modelos de simulación, análisis avanzado de datos e inteligencia artificial** para recrear y analizar el comportamiento de sistemas complejos en un entorno virtual. Estos sistemas permiten **modelar procesos industriales, cadenas de suministro, infraestructuras u operaciones técnicas**, incorporando variables dinámicas y algoritmos de aprendizaje que mejoran la precisión de las simulaciones a lo largo del tiempo. En muchos casos, estas simulaciones se relacionan con el desarrollo de **gemelos digitales (digital twins)**, capaces de representar virtualmente instalaciones o procesos reales y anticipar su comportamiento ante diferentes escenarios. En el artículo referenciado de Gartner, se sientan diversos casos de uso [35].

Relevancia e implicaciones

Para la **industria gallega**, la simulación inteligente puede convertirse en una herramienta relevante para evaluar **cambios operativos, optimizar procesos productivos y analizar escenarios de riesgo sin afectar a la operación real de las instalaciones**. En entornos industriales complejos, estas tecnologías permiten **probar modificaciones de configuración, evaluar impactos de incidentes o analizar el**

comportamiento de sistemas interconectados antes de aplicarlos en la infraestructura real. Ello resulta especialmente útil en ámbitos como **la planificación de producción, la gestión de activos industriales o el análisis de resiliencia de las infraestructuras críticas**.

Consideraciones adicionales

La simulación inteligente también está a adquirir relevancia en el ámbito de la **ciberseguridad industrial**, ya que permite recrear entornos virtuales en los que analizar **ataques, fallos técnicos o incidentes operacionales** sin comprometer los sistemas reales. Estos entornos pueden emplearse para **evaluar vulnerabilidades, probar medidas de defensa o formar equipos técnicos en la respuesta a incidentes**. La combinación de simulación avanzada con modelos de aprendizaje automático facilita además la **identificación de patrones de comportamiento anómalo y el análisis predictivo de riesgos operacionales**, contribuyendo a reforzar la resiliencia de las infraestructuras industriales digitalizadas.

3.2.2.7 IA encarnada (Embodied AI)

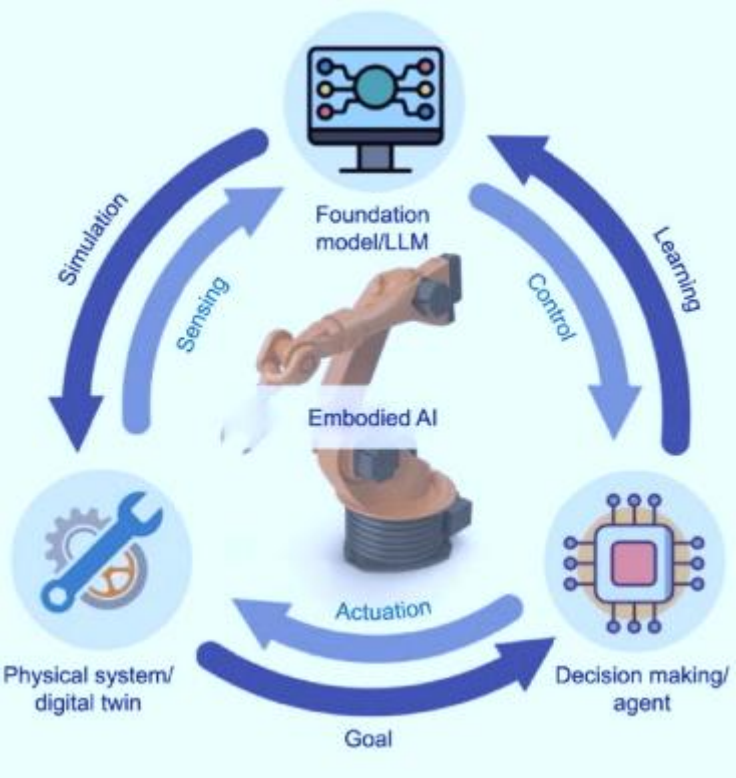
Descripción de la tendencia

La **IA encarnada (Embodied AI)** se refiere a sistemas de inteligencia artificial que **interactúan directamente con el mundo físico a través de sensores, actuadores o robots**, integrando percepción, decisión y acción en un mismo sistema [36][37]. La diferencia de los modelos de IA puramente digitales, estos sistemas están diseñados para **operar en entornos reales**, interpretando información procedente de cámaras, sensores industriales o sistemas de posicionamiento y actuando sobre máquinas o dispositivos físicos. Este enfoque está ganando relevancia con la evolución de la robótica avanzada, los sistemas autónomos y las plataformas industriales conectadas.

Relevancia e implicaciones

La IA encarnada puede tener aplicaciones en tareas como **inspección automática de instalaciones, operación de robots industriales, manipulación de materiales o mantenimiento asistido por sistemas autónomos**. La integración de sensores, visión artificial y algoritmos de aprendizaje permite que estos sistemas **interpreten el entorno industrial y ejecuten acciones con mayor grado de autonomía,** lo que puede contribuir a mejorar la productividad y la seguridad en determinadas operaciones.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027



Elementos que intervienen en la IA encarnada. Fuente: ScienceDirect (2025)

Al mismo tiempo, la introducción de sistemas capaces de actuar directamente sobre procesos físicos requiere **mecanismos robustos de supervisión, control y seguridad operativa**.

Consideraciones adicionales

La evolución de la IA encarnada está estrechamente vinculada al desarrollo de **robots colaborativos, vehículos autónomos industriales y sistemas de inspección automatizada**. Estos sistemas combinan percepción basada en sensores, análisis mediante IA y capacidad de actuación en el entorno físico. En entornos industriales, esto abre oportunidades para **automatizar tareas complejas, mejorar la seguridad laboral y reducir intervenciones humanas en operaciones de riesgo**. No obstante, también introduce nuevos retos relacionados con **la seguridad funcional, la fiabilidad de los sistemas autónomos y la protección frente a manipulaciones o fallos en los algoritmos que controlan la interacción con el mundo físico**.

3.2.2.8 IA física (Physical AI)

Descripción de la tendencia

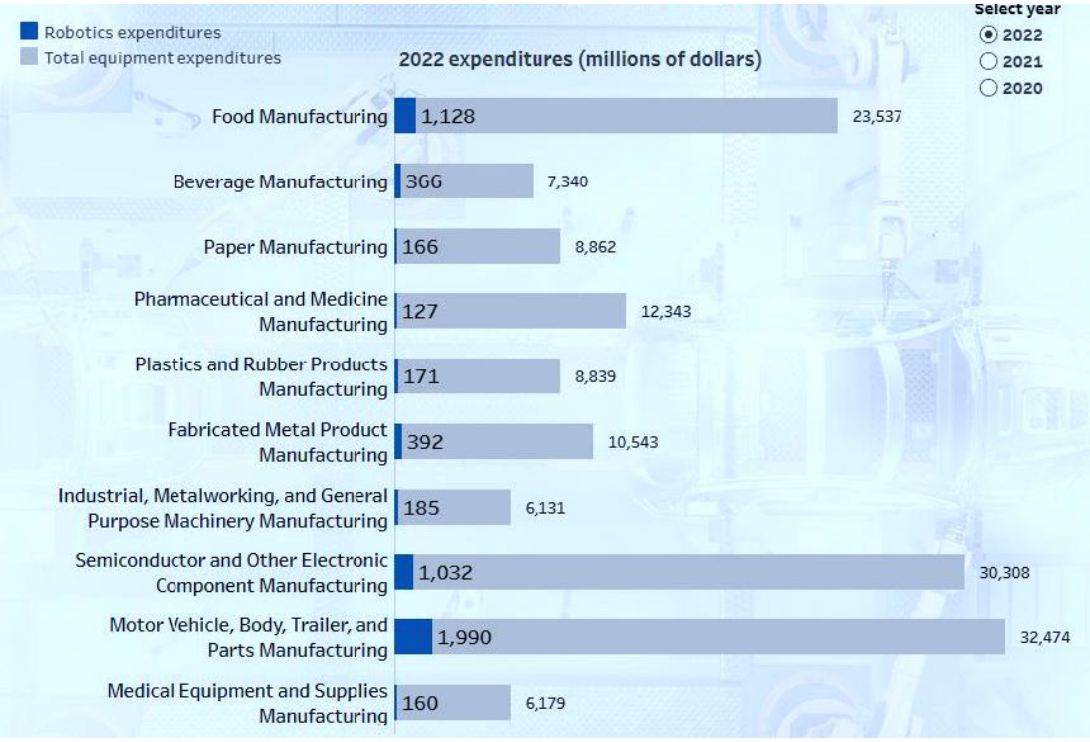
La **IA física** hace referencia a sistemas de inteligencia artificial diseñados para **interactuar directamente con entornos físicos complejos**, integrando capacidades

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

de percepción, planificación y control en máquinas o infraestructuras reales. La diferencia de la **IA encarnada** —que pone el foco en la interacción de un sistema autónomo con el entorno a través de sensores y actuadores—, la IA física se trae en **la integración de la inteligencia artificial en el funcionamiento de sistemas ciberfísicos completos**, como líneas de producción, infraestructuras industriales o sistemas energéticos [38][39]. En este enfoque, los algoritmos de IA analizan datos procedentes de sensores y toman decisiones que afectan al funcionamiento global de los procesos industriales. La evolución de la robótica avanzada, de la sensórica industrial y de la capacidad de procesamiento está facilitando el desarrollo de sistemas capaces de **adaptarse dinámicamente al entorno físico y optimizar el funcionamiento de instalaciones industriales o infraestructuras técnicas**.

Relevancia e implicaciones

Para el **tejido industrial gallego**, la IA física puede tener aplicaciones en ámbitos como **la automatización avanzada de procesos industriales como alimentación o automoción, la operación de maquinaria autónoma, la gestión inteligente de infraestructuras o la optimización de procesos energéticos**. En la siguiente figura, se muestran de forma ilustrativa las inversiones en robótica en diferentes sectores de actividad en los Estados Unidos en 2022.



Inversión en robótica en USA frente al resto de inversiones en equipo. Fuente: US Census Bureau (2022)

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Estos sistemas permiten integrar datos procedentes de sensores, sistemas de control y plataformas analíticas para **tomar decisiones operativas en tiempo real**, lo que puede mejorar la eficiencia, reducir tiempos de parada y optimizar el uso de recursos. Con todo, al tratarse de sistemas que interactúan directamente con el mundo físico, también resulta esencial garantizar **seguridad funcional, robustez de los algoritmos y mecanismos de supervisión humana**.

Consideraciones adicionales

La expansión de la IA física está ligada a la convergencia entre **inteligencia artificial, robótica, IoT industrial y sistemas de control**, configurando una nueva generación de infraestructuras industriales más autónomas y adaptativas. Esta evolución puede facilitar la creación de **fábricas más flexibles, sistemas de producción reconfigurables y operaciones industriales altamente automatizadas**. Al mismo tiempo, requiere prestar especial atención a la **seguridad de los sistemas ciberfísicos, a la protección frente a manipulaciones externas y la convalidación rigurosa de los algoritmos que controlan procesos físicos**, ya que errores o fallos en estos sistemas pueden tener impacto directo sobre instalaciones industriales o servicios críticos.

3.2.2.9 Experiencias adaptativas (Adaptive Experiences)

Descripción de la tendencia

Las **experiencias adaptativas (Adaptive Experiences)** describen sistemas digitales capaces de **ajustar dinámicamente su interfaz, comportamiento o funcionalidades en función del contexto, del perfil del usuario y de los datos de interacción**. Estos sistemas emplean técnicas de análisis de datos e inteligencia artificial para **personalizar la forma en la que se presenta la información o se ejecutan determinadas operaciones**, adaptándose a las necesidades específicas de cada usuario o situación operativa. En lugar de ofrecer una interfaz fija, las plataformas adaptativas evolucionan continuamente a partir del uso real que se hace de ellas [40].

Relevancia e implicaciones

En los entornos industriales, este enfoque puede aplicarse a **interfaces de supervisión, sistemas de apoyo a la decisión o herramientas de mantenimiento**, permitiendo que la información relevante se presente de manera distinta según el perfil del operador, el estado de la instalación o el tipo de tarea que se está realizando. Para el tejido industrial gallego, esto puede traducirse en **sistemas de control más intuitivos, mejor**

comprensión de la información operativa y reducción de errores humanos en tareas críticas. La adaptación de la interfaz también puede facilitar el trabajo de operadores con distintos niveles de experiencia o especialización.

Consideraciones adicionales

La implantación de experiencias adaptativas requiere prestar atención a la **transparencia de los algoritmos, a la trazabilidad de las decisiones y a la coherencia de las interfaces en entornos críticos**. En un sistema industrial, cambios excesivos o poco previsibles en la interfaz pueden dificultar la operación en situaciones de estrés o emergencia. Por este motivo, el diseño de estas soluciones debe equilibrar **adaptabilidad y estabilidad operativa**, garantizando que la personalización mejore la usabilidad sin comprometer la seguridad ni la comprensión del sistema por parte de los operadores.

3.2.2.10 Robots humanoides de trabajo (Humanoid Working Robots)

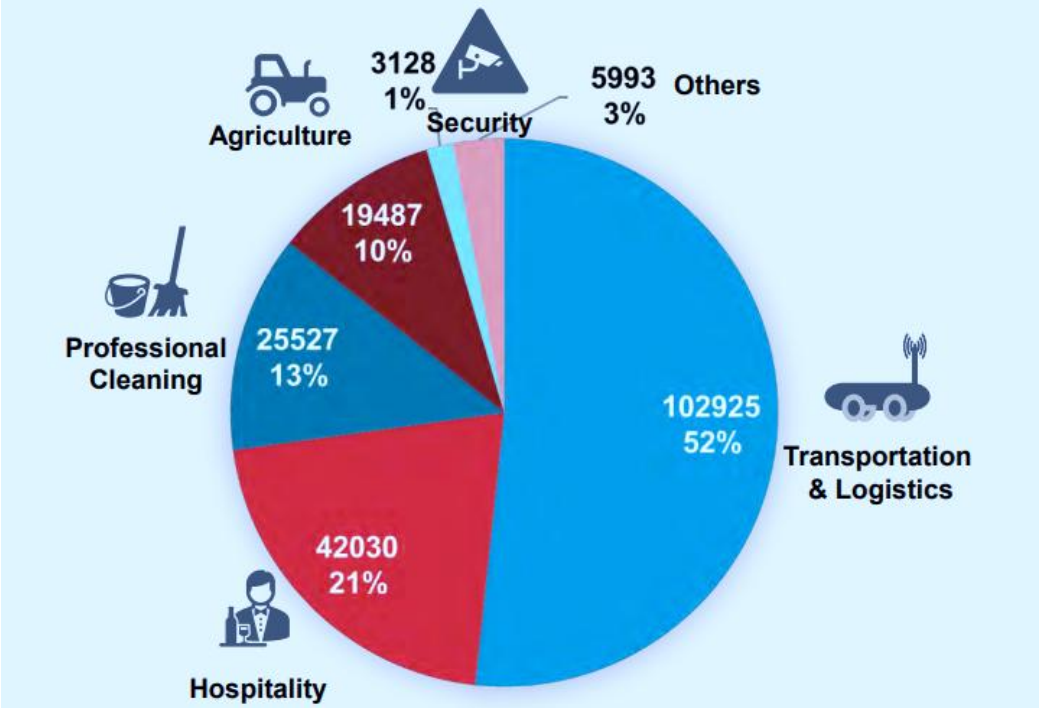
Descripción de la tendencia

Los **robots humanoides de trabajo** se refieren a sistemas robóticos diseñados con una **morfología similar a la humana**, capaces de realizar tareas físicas en entornos pensados originalmente para personas. Estos robots integran **sensores avanzados, visión artificial, control motor y algoritmos de inteligencia artificial**, lo que les permite interactuar con el entorno físico, manipular objetos y ejecutar tareas complejas en espacios industriales o logísticos. El interés por este tipo de sistemas ha aumentado recientemente gracias a los avances en **robótica, IA y sistemas de percepción**, que están haciendo viable su utilización en tareas reales.

Relevancia e implicaciones

En entornos industriales, los robots humanoides pueden utilizarse para **realizar tareas repetitivas, peligrosas o físicamente exigentes**, como manipulación de materiales, inspección de instalaciones u operación en espacios de difícil acceso. Para el **tejido industrial gallego**, caracterizado por la presencia de sectores como la automoción, la logística, la construcción naval o la industria alimentaria, estas tecnologías podrían contribuir a **aumentar la automatización de determinadas operaciones y reducir riesgos laborales**. Además, el diseño humanoide permite que estos robots **operen en infraestructuras existentes sin necesidad de rediseñar completamente los espacios de trabajo**. Según la Federación Internacional de Robótica el año pasado en

un estudio de casi mil fabricantes a nivel mundial, el 52% de los robots se dedicaron a labores de transporte y logística, con un crecimiento de un 14% interanual [41].



Sector de actividad de aplicación de robots. Fuente: Federación Internacional de Robótica (2025)

Consideraciones adicionales

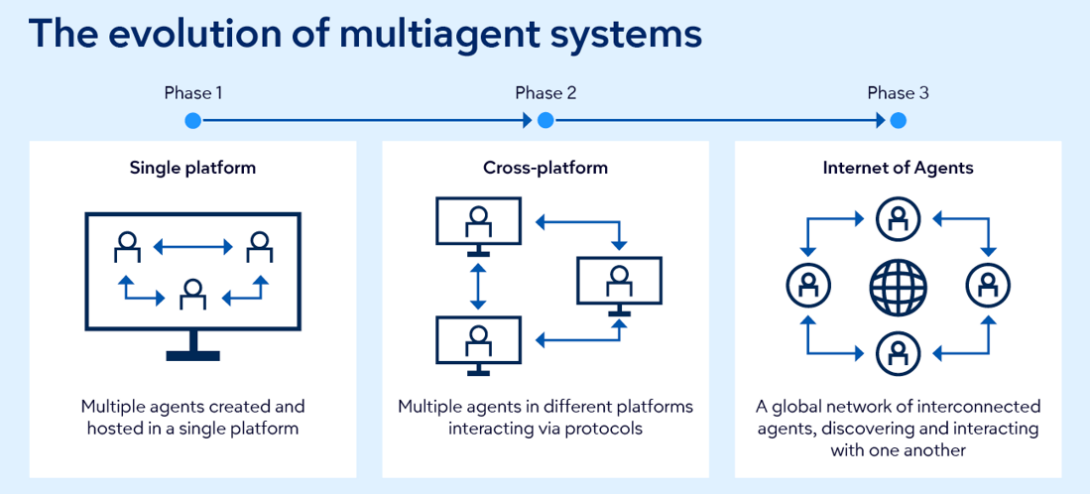
La introducción de robots humanoides también suscita cuestiones relacionadas con la **seguridad operativa, la convivencia entre trabajadores humanos y sistemas robóticos y la fiabilidad de los sistemas autónomos**. En entornos industriales, resulta fundamental garantizar **protocolos claros de seguridad, mecanismos de parada segura y sistemas de supervisión** que permitan controlar el comportamiento de estas máquinas. Al mismo tiempo, la evolución de estas tecnologías podría facilitar nuevas formas de colaboración humano-máquina, en las que los robots humanoides actúen como **asistentes físicos en tareas industriales o de mantenimiento**.

3.2.2.11 IA multiagente orientada a clientes (Multiagent AI)

Descripción de la tendencia

La **IA multiagente** se arroja a sistemas en los que **múltiples agentes de inteligencia artificial colaboran entre sí para resolver tareas complejas**, coordinando decisiones e intercambiando información en un mismo ecosistema digital [42]. Cada agente puede estar especializado en una función concreta —por ejemplo, análisis de datos, planificación de tareas, interacción con usuarios o ejecución de acciones— y trabaja de

manera coordinada con los demás para alcanzar un objetivo común. Este enfoque permite construir **arquitecturas de IA distribuidas y más flexibles**, en las que diferentes modelos cooperan y se adaptan al contexto operativo.



Evolución de los sistemas de IA multiagente. Fuente: Gartner (2025)

Relevancia e implicaciones

En los entornos industriales y empresariales, los sistemas multiagente pueden aplicarse a **procesos de atención a clientes, gestión de cadenas de suministro, planificación de producción o análisis de datos operacionales**. Para el tejido industrial gallego, este tipo de arquitecturas puede facilitar la creación de **plataformas inteligentes capaces de coordinar información procedente de múltiples sistemas empresariales**, integrando datos de producción, logística o mantenimiento. La cooperación entre agentes permite también **automatizar flujos de decisión más complejos**, en los que diferentes sistemas analizan información y proponen acciones de manera coordinada.

Consideraciones adicionales

La adopción de sistemas multiagente requiere prestar atención a aspectos como la **coordinación entre modelos, la gestión de permisos de acceso a la información y la supervisión de las decisiones tomadas por los distintos agentes**. Cuando estos sistemas interactúan con datos empresariales o industriales sensibles, resulta esencial establecer **mecanismos de control, trazabilidad y convalidación de las acciones ejecutadas por los agentes**. Un diseño adecuado de estas arquitecturas permite aprovechar las ventajas de la cooperación entre sistemas de IA manteniendo **niveles adecuados de seguridad y gobernanza tecnológica**.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

3.2.2.12 Infiltración de la IA en el aprovisionamiento B2B

Descripción de la tendencia

La creciente integración de la **inteligencia artificial en los procesos de aprovisionamiento entre empresas (B2B)** está transformando la forma en la que las organizaciones **analizan proveedores, negocian condiciones comerciales y gestionan contratos**. Sistemas basados en IA pueden examinar grandes volúmenes de datos de mercado, histórico de compras, rendimiento de proveedores y condiciones contractuales para **automatizar tareas de análisis, recomendación y toma de decisiones en el proceso de compra**. Además, la aparición de **agentes de IA capaces de interactuar con plataformas comerciales y sistemas empresariales** está facilitando la automatización parcial de negociaciones, selección de proveedores u optimización de cadenas de suministro.

Según Boston Consulting Group, las empresas más avanzadas ya están probando estos sistemas, que operan de forma continua y requieren respuestas rápidas y precisas sobre **precios, promociones, disponibilidad de inventario y plazos de entrega** [43].

Visión del enfoque agéntico en el aprovisionamiento B2B. Fuente: BCG (2025)

Relevancia e implicaciones

Para el **tejido industrial gallego**, caracterizado por la integración en cadenas de valor complejas y por la dependencia de múltiples proveedores tecnológicos e industriales, estas capacidades pueden mejorar **la eficiencia en la gestión de compras, la identificación de riesgos en la cadena de suministro y la optimización de costes operativos**. Sistemas de IA pueden analizar información procedente de diferentes fuentes para **evaluar la fiabilidad de proveedores, detectar posibles**

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

interrupciones en la cadena de suministro o identificar oportunidades de mejora en las condiciones contractuales.

Consideraciones adicionales

La incorporación de IA en los procesos de aprovisionamiento también introduce nuevos retos relacionados con la **transparencia de las decisiones automatizadas, la protección de información comercial sensible y la supervisión de las interacciones entre sistemas automatizados de distintas organizaciones**. En un escenario en el que algoritmos o agentes de IA participan en el análisis de ofertas o en la negociación de condiciones comerciales, resulta necesario establecer **mecanismos de gobernanza, trazabilidad de las decisiones y control humano en las etapas críticas del proceso**. La evolución de estos sistemas podría llevar a entornos en los que **plataformas empresariales, proveedores y sistemas de IA interactúen de manera cada vez más automatizada**, redefiniendo el funcionamiento tradicional de los mercados B2B.

3.2.2.13 Ascenso de las plataformas digitales estatales

Descripción de la tendencia

En los últimos años está emergiendo una nueva generación de **plataformas digitales impulsadas por estados o administraciones públicas**, diseñadas para ofrecer infraestructuras comunes de identidad digital, intercambio de datos, servicios administrativos e integración entre organismos públicos y empresas. Estas plataformas funcionan como **ecosistemas tecnológicos compartidos**, en los que diferentes organizaciones pueden desarrollar servicios digitales sobre una infraestructura común que garantice integración, seguridad y gobernanza de los datos. Ejemplos de este enfoque incluyen sistemas de **identidad digital, plataformas de datos públicos o infraestructuras de servicios digitales interoperables**. El Foro Económico Mundial lo considera un asunto clave para el futuro conectado [44][45].

Relevancia e implicaciones

Para el **tejido industrial gallego**, la expansión de estas plataformas puede facilitar una **mayor integración entre empresas y administraciones públicas**, simplificando procesos como la gestión de permisos, la presentación de información regulatoria o la participación en ecosistemas de datos industriales. La existencia de infraestructuras digitales estatales también puede favorecer la creación de **espacios de datos**

sectoriales, plataformas de innovación o sistemas de intercambio seguro de información entre empresas, organismos públicos y centros de investigación.

Consideraciones adicionales

El desarrollo de estas plataformas requiere prestar especial atención a la seguridad de las **infraestructuras digitales públicas, a la gobernanza de los datos compartidos y a la protección de la identidad digital de los usuarios**. Al convertirse en elementos centrales del ecosistema digital, estas plataformas pueden concentrar grandes volúmenes de información e interacciones críticas, por lo que deben diseñarse con **arquitecturas resilientes, mecanismos de autenticación robustos y controles estrictos de acceso a la información**. La evolución de este modelo apunta hacia administraciones públicas que operan como **plataformas digitales abiertas**, capaces de integrar servicios públicos y privados en un mismo ecosistema tecnológico.

3.2.2.14 Programación asistida por IA ("Vibe Coding")

Descripción de la tendencia

El llamado **"Vibe Coding"** describe un nuevo paradigma de desarrollo de software en el que **modelos de inteligencia artificial generativa participan activamente en la creación, modificación y revisión de código**. Herramientas basadas en modelos de lenguaje avanzados pueden interpretar instrucciones en lenguaje natural y transformarlas en fragmentos de código, estructuras de aplicaciones o soluciones técnicas completas. Este enfoque permite que desarrolladores y equipos técnicos **prototipen aplicaciones más rápidamente, automaticen tareas repetitivas de programación y exploren nuevas soluciones mediante interacción directa con sistemas de IA.** En opinión de Gartner es un cambio de paradigma que tendrá repercusión y adopción [46].

Relevancia e implicaciones

En el contexto de las organizaciones industriales, esta tendencia puede facilitar el **desarrollo más ágil de herramientas internas, scripts de automatización, sistemas de integración entre plataformas o aplicaciones de análisis de datos industriales**. Para el tejido productivo gallego, caracterizado por la presencia de pequeñas y medianas empresas con recursos limitados en desarrollo de software, estas herramientas pueden **reducir barreras técnicas y acelerar la creación de soluciones digitales adaptadas a las necesidades operativas**. Al mismo tiempo, el uso de código generado por IA

requiere **revisión técnica rigurosa y controles de calidad**, especialmente en entornos en los que el software interactúa con infraestructuras industriales o sistemas críticos.

Consideraciones adicionales

La expansión de este paradigma también introduce retos relacionados con la **seguridad del software, la trazabilidad del código generado y la protección de la propiedad intelectual**. El uso de modelos de IA en el proceso de desarrollo puede generar dependencias tecnológicas e introducir vulnerabilidades si el código generado no es revisado adecuadamente. Por este motivo, resulta recomendable integrar estas herramientas dentro de **procesos de desarrollo seguros, revisión de código y prácticas de seguridad desde el diseño**, garantizando que la productividad adicional no comprometa la fiabilidad ni la seguridad de las aplicaciones desarrolladas.

3.2.2.15 Computación espacial (Spatial Computing)

Descripción de la tendencia

La **computación espacial (Spatial Computing)** engloba tecnologías que permiten **interactuar con información digital integrada en el espacio físico**, combinando realidad aumentada (AR), realidad virtual (VR), sensores espaciales, visión artificial y modelado tridimensional. Estos sistemas permiten que usuarios y máquinas **visualicen y manipulen información digital directamente sobre el entorno físico**, creando interfaces tridimensionales que integran datos operativos, simulaciones o modelos virtuales en el propio espacio de trabajo [47][48].

Relevancia e implicaciones

En los entornos industriales, la computación espacial puede emplearse para **visualización avanzada de instalaciones, asistencia en tareas de mantenimiento, formación técnica o supervisión de procesos industriales complejos**. Mediante dispositivos de realidad aumentada o entornos virtuales, los operadores pueden acceder a **instrucciones contextuales, modelos 3D de equipos o datos en tiempo real sobre el estado de las máquinas**. Para el tejido industrial gallego, ello puede facilitar **la transferencia de conocimiento técnico, la reducción de errores operativos y la mejora de la eficiencia en tareas de inspección o reparación**.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Tres elementos industriales generados mediante computación espacial en gafas 3D. Fuente: Foxconn (2025)

Consideraciones adicionales

La adopción de estas tecnologías también introduce desafíos relacionados con la **integración de sistemas industriales con plataformas de visualización avanzada, la protección de la información técnica y la fiabilidad de las interfaces utilizadas en operaciones críticas**. En entornos industriales, los sistemas de computación espacial deben diseñarse garantizando **precisión en la representación del entorno, sincronización con los sistemas de control y protección de los datos operacionales** que se visualizan en los dispositivos. Cuando se implementan adecuadamente, estas tecnologías pueden convertirse en una herramienta relevante para **mejorar la comprensión de sistemas complejos y apoyar la toma de decisiones operativas**.

3.2.3 De vigilancia estratégica (prioridad #3)

3.2.3.1 Inteligencia Artificial General (AGI)

Descripción de la tendencia

La **Inteligencia Artificial General (Artificial General Intelligence, AGI)**, aunque con múltiples concepciones en la literatura, puede referirse a sistemas de inteligencia artificial capaces de **comprender, aprender y aplicar conocimiento de manera amplia en múltiples dominios**, con un nivel de flexibilidad cognitiva comparable al de la inteligencia humana. La diferencia de los sistemas actuales de IA —que adoptan estar especializados en tareas concretas—, la AGI implicaría la capacidad de **resolver problemas diversos, transferir aprendizajes entre contextos distintos y adaptarse**

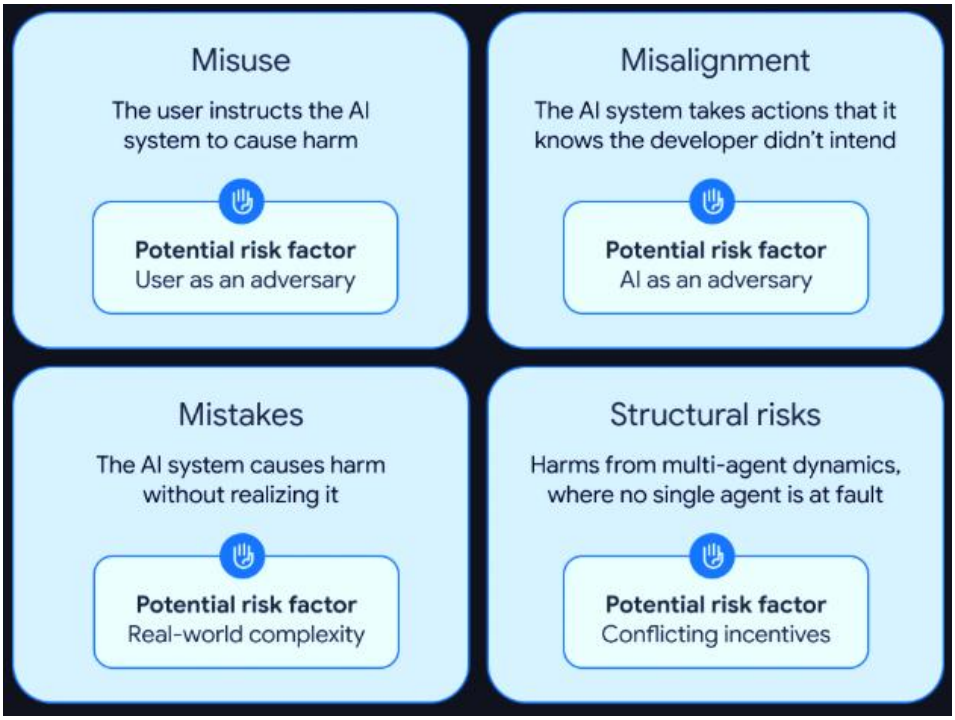
a situaciones nuevas sin necesidad de reentrenamiento específico. Actualmente se declara un objetivo de investigación a medio-largo plazo en el campo de la IA.

Relevancia e implicaciones

Aunque la AGI se sitúa en un horizonte tecnológico más alejado, su posible aparición podría tener **implicaciones profundas en la organización de las actividades económicas, industriales y científicas**. Sistemas con capacidad general de aprendizaje podrían asumir tareas complejas de análisis, planificación o diseño en ámbitos como la investigación tecnológica, la optimización de procesos industriales o la gestión de infraestructuras críticas. Para el ecosistema industrial gallego, esto podría traducirse **en una aceleración significativa de la innovación tecnológica y de la automatización de procesos de alto valor cognitivo**.

Consideraciones adicionales

El desarrollo de AGI también suscita cuestiones relevantes relacionadas con la **seguridad de los sistemas de IA, la gobernanza tecnológica y el impacto socioeconómico de la automatización avanzada**. Entre los retos asociados se incluyen **la alineación de los sistemas de IA con los objetivos humanos, el control de sistemas altamente autónomos y la evaluación de los riesgos asociados a capacidades tecnológicas muy avanzadas**.



Principales riesgos asociados a la AGI. Fuente: Google DeepMind (2025)

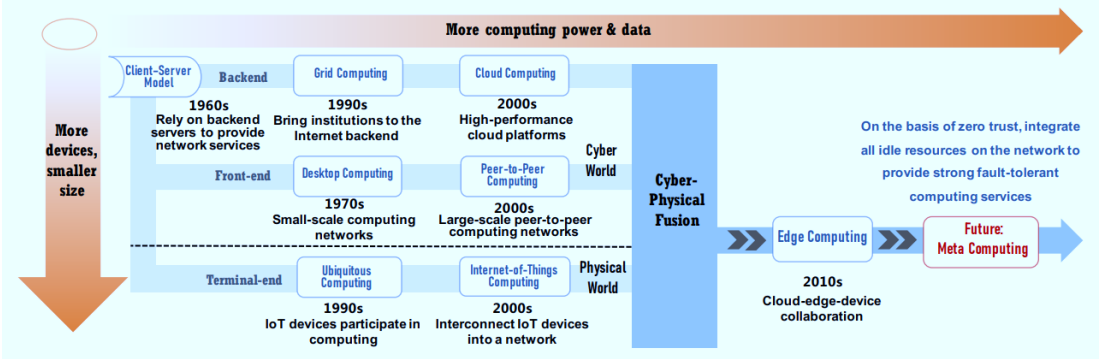
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Por este motivo, numerosos organismos y centros de investigación están analizando los posibles escenarios de desarrollo de la AGI y las medidas necesarias para garantizar un **despliegue seguro y responsable de estas tecnologías en el futuro** [49][50].

3.2.3.2 Meta-computación (Meta Computing)

Descripción de la tendencia

La **meta-computación (Meta Computing)** describe un enfoque en el que los sistemas informáticos son capaces de **coordinar, gestionar y optimizar automáticamente múltiples recursos computacionales distribuidos**, incluyendo cloud, edge computing, infraestructuras locales y plataformas especializadas de procesamiento [51]. En este paradigma, las aplicaciones y los sistemas de IA pueden **decidir dinámicamente donde y como ejecutar determinadas tareas**, adaptándose a la disponibilidad de recursos, a los requisitos de rendimiento o a las condiciones operativas del sistema.



Historia de los paradigmas de computación. Fuente: Scispace (paper Cheng, X. et. al., 2020)

Relevancia e implicaciones

En un contexto de creciente complejidad tecnológica, en el que las organizaciones combinan **infraestructuras cloud, entornos industriales conectados, dispositivos IoT y sistemas de análisis de datos**, la meta-computación puede facilitar una **gestión más eficiente de la capacidad de procesado y de los flujos de información**. Para el tejido industrial gallego, esto podría traducirse en arquitecturas tecnológicas capaces de **adaptar automáticamente la ejecución de procesos analíticos, simulaciones o sistemas de IA** según las condiciones operativas de las infraestructuras disponibles.

Consideraciones adicionales

La evolución hacia modelos de meta-computación está ligada al desarrollo de **arquitecturas distribuidas, plataformas de orquestación avanzada y sistemas de**

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

inteligencia artificial capaces de optimizar el uso de recursos computacionales. Este enfoque puede resultar especialmente relevante en entornos donde los sistemas deben combinar **procesamiento en tiempo real, análisis avanzado de datos e integración entre múltiples plataformas tecnológicas**. Al mismo tiempo, también requiere prestar atención a la **seguridad de las infraestructuras distribuidas, a la protección de los flujos de datos y a la gobernanza de las plataformas tecnológicas que participan en el ecosistema computacional.**

3.2.3.3 Comerciantes máquina (Machine Customers & Sellers)

Descripción de la tendencia

Los **comerciantes máquina** se añaden a **sistemas automatizados capaces de actuar como agentes económicos en procesos de compra y venta**, ejecutando **transacciones comerciales de forma autónoma** en nombre de personas u organizaciones. Estos sistemas, basados en **inteligencia artificial, analítica de datos e integración con plataformas digitales**, **pueden analizar información de mercado, comparar ofertas, negociar condiciones comerciales y completar operaciones de compra o venta sin intervención humana directa**.

La evolución de los **sistemas de agentes inteligentes, del comercio electrónico avanzado y de la automatización empresarial** está facilitando la aparición de **ecosistemas digitales en los que software y sistemas inteligentes participan directamente en interacciones comerciales**, ampliando el papel de los sistemas automatizados más allá de las funciones tradicionales de recomendación o asistencia [52].

Relevancia e implicaciones

En el contexto industrial y empresarial, los comerciantes máquina pueden intervenir **tanto en procesos de adquisición como de comercialización de productos o servicios**. Por una banda, pueden **identificar necesidades de suministro, analizar opciones disponibles y ejecutar pedidos de forma automatizada**; por otra, pueden **ofrecer productos, adaptar precios según la demanda o responder a solicitudes comerciales en tiempo real**.

Evolución prevista del modelo de cliente máquina. Fuente: Gartner (2022)

Para el **tejido industrial gallego**, esta tendencia podría traducirse en **sistemas capaces de supervisar inventarios, optimizar cadenas de suministro, gestionar ventas digitales o interactuar con plataformas comerciales automatizadas**, permitiendo **reducir tiempos de respuesta, mejorar la eficiencia operativa y optimizar la gestión de recursos**.

Consideraciones adicionales

La aparición de comerciantes máquina introduce **nuevos retos relacionados con la regulación de las transacciones automatizadas, la responsabilidad legal de las decisiones tomadas por sistemas autónomos y la seguridad de las plataformas comerciales digitales**. Además, la interacción entre distintos sistemas automatizados —por ejemplo, entre **clientes máquina y vendedores máquina**— podría dar lugar a **ecosistemas económicos parcialmente automatizados**, en los que **negociaciones y transacciones se realicen directamente entre agentes software**.

En este escenario, las organizaciones deberán **adaptarse a nuevas dinámicas comerciales digitales y establecer mecanismos de supervisión que garanticen transparencia, seguridad y control sobre los procesos automatizados**, especialmente en entornos en los que **software y agentes inteligentes interactúan directamente en mercados digitales**.

3.2.3.4 Aprovisionamiento autónomo (Autonomous Sourcing)

Descripción de la tendencia

El **aprovisionamiento autónomo** se refiere al uso de **sistemas automatizados e inteligencia artificial para identificar necesidades de suministro, seleccionar proveedores y ejecutar procesos de compra de forma autónoma**. Estos sistemas pueden **analizar datos operativos, niveles de inventario, previsiones de demanda**

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

o condiciones de mercado, permitiendo **activar procesos de adquisición sin intervención humana directa**.

La evolución de la **analítica avanzada, de la inteligencia artificial aplicada a la gestión empresarial y de las plataformas digitales de compras** está permitiendo que determinados procesos de aprovisionamiento sean **automatizados de extremo a extremo**, desde la detección de la necesidad hasta la ejecución del pedido y el seguimiento de la entrega.

Relevancia e implicaciones

En el ámbito industrial y empresarial, el aprovisionamiento autónomo puede contribuir a **optimizar la gestión de cadenas de suministro y reducir tiempos de respuesta en los procesos de adquisición**. Los sistemas pueden **monitorizar continuamente los niveles de inventario, detectar necesidades de reposición y seleccionar automáticamente proveedores según criterios de coste, disponibilidad o calidad**. Esta tendencia podría traducirse en **sistemas capaces de gestionar automáticamente pedidos de materias primas, componentes o servicios necesarios para la producción**, mejorando la **eficiencia operativa, la planificación de recursos y la resiliencia de las cadenas de suministro** [53].

Consideraciones adicionales

La implantación de sistemas de aprovisionamiento autónomo introduce **nuevos retos relacionados con la gobernanza de los procesos de compra automatizados, la transparencia de las decisiones algorítmicas y la seguridad de las plataformas digitales de suministro**. Además, el uso de estos sistemas puede **modificar las relaciones tradicionales entre empresas y proveedores**, al integrar **plataformas digitales, mercados electrónicos y sistemas automatizados de negociación**.

En este contexto, será necesario establecer **mecanismos de supervisión, auditoría y control que garantan la fiabilidad de las decisiones automatizadas**, así como **marcos normativos que regulen la responsabilidad y la seguridad en los procesos de adquisición basados en sistemas autónomos.**

3.2.3.5 Compañero cibernético (Cybernetic Teammate)

Descripción de la tendencia

El **compañero cibernético** se refiere a la aparición de **sistemas de inteligencia artificial diseñados para colaborar activamente con personas en tareas**

profesionales, actuando como **asistentes avanzados capaces de participar en procesos de toma de decisiones, análisis de información o ejecución de tareas complejas**.

La diferencia de los sistemas tradicionales de automatización, estos sistemas están orientados a **trabajar junto a los profesionales humanos**, proporcionando **apoyo cognitivo, análisis de datos en tiempo real y recomendaciones basadas en inteligencia artificial**. La evolución de la **IA generativa, de los modelos lingüísticos avanzados y de las plataformas de colaboración digital** está facilitando la integración de estos sistemas en entornos laborales cada vez más complejos, que permiten optimizar los tiempos de repuesta (hasta un 16% según un estudio de Harvard, a la vez que mejorando la calidad de las propuestas formuladas) [54][55].

Relevancia e implicaciones

En el ámbito empresarial e industrial, los compañeros cibernéticos pueden **apoyar a profesionales en tareas como análisis de datos, gestión de conocimiento, planificación operativa o supervisión de procesos**. Estos sistemas pueden **interpretar grandes volúmenes de información, detectar patrones y sugerir acciones**, contribuyendo a **mejorar la toma de decisiones y la eficiencia organizativa**.

Para el **tejido empresarial gallego**, esta tendencia podría materializarse en **sistemas de apoyo a la toma de decisiones, asistentes inteligentes para equipos técnicos o herramientas de colaboración basadas en IA**, capaces de **incrementar la productividad y facilitar la gestión de entornos complejos como cadenas de suministro, operaciones industriales o análisis de riesgo**.

Consideraciones adicionales

La incorporación de compañeros cibernéticos en los entornos laborales también introduce **nuevos desafíos relacionados con la confianza en los sistemas automatizados, la supervisión humana de las decisiones algorítmicas y la protección de la información sensible utilizada por estos sistemas**. Además, la integración de estos sistemas puede **modificar dinámicas organizativas y procesos de trabajo**, requiriendo nuevas **competencias profesionales y modelos de colaboración entre personas y sistemas inteligentes**.

En este contexto, será necesario establecer **marcos de gobernanza que garanticen la transparencia, la seguridad y la responsabilidad en el uso de sistemas de**

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

inteligencia artificial colaborativa, asegurando que estos sistemas **complementen las capacidades humanas sin sustituir a los mecanismos de control y supervisión necesarios**.

3.2.3.6 Descarga cognitiva (Cognitive Offloading)

Descripción de la tendencia

La **descarga cognitiva** se refiere al proceso por el cual las personas **delegan tareas cognitivas —como recordar información, analizar datos o tomar decisiones— en sistemas tecnológicos**, especialmente en herramientas basadas en **inteligencia artificial, asistentes digitales y sistemas de apoyo a la decisión**. Este fenómeno, ya presente desde la aparición de herramientas como buscadores o sistemas de navegación, está intensificada con la expansión de la **IA generativa y de los sistemas avanzados de automatización cognitiva**.

La capacidad de estos sistemas para **procesar grandes volúmenes de información, sintetizar conocimiento y proporcionar recomendaciones en tiempo real** está permitiendo que determinadas tareas intelectuales sean externalizadas a herramientas tecnológicas, modificando la forma en que las personas interactúan con la información y toman decisiones.

Relevancia e implicaciones

En el ámbito profesional y empresarial, la descarga cognitiva puede contribuir a **reducir la carga mental asociada a la gestión de información compleja**, permitiendo que los profesionales se centren en **tareas estratégicas o creativas** mientras los sistemas tecnológicos realizan procesos de análisis, filtrado o síntesis de información.

Este fenómeno en la industria podría traducirse en el uso de **sistemas de apoyo a la toma de decisiones, herramientas de análisis automatizado de datos o asistentes inteligentes para tareas técnicas y operativas**, facilitando **la gestión de conocimiento, el análisis de riesgos o la planificación de procesos**.

Consideraciones adicionales

La extensión de la descarga cognitiva también introduce **nuevos desafíos relacionados con la dependencia tecnológica, la pérdida potencial de habilidades cognitivas o la confianza excesiva en los sistemas automatizados**. Además, el uso intensivo de sistemas basados en IA para tareas intelectuales puede **modificar procesos de aprendizaje, toma de decisiones y gestión del conocimiento en las organizaciones**.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

En este contexto, será necesario desarrollar **estrategias de uso responsable de estas herramientas**, garantizando que la tecnología **complemente las capacidades humanas sin sustituir el pensamiento crítico o la supervisión profesional, ni degradando las cualidades mentales humanas** (lazy-thinking) [56]. La investigación reciente destaca que la externalización de procesos cognitivos hacia sistemas digitales puede mejorar la eficiencia, pero requiere **modelos equilibrados de colaboración entre personas y sistemas inteligentes**.

3.2.3.7 Conocimiento fluido (Fluid Knowledge)

Descripción de la tendencia

El **conocimiento fluido** se refiere a un modelo emergente de creación, distribución y uso del conocimiento en el que la información **circula de manera dinámica entre personas, organizaciones y sistemas digitales**, adaptándose continuamente a los contextos y necesidades. En este paradigma, el conocimiento **deja de estar almacenado de forma estática en documentos o repositorios** para convertirse en un recurso **dinámico, distribuido y continuamente actualizado**, facilitado por tecnologías como **inteligencia artificial, plataformas colaborativas y sistemas avanzados de gestión de la información** [57].

La expansión de herramientas basadas en **IA generativa, motores de búsqueda semánticos y sistemas de recomendación** está permitiendo que el conocimiento sea **generado, contextualizado y adaptado en tiempo real**, favoreciendo nuevas formas de colaboración y aprendizaje dentro de las organizaciones.

Relevancia e implicaciones

En el ámbito empresarial e industrial, el conocimiento fluido puede contribuir a **mejorar la capacidad de las organizaciones para acceder, interpretar y utilizar información relevante en tiempo real**. Sistemas basados en inteligencia artificial pueden **integrar datos procedentes de múltiples fuentes, identificar patrones y proporcionar recomendaciones contextualizadas**, facilitando procesos como la **toma de decisiones, la innovación o la resolución de problemas complejos**.

Para el **tejido empresarial gallego**, esta tendencia podría materializarse en **plataformas de gestión de conocimiento basadas en IA, sistemas de documentación inteligente o herramientas colaborativas que permitan compartir y actualizar información de forma continua**, mejorando la **eficiencia organizativa y la transferencia de conocimiento entre equipos y organizaciones**.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Consideraciones adicionales

La adopción de modelos de conocimiento fluido también introduce nuevos **retos relacionados con la fiabilidad de la información, la gobernanza del conocimiento y la protección de datos sensibles**. Además, la dependencia de sistemas automatizados para la generación o interpretación de información puede **incrementar el riesgo de difusión de información incorrecta o descontextualizada**, especialmente cuando los sistemas se basan en modelos de inteligencia artificial.

En este contexto, será necesario establecer **mecanismos de convalidación, supervisión y gobernanza de la información**, garantizando que los sistemas que facilitan el conocimiento fluido mantengan **estándares adecuados de calidad, trazabilidad y seguridad de la información.**

3.2.3.8 Interfaces bidireccionales cerebro-máquina

Descripción de la tendencia

Las **interfaces bidireccionales cerebro-máquina** se refieren a sistemas tecnológicos capaces de **establecer comunicación directa entre el cerebro humano y dispositivos digitales**, permitiendo **transmitir información en ambos sentidos: del cerebro al sistema y del sistema al cerebro**. Estas tecnologías combinan **neurociencia, sensores biomédicos, inteligencia artificial y sistemas de procesamiento de señales** para interpretar actividad neuronal y traducirla en comandos digitales o, en el sentido inverso, estimular el sistema nervioso mediante señales eléctricas u otros métodos.

La evolución reciente de las **tecnologías neurotecnológicas, de los sistemas de lectura neuronal no invasivos y de la inteligencia artificial aplicada al procesamiento de señales cerebrales** está a acelerar el desarrollo de estas interfaces, abriendo nuevas posibilidades de interacción entre humanos y sistemas digitales.

Relevancia e implicaciones

En el ámbito sanitario, estas tecnologías pueden permitir **restaurar o mejorar capacidades motoras o sensoriales en personas con lesiones neurológicas**, facilitando la comunicación o el control de dispositivos mediante señales cerebrales. En otros ámbitos, como la industria o los servicios tecnológicos, las interfaces cerebro-máquina podrían **habilitar nuevas formas de interacción humano-máquina**,

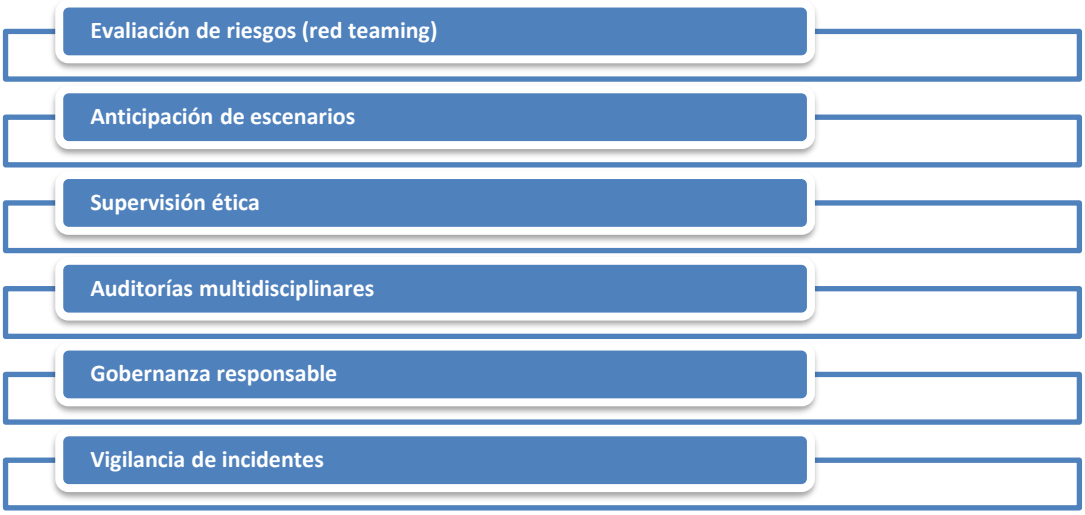
reduciendo barreras entre pensamiento y acción en determinados sistemas tecnológicos.

Consideraciones adicionales

El desarrollo de estas tecnologías también introduce **importantes cuestiones éticas, legales y de seguridad**, relacionadas con **la privacidad de la actividad cerebral, la protección de datos neurobiológicos y los posibles riesgos asociados a la manipulación o acceso no autorizado a señales neuronales**. Además, la integración de estas interfaces en entornos tecnológicos avanzados puede requerir **nuevos marcos regulatorios y estándares de seguridad específicos para las neurotecnologías**.

En este contexto, organismos internacionales y centros de investigación están destacando la necesidad de **garantizar principios de transparencia, control humano y protección de la integridad cognitiva** en el desarrollo de interfaces cerebro-máquina, especialmente a medida que estas tecnologías evolucionen hacia sistemas más avanzados de interacción bidireccional.

Las recomendaciones específicas de la OCDE (Organización para la Cooperación y el Desarrollo Económico) del informe anterior, son las siguientes:



Recomendaciones de la OCDE en el ámbito de la neurotecnología. Fuente: OCDE (2025)

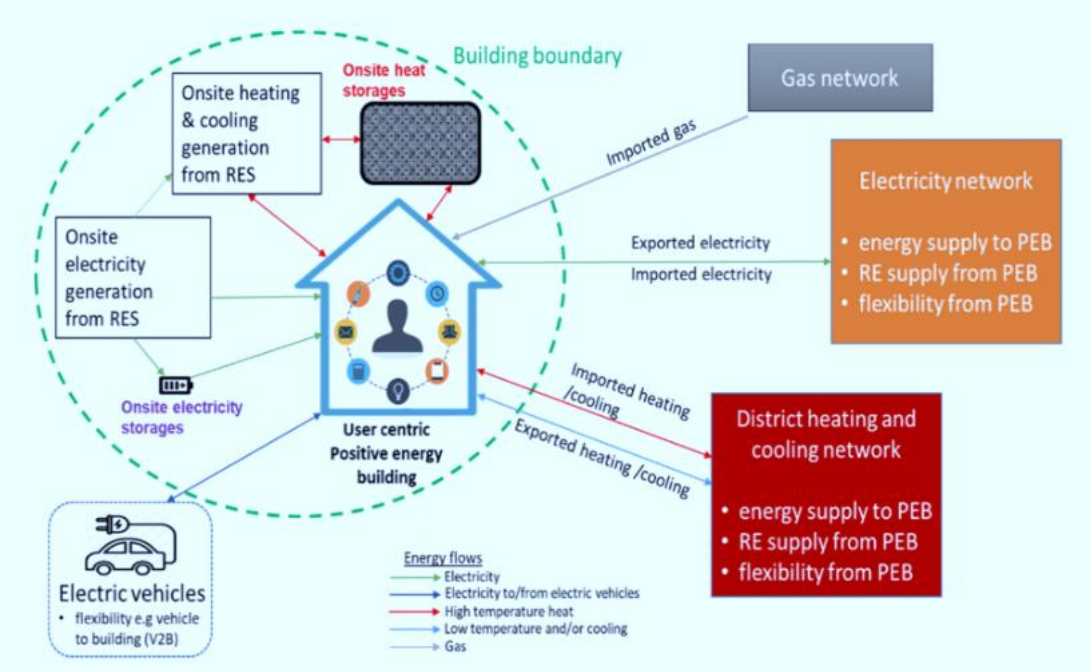
3.2.3.9 Edificios con balance positivo de recursos (Resource-Positive Buildings)

Descripción de la tendencia

Los **edificios con balance positivo de recursos** son infraestructuras diseñadas para **generar más recursos de los que consumen a lo largo de su ciclo de vida**, especialmente en términos de **energía, agua o materiales**. Este enfoque va más allá de

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

los edificios energéticamente eficientes o de consumo casi nulo, integrando **tecnologías de producción renovable, sistemas avanzados de gestión energética y soluciones de economía circular** que permiten que los edificios contribuyan activamente a la sostenibilidad ambiental [58].



Concepto de edificio con balance positivo de recursos. Fuente: Ala-Juusela, M. et al. (2021)

La evolución de las **tecnologías de generación distribuida, sensores IoT, sistemas inteligentes de gestión de edificios (BMS) y plataformas de análisis de datos** está facilitando el desarrollo de infraestructuras capaces de **optimizar el uso de recursos y producir excedentes energéticos o ambientales**.

Relevancia e implicaciones

En el ámbito urbano y empresarial, los edificios con balance positivo pueden contribuir a **reducir el impacto ambiental de las infraestructuras, mejorar la eficiencia en el uso de recursos e incrementar la resiliencia energética de las ciudades y de las organizaciones**. Estos sistemas pueden **generar energía renovable localmente, reutilizar recursos y optimizar el consumo mediante sistemas inteligentes de control y monitorización**.

Para nuestra industria, esta tendencia puede traducirse en la **integración de tecnologías de eficiencia energética, autoconsumo renovable, sistemas inteligentes de gestión de edificios y soluciones de economía circular**,

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

contribuyendo a la **descarbonización del parque edificatorio y a la sostenibilidad de las infraestructuras**.

Consideraciones adicionales

La implantación de este modelo también introduce **nuevos desafíos relacionados con la integración tecnológica, la interoperabilidad de los sistemas de gestión de edificios y la ciberseguridad de las infraestructuras digitales que controlan estos sistemas**. Además, el incremento de la conectividad y de la automatización en los edificios inteligentes requiere **estrategias de protección frente a riesgos cibernéticos que puedan afectar a los sistemas de control o a la gestión de recursos**.

En este contexto, entidades internacionales e iniciativas de investigación destacan la importancia de **combinar eficiencia energética, innovación tecnológica y gobernanza sostenible para desarrollar edificios capaces de generar impactos positivos en el medio ambiente y en las comunidades** [59].

3.2.3.10 Evaluación de competencias en la era de la IA (Test for Skills in the AI Era)

Descripción de la tendencia

La creciente integración de la **inteligencia artificial en los procesos educativos y profesionales** está impulsando una transformación en los modelos de evaluación de conocimientos y habilidades. Los sistemas tradicionales, centrados principalmente en la memorización de contenidos, están evolucionando hacia métodos que buscan medir **competencias aplicadas, pensamiento crítico, capacidad de resolución de problemas e interacción efectiva con herramientas basadas en IA**. En este contexto, están emergiendo nuevos enfoques de evaluación basados en **simulaciones, escenarios prácticos y análisis automatizado del desempeño**, más próximos a las situaciones reales de trabajo, y alineadas con las necesidades futuras previstas en el campo de la empleabilidad.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

Habilidades profesionales con mayor crecimiento esperado hasta 2030. Fuente: WEF (2025)

Relevancia e implicaciones

La adopción de estos modelos de evaluación responde a la necesidad de **adaptar los sistemas educativos y de formación a las nuevas demandas de un mercado laboral crecientemente digitalizado**. La capacidad de **trabajar con sistemas de inteligencia artificial, interpretar resultados generados por algoritmos o integrar herramientas digitales en los procesos de trabajo** se convierte en una competencia clave.

Para el **ecosistema formativo y empresarial gallego incluso más allá del sector industrial**, esta tendencia podría traducirse en el desarrollo de **nuevos sistemas de certificación de competencias digitales, programas de formación adaptados a la Herramientas de evaluación más dinámicas y contextualizadas**.

Consideraciones adicionales

La implantación de estos sistemas también introduce desafíos relacionados con la **equidad en los procesos de evaluación, la transparencia de los algoritmos utilizados y la protección de los datos personales de los estudiantes o profesionales evaluados**. Además, será necesario garantizar que los sistemas automatizados de evaluación **complementen la supervisión humana y eviten posibles sesgos algorítmicos**. Por este motivo, diferentes instituciones internacionales

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

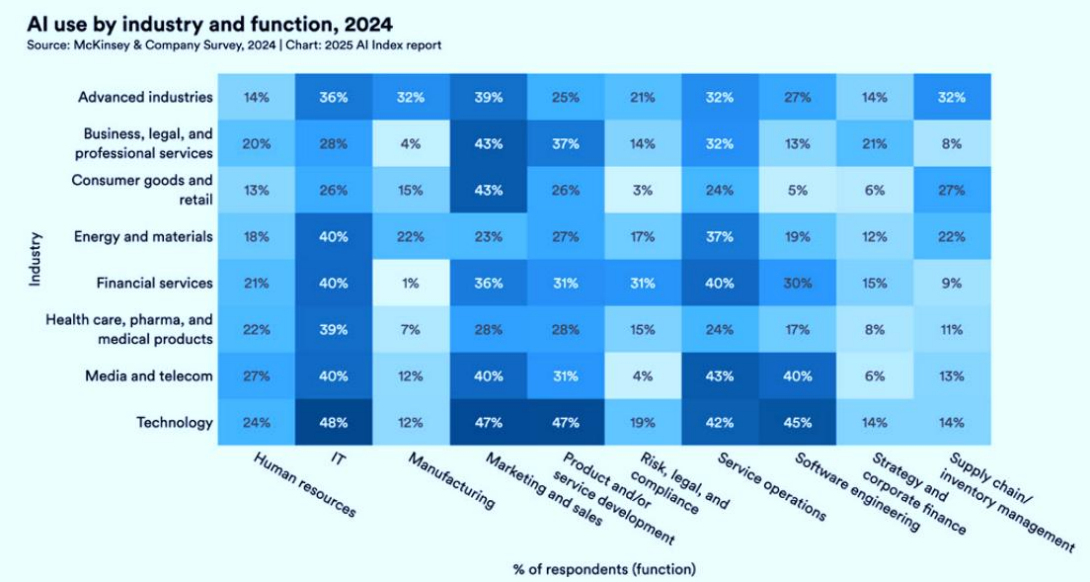
están analizando como **adaptar los marcos educativos y de evaluación de competencias a la era de la inteligencia artificial**, promoviendo modelos que integren habilidades tecnológicas, cognitivas y éticas necesarias para interactuar con sistemas avanzados de IA [60].

3.2.3.11 Economía de modelos de IA (AI Model Economy)

Descripción de la tendencia

La **economía de modelos de IA** se refiere a la aparición de un nuevo ecosistema económico en el que **modelos de inteligencia artificial se desarrollan, comercializan, intercambian e integran como activos tecnológicos clave**. En este contexto, los modelos de IA —especialmente los basados en **modelos fundacionales e IA generativa**— se convierten en un recurso central para empresas y organizaciones, que pueden **crear, adaptar o consumir modelos como servicios a través de plataformas digitales**.

Este paradigma está impulsado por la expansión de las **plataformas de computación en la nube, los mercados de modelos (model marketplaces) y los ecosistemas de desarrollo de IA**, que permiten reutilizar modelos preentrenados e integrarlos rápidamente en aplicaciones empresariales o industriales, y tienen cada vez mayor penetración en el mercado.



Encuesta de uso de la IA por industria y función en 2024. Fuente: McKinsey (2024)

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Relevancia e implicaciones

La economía de modelos de IA puede transformar la forma en que las organizaciones **acceden a las capacidades de inteligencia artificial**, facilitando la adopción de tecnologías avanzadas sin necesidad de desarrollar modelos desde cero. Ello permite **acelerar la innovación, reducir costes de desarrollo y facilitar la integración de la IA en múltiples procesos empresariales**, desde el análisis de datos hasta la automatización de tareas o la interacción con clientes.

Para el **tejido empresarial gallego**, esta tendencia podría favorecer el acceso a **capacidades avanzadas de IA a través de plataformas y servicios especializados**, permitiendo que empresas de diferentes tallas incorporen herramientas basadas en IA en sus procesos productivos, comerciales o de análisis.

Consideraciones adicionales

El desarrollo de este ecosistema también introduce retos relacionados con la **propiedad intelectual de los modelos, la transparencia de los sistemas de IA, la seguridad de las cadenas de suministro tecnológicos y la dependencia de plataformas tecnológicas globales**. Además, la proliferación de modelos de IA requiere **mecanismos de evaluación, control y gobernanza que garanticen la fiabilidad, la seguridad y el uso responsable de estas tecnologías**.

En este contexto, organismos internacionales y centros de investigación están analizando el impacto económico y tecnológico de este nuevo mercado de modelos de IA, destacando su papel en la transformación de los ecosistemas de innovación digital [61].

3.2.3.12 Fin del modelo tradicional de experiencia de usuario (35-Year-Old Productivity UX Will End)

Descripción de la tendencia

Durante más de tres décadas, el diseño de interfaces de productividad estuvo basado en un modelo centrado en **aplicaciones, menús, iconos e interacción directa con el software**. La expansión de la **inteligencia artificial, los asistentes conversacionales y los sistemas basados en lenguaje natural** está impulsando un cambio significativo en este paradigma. En este nuevo enfoque, los usuarios interactúan con los sistemas **mediante instrucciones, contexto o intenciones**, permitiendo que la IA interprete la

solicitud y ejecute acciones complejas sin necesidad de navegar por múltiples interfaces tradicionales.

Relevancia e implicaciones

La evolución hacia interfaces basadas en **interacción conversacional, automatización contextual y sistemas de agentes inteligentes** puede transformar profundamente la forma en que las personas utilizan herramientas digitales. En lugar de aprender a utilizar aplicaciones complejas, los usuarios podrán **expresar necesidades u objetivos directamente al sistema**, que se encargará de ejecutar tareas, integrar información de diferentes fuentes o coordinar procesos. Para el **ecosistema empresarial y tecnológico gallego,** esto puede suponer una transición hacia **entornos de trabajo más automatizados, interfaces más intuitivas y herramientas digitales centradas en intenciones y resultados**.

Consideraciones adicionales

Este cambio también introduce nuevos retos relacionados con la **usabilidad, la confianza en los sistemas automatizados y la seguridad de las interacciones basadas en IA**. A medida que los sistemas ejecuten tareas complejas en nombre de los usuarios, será necesario garantizar **transparencia en las acciones realizadas por los sistemas, control humano sobre los procesos automatizados y protección de la información utilizada en estas interacciones**. Expertos apuntan a que el verdadero futuro de la UX no consiste en **mejorar pantallas individuales**, sino en **orquestar experiencias completas del usuario a lo largo del tiempo**, combinando **pensamiento centrado en las personas, análisis de datos e inteligencia artificial** [62].

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

4 Reglamentación en el sector

4.1 Introducción

La dimensión reglamentaria de la ciberseguridad industrial está adquiriendo un peso creciente en el conjunto de la Unión Europea y, por extensión, también en Galicia. Sin embargo, dado que este informe analizó una gran cantidad de tendencias tecnológicas y de transformación del ecosistema digital, el abordaje detallado del marco normativo y de las obligaciones de cumplimiento asociadas a los entornos **ICS/OT** se pospone para una edición posterior específica.

Esta decisión resulta coherente con la existencia de una **Guía normativa de ciberseguridad industrial** ya elaborada en el marco del Observatorio, que **constituye la referencia principal para un análisis más extenso y sistemático del panorama reglamentario actual** [20].

Con todo, resulta útil incorporar en esta edición una visión introductoria que permita **abrir foco sobre los principales cambios normativos y de estandarización que deberán ser vigiados en los próximos años**, tanto por el sector público como por el tejido empresarial e industrial gallego. La razón es clara: la presión reglamentaria ya no se limita al cumplimiento formal, sino que se está traduciendo en **nuevas exigencias operativas, nuevas evidencias auditables y nuevos criterios de compra y relación con proveedores**, con impacto directo sobre la gobernanza, la arquitectura tecnológica y la operación de los entornos industriales.

4.2 Principales vectores reglamentarios que vigilar

El primer gran eje de seguimiento es la consolidación del **nuevo marco europeo de ciberseguridad y resiliencia**, en el que destacan tres piezas especialmente relevantes.

- En primer lugar, la **Directiva NIS2**, que refuerza las obligaciones de gestión de riesgos, gobernanza, reporte de incidentes y seguridad de la cadena de suministro para entidades esenciales e importantes [63].
- En segundo lugar, la **Directiva CER**, que amplía la perspectiva desde la ciberseguridad hacia la **resiliencia integral de entidades críticas**, incluyendo amenazas físicas, híbridas y de continuidad de servicio [64].
- En tercer lugar, el **Cyber Resilience Act (CRA)**, que introduce requisitos obligatorios de seguridad para productos con elementos digitales y tendrá un

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

efecto tractor muy relevante sobre la compra, integración y operación de tecnología en ambientes ICS/OT [65][66].

El segundo eje relevante es el **aterrizaje práctico de este marco en el ordenamiento español y en la operativa de las organizaciones,** lo que previsiblemente reforzará la exigencia efectiva sobre Administraciones públicas, operadores de servicios esenciales y cadenas de proveedores.

- En este contexto, es de seguir la evolución del **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**, orientado a la transposición de NIS2 [67],
- así como el desarrollo del **Anteproyecto de Ley de protección y resiliencia de entidades críticas**, llamado a incorporar al ordenamiento interno los principios de la Directiva CER [68].

Para Galicia, esto implicará previsiblemente una mayor demanda de **evidencias formales de gobernanza, procedimientos de notificación, análisis de riesgos, continuidad y control de terceros**, especialmente en sectores intensivos en componente OT.

El tercer ámbito que deberá ser monitorizado con atención es el que afecta a la **cadena de suministro tecnológico y a la transparencia de componentes**. La tendencia reglamentaria apunta hacia una mayor exigencia en materia de **gestión de vulnerabilidades, trazabilidad técnica, relación con integradores y control de dependencias de software y hardware**, en un contexto en el que el CRA, los trabajos de ENISA sobre **SBOM** (Software Bill of Materials, inventario estructurado de los componentes de software que forman parte de una aplicación, sistema o producto digital) y los estándares asociados, pueden convertir este tipo de evidencias en un requisito de facto para muchos procesos de compra y convalidación tecnológica [69][70][71].

Un cuarto ejemplo emergente es el de la **criptografía post-cuántica (PQC)** y la llamada **cripto-agilidad**, tendencia mencionada en el Informe en la sección previa (en el grupo de prioridad #1). La Comisión Europea ya ha puesto en marcha una hoja de ruta específica para promover la transición coordinada hacia algoritmos resistentes a la computación cuántica [72][73].

Aunque el impacto inmediato en entornos industriales no será uniforme, este movimiento normativo y técnico anticipa la necesidad de que organizaciones con activos

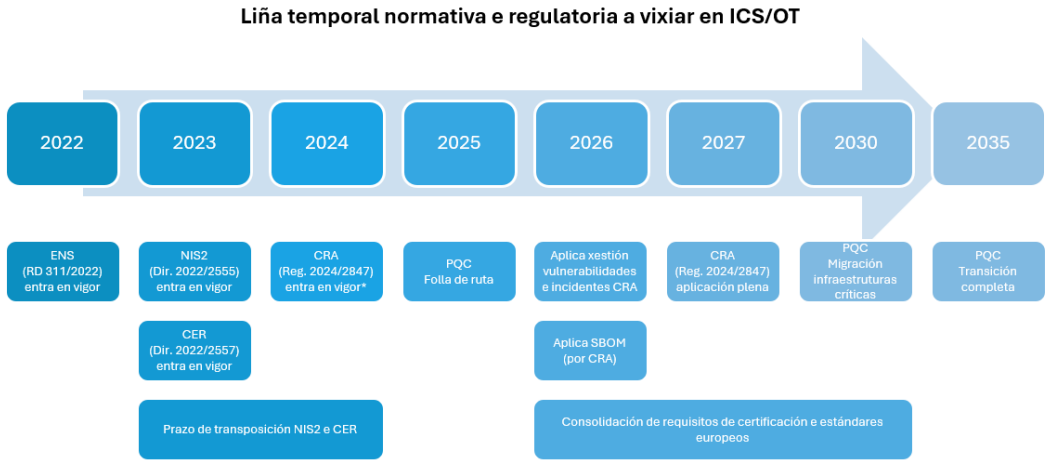
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

de larga vida útil —como adopta ocurrir en ICS/OT— comiencen a trabajar en **inventarios criptográficos, planificación de migración y revisión de dependencias tecnológicas críticas**.

El quinto elemento que seguir es la creciente convergencia entre **regulación tecnológica, certificación y compra pública o industrial**. Además de las obligaciones legales directas, todo apunta a que los próximos años traerán un mayor peso de las **certificaciones europeas de ciberseguridad, los estándares armonizados y los requisitos contractuales ligados a la seguridad por diseño**, incluyendo ámbitos en los que la automatización y el control industrial tienen especial relevancia [74].

Para el ecosistema gallego, esto es particularmente importante porque puede condicionar no sólo el cumplimiento, sino también la **capacidad de competir en cadenas de valor, contrataciones públicas y proyectos industriales avanzados**.

A continuación, un resumen gráfico de todo lo anterior:



Línea temporal normativa y reglamentaria a vigilar en ICS/OT (2022–2030)

4.3 Implicaciones

Desde la perspectiva gallega, lo más relevante no será sólo conocer el marco normativo, sino **anticipar cómo se traducirá en requerimientos operativos concretos**. Esto afecta tanto al sector público —en el que el **ENS** sigue siendo una referencia estructura [75]— como a las organizaciones privadas que, por su actividad, talla o criticidad, puedan quedar dentro del ámbito de aplicación de NIS2 [63] o de los futuros desarrollos asociados a la resiliencia de entidades críticas.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

En términos prácticos, habrá que prestar especial atención a la capacidad de demostrar **inventario de activos, trazabilidad, gobernanza TI-OT, procedimientos de reporte, gestión de incidentes, relación con terceros, continuidad y seguridad de la cadena de suministro**. En paralelo, la evolución de los estándares internacionales de referencia —como **NIST CSF 2.0**, los trabajos sobre seguridad OT de NIST o la serie **ISA/IEC 62443**— seguirá actuando como marco de apoyo para traducir requisitos legales a controles, evidencias y hojas de ruta de madurez [76][28][77].

Podemos cerrar diciendo que la regulación de la ciberseguridad industrial está entrando en una nueva fase, caracterizada por una mayor interrelación entre **cumplimiento, resiliencia operativa, compra tecnológica y gobernanza del riesgo**.

La presente edición no desarrolla en profundidad este ámbito por razones de foco y extensión, pero sí deja apuntados los principales vectores que deberán ser observados con atención: **NIS2, CER, CRA, cadena de suministro y SBOM, criptografía post-cuántica, certificación europea y adaptación normativa en España y Galicia**. Estos elementos podrán constituir la base de una futura entrega específica centrada en la dimensión reglamentaria a futuro, complementaria a la Guía Normativa ya disponible en el Observatorio [20].

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

5 Conclusiones

El análisis desarrollado en este informe permite concluir que la **ciberseguridad industrial** está evolucionar en un contexto marcado por una interacción cada vez más estrecha entre **transformación tecnológica, cambio organizativo y evolución reglamentaria**. Los entornos **ICS/OT**, históricamente más cerrados y orientados a la estabilidad operativa, se ven ahora afectados por dinámicas mucho más amplias: incorporación de **inteligencia artificial en procesos industriales**, expansión de **modelos de automatización cognitiva y agéntica**, aparición de **nuevas dependencias digitales**, uso creciente de **plataformas conectadas**, evolución de la **computación distribuida,** nuevas formas de interacción humano-máquina y mayor exposición a cambios normativos y geopolíticos.

En este contexto, el principal valor aportado por el informe es ofrecer una **visión panorámica y transversal** de un escenario particularmente complejo, apoyándose en **fuentes internacionales de alta relevancia** y en un ejercicio de síntesis orientado a la utilidad práctica. En particular, el análisis construido a partir del **Hype Cycle for Emerging Technologies de Gartner**, del informe **Top Strategic Predictions for 2026 and Beyond** y, de manera especialmente relevante, del **Informe de Riesgos Tecnológicos del propio Observatorio**, permite condensar en una única pieza una lectura estructurada de señales de cambio que, de otro modo, aparecerían dispersos en múltiples fuentes de referencia. En este sentido, el informe no pretende sustituir análisis técnicos específicos y exhaustivos, sino **ordenar, contextualizar y priorizar** tendencias y vectores de cambio con potencial impacto real para Galicia.

Otra conclusión relevante es que no todas las tendencias tienen la misma materialidad ni el mismo horizonte de impacto. El ejercicio de priorización realizado permite distinguir entre aquellas que requieren **atención inmediata**, las que deben incorporarse de manera **programada a la reflexión estratégica y tecnológica, y** aquellas que conviene mantener en **vigilancia** por ser aún más inciertas o de maduración más lenta. Esta diferenciación resulta especialmente útil en un ámbito como el de la ciberseguridad industrial, en el que la acumulación de señales tecnológicas puede generar ruido si no se acompaña de un criterio claro de selección y relevancia.

La lectura conjunta de las tendencias analizadas muestra, además, que el riesgo industrial ya no puede entenderse únicamente desde parámetros clásicos de exposición técnica. Junto con los retos tradicionales, emergen con fuerza cuestiones como la

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

automatización de la decisión, la **gobernanza de la IA,** la evolución hacia **sistemas más autónomos**, la creciente importancia de la **soberanía tecnológica**, los cambios en las **interfaces y modelos de interacción**, la transformación de los procesos de compra y aprovisionamiento mediante sistemas inteligentes, o la necesidad de prepararse para futuros cambios criptográficos y computacionales. Todo ello obliga a ampliar la mirada y a ubicar la ciberseguridad industrial también en el terreno de la **estrategia,** de la **organización y** de la **antelación tecnológica**.

Desde la perspectiva de la reglamentación, la conclusión principal es que el marco europeo y nacional está consolidándose como un factor de transformación directa de la operación industrial. La combinación de **NIS2, CER y CRA**, junto con la evolución de cuestiones como el **SBOM, la certificación europea, los estándares armonizados o la transición hacia la criptografía post-cuántica**, apunta a un escenario en el que la exigencia no será sólo normativa, sino también operativa y demostrable. En esta parte del informe se acompaña además un **gráfico a modo de hoja de ruta de seguimiento**, pensado para visualizar de manera sintética los **hitos más relevantes que deberán ser monitorizados en los próximos años** en el ámbito de la regulación y de la estandarización aplicable a entornos ICS/OT.

Para Galicia, el informe deja una idea clara: la preparación ante los nuevos retos de la ciberseguridad industrial deberá apoyarse en un **enfoque simultáneamente estratégico, selectivo y aplicable**. Estratégico, porque será necesario mantener capacidad de observación e interpretación de lo que está cambiando a escala internacional. Selectivo, porque no todas las innovaciones ni todas las presiones reglamentarias requieren la misma respuesta ni en el mismo momento. Y aplicable, porque la utilidad final de este tipo de ejercicios reside en traducir el análisis en decisiones realistas sobre prioridades, capacidades y hojas de ruta.

En definitiva, el panorama analizado confirma que la ciberseguridad industrial debe entenderse como un punto de encuentro entre **tecnología, operación, regulación, resiliencia y gobernanza**. La aportación de este informe consiste precisamente en proporcionar una lectura de conjunto, ordenada y útil, que permita interpretar con mayor claridad un escenario creciente en complejidad. Con ello, se pretende reforzar la capacidad del **Observatorio de Ciberseguridad Industrial de Galicia** para seguir actuando como herramienta de apoyo a la decisión, de síntesis de conocimiento y de orientación estratégica para el ecosistema industrial e institucional gallego.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Bibliografía

[1] Gartner (2025). *Hype Cycle for Emerging Technologies, 2025*. Informe de análisis tecnológico. Recuperado de https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

[2] Gartner (2025). *Signature Series: Top Strategic Predictions for 2026 and Beyond*. Informe de predicciones estratégicas. Recuperado de https://www.gartner.com/en/articles/strategic-predictions-for-2026

[3] Observatorio de Ciberseguridad Industrial de Galicia – AMTEGA (2025). *Informe de riesgos tecnológicos.* Recuperado de https://ciberseguridadegalicia.gal/es

[4] ENISA (2025). *ENISA Threat Landscape 2025*. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[5] SANS Institute (2025). *SANS 2025 State of ICS/OT Security Survey*. Recuperado de https://www.sans.org/white-papers/state-of-ics-ot-security-2025

[6] CISA (n.d.). *Zero Trust Maturity Model.* Recuperado de https://www.cisa.gov/topics/cybersecurity-best-practices/zero-trust

[7] Deloitte (2017). *The Augmented Workforce: The Future of Work in the Digital Age*. Recuperado de https://www.deloitte.com/us/en/insights/topics/talent/human-capital-trends/2017/future-workforce-changing-nature-of-work.html

[8] World Economic Forum (2022). *Augmented Workforce: Empowering People, Transforming Manufacturing*. Recuperado de https://www.weforum.org/publications/augmented-workforce-empowering-people-transforming-manufacturing/

[9] Microsoft (2025). *Microsoft Digital Defense Report 2025*. Recuperado de https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

[10] Mohammed, M., Skibniewski, M. (2023). *The Role of Generative AI in Managing Industry Projects: Transforming Industry 4.0 Into Industry 5.0 Driven Economy.* Recuperado de https://reference-global.com/download/article/10.2478/law-2023-0006.pdf

[11]Deloitte (2024). *AI Governance Framework: Managing Risks and Maximizing Value from Artificial Intelligence*. Recuperado de https://www.deloitte.com/us/en/services/consulting/blogs/human-capital/ai-governance-framework.html

[12] Comisión Europea (2024). *Regulatory Framework for Artificial Intelligence (AI Act)*. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[13] World Economic Forum (2024). *Governance in the Age of Generative AI: A 360º Approach for Resilient Policy and Regulation*. Recuperado de https://www3.weforum.org/docs/WEF_Governance_in_the_Age_of_Generative_AI_2024.pdf

[14] Deloitte (2026). *How Agentic, Physical and Sovereign AI Are Rewriting the Rules of Enterprise Innovation*. Forbes. Recuperado de https://www.forbes.com/sites/deloitte/2026/01/21/how-agentic-physical-and-sovereign-ai-are-rewriting-the-rules-of-enterprise-innovation/

[15] Moser, M. (2025). *Turning Gartner's Decision Intelligence Definition into Action*. Recuperado de https://www.linkedin.com/pulse/turning-gartners-decision-intelligence-definition-action-moser-uq4tc/

[16] Hendrycks, D.; Mazeika, M.; Woodside, T. (2023). An Overview of Catastrophic AI Risks. Recuperado de https://arxiv.org/pdf/2306.12001

[17] ISO/IEC (2023). *Information technology — Artificial intelligence — Management system*. Recuperado de https://www.iso.org/standard/42001

[18] SANS Institute (2025). *Risk-Based Vulnerability Management and Patching Industrial Systems*. Recuperado de https://www.sans.org/blog/risk-based-vulnerability-management-and-patching-industrial-systems

[19] Observatorio de Ciberseguridad Industrial de Galicia – AMTEGA (2025). *Informe de ciberalertas - II.* Recuperado de https://ciberseguridadegalicia.gal/es

[20] Observatorio de Ciberseguridad Industrial de Galicia – AMTEGA (2025). *Guia normativa de ciberseguridad industrial.* Recuperado de https://ciberseguridadegalicia.gal/es

[21] Comisión Europea (2020). *Shaping Europe's Digital Future*. Recuperado de https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[22] Parlamento Europeo (2020). *Digital Sovereignty for Europe: Briefing*. European Parliamentary Research Service (EPRS). Recuperado de https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[23] ENISA (2021). *ENISA Threat Landscape for Supply Chain Attacks*. Recuperado de https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

[24] Splunk (2023). *What Is a Digital Immune System?* Recuperado de https://www.splunk.com/en_us/blog/learn/digital-immune-system.html

[25] NIST (2023). *Transitioning to PostQuantum Cryptography: Preparation and Cryptographic Agility*. Recuperado de https://www.nist.gov/pqc

[26] NCSC (2025). *Post-Quantum Cryptography Migration Timelines*. National Cyber Security Centre (UK). Recuperado de https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[27] Cloud Security Alliance (CSA) (2024). *Security Guidance for Critical Areas of Focus in Cloud Computing*. Recuperado de https://cloudsecurityalliance.org/research/guidance

[28] NIST (2023). *Guide to Operational Technology (OT) Security – NIST Special Publication 800-82 Revision 3*. Recuperado de https://csrc.nist.gov/pubs/sp/800/82/r3/final

[29] Confidential Computing Consortium (2023). *Confidential Computing: Protecting Data in Use*. Recuperado de https://confidentialcomputing.io

[30] HomomorphicEncryption.org (2017). *Homomorphic Encryption Standardization Initiative*. Recuperado de https://homomorphicencryption.org/

[31] NIST (2024). *Fully Homomorphic Encryption (FHE): Overview and Applications*. *Workshop on Privacy Enhancing Cryptography (WPEC).* Recuperado de https://csrc.nist.gov/csrc/media/presentations/2024/wpec2024-2b1/images-media/wpec2024-2b1-slides-daniele--FHE-overview.pdf

[32] European Commission (2022). *Tackling Online Disinformation: European Approach*. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

[33] European Commission (n.d.). *A European Strategy for Data*. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[34] Anthropic (2024). *Introducing the Model Context Protocol*. Recuperado de https://www.anthropic.com/news/model-context-protocol

[35] Gartner (2025). *Emerging Tech: Top Use Cases in Intelligent Simulation.* Recuperado de https://www.gartner.com/en/documents/6863666

[36] Zhang, J., Wang, L., Gao, R. (2025). *Embodied AI: A Foundation for Intelligent and Autonomous Manufacturing*. Recuperado de https://www.sciencedirect.com/science/article/pii/S209580992500815X

[37] Wei, K. (2025). *What is embodied artificial intelligence and why it matters to ITU?*. International Telecommunication Union (ITU-T). Recuperado de https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2025/1010/Documents/Wei%20Kai.pdf

[38] NVIDIA (2024). *What is Physical AI*? Recuperado de https://www.nvidia.com/en-us/glossary/generative-physical-ai/

[39] Center for Security and Emerging Technology – Georgetown University (2026). *Physical AI. A Primer for Policymakers on AI-Robotics Convergence*. Recuperado de https://cset.georgetown.edu/publication/physical-ai/

[40] Gartner (2025). *How to Get Started With Adaptive Experience for CX.* Recuperado de https://www.gartner.com/en/documents/6402975

[41] International Federation of Robotics (2025). *World Robotics – Service Robots Report 2025*. Recuperado de https://ifr.org/downloads/press_docs/Press_Conference_2025_SR.pdf

[42] Gartner (2025). Multiagent Systems: A New Era in AI-Driven Enterprise Automation. Recuperado de https://www.gartner.com/en/articles/multiagent-systems

[43] Boston Consulting Group (2025). *AI-First Companies Win the Future*. Recuperado de https://media-publications.bcg.com/BCG-Executive-Perspectives-AI-First-Companies-Retail-Issue7-30Oct2025.pdf

[44] World Economic Forum (2024). *What is Digital Public Infrastructure and why does it matter?* Recuperado de https://www.weforum.org/stories/2024/12/can-digital-public-infrastructure-help-guide-the-transformation/

[45] World Economic Forum (2025). *Why digital public infrastructure is key to building a connected future*. Recuperado de https://www.weforum.org/stories/2025/04/digital-public-infrastructure-building-connected-future/

[46] Gartner (2025). *Why Vibe Coding Needs to Be Taken Seriously*. Recuperado de https://www.gartner.com/en/documents/6494971

[47] NVIDIA (2024). What is *Spatial Computing*? Recuperado de https://www.nvidia.com/en-us/glossary/spatial-computing/

[48] World Economic Forum (2025). *Spatial Computing: Wearables, Robots and AI as the Next Frontier*. Recuperado de https://www.weforum.org/stories/2025/04/spatial-computing-wearables-robots-ai-next-frontier/

[49] Google DeepMind (2025). *Taking a Responsible Path to AGI*. Recuperado de https://deepmind.google/blog/taking-a-responsible-path-to-agi/

[50] AI Frontiers (2025). *Uncontained AGI Would Replace Humanity*. Recuperado de https://ai-frontiers.org/articles/uncontained-agi-would-replace-humanity

[51] Cheng, X., Ju, M. et al. (2020). *Meta-Computing*. Recuperado de https://scispace.com/pdf/meta-computing-yfe3mfhq.pdf

[52] Gartner (2023). *When Machines Become Customers*. Recuperado de https://www.gartner.com/en/publications/when-machines-become-customers

[53] Deloitte (n.d.). *The IA opportunity in sourcing and procurement*. Recuperado de https://cdn-assets.inwink.com/b09e8996-f8d6-49a3-acdb-902dca6a2be3/2357fb65-c224-4a24-93b1-64b3ea3da721

[54] Harvard Business School – Digital Data Design Institute (2025). *The Cybernetic Teammate: How AI Is Reshaping Collaboration and Expertise in the Workplace*.

Recuperado de https://d3.harvard.edu/the-cybernetic-teammate-how-ai-is-reshaping-collaboration-and-expertise-in-the-workplace/

[55] Dell'Acqua, F., Ayoubi, C., et al. (2025). *The Cybernetic Teammate: A Field Experiment on Generative AI Reshaping Teamwork and Expertise*. SSRN Working Paper. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5188231

[56] IE University (2025). *AI's Cognitive Implications: The Decline of Our Thinking Skills*? Recuperado de https://www.ie.edu/center-for-health-and-well-being/blog/ais-cognitive-implications-the-decline-of-our-thinking-skills/

[57] Squirro (2025). *What Is Fluid Knowledge in Generative AI.* Recuperado de https://squirro.com/squirro-blog/what-is-fluid-knowledge-in-generative-ai

[58] NetZeroCities (n.d.). *Concept: Positive Energy Buildings (PEBs).* Recuperado de https://netzerocities.app/resource-3374

[59] World Green Building Council (s.d.). *World Green Building Council – Sitio oficial*. Recuperado de https://worldgbc.org/

[60] World Economic Forum (2025). *The Future of Jobs Report 2025*. Recuperado de https://www.weforum.org/publications/the-future-of-jobs-report-2025/

[61] Stanford University – Institute for Human-Centered Artificial Intelligence (HAI) (2025). *AI Index Report 2025*. Recuperado de https://hai.stanford.edu/ai-index/2025-ai-index-report

[62] Nielsen Norman Group (2025). UX is dead, l*ong Live UX*. Recuperado de https://www.nngroup.com/articles/long-live-ux/

[63] Unión Europea (2022). *Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (NIS2)*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

[64] Unión Europea (2022). *Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo sobre la resiliencia de las entidades críticas (CER)*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2557

[65] Unión Europea (2024). *Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para productos con*

elementos digitales (Cyber Resilience Act). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R2847

[66] Comisión Europea (2024). *Cyber Resilience Act – Questions and Answers*. Recuperado de https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

[67] Gobierno de España – Ministerio de la Presidencia, Justicia y Relaciones con las Cortes (2025). *Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (transposición de la Directiva NIS2)*. Recuperado de https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf

[68] Gobierno de España – Ministerio del Interior (2025). *Anteproyecto de Ley de protección y resiliencia de entidades críticas (transposición de la Directiva CER)*. Recuperado de https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/08_2025_Anteproyecto_ley_proteccion_resiliencia_entidades_criticas.pdf

[69] European Union Agency for Cybersecurity – ENISA (2024). *Cyber Resilience Act Requirements Standards Mapping*. Recuperado de https://www.enisa.europa.eu/publications/cra-requirements-standards-mapping

[70] European Union Agency for Cybersecurity – ENISA (2025). *Software Bill of Materials (SBOM): An Introduction*. Recuperado de https://www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide_v1.20-Published.pdf

[71] Linux Foundation / SPDX Project (2011). *Software Package Data Exchange (SPDX) Specification*. Recuperado de https://spdx.dev

[72] Comisión Europea (2024). *Recomendación (UE) 2024/1101 de la Comisión sobre una hoja de ruta coordinada para la transición hacia la criptografía post-cuántica*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024H1101

[73] Comisión Europea (2025). *Post-Quantum Cryptography: EU Roadmap and Supporting Actions*. Recuperado de https://digital-

strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[74] Comisión Europea (2026). *European Cybersecurity Certification Framework*. Recuperado de https://digital-strategy.ec.europa.eu/en/factpages/european-cybersecurity-certification-framework

[75] Gobierno de España (2022). *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*. Recuperado de https://www.boe.es/eli/es/rd/2022/05/03/311

[76] National Institute of Standards and Technology – NIST (2024). *Cybersecurity Framework 2.0*. Recuperado de https://www.nist.gov/cyberframework

[77] International Society of Automation – ISA (2009). *ISA/IEC 62443 Series of Standards for Industrial Automation and Control Systems Security*. Recuperado de https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial
Informe de tendencias y reglamento

Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Xacobeo 2027