CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial

Informe de tendencias e regulamento

Abril 2026

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

Edita: Xunta de Galicia

Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Ano: 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 Introdución

Este informe forma parte do **Observatorio de Ciberseguridade Industrial**. Intégrase no marco do **Laboratorio e Centro Demostrador de Ciberseguridade en Produtos con Elementos Dixitais e Ciberseguridade Industrial**, pertencente á **Rede de Laboratorios e Centros Demostradores de Ciberseguridade da Xunta de Galicia**. A iniciativa forma parte do **Programa de Redes Territoriais de Especialización Tecnolóxica (RETECH)**, impulsado pola Secretaría de Estado de Dixitalización e Intelixencia Artificial.

O proxecto está financiado pola **Unión Europea a través de NextGenerationEU** no **marco do Plan de Recuperación, Transformación e Resiliencia (PRTR)**, e desenvólvese conforme aos requisitos establecidos polo **Instituto Nacional de Ciberseguridade (INCIBE).**

O Observatorio constitúe **un eixo estratéxico dentro desta estrutura transversal, orientado á análise de tendencias, ameazas e necesidades do ecosistema de ciberseguridade industrial galego**, así como á dinamización e fortalecemento do tecido empresarial e tecnolóxico da nosa terra.

--

No actual escenario de transformación dixital, os sistemas industriais —incluíndo contornos **ICS/OT (Industrial Control Systems / Operational Technology)**— están a experimentar unha progresiva converxencia con infraestruturas dixitais, redes corporativas e servizos conectados. Esta evolución introduce **novas oportunidades de eficiencia, automatización e optimización operativa**, pero tamén amplía a superficie de exposición a **riscos cibernéticos, dependencias tecnolóxicas e interaccións complexas entre sistemas físicos e dixitais**.

Neste contexto, a capacidade de **anticipar tendencias tecnolóxicas, regulamentarias e de mercado** convértese nun elemento clave para reforzar a resiliencia das organizacións e das infraestruturas críticas. A identificación temperá de cambios no ecosistema tecnolóxico permite comprender mellor **como poden evolucionar as ameazas, que novos requisitos de gobernanza ou cumprimento poden emerxer e que adaptacións estratéxicas poden resultar necesarias no medio prazo**.

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 ten como finalidade ofrecer unha **visión estruturada das principais tendencias con potencial impacto na ciberseguridade industrial**, así como unha aproximación inicial aos **principais vectores regulamentarios que poderán influír na evolución do sector nos próximos anos**. A análise é de aplicación directa para o **ecosistema industrial e institucional galego**, tendo en conta a crecente importancia da protección dos sistemas que soportan procesos produtivos, servizos esenciais e infraestruturas críticas.

A diferenza doutras publicacións centradas exclusivamente na análise de ameazas ou incidentes, este documento adopta unha aproximación de **vixilancia estratéxica**, orientada a identificar sinais de cambio que poidan condicionar a seguridade e a resiliencia dos sistemas industriais no horizonte próximo. O informe combina así a análise de **tendencias tecnolóxicas emerxentes** cunha aproximación sintética ao **contexto normativo europeo e nacional**.

O documento estrutúrase en dúas partes principais. En primeiro lugar, preséntase unha análise das **tendencias con potencial impacto nos contornos ICS/OT**, clasificadas segundo o seu grao de prioridade ou horizonte de atención. En segundo lugar, introdúcese unha **visión inicial do contexto normativo relevante para a ciberseguridade industrial**, identificando os principais marcos e evolucións que deberán ser monitorizadas nos próximos anos.

Con esta aproximación, o informe pretende contribuír a **mellorar a capacidade de anticipación e preparación das organizacións galegas**, facilitando unha lectura contextualizada das transformacións tecnolóxicas e normativas que están a redefinir o panorama da **ciberseguridade 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 Resumo executivo

A **ciberseguridade industrial** está a experimentar unha transformación profunda como consecuencia da converxencia entre **dixitalización, automatización, conectividade e presión regulamentaria**. Os contornos **ICS/OT**, tradicionalmente máis estables, pechados e orientados á continuidade operativa, están a integrarse progresivamente con infraestruturas dixitais, plataformas cloud, servizos remotos, ferramentas baseadas en datos e sistemas de intelixencia artificial. Esta evolución achega oportunidades relevantes en termos de eficiencia, visibilidade e optimización, pero tamén introduce **novas superficies de exposición, dependencias tecnolóxicas e riscos ciberfísicos**.

Neste contexto, o presente informe ofrece unha lectura estruturada de dúas dimensións que condicionarán de forma crecente a resiliencia das organizacións industriais e das administracións con activos críticos en Galicia:

- por unha banda, as **tendencias tecnolóxicas e organizativas con potencial impacto en ICS/OT**;
- por outra, os **principais vectores regulamentarios e de estandarización** que deberán ser monitorizados nos próximos anos.

No plano tecnolóxico, o informe identifica un conxunto de tendencias, que xa están a influír —ou o farán a curto e medio prazo— na arquitectura, operación e gobernanza da ciberseguridade industrial. Entre as de maior prioridade destacan a **converxencia IT/OT**, a **conectividade remota en contornos industriais**, a expansión dunha **forza laboral conectada e aumentada**, a **integración transversal da intelixencia artificial**, o uso crecente de **axentes de IA**, a necesidade de **xestión de vulnerabilidades orientada a risco en OT**, o reforzo da **segmentación de redes industriais**, a atención á **cadea de subministración tecnolóxica**, a evolución cara a **arquitecturas OT defendibles,** a **"cloudización",** os **sistemas dixitais inmunes,** a importancia crecente da **cripto-axilidade** ante futuras transicións criptográficas, ou a **soberanía tecnolóxica** nun mundo cada vez mais inestable.

Xunto a estas tendencias de atención inmediata, o informe recolle outras de **materialidade moderada**, como a **computación confidencial**, o **cifrado homomórfico**, a **seguridade fronte á desinformación**, a **xeopatriación**, a **simulación**

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

intelixente, a **computación espacial** ou a progresiva incorporación de **IA encarnada e IA física** a procesos industriais e contornos automatizados.

A elas súmanse tendencias de **vixilancia estratéxica**, entre as que figuran a posible evolución cara á **intelixencia artificial xeral (AGI)**, a **meta-computación**, os **comerciantes máquina**, o **aprovisionamento autónomo**, os **compañeiros cibernéticos**, a **descarga cognitiva**, o **coñecemento fluído**, as **interfaces cerebro-máquina** ou a **transformación do modelo tradicional de experiencia de usuario**.

Todas as anteriores e incluso mais, ata chegar a unha totalidade de **45 tendencias extraídas principalmente de fontes como informes de Gartner (de tecnoloxías emerxentes e tendencias estratéxicas), ou o propio Informe de Riscos Tecnolóxicos dende Observatorio**, preséntanse en fichas homoxéneas e concisas con cadansúa descrición, relevancia e consideracións adicionais.

O conxunto destas tendencias evidencia que a ciberseguridade industrial xa non pode analizarse unicamente dende a lóxica clásica da protección perimetral. A realidade actual esixe unha aproximación máis ampla, na que a exposición vén determinada tamén pola **interoperabilidade entre sistemas**, pola dependencia de **terceiros e provedores**, pola crecente presenza de **software e servizos conectados**, pola automatización de procesos cognitivos e pola necesidade de manter a **seguridade funcional e a continuidade operativa** en contornos con impacto físico.

No plano regulamentario, o informe sinala que a ciberseguridade industrial entra nunha **nova fase marcada pola consolidación do marco europeo de ciberseguridade e resiliencia**. Neste escenario sobresaen tres pezas fundamentais: a **Directiva NIS2**, que reforza as obrigas de xestión de riscos, reporte e gobernanza; a **Directiva CER**, que amplía o foco cara á resiliencia integral das entidades críticas; e o **Cyber Resilience Act (CRA)**, que introduce requisitos obrigatorios de seguridade para produtos con elementos dixitais e terá un impacto relevante sobre a compra, integración e operación de tecnoloxía nos contornos industriais.

A este marco europeo súmase a súa **aterraxe práctica no ordenamento español**, especialmente a través dos procesos de transposición de NIS2 e CER, así como a evolución doutras iniciativas que afectarán á gobernanza, á evidencia de cumprimento e á relación con provedores. O informe destaca tamén tres frontes adicionais que deberán ser seguidas con atención: o avance de esixencias arredor da **cadea de subministración e o SBOM (***Software Bill of Materials* ou Listado de Materiais de Software), a progresiva incorporación da **criptografía post-cuántica** e da **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

axilidade ás follas de ruta europeas, e a crecente relevancia das **certificacións europeas de ciberseguridade, os estándares harmonizados e os requisitos de seguridade por deseño**.

Para Galicia, a conclusión principal é que o impacto destas transformacións non será só tecnolóxico nin só normativo: será tamén **operativo, organizativo e estratéxico**. As organizacións terán que reforzar a súa capacidade para **inventariar activos**, **comprender dependencias, mellorar a gobernanza TI-OT, controlar o acceso de terceiros, xestionar vulnerabilidades con enfoque realista, protexer cadeas de subministración e xerar evidencias de cumprimento e madurez**. Ao mesmo tempo, deberán **integrar criterios de anticipación tecnolóxica que lles permitan avaliar que innovacións son realmente prioritarias, cales deben incorporarse de maneira planificada e cales convén manter baixo observación.**

Esta análise mostra que a ciberseguridade industrial está a evolucionar cara a un escenario no que **tecnoloxía, regulación, resiliencia operativa e gobernanza do risco** aparecen cada vez máis interrelacionadas. A capacidade de Galicia para adaptarse a este novo contexto dependerá, en boa medida, de combinar **vixilancia estratéxica, planificación técnica e criterio de priorización**, tanto no ámbito público como no 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 Introdución

3.1.1 Obxectivo

Esta sección ten como finalidade **identificar e priorizar tendencias** —tecnolóxicas e tamén de natureza organizativa, xeopolítica ou de mercado— que poidan **afectar á ciberseguridade e á resiliencia operativa** dos contornos **ICS/OT** (Industrial Control Systems / Operational Technology) do **tecido produtivo galego** e das **administracións públicas** con activos e servizos críticos.

O foco non é describir "innovación" por si mesma, senón **traducir sinais de cambio** en:

- **Implicacións de risco** (novas superficies de ataque, dependencias, modos de fallo, impactos ciberfísicos).
- **Implicacións operativas** (dispoñibilidade, seguridade funcional, continuidade, mantemento, teleoperación).
- **Implicacións de gobernanza** (controis necesarios, evidencias, roles e responsabilidades, coordinación TI–OT).

A lectura está orientada á práctica: cada tendencia recóllese con **descrición executiva**, **por que importa en OT/ICS**, e unha **prioridade de atención** para apoiar a toma de decisións.

3.1.2 Fontes de información

Para garantir unha visión equilibrada entre **prospectiva global** e **materialidade local**, este apartado integra información de tres pezas documentais principais.

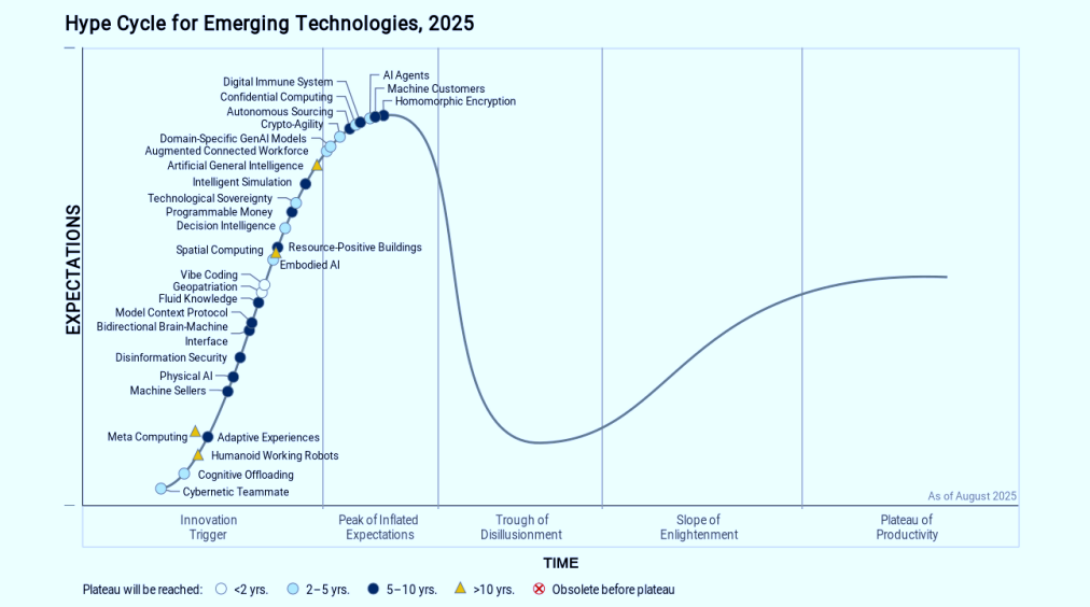
En primeiro lugar, o **Hype Cycle for Emerging Technologies (2025)** [1]. Documento de referencia de Gartner, empresa líder mundial en investigación e asesoramento tecnolóxico, proporcionando análises obxetivas, ferramentas prácticas e consultoría para mellorar o desempeño empresarial. **Condensa e clasifica tecnoloxías emerxentes** (nun conxunto reducido de "must-know" fronte a un universo moito maior) e organízaas segundo o seu **grao de madurez e horizonte de adopción**. A súa utilidade para este informe é 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 estruturado** para identificar tecnoloxías con potencial transformador.
- Permite situar cada tecnoloxía nun **horizonte temporal de adopción**, útil para anticipación.
- Inclúe liñas e temas especialmente relevantes para **resiliencia e seguridade** (p.ex. fraxilidade tecno-social, criptografía, protección de datos, sistemas autónomos).

Adicionalmente, o **Gartner – Signature Series: Top Strategic Predictions for 2026 and Beyond** [2]. Esta é unha peza de prospectiva estratéxica sintetizada que recolle **10 predicións de alto nivel** sobre como evolucionarán as organizacións, a tecnoloxía e o comportamento socioeconómico no curto e medio prazo (2026–2030). A súa contribución a esta sección céntrase en:

- Identificar **forzas motrices non estritamente tecnolóxicas** (talento, gobernanza, automatización de decisións, plataformas, cambios na economía dixital...).
- Aportar un marco de **impacto estratéxico**, especialmente en ámbitos como **axentes de IA**, **automatización**, **compras a terceiros**, e **gobernanza**.
- Servir como "ponte" entre tecnoloxía e **decisión executiva** (riscos, prioridades e accountability).



Gartner Hype Cycle. Fonte: 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

E como non podería ser doutro xeito, o propio **Observatorio de Ciberseguridade Industrial (AMTEGA), mediante o seu *Informe de riscos tecnolóxicos*** [3]**.** Traballo propio do Observatorio que ofrece unha visión aplicada a contornos industriais e infraestruturas críticas, incorporando:

- Unha lectura do **risco ciberfísico** en OT/ICS (impacto económico, continuidade e seguridade funcional).
- Unha identificación de **riscos e vectores de preocupación** en Galicia nos diferentes sectores de actividade (enerxía, auga, automoción, alimentación, loxística, manufactura, etc.), non estritamente no ámbito tecnolóxico.
- Unha orientación práctica cara a medidas de **arquitectura OT**, **conectividade segura**, **goberno** e **resiliencia**.

Esta fonte é especialmente importante porque actúa como **filtro de realidade**: permite priorizar tendencias en función do seu encaixe coas restricións e dinámicas reais de operación OT e os niveis de risco xeral.

Adicionalmente, incorpórase algunha tendencia adicional non referida explícitamente pero afín, ou que claramente parece que experimentará o sector industrial a curto, medio ou longo prazo, segundo o caso.

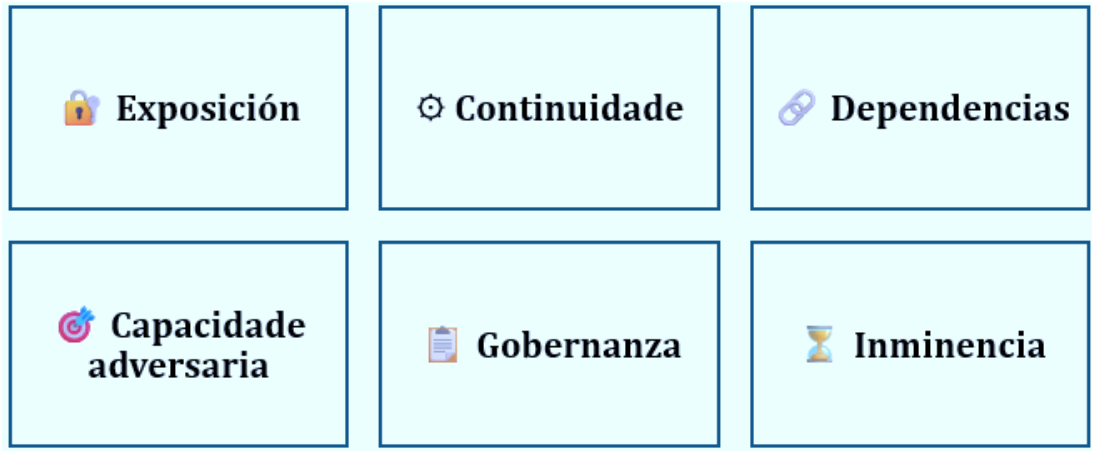
3.1.3 Criterios de selección de tendencias

Co obxectivo de **non descartar tendencias relacionadas** (dado o carácter executivo do informe e o número limitado de fontes), a metodoloxía empregada non elimina elementos a priori, senón que **ordena por prioridade de atención**.

Para iso aplicáronse os seguintes **criterios de inclusión**. Unha tendencia considérase "relevante" cando contribúe de forma clara a **polo menos dous** destes criterios (aínda que pode incluírse con menor prioridade cando só cumpre un, se achega contexto estratéxico):

1. **Impacto na superficie de ataque OT/ICS**: incrementa exposición, interconexión, acceso remoto, IIoT, integración con cloud/edge ou dependencia de identidades.
2. **Impacto na continuidade e na seguridade funcional (safety)**: pode afectar dispoñibilidade, operación segura, tolerancia a fallos, recuperación e resposta a incidentes con consecuencias físicas.

3. **Incremento de complexidade e dependencia de terceiros**: introduce novas capas (software, plataformas, provedores, integradores), cadea de subministración e riscos sistémicos.
4. **Efecto multiplicador no adversario**: facilita automatización, escalabilidade, evasión, fraude ou aceleración de cadeas de intrusión.
5. **Implicacións de gobernanza e cumprimento**: demanda novos controis, procedementos, evidencias auditables, roles e coordinación TI–OT.
6. **Proximidade temporal (inminencia)**: tendencia xa observable ou con adopción probable no horizonte 2–5 anos en sectores industriais.



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

Adicionalmente, a fin de manter a sección **operativa e accionable**, cada tendencia clasifícase nunha das seguintes categorías de prioridade:

Prioridade	Denominación	Definición executiva	Cumprimento de criterios
1	**Atención inmediata / Alta materialidade**	Tendencias con **alto impacto potencial en OT/ICS** e/ou **alta inminencia**, que adoitan implicar cambios en **arquitectura, operación ou gobernanza**.	Cumpren **3 ou máis criterios**, incluíndo habitualmente os criterios **1 (Exposición)** e **2 (Continuidade / safety)**.
2	**Atención programada /**	Tendencias con **impacto plausible**, pero máis dependentes do sector, do	Cumpren **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

	Materialidade moderada	ritmo de modernización ou cun horizonte máis medio. Recoméndase incorporalas á **planificación, avaliación de risco e pilotos controlados**.	
3	**Vixilancia estratéxica / Horizonte longo**	Tendencias con relevancia principalmente **contextual ou indirecta** para OT/ICS, ou cun horizonte máis longo e maior incerteza. Deben manterse baixo **observación**, sen desprazar prioridades operativas.	Cumpren **1–2 criterios** ou presentan impacto de menor intensidade.

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

A continuación describiranse as tendencias unha a unha, agrupadas por estas tres prioridades.

3.2 Tendencias

Co obxectivo de facilitar unha análise clara e homoxénea das principais tendencias que afectan á ciberseguridade industrial, cada unha das tendencias incluídas neste informe preséntase mediante unha ficha estruturada en tres apartados.

- En primeiro lugar, a **Descrición da tendencia** ofrece unha explicación sintética do fenómeno tecnolóxico, organizativo ou estratéxico identificado, contextualizando a súa aparición e os factores que impulsan a súa evolución.
- A continuación, o apartado **Relevancia e implicacións** analiza o impacto potencial da tendencia no ámbito da ciberseguridade industrial, considerando especialmente o contexto do tecido produtivo e das infraestruturas críticas se aplica.
- Finalmente, en **Consideracións adicionais** recóllense elementos complementarios que permiten ampliar a comprensión da tendencia, tales como evidencias, evolución observada, posibles riscos asociados ou oportunidades e medidas de mitigación cando proceda.

Esta estrutura pretende ofrecer unha visión equilibrada entre explicación conceptual, interpretación estratéxica e elementos prácticos de apoio á toma de decisións.

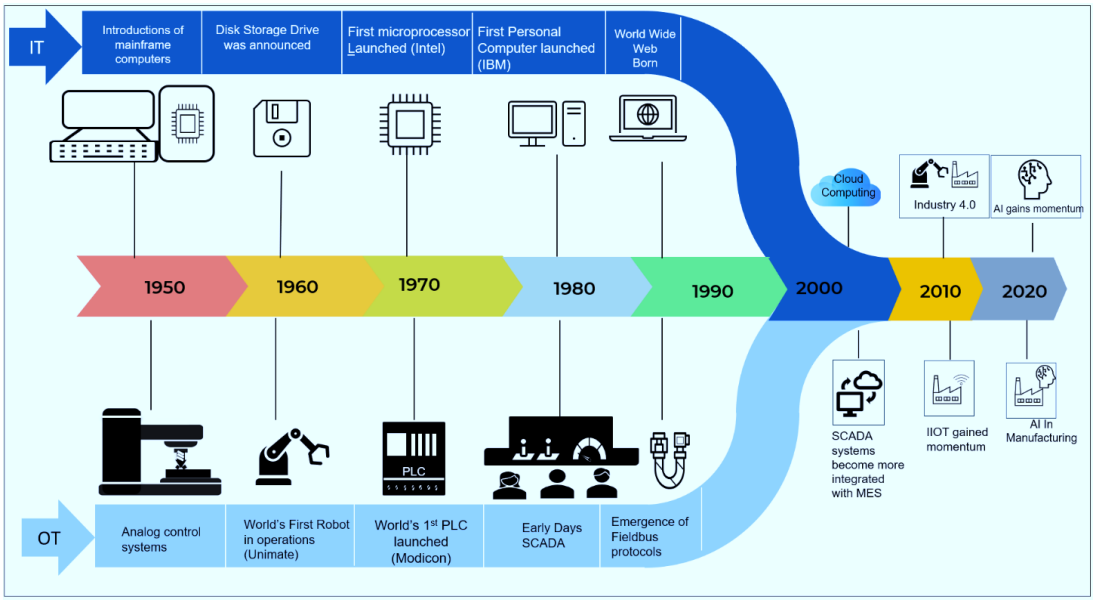
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

3.2.1 De atención inmediata (prioridade #1)

3.2.1.1 Converxencia acelerada IT/OT

Descrición da tendencia

A **converxencia entre tecnoloxías da información (IT) e tecnoloxías operacionais (OT)** constitúe unha das transformacións estruturais máis relevantes da industria moderna. A progresiva **dixitalización dos procesos industriais**, a adopción de sistemas de **monitorización avanzada**, a integración con **plataformas de análise de datos** e a necesidade de operacións máis eficientes están a impulsar a interconexión entre sistemas tradicionalmente illados. Como resultado, **redes industriais, sistemas de control e plataformas corporativas comparten cada vez máis infraestruturas, protocolos e fluxos de datos**, xerando arquitecturas híbridas nas que os límites entre IT e OT son progresivamente máis difusos.



Converxencia IT-OT. Fonte: Inductive Automation (2025)

Relevancia e implicacións

Para o **tecido industrial galego**, caracterizado por unha forte presenza de sectores como a **automoción, a alimentación, a enerxía ou a loxística portuaria**, esta converxencia supón unha oportunidade para **mellorar a eficiencia operativa, a trazabilidade e a capacidade de análise dos procesos produtivos**. Con todo, tamén introduce **novos retos de ciberseguridade**, xa que a integración de sistemas OT con contornos IT expostos a internet **amplía a superficie de ataque** e facilita posibles **vectores de intrusión cara a infraestruturas industriais críticas**. A protección

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

destas arquitecturas converxentes require enfoques específicos que combinen **prácticas de seguridade IT tradicionais** con medidas adaptadas ás **particularidades dos sistemas industriais**.

Consideracións adicionais

Diversos estudos e informes especializados sinalan que a **converxencia IT/OT é un dos principais factores que están a redefinir o panorama de risco nos contornos industriais modernos** [4]. A interdependencia crecente entre **sistemas corporativos e sistemas de control** fai que incidentes inicialmente limitados ao ámbito IT poidan ter **repercusións operacionais sobre procesos físicos**, especialmente en sectores industriais altamente automatizados. Ao mesmo tempo, esta tendencia impulsa a adopción de novos modelos de seguridade baseados en **visibilidade de activos industriais, segmentación de redes OT, monitorización específica de protocolos industriais e integración da ciberseguridade no deseño das arquitecturas industriais**. A correcta xestión desta converxencia converterase previsiblemente nun **elemento clave para a resiliencia das organizacións industriais nos próximos anos**.

3.2.1.2 Conectividade segura en OT e acceso remoto (modernización)

Descrición da tendencia

A modernización das infraestruturas industriais está a impulsar unha adopción crecente de **mecanismos de conectividade remota en contornos OT**, destinados a facilitar operacións como o **mantemento remoto, a supervisión centralizada, a xestión de activos industriais e a integración con plataformas dixitais corporativas**. Historicamente, moitos sistemas industriais operaban en redes illadas ou con conectividade moi limitada; porén, a necesidade de optimizar operacións, reducir custos de desprazamento técnico e permitir a asistencia de fabricantes está a favorecer a introdución de **accesos remotos controlados, pasarelas seguras e solucións de acceso específico para sistemas industriais**.

Relevancia e implicacións

No contexto da **industria galega**, onde moitas instalacións industriais e infraestruturas críticas están distribuídas territorialmente (plantas industriais, instalacións enerxéticas, portos ou instalacións de tratamento de auga), a conectividade remota permite **mellorar a eficiencia operativa e a capacidade de resposta ante incidencias técnicas**. Non obstante, tamén introduce **novos vectores de risco**, xa que

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

os accesos remotos constitúen un dos puntos de entrada máis habituais en incidentes de ciberseguridade industrial. A adopción de **arquitecturas de acceso remoto especificamente deseñadas para contornos OT**, con autenticación forte, control de sesións e monitorización continua, convértese así nun elemento clave para garantir a seguridade destes sistemas.

Consideracións adicionais

O **acceso remoto non autorizado ou mal configurado segue sendo un dos factores máis frecuentes en incidentes que afectan a contornos OT** segundo o SANS Institute [5]. En particular, o uso de **VPN tradicionais, credenciais compartidas ou accesos persistentes sen control de sesión** pode facilitar a intrusión de actores maliciosos nos sistemas industriais. Como resposta a este escenario, están a emerxer modelos de acceso máis seguros baseados en **acceso remoto consciente do contexto industrial, rexistro e gravación de sesións, segmentación de rede e integración con modelos Zero Trust** [6]. A modernización da conectividade en contornos OT debe ir acompañada, polo tanto, dun **deseño de seguridade específico para sistemas industriais**, que teña en conta as limitacións operativas e os requisitos de continuidade do servizo destes contornos.

3.2.1.3 Forza laboral conectada aumentada (Augmented Connected Workforce)

Descrición da tendencia

A tendencia coñecida como **Augmented Connected Workforce (ACWF)** refírese á incorporación de **tecnoloxías dixitais que amplían as capacidades dos traballadores industriais**, combinando conectividade, análise de datos e ferramentas de asistencia intelixente. Isto inclúe o uso de **dispositivos móbiles industriais, realidade aumentada (AR), sistemas de asistencia remota, sensores portátiles e plataformas de xestión do coñecemento**, que permiten aos operarios acceder a información contextualizada sobre procesos, equipos ou incidencias en tempo real. O obxectivo principal é **mellorar a eficiencia operativa, reducir erros humanos e facilitar a transferencia de coñecemento técnico**, especialmente nun contexto de crecente complexidade tecnolóxica nas plantas industriais.

Relevancia e implicacións

Esta tendencia resulta especialmente relevante en sectores intensivos en operacións técnicas como a **automoción, a industria naval, a alimentación ou a enerxía**. A utilización de ferramentas de asistencia dixital permite **optimizar tarefas de**

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

mantemento, diagnóstico de fallos e formación de persoal, reducindo tempos de intervención e mellorando a continuidade operativa. Porén, tamén introduce novos retos de ciberseguridade, xa que a incorporación de **dispositivos conectados, aplicacións móbiles industriais e plataformas de soporte remoto** amplía a superficie de exposición dos contornos OT. A protección destes ecosistemas require integrar **medidas de xestión de identidades, control de dispositivos, segmentación de rede e monitorización de accesos**.

Consideracións adicionais

A adopción dunha forza laboral conectada está directamente relacionada coa **transformación dixital da industria e coa escaseza de perfís técnicos especializados**, factores que impulsan o desenvolvemento de ferramentas de asistencia baseadas en datos e conectividade. Diversos estudos como os de Deloitte ou o Foro Económico Mundial sinalan que a implementación de solucións ACWF pode mellorar significativamente a **produtividade, a seguridade laboral e a capacidade de resolución de incidencias en contornos industriais complexos** [7][8]. Con todo, tamén require abordar cuestións como a **seguridade dos dispositivos utilizados polos operarios, a protección da información operativa e a correcta integración destas ferramentas nas arquitecturas de ciberseguridade industrial existentes** [9].

3.2.1.4 Intelixencia Artificial en OT (integración transversal)

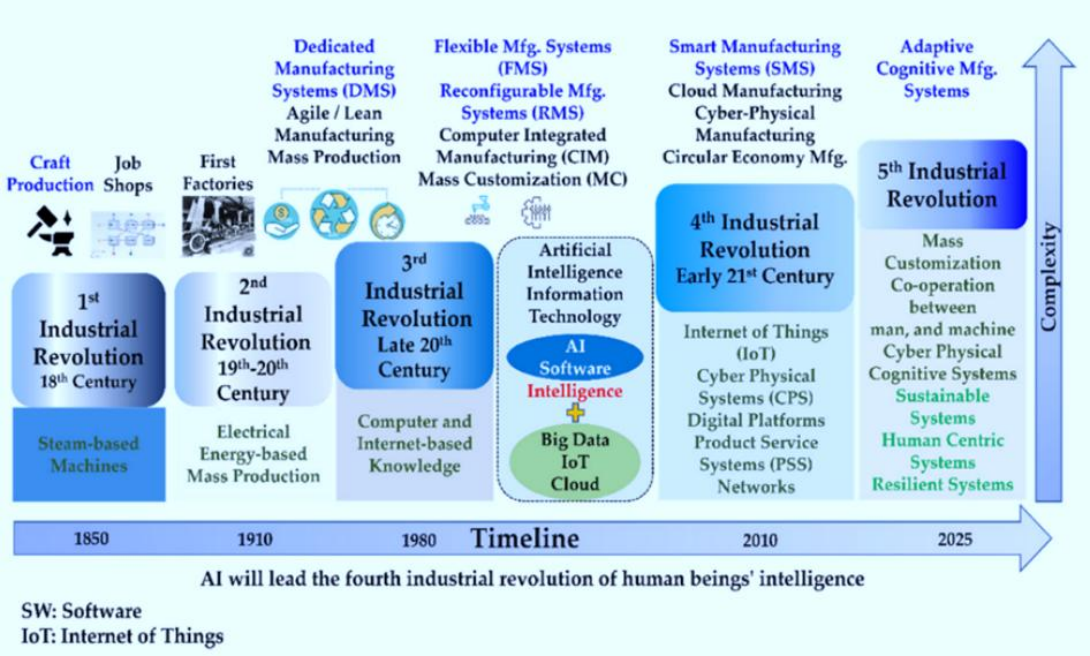
Descrición da tendencia

A incorporación da **intelixencia artificial (IA) en contornos de tecnoloxía operacional (OT)** está a converterse nun elemento transversal da transformación dixital industrial. A medida que as plantas industriais incorporan sensores, sistemas de monitorización e plataformas de análise de datos, xérase unha gran cantidade de información operacional susceptible de ser analizada mediante algoritmos de **aprendizaxe automática, análise preditiva e sistemas de optimización baseados en IA**. Estas capacidades permiten desenvolver aplicacións como **mantemento preditivo, optimización de procesos produtivos, detección temperá de anomalías ou mellora da eficiencia enerxética**, integrando a IA directamente nos fluxos operacionais das instalacións industriais [10].

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

Relevancia e implicacións

No caso da **industria galega**, onde sectores como a automoción, a produción alimentaria, a enerxía ou a industria marítima están a avanzar cara a modelos de **industria 4.0**, a integración de IA nos sistemas industriais pode contribuír a **mellorar a eficiencia produtiva, reducir custos operativos e incrementar a capacidade de análise en tempo real dos procesos industriais**. Non obstante, a introdución de sistemas baseados en IA tamén introduce **novos retos de ciberseguridade**, xa que estes sistemas dependen de grandes volumes de datos e de infraestruturas dixitais interconectadas. A manipulación de datos, os ataques contra modelos de IA ou a explotación de vulnerabilidades nas plataformas que os soportan poden afectar directamente á fiabilidade dos sistemas industriais.



Impacto da IA na evolución industrial. Fonte: Moyassar Y. Mohammed, Mirosław J. Skibniewski (2023)

Consideracións adicionais

A crecente adopción de IA no ámbito industrial está acompañada dun aumento do interese dos actores de ameaza por **explotar vulnerabilidades asociadas a modelos de aprendizaxe automática, cadeas de datos e sistemas de decisión automatizados**. Ademais, a dependencia de datos operacionais fai que a **integridade e a dispoñibilidade da información industrial** sexan factores críticos para garantir o correcto funcionamento destes sistemas. Neste contexto, organismos e informes internacionais subliñan a necesidade de integrar **principios de seguridade e gobernanza da IA** no deseño e despregamento destas solucións, incluíndo mecanismos

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 supervisión humana, validación de modelos e protección fronte a manipulacións de datos [11][12].

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

Descrición da tendencia

Nos últimos anos está a emerxer unha nova xeración de **modelos de intelixencia artificial xerativa especializados en dominios concretos**, coñecidos como Domain-Specific Generative AI. A diferenza dos modelos xerais de linguaxe ou imaxe, estes sistemas están **adestrados con datos e coñecemento propio dun sector ou dunha función industrial concreta**, como operacións de mantemento, procesos industriais, documentación técnica ou análise de incidentes. Isto permite desenvolver asistentes e ferramentas capaces de **interpretar documentación técnica, apoiar o diagnóstico de fallos, xerar procedementos operativos ou asistir a persoal técnico en tempo real**, cun nivel de precisión maior que os modelos xenéricos.

Relevancia e implicacións

Os modelos de **IA xerativa específicos de dominio poden contribuír a mellorar a xestión do coñecemento industrial, a formación de persoal e a resolución de incidencias técnicas**. Ao mesmo tempo, a súa integración nos fluxos operativos introduce novos retos en materia de **seguridade da información, protección de datos industriais sensibles e control das decisións automatizadas**. O uso destes sistemas require establecer **políticas claras de gobernanza da IA, control do acceso á información e validación das respostas xeradas polos modelos**, especialmente cando se aplican a procesos críticos.

Consideracións adicionais

Estes modelos xerativos especializados están a ser adoptados progresivamente en ámbitos como o **soporte técnico industrial, a análise de documentación de enxeñaría, a xestión de coñecemento corporativo ou a automatización de tarefas cognitivas complexas**. Con todo, diversos estudos sinalan que estes sistemas poden introducir riscos asociados á **filtración de información sensible, á xeración de respostas incorrectas (alucinacións) ou á manipulación dos modelos mediante ataques de prompt injection ou envelenamento de datos**. Por este motivo, organismos e informes especializados destacan a necesidade de aplicar **mecanismos de gobernanza, avaliación continua de modelos e control da calidade dos datos**

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

empregados no adestramento como parte esencial da súa implantación en contornos industriais [13].

3.2.1.6 Axentes de IA (AI Agents)

Descrición da tendencia

Os **axentes de intelixencia artificial (AI Agents)** representan unha evolución dos sistemas tradicionais baseados en modelos de IA cara a **entidades software capaces de executar tarefas de forma autónoma, interactuar con sistemas externos e tomar decisións baseadas en obxectivos definidos**. A diferenza dos sistemas de análise ou recomendación convencionais, os axentes de IA poden **interpretar información, planificar accións, executar procesos e adaptar o seu comportamento en función do contexto operativo**. No ámbito industrial, estes axentes poden empregarse para **coordinar operacións, xestionar fluxos de datos industriais, asistir na supervisión de procesos ou automatizar tarefas complexas de análise e control**.

Relevancia e implicacións

Para o **ecosistema industrial galego**, a introdución de axentes de IA pode contribuír a **automatizar procesos de análise, mellorar a xestión operativa e optimizar a toma de decisións en contornos industriais complexos**. Estudios coma o seguinte de IBM avalan esta tese:

Enquisa de impacto da IA axéntica na empresa. Fonte: IBM (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

En sectores con operacións distribuídas ou con sistemas altamente interconectados, estes sistemas poden apoiar tarefas como **monitorización continua de activos, detección de anomalías operacionais ou coordinación de respostas ante incidencias técnicas**. Non obstante, o uso de axentes autónomos tamén introduce **novos retos en materia de control, supervisión e ciberseguridade**, xa que a capacidade destes sistemas para interactuar con múltiples compoñentes da infraestrutura industrial pode amplificar o impacto de posibles erros, manipulacións ou vulnerabilidades.

Consideracións adicionais

Diversos informes tecnolóxicos sinalan que os axentes de IA están a evolucionar rapidamente cara a **arquitecturas multi-axente**, nas que diferentes sistemas cooperan para resolver tarefas complexas ou coordinar procesos distribuídos. Esta evolución abre oportunidades para **automatizar operacións industriais e mellorar a eficiencia operativa**, pero tamén require establecer **mecanismos robustos de gobernanza, supervisión humana e control das accións executadas polos axentes** [14]. Ademais, dende o punto de vista da ciberseguridade, resulta esencial garantir a **integridade dos datos utilizados polos axentes, a autenticidade das interaccións entre sistemas e a capacidade de auditoría das decisións automatizadas**, especialmente cando estes sistemas se integran en procesos industriais críticos.

3.2.1.7 Axentes de IA que transforman procesos (AI Agents Transcend Processes)

Descrición da tendencia

Unha evolución recente no desenvolvemento de sistemas baseados en intelixencia artificial é a aparición de **axentes capaces de transcender procesos individuais e coordinar cadeas completas de actividade**, coñecidos como AI Agents Transcend Processes. Mentres que os primeiros axentes de IA estaban orientados a tarefas específicas —como análise de datos ou execución de accións limitadas—, os novos modelos permiten **orquestrar múltiples procesos, integrar información procedente de diferentes sistemas e adaptar dinámicamente os fluxos de traballo**. Estes sistemas poden interactuar con aplicacións empresariais, sistemas industriais ou plataformas de análise para **automatizar secuencias completas de decisión e execución**, converténdose nun elemento clave da próxima xeración de automatización empresarial.

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 implicacións

Esta tendencia pode ter un impacto significativo na forma en que se xestionan **procesos produtivos complexos, cadeas de subministración e operacións distribuídas**. A capacidade de coordinar múltiples sistemas e procesos mediante axentes intelixentes pode contribuír a **optimizar fluxos de produción, mellorar a resposta ante incidencias e aumentar a eficiencia operativa**. Con todo, a introdución destes sistemas tamén amplía a **dependencia de infraestruturas dixitais e de decisións automatizadas**, o que require reforzar os mecanismos de **control, supervisión humana e gobernanza da automatización** en contornos industriais.

Consideracións adicionais

Os sistemas de axentes capaces de coordinar procesos completos están asociados ao desenvolvemento de **arquitecturas multi-axente e plataformas de automatización intelixente**, nas que diferentes compoñentes cooperan para resolver tarefas complexas. Esta evolución pode impulsar unha nova fase da **automatización industrial e da xestión baseada en datos**, pero tamén introduce novos riscos asociados á **dependencia de decisións automatizadas, á manipulación de fluxos de información e á posible propagación de erros entre sistemas interconectados**. Por este motivo, os riscos son similares aos das tendencias previas. O enfoque é tan novidoso que apenas hai aínda literatura ao respecto.

3.2.1.8 Intelixencia para a toma de decisións (Decision Intelligence)

Descrición da tendencia

A **Decision Intelligence** refírese ao uso combinado de **intelixencia artificial, análise avanzada de datos, modelos de decisión e simulación** para mellorar a calidade e a rapidez das decisións organizativas. Este enfoque integra técnicas de **aprendizaxe automática, análise preditiva, optimización e modelado de escenarios** para apoiar aos responsables operativos na selección das mellores opcións en contextos complexos. No ámbito industrial, a Decision Intelligence permite **analizar grandes volumes de datos operacionais, identificar patróns relevantes e recomendar accións baseadas en evidencias**, contribuíndo a optimizar procesos produtivos, xestionar riscos e mellorar a planificación das operacións.

Neste artigo, Roger Moser baixa ó terreo a definición teórica de Gartner para facela accionable [15].

Relevancia e implicacións

A adopción de sistemas de Decision Intelligence pode facilitar unha **mellor xestión de procesos produtivos, cadeas de subministración e operacións enerxéticas**, especialmente en contornos caracterizados por múltiples variables operativas. A integración destas ferramentas permite **anticipar fallos, optimizar a planificación da produción e apoiar a toma de decisións en tempo real**, reforzando a competitividade das organizacións industriais. Non obstante, tamén introduce retos relacionados coa **fiabilidade dos modelos, a dependencia de datos de calidade e a seguridade das plataformas analíticas**, aspectos especialmente relevantes cando estas decisións teñen impacto directo sobre procesos físicos ou infraestruturas críticas.

Consideracións adicionais

A evolución cara a sistemas de Decision Intelligence está estreitamente vinculada á crecente dispoñibilidade de **datos industriais, sensores IoT e plataformas de análise avanzada**, que permiten construír modelos de decisión cada vez mais sofisticados. Con todo, diversos estudos subliñan que a eficacia destes sistemas depende en gran medida da **calidade dos datos utilizados, da transparencia dos algoritmos e da capacidade de supervisión humana das recomendacións xeradas**. Dende a perspectiva da ciberseguridade industrial, resulta fundamental garantir a **integridade dos datos empregados nos procesos de análise, a protección das plataformas analíticas e a resiliencia dos sistemas de apoio á decisión**, xa que a manipulación destes elementos podería influír directamente na toma de decisións operativas.

3.2.1.9 Automatización da decisión con IA e risco de perdas catastróficas

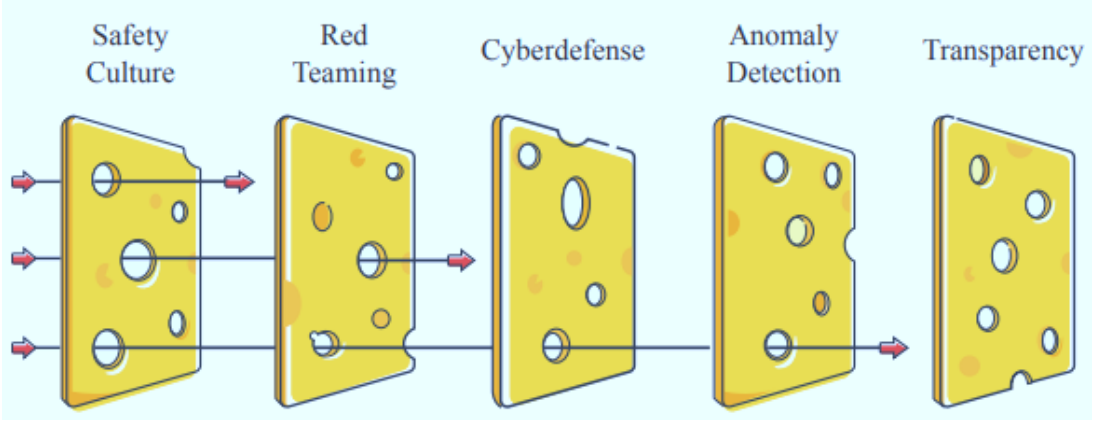
Descrición da tendencia

A crecente integración da **intelixencia artificial en sistemas de apoio á decisión** está a impulsar unha progresiva **automatización de decisións operativas e estratéxicas** en múltiples ámbitos empresariais e industriais. Sistemas baseados en **aprendizaxe automática, análise preditiva e modelos de optimización** son capaces de executar decisións de forma autónoma ou semiautónoma en áreas como planificación da produción, xestión de inventarios, mantemento de activos ou control de procesos industriais. Esta evolución permite **incrementar a velocidade e a eficiencia das operacións**, pero tamén introduce o risco de que decisións automatizadas incorrectas ou manipuladas poidan xerar **impactos operacionais de gran magnitude**.

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 implicacións

No contexto da **industria galega**, onde numerosos procesos industriais dependen de **sistemas automatizados de control e supervisión** (loxística, enerxía, etc.), a automatización da toma de decisións mediante IA pode contribuír a **optimizar operacións e mellorar a capacidade de resposta ante variacións na produción ou no mercado**. Non obstante, tamén implica unha maior **dependencia de sistemas algorítmicos e de datos operacionais**, o que pode amplificar o impacto de posibles erros de modelado, manipulación de datos ou fallos nos sistemas de decisión. En contornos industriais críticos, unha decisión automatizada incorrecta podería **propagar efectos adversos ao longo de cadeas de produción ou sistemas interconectados**, xerando perdas económicas ou interrupcións operativas severas.



Defensa en profundidade para mellorar a seguridade organizacional. Fonte: Center for AI Safety (2023)

Consideracións adicionais

A automatización completa de decisións en sistemas complexos pode introducir **riscos sistémicos difíciles de anticipar**, especialmente cando os modelos operan con pouca supervisión humana ou con datos incompletos. Entre os riscos identificados atópanse a **propagación de erros algorítmicos, a manipulación de datos utilizados polos modelos, malware, ou a perda de capacidade ou manipulación da intervención humana en procesos críticos** [16]. Por este motivo, organismos e expertos recomendan aplicar **principios de supervisión humana significativa, mecanismos de auditoría algorítmica e controis de seguridade nos sistemas de decisión automatizados**, especialmente cando estes teñen impacto directo sobre operacións industriais ou infraestruturas críticas.

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

3.2.1.10 Gobernanza da IA como factor crítico organizativo

Descrición da tendencia

A rápida adopción de sistemas baseados en **intelixencia artificial (IA)** en múltiples ámbitos empresariais e industriais está a impulsar a aparición dun novo ámbito de xestión coñecido como **gobernanza da IA**. Este concepto refírese ao conxunto de **políticas, procesos, mecanismos de control e estruturas organizativas** destinados a garantir que o desenvolvemento, despregamento e uso da IA se realice de maneira **segura, transparente, responsable e conforme ás regulacións aplicables**. A gobernanza da IA inclúe aspectos como a **xestión do risco algorítmico, a supervisión humana das decisións automatizadas, a trazabilidade dos modelos e a protección dos datos utilizados nos sistemas de IA**.

Relevancia e implicacións

A gobernanza da IA convértese nun elemento cada vez máis relevante a medida que as organizacións incorporan **sistemas de análise avanzada, automatización baseada en datos e ferramentas de apoio á decisión**. A ausencia de marcos claros de gobernanza pode provocar **dependencia excesiva de decisións automatizadas, falta de control sobre os modelos empregados ou exposición a riscos legais e reputacionais**. Ademais, a progresiva aparición de **regulación específica sobre intelixencia artificial**, especialmente no ámbito europeo, implica que as organizacións deberán establecer **estruturas de control, avaliación de riscos e procedementos de supervisión** para garantir o cumprimento normativo e a utilización responsable destas tecnoloxías.

Consideracións adicionais

A gobernanza da IA está a consolidarse como un dos principais eixes da transformación dixital responsable. Diversos organismos internacionais e iniciativas reguladoras subliñan que as organizacións deben implementar **marcos de gobernanza que inclúan avaliación de riscos, mecanismos de auditoría dos modelos, control da calidade dos datos e supervisión humana significativa**. Neste contexto, está a emerxer o concepto de **Sistemas de Xestión da Intelixencia Artificial (SXIA)**, que buscan estruturar de forma sistemática a gobernanza destas tecnoloxías dentro das organizacións. A norma **ISO/IEC 42001** [17], publicada recentemente, establece os requisitos para implementar un **sistema de xestión específico para a IA**, inspirado en

modelos de xestión xa consolidados como **ISO 27001 para seguridade da información** ou **ISO 9001 para xestión da calidade**.

No contexto europeo, ademais, o desenvolvemento do **Regulamento de Intelixencia Artificial da Unión Europea (AI Act)** [12] establece un marco normativo destinado a **regular o uso de sistemas de IA en función do seu nivel de risco**, o que reforza a necesidade de que as organizacións adopten **estruturas formais de gobernanza, avaliación de riscos e control do ciclo de vida dos modelos de IA**.

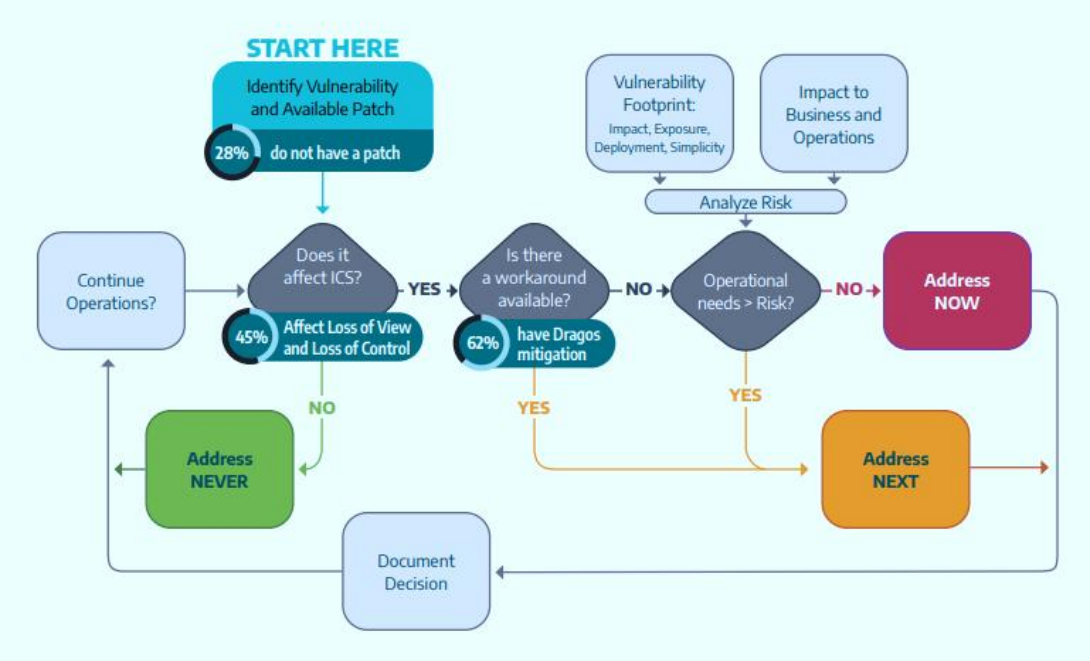
A converxencia entre regulación europea e estándares internacionais apunta a que, nos próximos anos, a implantación de **SXIA (Sistemas de Xestión da IA) baseados en ISO 42001** podería converterse nun elemento clave para demostrar **cumprimento normativo, responsabilidade algorítmica e confianza nas solucións baseadas en IA.**

3.2.1.11 Xestión de vulnerabilidades e parcheo en OT orientado a risco

A **xestión de vulnerabilidades en contornos OT** está a evolucionar dende enfoques tradicionais baseados unicamente na aplicación periódica de parches cara a modelos máis avanzados de **xestión de vulnerabilidades orientada a risco** [18]. Nos sistemas industriais, a aplicación directa de actualizacións de software pode resultar complexa debido a factores como a **necesidade de continuidade operativa, a dependencia de fabricantes, a certificación de equipos ou a antigüidade de determinados sistemas de control**.

Por este motivo, cada vez máis organizacións industriais adoptan enfoques que combinan **avaliación do risco, priorización de vulnerabilidades, medidas compensatorias e planificación controlada de actualizacións**, co obxectivo de reducir a exposición sen comprometer a estabilidade das operacións:

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



Árbore de decisión de parcheo urxente do DHS americano. Fonte: Dragos (2024)

Relevancia e implicacións

No caso do **tecido industrial galego e no sector en xeral**, caracterizado pola presenza de **instalacións industriais con ciclos de vida longos e infraestruturas críticas distribuídas**, a xestión de vulnerabilidades en OT representa un desafío significativo. Moitos sistemas industriais non poden actualizarse coa mesma frecuencia que os sistemas IT convencionais, o que fai necesario adoptar **estratexias de priorización baseadas no impacto operativo, na criticidade dos activos e na probabilidade de explotación das vulnerabilidades**. A implementación de procesos estruturados de xestión de vulnerabilidades permite **reducir a superficie de ataque, mellorar a visibilidade dos activos industriais e fortalecer a resiliencia das instalacións fronte a ameazas cibernéticas**.

Consideracións adicionais

A xestión de vulnerabilidades orientada a risco implica combinar **diferentes medidas técnicas e organizativas** cando a aplicación inmediata dun parche non é viable. Entre estas medidas inclúense a **segmentación de redes industriais, a limitación de accesos remotos, a monitorización específica de protocolos OT ou a implantación de controis compensatorios** que reduzan a probabilidade de explotación.

No Informe de Ciberalertas OT II do Observatorio de Ciberseguridade Industrial de Galicia [19] analízanse precisamente **estratexias de priorización baseadas no risco**

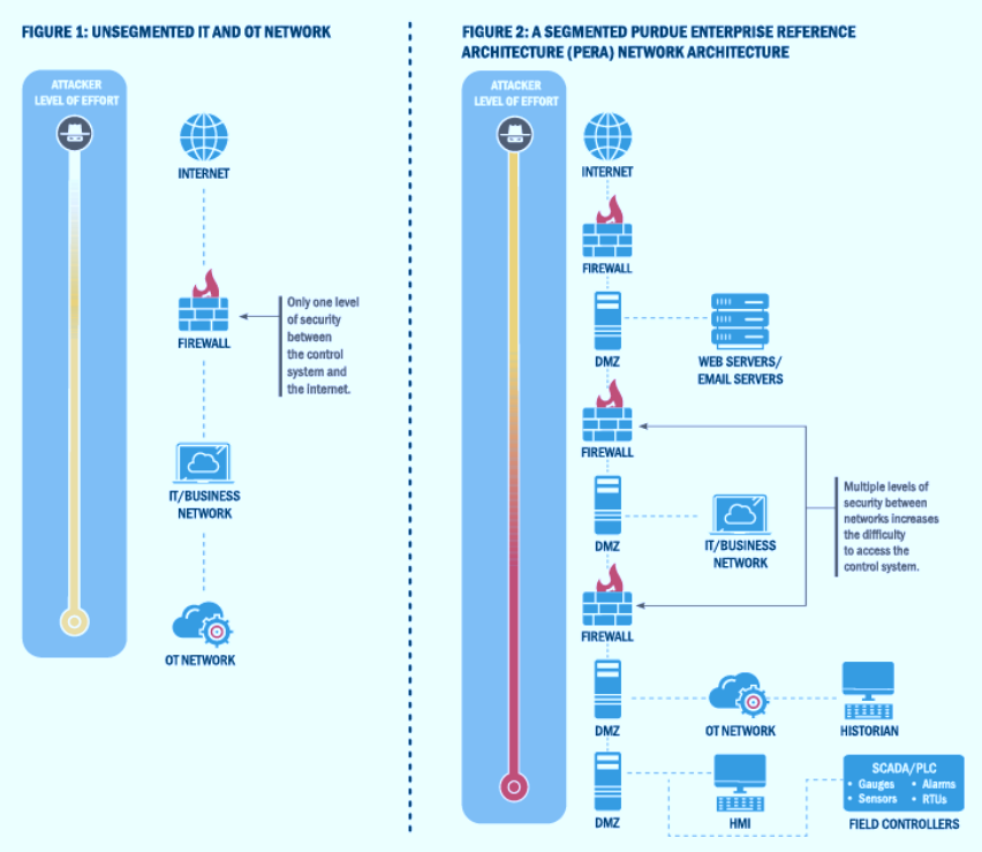
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

para a xestión de vulnerabilidades, destacando a importancia de avaliar non só a gravidade técnica dunha vulnerabilidade, senón tamén **o contexto operativo no que se atopa o activo industrial**. Esta aproximación permite adoptar decisións máis realistas sobre cando e como aplicar actualizacións, mantendo o equilibrio entre **seguridade e continuidade das operacións industriais**.

3.2.1.12 Segmentación e segregación de redes OT

Descrición da tendencia

A **segmentación e segregación de redes industriais** constitúe un dos principios fundamentais da arquitectura de ciberseguridade en contornos OT. Este enfoque baséase en **dividir a infraestrutura de rede en zonas ou segmentos con diferentes niveis de confianza**, limitando as comunicacións entre sistemas e reducindo a propagación de incidentes. Nos contornos industriais modernos, onde conviven sistemas de control, redes corporativas e servizos conectados á internet, a segmentación permite **establecer barreiras de protección entre dominios IT e OT**, así como entre distintos niveis da propia rede industrial.



Arquitectura segmentada IT/OT fronte a non segmentada. Fonte: CISA (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

Relevancia e implicacións

A implantación de arquitecturas segmentadas é clave para **protexer procesos críticos e reducir o impacto potencial dun incidente de ciberseguridade**. A separación adecuada entre redes corporativas e sistemas industriais dificulta que un ataque iniciado nun sistema IT poida alcanzar directamente os sistemas de control. Ademais, a segmentación permite **controlar e monitorizar con maior precisión os fluxos de comunicación entre equipos industriais**, facilitando a detección de comportamentos anómalos ou accesos non autorizados.

Consideracións adicionais

Na práctica, a segmentación en contornos OT adoita implementarse mediante **zonas de seguridade, condutos de comunicación controlados** (descrito con detalle na Guía normativa de ciberseguridade industrial dende mesmo Observatorio, no apartado dedicado a ISA/IEC 62443 [20]), **firewalls industriais e políticas de acceso específicas para protocolos industriais**. Este enfoque permite establecer **capas adicionais de protección** sen interferir na operación normal das instalacións. Ao mesmo tempo, a segmentación facilita a aplicación de outras medidas de seguridade, como a **monitorización do tráfico industrial, a xestión de accesos remotos ou a aplicación de controis compensatorios cando determinados sistemas non poden actualizarse con frecuencia**. A adopción de arquitecturas de rede baseadas en zonas e condutos forma parte das boas prácticas de seguridade industrial e contribúe a **incrementar a resiliencia das infraestruturas industriais fronte a incidentes**.

3.2.1.13 Soberanía tecnolóxica (Technological Sovereignty)

Descrición da tendencia

A **soberanía tecnolóxica** refírese á capacidade dun país, rexión ou organización para **controlar e desenvolver as tecnoloxías críticas das que dependen as súas infraestruturas e actividades económicas**, reducindo a dependencia excesiva de provedores externos. No ámbito industrial e dixital, este concepto abrangue aspectos como a **autonomía en software, hardware, infraestruturas de datos, servizos cloud, semicondutores ou tecnoloxías de intelixencia artificial**. Nos últimos anos, especialmente dende a guerra entre Rusia e Ucraína, a crecente tensión xeopolítica, as interrupcións nas cadeas de subministración e a importancia estratéxica das tecnoloxías dixitais impulsaron políticas públicas orientadas a **reforzar a autonomía tecnolóxica e por ende a resiliencia industrial** [21][22].

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 implicacións

O **ecosistema industrial galego**, integrado en cadeas de valor globais e fortemente dependente de tecnoloxías dixitais e industriais importadas, a cuestión da soberanía tecnolóxica está directamente relacionada coa **resiliencia das infraestruturas industriais e a seguridade das cadeas de subministración tecnolóxica**. A dependencia de determinados provedores ou plataformas pode introducir **riscos de continuidade operativa, limitacións na capacidade de resposta ante incidentes ou dificultades para aplicar políticas de seguridade adaptadas ao contexto local**. Neste sentido, reforzar a diversidade de provedores, fomentar capacidades tecnolóxicas propias e adoptar estándares abertos contribúe a **reducir vulnerabilidades estruturais e aumentar a capacidade de control sobre as infraestruturas críticas**.

Consideracións adicionais

A soberanía tecnolóxica non implica necesariamente substituír tecnoloxías externas, senón **garantir que as organizacións manteñan capacidade de decisión e control sobre os sistemas que sustentan a súa actividade**. No ámbito europeo, este enfoque está a materializarse en iniciativas orientadas a **reforzar a autonomía dixital, promover ecosistemas industriais propios e reducir dependencias estratéxicas en tecnoloxías críticas**. Para as organizacións industriais, isto tradúcese en prácticas como **avaliar riscos asociados a provedores tecnolóxicos, diversificar cadeas de subministración, adoptar estándares interoperables e reforzar a transparencia sobre compoñentes e software utilizados nos sistemas industriais**.

3.2.1.14 Cadea de subministración e dependencia de terceiros en OT

Descrición da tendencia

Os sistemas industriais actuais dependen cada vez máis dunha **cadea de subministración complexa que inclúe fabricantes de hardware, provedores de software, integradores de sistemas, servizos de mantemento e plataformas de conectividade**. Esta realidade implica que unha parte significativa das tecnoloxías utilizadas nos contornos OT non é desenvolvida nin controlada directamente polas organizacións que operan as infraestruturas industriais. Como consecuencia, os riscos asociados á **cadea de subministración tecnolóxica** convertéronse nun elemento central da ciberseguridade industrial, xa que vulnerabilidades ou incidentes nun provedor poden afectar a múltiples organizacións de forma simultánea.

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 implicacións

De novo, para os sectores caracterizados pola integración en **cadeas de valor internacionais e polo uso intensivo de tecnoloxía industrial especializada**, a dependencia de terceiros é unha realidade estrutural. Fabricantes de equipos industriais, provedores de software de control, integradores de automatización ou empresas de mantemento remoto participan de maneira directa na operación das infraestruturas industriais. Isto implica que a seguridade destes sistemas non depende unicamente das medidas internas das organizacións, senón tamén da **madurez de ciberseguridade dos provedores e das condicións de seguridade establecidas nos contratos e relacións comerciais**, como se pode ver neste estudio de ENISA [23].

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 comúns para comprometer a cadea de subministración. Fonte: ENISA (2021)

Consideracións adicionais

A xestión do risco asociado á cadea de subministración require incorporar prácticas como a **avaliación de seguridade de provedores, a definición de requisitos de ciberseguridade en contratos, a supervisión do acceso remoto de terceiros e a análise da procedencia dos compoñentes tecnolóxicos utilizados nos sistemas industriais**. Ademais, a crecente complexidade das arquitecturas industriais fai recomendable manter **inventarios actualizados de activos e dependencias tecnolóxicas**, co fin de comprender como un incidente nun provedor podería afectar á

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

operación industrial. A adopción deste tipo de medidas permite **reducir a exposición a riscos derivados de terceiros e fortalecer a resiliencia das cadeas industriais dixitalizadas**.

3.2.1.15 Sistema dixital inmune (Digital Immune System)

Descrición da tendencia

O concepto de **Sistema Dixital Inmune (Digital Immune System)** describe un enfoque de arquitectura tecnolóxica orientado a **aumentar a resiliencia dos sistemas dixitais mediante a detección temperá de erros, a resposta automática a incidentes e a capacidade de recuperación continua**. Inspirado na idea do sistema inmunitario biolóxico, este enfoque combina **observabilidade avanzada, automatización, intelixencia artificial, probas continuas e mecanismos de autorrecuperación** para identificar anomalías e responder rapidamente antes de que os fallos ou incidentes teñan impacto significativo nas operacións. No ámbito industrial, estes sistemas poden integrarse en plataformas de monitorización, sistemas de control e infraestruturas dixitais para **anticipar incidentes e manter a continuidade operativa**. O concepto explícase con maior profundidade neste artigo, aplicado a produtos dixitais [24].

Elementos dun sistema dixital inmune. Fonte: Gartner (2021)

Relevancia e implicacións

Para a **industria galega**, onde gran parte das instalacións industriais dependen de **sistemas de control e supervisión que deben operar de forma continua**, a incorporación de capacidades propias dun sistema dixital inmune pode contribuír a **reducir o tempo de detección de incidentes, mellorar a capacidade de resposta e limitar o impacto de fallos técnicos ou ataques de ciberseguridade**. A integración de ferramentas de observabilidade, análise automatizada e resposta coordinada permite **identificar anomalías en procesos industriais, detectar comportamentos anómalos na rede OT e activar mecanismos de mitigación de forma máis rápida**.

Consideracións adicionais

A implantación de sistemas dixitais inmunes adoita combinar **monitorización continua de activos, análise de telemetría, automatización de resposta e mecanismos de probas e validación constantes**. Este enfoque resulta especialmente relevante en contornos industriais onde os sistemas deben operar durante longos períodos sen interrupcións. A adopción destas capacidades contribúe a **incrementar a resiliencia operativa das infraestruturas industriais**, permitindo detectar anomalías antes de que se convertan en incidentes graves e facilitando a recuperación rápida dos sistemas afectados.

3.2.1.16 Cripto-axilidade (Crypto-Agility)

Descrición da tendencia

A **cripto-axilidade** refírese á capacidade dun sistema tecnolóxico para **adaptar ou substituír rapidamente os algoritmos criptográficos utilizados para protexer datos e comunicacións** cando estes deixan de ser seguros ou quedan obsoletos. Nun contexto no que evolucionan constantemente as técnicas de ataque e aparecen novas capacidades computacionais —como a computación cuántica—, as organizacións necesitan infraestruturas capaces de **actualizar mecanismos de cifrado, xestión de claves e protocolos de seguridade sen interromper os servizos**. Nos contornos industriais, isto implica deseñar sistemas e arquitecturas que permitan **modificar algoritmos criptográficos ou renovar certificados e claves de forma controlada ao longo do ciclo de vida das instalacións**.

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 implicacións

Nun **sector industrial** onde numerosos sistemas OT teñen ciclos de vida que poden superar as dúas décadas, a capacidade de adaptar mecanismos criptográficos convértese nun factor clave de seguridade a longo prazo. Moitos sistemas industriais incorporan **protocolos de comunicación, dispositivos embebidos ou sistemas de autenticación deseñados hai anos**, o que pode dificultar a actualización dos mecanismos de cifrado (supoñendo que dispoñen deles en primeiro lugar). As arquitecturas con capacidade de evolución criptográfica permite **protexer comunicacións industriais, accesos remotos e intercambio de datos entre sistemas** mesmo cando os algoritmos empregados inicialmente deixan de ser considerados seguros.

Consideracións adicionais

A transición cara a modelos de cripto-axilidade está estreitamente relacionada coa preparación para **novos estándares criptográficos e co desenvolvemento de criptografía poscuántica**. Para as organizacións industriais, isto supón a necesidade de **inventariar algoritmos criptográficos empregados nos sistemas, establecer políticas de xestión de claves robustas e garantir que as plataformas tecnolóxicas permiten actualizar mecanismos de seguridade ao longo do tempo**. A adopción deste enfoque reduce o risco de dependencia de tecnoloxías criptográficas obsoletas e facilita a adaptación das infraestruturas industriais a futuros requirimentos de seguridade [25]. Segundo o NCSC (national Cyber Security Centre) británico, en 2035 as organizacións deberían completar a migración dos seus sistemas a algoritmos post-cuánticos [26].

3.2.1.17 SCADA na nube e cloudización de contornos OT

Descrición da tendencia

A progresiva dixitalización da industria está a favorecer a **migración de determinadas funcións dos sistemas industriais cara a infraestruturas cloud**, incluíndo plataformas de supervisión, análise de datos ou integración de sistemas SCADA. Tradicionalmente, os sistemas **SCADA (Supervisory Control and Data Acquisition)** operaban en contornos locais e altamente illados; porén, a necesidade de **analizar grandes volumes de datos operacionais, integrar sistemas distribuídos e habilitar operacións remotas** está a impulsar modelos híbridos nos que parte das 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 supervisión e análise se executan en contornos cloud ou en arquitecturas combinadas de **edge computing e cloud industrial**.

Relevancia e implicacións

Galicia non é excepción en canto a que existen instalacións industriais e infraestruturas críticas distribuídas xeograficamente. Neste eido, a cloudización de compoñentes SCADA pode facilitar **unha maior visibilidade operativa, mellores capacidades de análise de datos industriais e unha xestión máis centralizada das operacións**. A integración con plataformas cloud tamén permite **aproveitar ferramentas avanzadas de análise, intelixencia artificial ou mantemento preditivo**. Non obstante, esta evolución introduce novos retos en materia de **seguridade da conectividade, protección de datos industriais e control das comunicacións entre sistemas OT e plataformas externas**, polo que resulta esencial deseñar arquitecturas que manteñan **zonas de seguridade claramente definidas e mecanismos de protección para as comunicacións industriais en base a boas prácticas** [27].

Consideracións adicionais

A adopción de modelos híbridos OT–cloud require abordar cuestións como a **seguridade das pasarelas de comunicación, a autenticación dos dispositivos industriais, a protección das API utilizadas para integrar sistemas e a visibilidade do tráfico entre contornos industriais e plataformas cloud**. Ademais, a separación adecuada entre **funcións críticas de control e servizos de análise ou supervisión na nube** resulta fundamental para evitar que incidentes nun contorno externo afecten directamente aos procesos físicos. Un deseño adecuado destas arquitecturas permite **aproveitar as vantaxes da computación cloud mantendo os requisitos de seguridade e continuidade operativa propios dos sistemas industriais**.

3.2.1.18 Arquitectura OT "defendible" (resiliente por deseño)

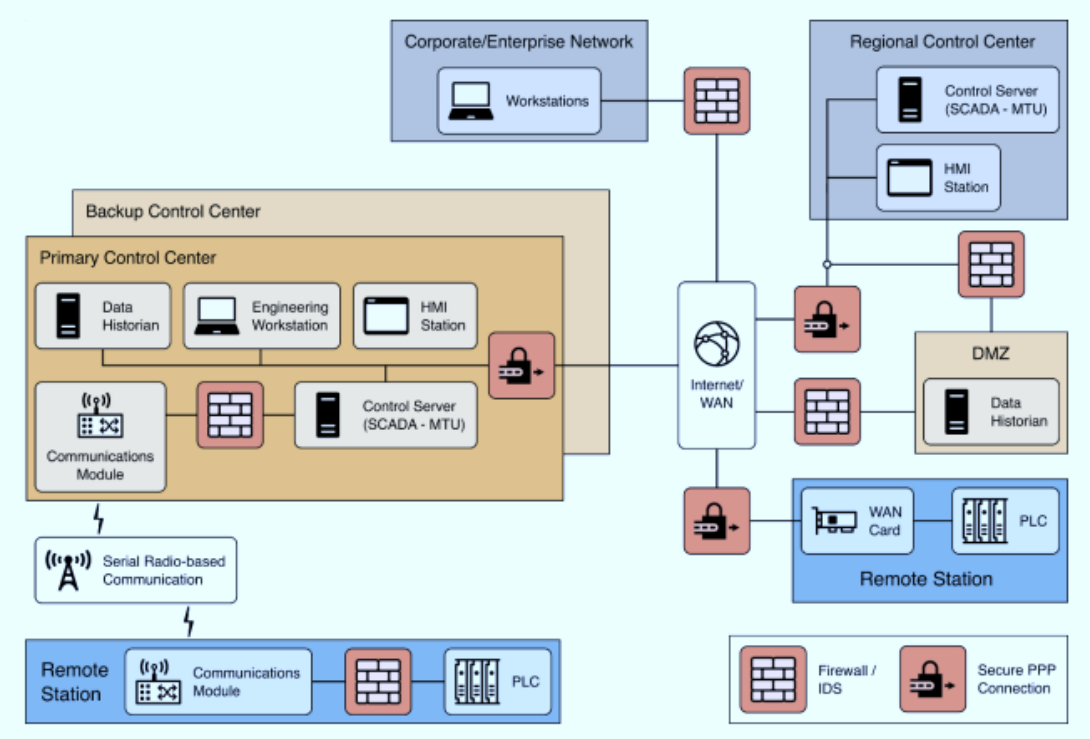
Descrición da tendencia

O concepto de **arquitectura OT defendible** refírese ao deseño de infraestruturas industriais nas que a **seguridade e a resiliencia se incorporan dende a propia arquitectura dos sistemas**, e non unicamente mediante medidas adicionais aplicadas posteriormente. Este enfoque implica estruturar as redes e os sistemas industriais de maneira que **un incidente ou intrusión non poida propagarse facilmente nin comprometer a totalidade da operación**. Para iso combínanse entre outros, principios como **segmentación por zonas, control estrito das comunicacións,**

monitorización continua, autenticación robusta e mecanismos de resposta ante incidentes, integrados no propio deseño da infraestrutura.

Relevancia e implicacións

No contexto rexional, onde moitas instalacións industriais combinan sistemas modernos con equipos herdados e ciclos de vida tecnolóxicos longos, o deseño dunha arquitectura defendible resulta fundamental para **limitar o impacto potencial de incidentes de ciberseguridade**. Unha infraestrutura deseñada con estes principios permite **conter intrusións, protexer os sistemas de control críticos e manter a continuidade operativa mesmo ante incidentes que afecten a partes da rede industrial**. Ademais, facilita a integración progresiva de novas tecnoloxías —como conectividade remota, análise de datos ou plataformas cloud— mantendo **contornos claramente delimitados e controlados**. No informe **Guía normativa do Observatorio** recompílanse algúns dos controis mais habituais empregados en contornos ICS/OT [20].



Exemplo de arquitectura de seguridade para un sistema SCADA. Fonte: NIST (2023)

Consideracións adicionais

A construción de arquitecturas OT defendibles adoita basearse en **modelos de referencia de seguridade industrial, boas prácticas de segmentación e enfoques de defensa en profundidade**, nos que múltiples capas de protección reducen a

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

probabilidade de compromiso completo do sistema. Este enfoque tamén require **inventariar activos industriais, comprender as dependencias entre sistemas e establecer controis específicos para os fluxos de comunicación entre compoñentes da infraestrutura**. Aplicar estes principios permite ás organizacións **anticipar escenarios de risco e deseñar infraestruturas capaces de absorber e recuperar rapidamente de incidentes**, reforzando a resiliencia das operacións industriais dixitalizadas. Unha inspiración de boas prácticas neste eido é a guía do NIST (Instituto Nacional de Estándares e Tecnoloxía americano) SP 800-82 [28].

3.2.2 De atención programada (prioridade #2)

3.2.2.1 Computación confidencial (Confidential Computing)

Descrición da tendencia

A **computación confidencial** refírese a un conxunto de tecnoloxías destinadas a **protexer os datos mentres están a ser procesados**, non só cando están almacenados ou transmitidos. Tradicionalmente, os sistemas informáticos cifran a información en repouso ou en tránsito, pero durante o procesamento os datos adoitan permanecer descifrados na memoria. A computación confidencial introduce mecanismos baseados en **enclaves seguros de hardware, contornos de execución confiables (TEE) e procesamento cifrado**, que permiten executar operacións sobre datos sensibles mantendo a súa protección incluso durante o cálculo.

Relevancia e implicacións

Para organizacións industriais que manexan **datos operacionais, información de produción ou telemetría de sistemas industriais**, este enfoque abre novas posibilidades para **compartir e analizar información sen expor directamente os datos sensibles**. Isto pode resultar especialmente útil en contornos nos que diferentes entidades —como operadores industriais, provedores tecnolóxicos ou centros de análise— necesitan colaborar sobre datos industriais mantendo garantías de confidencialidade. En escenarios de **integración OT–cloud ou análise avanzada de datos industriais**, a computación confidencial permite reducir os riscos asociados á exposición de información crítica.

Consideracións adicionais

A adopción destas tecnoloxías está estreitamente ligada á evolución das **arquitecturas cloud seguras e das plataformas de análise de datos distribuídas**. No ámbito

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

industrial, a computación confidencial pode facilitar modelos nos que a información operativa se analiza externamente sen revelar o contido completo dos datos. Isto resulta relevante para casos de uso como **análise de rendemento industrial, detección de anomalías ou colaboración entre organizacións** que necesitan compartir información de maneira controlada. O desenvolvemento de estándares e ecosistemas tecnolóxicos arredor desta tecnoloxía está impulsando a súa adopción progresiva en contornos onde a **protección da información é un requisito esencial** [29].

3.2.2.2 Cifrado homomórfico (Homomorphic Encryption)

Descrición da tendencia

O **cifrado homomórfico** é unha técnica criptográfica que permite **realizar operacións matemáticas sobre datos cifrados sen necesidade de descifralos previamente** [30][31]. Isto significa que os sistemas poden procesar información sensible mantendo os datos protexidos durante todo o ciclo de tratamento, por exemplo no sector saúde. Aínda que durante moito tempo foi considerado un enfoque teórico ou con limitacións prácticas, os avances recentes en algoritmos e capacidade computacional están a facer posible a súa aplicación en determinados escenarios reais, especialmente en ámbitos nos que a **privacidade e a protección da información son críticas**.

Relevancia e implicacións

No contexto industrial, o cifrado homomórfico abre a porta a **novos modelos de colaboración e análise de datos** entre organizacións sen necesidade de revelar información sensible. Isto pode resultar útil en casos como **análise conxunta de datos industriais, investigación colaborativa entre empresas ou tratamento de información operativa en plataformas externas**, mantendo a confidencialidade dos datos de orixe. Para o tecido industrial galego, esta tecnoloxía podería facilitar a **cooperación en cadeas de valor industriais ou proxectos de innovación compartidos**, permitindo analizar información agregada sen comprometer segredos industriais ou datos estratéxicos.

Consideracións adicionais

A pesar do seu potencial, o cifrado homomórfico segue presentando **desafíos en termos de rendemento e complexidade computacional**, polo que actualmente adoita empregarse en escenarios específicos onde a protección da información xustifica o custo adicional de procesamento. A súa evolución está estreitamente vinculada ao desenvolvemento de **plataformas de análise segura de datos e arquitecturas cloud**

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

orientadas á privacidade. Co avance das tecnoloxías de procesamento e a aparición de ferramentas máis eficientes, espérase que estas técnicas poidan incorporarse progresivamente a contornos nos que a **confidencialidade dos datos industriais e a colaboración segura entre organizacións** sexan requisitos prioritarios.

3.2.2.3 Seguridade fronte á desinformación (Disinformation Security)

Descrición da tendencia

A **seguridade fronte á desinformación** refírese ao conxunto de estratexias destinadas a **detectar, analizar e mitigar campañas de manipulación informativa que poden afectar organizacións, infraestruturas críticas ou procesos económicos**. A expansión das redes sociais, das plataformas dixitais e das ferramentas baseadas en intelixencia artificial está a facilitar a creación e difusión de contido manipulado a gran escala, incluíndo **mensaxes coordinadas, contido sintético ou información falsa xerada automaticamente**. Este fenómeno converteuse nun risco relevante para a estabilidade institucional, a reputación das organizacións e a confianza pública nos sistemas tecnolóxicos, polo que incluso as institución europeas están tomando cartas no asunto [32].

Relevancia e implicacións

Aínda que a desinformación adoita asociarse a contextos políticos ou sociais, tamén pode ter **impacto directo sobre sectores industriais e infraestruturas críticas**. A difusión de información falsa sobre incidentes industriais, interrupcións de servizos ou supostos fallos de seguridade pode **afectar á reputación das organizacións, provocar reaccións no mercado ou xerar alarma social**. Nun contexto como o galego, onde determinados sectores industriais teñen forte impacto territorial e económico, a capacidade de **monitorizar o ecosistema informativo e responder con rapidez a narrativas falsas** convértese nun elemento adicional da resiliencia organizativa.

Consideracións adicionais

A xestión deste tipo de riscos require combinar **capacidades de análise de información aberta, monitorización de redes sociais, análise de patróns de difusión e verificación de contidos**. Ademais, as organizacións deben contar con **estratexias de comunicación claras e protocolos de resposta ante información incorrecta ou manipulada**, especialmente cando poden afectar á confianza pública ou á continuidade de operacións críticas. O desenvolvemento de ferramentas baseadas en intelixencia artificial para detectar contido manipulado e identificar campañas

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

coordinadas está a converterse nun compoñente relevante das estratexias modernas de seguridade informativa.

3.2.2.4 Xeopatriación (Geopatriation)

Descrición da tendencia

A **xeopatriación** describe o proceso polo cal **datos, infraestruturas dixitais ou capacidades tecnolóxicas son relocalizadas ou mantidas dentro dunha determinada xurisdición xeográfica** por razóns de seguridade, control regulamentario ou autonomía tecnolóxica. Esta tendencia está a gañar relevancia nun contexto de crecente competencia xeopolítica e preocupación pola dependencia de infraestruturas tecnolóxicas estranxeiras [33]. Como consecuencia, gobernos e organizacións están a impulsar políticas e axudas destinadas a **garantir que datos críticos, sistemas dixitais ou servizos tecnolóxicos clave permanezan baixo control territorial ou xurisdicional específico**.

Relevancia e implicacións

A xeopatriación pode influír na forma en que as organizacións **seleccionan provedores tecnolóxicos, localizan os seus datos ou despregan infraestruturas dixitais**. Determinadas regulacións europeas e nacionais están a promover que **datos sensibles, sistemas de control ou información estratéxica se almacenen ou procesen dentro do espazo xurisdicional europeo**, o que pode afectar decisións relacionadas coa adopción de plataformas cloud, servizos de análise de datos ou infraestruturas dixitais compartidas. Esta tendencia tamén se relaciona coa necesidade de **avaliar riscos asociados á dependencia tecnolóxica de provedores situados fóra do ámbito regulamentario europeo**.

Consideracións adicionais

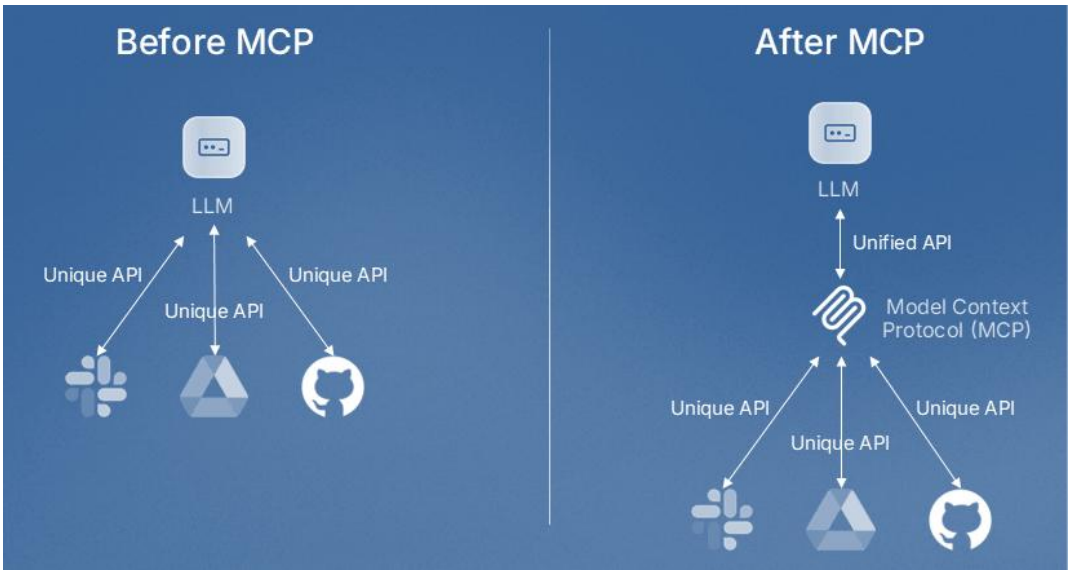
A xeopatriación está estreitamente ligada a conceptos como **soberanía dixital, control das cadeas tecnolóxicas e resiliencia das infraestruturas críticas**. Para as organizacións industriais, isto pode implicar revisar a **localización de centros de datos, a procedencia de determinados servizos tecnolóxicos ou as condicións xurídicas aplicables ao tratamento de información industrial**. Ao mesmo tempo, a evolución das políticas europeas en materia de datos e infraestruturas dixitais apunta a un escenario no que a **localización e gobernanza dos datos industriais** converteranse nun factor relevante na planificación tecnolóxica das organizacións.

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)

Descrición da tendencia

O **Model Context Protocol (MCP)** é unha proposta emerxente destinada a **estandarizar a forma na que os sistemas de intelixencia artificial acceden a información, ferramentas e fontes de datos externas**. A medida que os modelos de IA pasan de funcionar como sistemas illados a formar parte de ecosistemas máis complexos —integrándose con aplicacións empresariais, bases de datos ou servizos en liña— xorde a necesidade de definir **mecanismos estruturados para proporcionar contexto operativo aos modelos**.



Complexidade de integración antes e despois de MCP. Fonte: Descope (2026)

O MCP propón un marco no que aplicacións, ferramentas e modelos poden **intercambiar información de forma controlada e interoperable**, facilitando que os sistemas de IA comprendan o contorno no que operan e executen tarefas máis complexas. MCP foi presentado pola empresa de IA Anthropic (creadores de Claude Code) a finais de 2024 [34].

Relevancia e implicacións

Para organizacións industriais que comezan a integrar **sistemas de IA en procesos operativos, plataformas de análise ou sistemas de apoio á decisión**, a existencia de protocolos estandarizados para xestionar o contexto dos modelos pode facilitar a **interoperabilidade entre ferramentas e a integración de IA en infraestruturas tecnolóxicas existentes**. Nun escenario de crecente automatización baseada en IA, estes protocolos poden permitir que os modelos **accedan a datos industriais,**

documentación técnica ou sistemas de monitorización de forma estruturada e controlada. Ao mesmo tempo, isto require establecer **políticas claras de control de acceso, xestión de permisos e supervisión das interaccións entre modelos e sistemas empresariais**.

Consideracións adicionais

A evolución de protocolos como MCP está ligada ao desenvolvemento de **ecosistemas de IA compostos por múltiples modelos, axentes e servizos interconectados**. Neste contexto, a forma na que os modelos reciben contexto e acceden a datos convértese nun elemento crítico tanto para o **rendemento dos sistemas como para a súa seguridade**. Para as organizacións industriais, isto implica prestar atención a aspectos como a **autenticación das fontes de datos, a trazabilidade das interaccións dos modelos e a limitación das capacidades de acceso das ferramentas baseadas en IA**. Unha implementación adecuada destes mecanismos pode contribuír a **integrar sistemas de IA de maneira máis segura e controlada nas infraestruturas dixitais das organizacións**.

3.2.2.6 Simulación intelixente (Intelligent Simulation)

Descrición da tendencia

A **simulación intelixente** refírese ao uso combinado de **modelos de simulación, análise avanzada de datos e intelixencia artificial** para recrear e analizar o comportamento de sistemas complexos nun contorno virtual. Estes sistemas permiten **modelar procesos industriais, cadeas de subministración, infraestruturas ou operacións técnicas**, incorporando variables dinámicas e algoritmos de aprendizaxe que melloran a precisión das simulacións ao longo do tempo. En moitos casos, estas simulacións relaciónanse co desenvolvemento de **xemelgos dixitais (digital twins)**, capaces de representar virtualmente instalacións ou procesos reais e anticipar o seu comportamento ante diferentes escenarios. No artigo referenciado de Gartner, preséntanse diversos casos de uso [35].

Relevancia e implicacións

Para a **industria galega**, a simulación intelixente pode converterse nunha ferramenta relevante para **avaliar cambios operativos, optimizar procesos produtivos e analizar escenarios de risco sen afectar á operación real das instalacións**. En contornos industriais complexos, estas tecnoloxías permiten **probar modificacións de configuración, avaliar impactos de incidentes ou analizar o comportamento de**

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

sistemas interconectados antes de aplicalos na infraestrutura real. Isto resulta especialmente útil en ámbitos como a **planificación de produción, a xestión de activos industriais ou a análise de resiliencia das infraestruturas críticas**.

Consideracións adicionais

A simulación intelixente tamén está a adquirir relevancia no ámbito da **ciberseguridade industrial**, xa que permite recrear contornos virtuais nos que analizar **ataques, fallos técnicos ou incidentes operacionais** sen comprometer os sistemas reais. Estes contornos poden empregarse para **avaliar vulnerabilidades, probar medidas de defensa ou formar equipos técnicos na resposta a incidentes**. A combinación de simulación avanzada con modelos de aprendizaxe automática facilita ademais a **identificación de patróns de comportamento anómalo e a análise preditiva de riscos operacionais**, contribuíndo a reforzar a resiliencia das infraestruturas industriais dixitalizadas.

3.2.2.7 IA encarnada (Embodied AI)

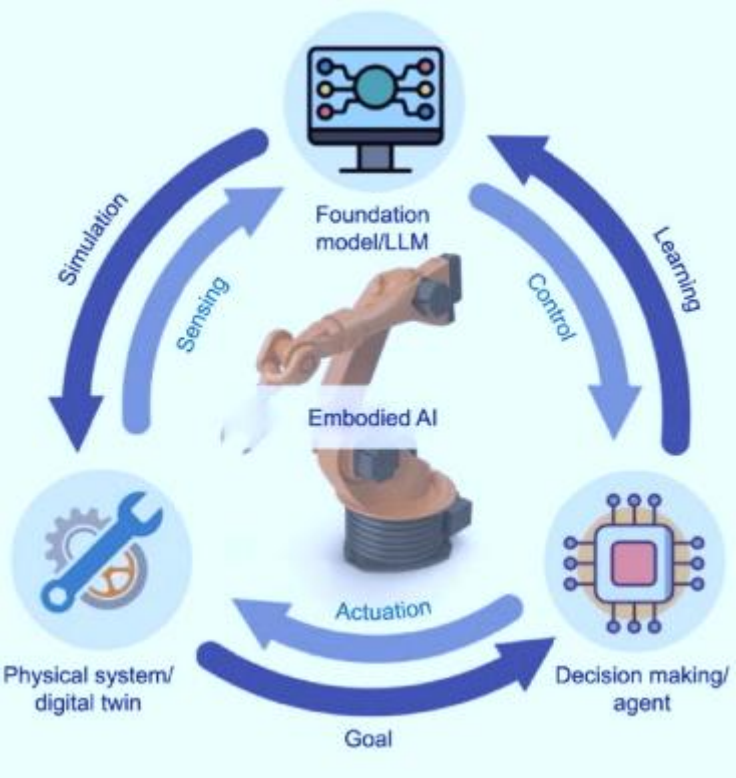
Descrición da tendencia

A **IA encarnada (Embodied AI)** refírese a sistemas de intelixencia artificial que **interactúan directamente co mundo físico a través de sensores, actuadores ou robots**, integrando percepción, decisión e acción nun mesmo sistema [36][37]. A diferenza dos modelos de IA puramente dixitais, estes sistemas están deseñados para **operar en contornos reais**, interpretando información procedente de cámaras, sensores industriais ou sistemas de posicionamento e actuando sobre máquinas ou dispositivos físicos. Este enfoque está a gañar relevancia coa evolución da robótica avanzada, os sistemas autónomos e as plataformas industriais conectadas.

Relevancia e implicacións

A IA encarnada pode ter aplicacións en tarefas como **inspección automática de instalacións, operación de robots industriais, manipulación de materiais ou mantemento asistido por sistemas autónomos**. A integración de sensores, visión artificial e algoritmos de aprendizaxe permite que estes sistemas **interpreten o contorno industrial e executen accións con maior grao de autonomía**, o que pode contribuír a mellorar a produtividade e a seguridade en determinadas operacións.

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 interveñen na IA encarnada. Fonte: ScienceDirect (2025)

Ao mesmo tempo, a introdución de sistemas capaces de actuar directamente sobre procesos físicos require **mecanismos robustos de supervisión, control e seguridade operativa**.

Consideracións adicionais

A evolución da IA encarnada está estreitamente vinculada ao desenvolvemento de **robots colaborativos, vehículos autónomos industriais e sistemas de inspección automatizada**. Estes sistemas combinan percepción baseada en sensores, análise mediante IA e capacidade de actuación no contorno físico. En contornos industriais, isto abre oportunidades para **automatizar tarefas complexas, mellorar a seguridade laboral e reducir intervencións humanas en operacións de risco**. Non obstante, tamén introduce novos retos relacionados coa **seguridade funcional, a fiabilidade dos sistemas autónomos e a protección fronte a manipulacións ou fallos nos algoritmos que controlan a interacción co mundo físico**.

3.2.2.8 IA física (Physical AI)

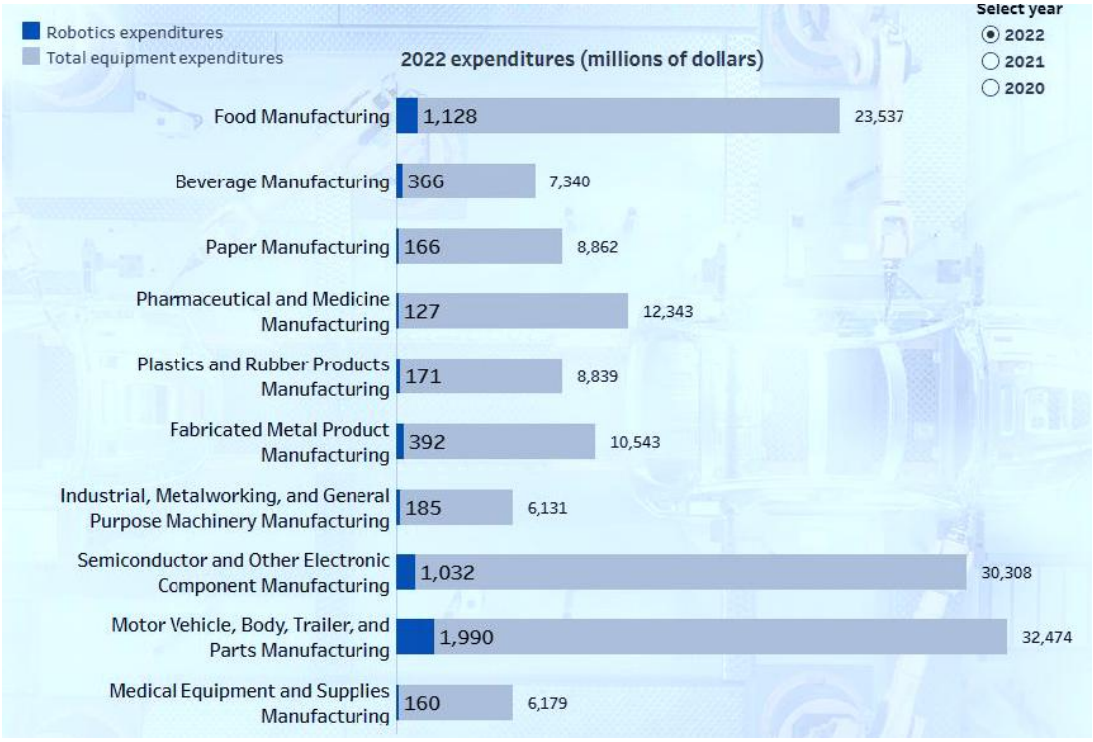
Descrición da tendencia

A **IA física** fai referencia a sistemas de intelixencia artificial deseñados para **interactuar directamente con contornos físicos complexos**, integrando capacidades de

percepción, planificación e control en máquinas ou infraestruturas reais. A diferenza da **IA encarnada** —que pon o foco na interacción dun sistema autónomo co contorno a través de sensores e actuadores—, a IA física céntrase na **integración da intelixencia artificial no funcionamento de sistemas ciberfísicos completos**, como liñas de produción, infraestruturas industriais ou sistemas enerxéticos [38][39]. Neste enfoque, os algoritmos de IA analizan datos procedentes de sensores e toman decisións que afectan ao funcionamento global dos procesos industriais. A evolución da robótica avanzada, da sensórica industrial e da capacidade de procesamento está a facilitar o desenvolvemento de sistemas capaces de **adaptarse dinámicamente ao contorno físico e optimizar o funcionamento de instalacións industriais ou infraestruturas técnicas**.

Relevancia e implicacións

Para o **tecido industrial galego**, a IA física pode ter aplicacións en ámbitos como a **automatización avanzada de procesos industriais como alimentación ou automoción, a operación de maquinaria autónoma, a xestión intelixente de infraestruturas ou a optimización de procesos enerxéticos**. Na seguinte figura, amósanse de xeito ilustrativo as inversión en robótica en diferentes sectores de actividade nos Estados Unidos en 2022.



Inversión en robótica en USA fronte ao resto de inversións en equipamento. Fonte: US Census Bureau (2022)

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

Estes sistemas permiten integrar datos procedentes de sensores, sistemas de control e plataformas analíticas para **tomar decisións operativas en tempo real**, o que pode mellorar a eficiencia, reducir tempos de parada e optimizar o uso de recursos. Con todo, ao tratarse de sistemas que interactúan directamente co mundo físico, tamén resulta esencial garantir **seguridade funcional, robustez dos algoritmos e mecanismos de supervisión humana**.

Consideracións adicionais

A expansión da IA física está ligada á converxencia entre **intelixencia artificial, robótica, IoT industrial e sistemas de control**, configurando unha nova xeración de infraestruturas industriais máis autónomas e adaptativas. Esta evolución pode facilitar a creación de **fábricas máis flexibles, sistemas de produción reconfigurables e operacións industriais altamente automatizadas**. Ao mesmo tempo, require prestar especial atención á **seguridade dos sistemas ciberfísicos, á protección fronte a manipulacións externas e á validación rigorosa dos algoritmos que controlan procesos físicos**, xa que erros ou fallos nestes sistemas poden ter impacto directo sobre instalacións industriais ou servizos críticos.

3.2.2.9 Experiencias adaptativas (Adaptive Experiences)

Descrición da tendencia

As **experiencias adaptativas (Adaptive Experiences)** describen sistemas dixitais capaces de **axustar dinámicamente a súa interface, comportamento ou funcionalidades en función do contexto, do perfil do usuario e dos datos de interacción**. Estes sistemas empregan técnicas de análise de datos e intelixencia artificial para **personalizar a forma na que se presenta a información ou se executan determinadas operacións**, adaptándose ás necesidades específicas de cada usuario ou situación operativa. En lugar de ofrecer unha interface fixa, as plataformas adaptativas evolucionan continuamente a partir do uso real que se fai delas [40].

Relevancia e implicacións

Nos contornos industriais, este enfoque pode aplicarse a **interfaces de supervisión, sistemas de apoio á decisión ou ferramentas de mantemento**, permitindo que a información relevante se presente de maneira distinta segundo o perfil do operador, o estado da instalación ou o tipo de tarefa que se está a realizar. Para o tecido industrial galego, isto pode traducirse en **sistemas de control máis intuitivos, mellor comprensión da información operativa e redución de erros humanos en tarefas**

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

críticas. A adaptación da interface tamén pode facilitar o traballo de operadores con distintos niveis de experiencia ou especialización.

Consideracións adicionais

A implantación de experiencias adaptativas require prestar atención á **transparencia dos algoritmos, á trazabilidade das decisións e á coherencia das interfaces en contornos críticos**. Nun sistema industrial, cambios excesivos ou pouco previsibles na interface poden dificultar a operación en situacións de estrés ou emerxencia. Por este motivo, o deseño destas solucións debe equilibrar **adaptabilidade e estabilidade operativa**, garantindo que a personalización mellore a usabilidade sen comprometer a seguridade nin a comprensión do sistema por parte dos operadores.

3.2.2.10 Robots humanoides de traballo (Humanoid Working Robots)

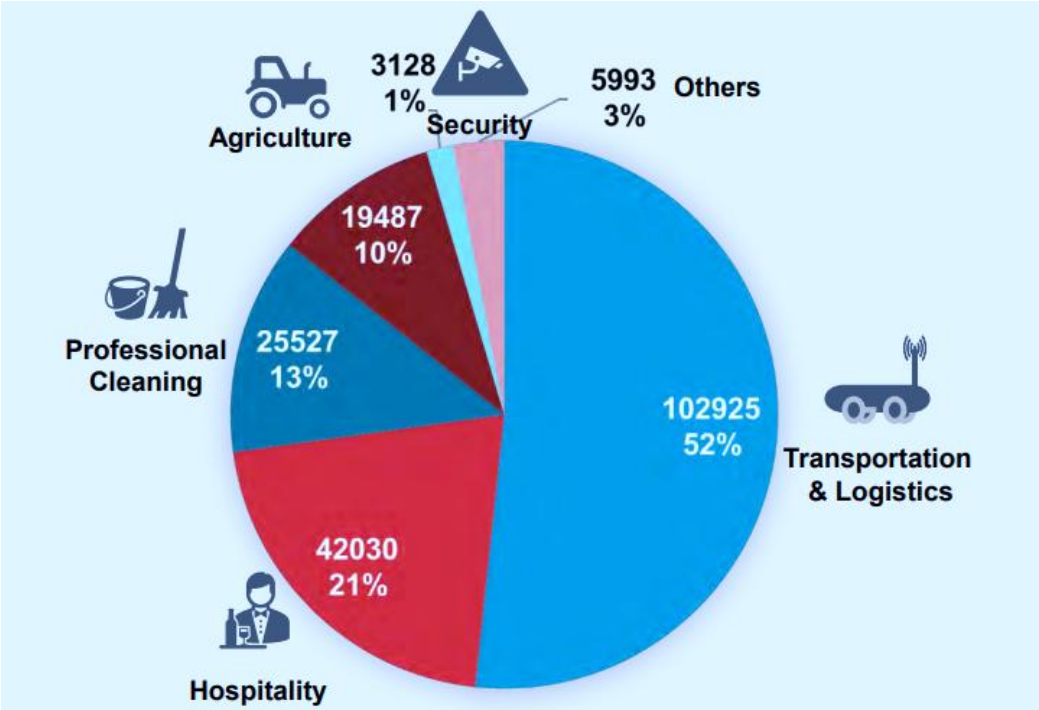
Descrición da tendencia

Os **robots humanoides de traballo** refírense a sistemas robóticos deseñados cunha **morfología similar á humana**, capaces de realizar tarefas físicas en contornos pensados orixinalmente para persoas. Estes robots integran **sensores avanzados, visión artificial, control motor e algoritmos de intelixencia artificial**, o que lles permite interactuar co contorno físico, manipular obxectos e executar tarefas complexas en espazos industriais ou loxísticos. O interese por este tipo de sistemas aumentou recentemente grazas aos avances en **robótica, IA e sistemas de percepción**, que están a facer viable a súa utilización en tarefas reais.

Relevancia e implicacións

En contornos industriais, os robots humanoides poden utilizarse para **realizar tarefas repetitivas, perigosas ou fisicamente esixentes**, como manipulación de materiais, inspección de instalacións ou operación en espazos de difícil acceso. Para o **tecido industrial galego**, caracterizado pola presenza de sectores como a automoción, a loxística, a construción naval ou a industria alimentaria, estas tecnoloxías poderían contribuír a **aumentar a automatización de determinadas operacións e reducir riscos laborais**. Ademais, o deseño humanoide permite que estes robots **operen en infraestruturas existentes sen necesidade de redeseñar completamente os espazos de traballo**. Segundo a Federación Internacional de Robótica o ano pasado nun estudio de case mil fabricantes a nivel mundial, o 52% dos robots adicáronse a labores de transporte e loxística, cun crecemento dun 14% interanual [41].

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



Sector de actividade de aplicación de robots. Fonte: Federación Internacional de Robótica (2025)

Consideracións adicionais

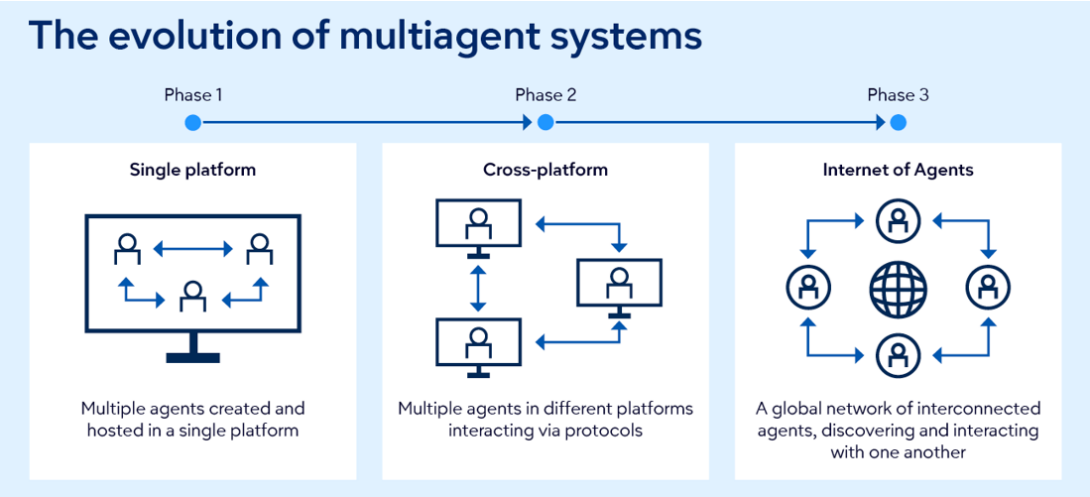
A introdución de robots humanoides tamén suscita cuestións relacionadas coa **seguridade operativa, a convivencia entre traballadores humanos e sistemas robóticos e a fiabilidade dos sistemas autónomos**. En contornos industriais, resulta fundamental garantir **protocolos claros de seguridade, mecanismos de parada segura e sistemas de supervisión** que permitan controlar o comportamento destas máquinas. Ao mesmo tempo, a evolución destas tecnoloxías podería facilitar novas formas de colaboración humano-máquina, nas que os robots humanoides actúen como **asistentes físicos en tarefas industriais ou de mantemento**.

3.2.2.11 IA multiaxente orientada a clientes (Multiagent AI)

Descrición da tendencia

A **IA multiaxente** refírese a sistemas nos que **múltiples axentes de intelixencia artificial colaboran entre si para resolver tarefas complexas**, coordinando decisións e intercambiando información nun mesmo ecosistema dixital [42]. Cada axente pode estar especializado nunha función concreta —por exemplo análise de datos, planificación de tarefas, interacción con usuarios ou execución de accións— e traballa de maneira coordinada cos demais para acadar un obxectivo común. Este enfoque permite construír **arquitecturas de IA distribuídas e máis flexibles**, nas que diferentes modelos cooperan e se adaptan ao contexto operativo.

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



Evolución dos sistemas de IA multiaxente. Fonte: Gartner (2025)

Relevancia e implicacións

Nos contornos industriais e empresariais, os sistemas multiaxente poden aplicarse a **procesos de atención a clientes, xestión de cadeas de subministración, planificación de produción ou análise de datos operacionais**. Para o tecido industrial galego, este tipo de arquitecturas pode facilitar a creación de **plataformas intelixentes capaces de coordinar información procedente de múltiples sistemas empresariais**, integrando datos de produción, loxística ou mantemento. A cooperación entre axentes permite tamén **automatizar fluxos de decisión máis complexos**, nos que diferentes sistemas analizan información e propoñen accións de maneira coordinada.

Consideracións adicionais

A adopción de sistemas multiaxente require prestar atención a aspectos como a **coordinación entre modelos, a xestión de permisos de acceso á información e a supervisión das decisións tomadas polos distintos axentes**. Cando estes sistemas interactúan con datos empresariais ou industriais sensibles, resulta esencial establecer **mecanismos de control, trazabilidade e validación das accións executadas polos axentes**. Un deseño adecuado destas arquitecturas permite aproveitar as vantaxes da cooperación entre sistemas de IA mantendo **niveles adecuados de seguridade e gobernanza tecnolóxica**.

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 da IA no aprovisionamento B2B

Descrición da tendencia

A crecente integración da **intelixencia artificial nos procesos de aprovisionamento entre empresas (B2B)** está a transformar a forma na que as organizacións **analizan provedores, negocian condicións comerciais e xestionan contratos**. Sistemas baseados en IA poden examinar grandes volumes de datos de mercado, histórico de compras, rendemento de provedores e condicións contractuais para **automatizar tarefas de análise, recomendación e toma de decisións no proceso de compra**. Ademais, a aparición de **axentes de IA capaces de interactuar con plataformas comerciais e sistemas empresariais** está a facilitar a automatización parcial de negociacións, selección de provedores ou optimización de cadeas de subministración.

Segundo Boston Consulting Group, as empresas máis avanzadas xa están a probar estes sistemas, que operan de forma continua e requiren respostas rápidas e precisas sobre **prezos, promocións, dispoñibilidade de inventario e prazos de entrega** [43].

Visión do enfoque axéntico no aprovisionamento B2B. Fonte: BCG (2025)

Relevancia e implicacións

Para o **tecido industrial galego**, caracterizado pola integración en cadeas de valor complexas e pola dependencia de múltiples provedores tecnolóxicos e industriais, estas capacidades poden mellorar a **eficiencia na xestión de compras, a identificación de riscos na cadea de subministración e a optimización de custos operativos**. Sistemas de IA poden analizar información procedente de diferentes fontes para **avaliar a fiabilidade de provedores, detectar posibles interrupcións na cadea de subministración ou identificar oportunidades de mellora nas condicións contractuais**.

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

Consideracións adicionais

A incorporación de IA nos procesos de aprovisionamento tamén introduce novos retos relacionados coa **transparencia das decisións automatizadas, a protección de información comercial sensible e a supervisión das interaccións entre sistemas automatizados de distintas organizacións**. Nun escenario no que algoritmos ou axentes de IA participan na análise de ofertas ou na negociación de condicións comerciais, resulta necesario establecer **mecanismos de gobernanza, trazabilidade das decisións e control humano nas etapas críticas do proceso**. A evolución destes sistemas podería levar a contornos nos que **plataformas empresariais, provedores e sistemas de IA interactúen de maneira cada vez máis automatizada**, redefinindo o funcionamento tradicional dos mercados B2B.

3.2.2.13 Ascenso das plataformas dixitais estatais

Descrición da tendencia

Nos últimos anos está a emerxer unha nova xeración de **plataformas dixitais impulsadas por estados ou administracións públicas**, deseñadas para ofrecer infraestruturas comúns de identidade dixital, intercambio de datos, servizos administrativos e integración entre organismos públicos e empresas. Estas plataformas funcionan como **ecosistemas tecnolóxicos compartidos**, nos que diferentes organizacións poden desenvolver servizos dixitais sobre unha infraestrutura común que garante integración, seguridade e gobernanza dos datos. Exemplos deste enfoque inclúen sistemas de **identidade dixital, plataformas de datos públicos ou infraestruturas de servizos dixitais interoperables**. O Foro Económico Mundial considérao un asunto clave para o futuro conectado [44][45].

Relevancia e implicacións

Para o **tecido industrial galego**, a expansión destas plataformas pode facilitar unha **maior integración entre empresas e administracións públicas**, simplificando procesos como a xestión de permisos, a presentación de información regulatoria ou a participación en ecosistemas de datos industriais. A existencia de infraestruturas dixitais estatais tamén pode favorecer a creación de **espazos de datos sectoriais, plataformas de innovación ou sistemas de intercambio seguro de información** entre empresas, organismos públicos e centros de investigación.

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

Consideracións adicionais

O desenvolvemento destas plataformas require prestar especial atención á **seguridade das infraestruturas dixitais públicas, á gobernanza dos datos compartidos e á protección da identidade dixital dos usuarios**. Ao converterse en elementos centrais do ecosistema dixital, estas plataformas poden concentrar grandes volumes de información e interaccións críticas, polo que deben deseñarse con **arquitecturas resilientes, mecanismos de autenticación robustos e controis estritos de acceso á información**. A evolución deste modelo apunta cara a administracións públicas que operan como **plataformas dixitais abertas**, capaces de integrar servizos públicos e privados nun mesmo ecosistema tecnolóxico.

3.2.2.14 Programación asistida por IA ("Vibe Coding")

Descrición da tendencia

O chamado **"Vibe Coding"** describe un novo paradigma de desenvolvemento de software no que **modelos de intelixencia artificial xerativa participan activamente na creación, modificación e revisión de código**. Ferramentas baseadas en modelos de linguaxe avanzados poden interpretar instrucións en linguaxe natural e transformalas en fragmentos de código, estruturas de aplicacións ou solucións técnicas completas. Este enfoque permite que desenvolvedores e equipos técnicos **prototipen aplicacións máis rapidamente, automaticen tarefas repetitivas de programación e exploren novas solucións mediante interacción directa con sistemas de IA.** En opinión de Gartner é un cambio de paradigma que terá repercusión e adopción [46].

Relevancia e implicacións

No contexto das organizacións industriais, esta tendencia pode facilitar o **desenvolvemento máis áxil de ferramentas internas, scripts de automatización, sistemas de integración entre plataformas ou aplicacións de análise de datos industriais**. Para o tecido produtivo galego, caracterizado pola presenza de pequenas e medianas empresas con recursos limitados en desenvolvemento de software, estas ferramentas poden **reducir barreiras técnicas e acelerar a creación de solucións dixitais adaptadas ás necesidades operativas**. Ao mesmo tempo, o uso de código xerado por IA require **revisión técnica rigorosa e controis de calidade**, especialmente en contornos nos que o software interactúa con infraestruturas industriais ou sistemas 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

Consideracións adicionais

A expansión deste paradigma tamén introduce retos relacionados coa **seguridade do software, a trazabilidade do código xerado e a protección da propiedade intelectual**. O uso de modelos de IA no proceso de desenvolvemento pode xerar dependencias tecnolóxicas e introducir vulnerabilidades se o código xerado non é revisado adecuadamente. Por este motivo, resulta recomendable integrar estas ferramentas dentro de **procesos de desenvolvemento seguros, revisión de código e prácticas de seguridade dende o deseño**, garantindo que a produtividade adicional non comprometa a fiabilidade nin a seguridade das aplicacións desenvolvidas.

3.2.2.15 Computación espacial (Spatial Computing)

Descrición da tendencia

A **computación espacial (Spatial Computing)** engloba tecnoloxías que permiten **interactuar con información dixital integrada no espazo físico**, combinando realidade aumentada (AR), realidade virtual (VR), sensores espaciais, visión artificial e modelado tridimensional. Estes sistemas permiten que usuarios e máquinas **visualicen e manipulen información dixital directamente sobre o contorno físico**, creando interfaces tridimensionais que integran datos operativos, simulacións ou modelos virtuais no propio espazo de traballo [47][48].

Relevancia e implicacións

Nos contornos industriais, a computación espacial pode empregarse para **visualización avanzada de instalacións, asistencia en tarefas de mantemento, formación técnica ou supervisión de procesos industriais complexos**. Mediante dispositivos de realidade aumentada ou entornos virtuais, os operadores poden acceder a **instrucións contextuais, modelos 3D de equipos ou datos en tempo real sobre o estado das máquinas**. Para o tecido industrial galego, isto pode facilitar a **transferencia de coñecemento técnico, a redución de erros operativos e a mellora da eficiencia en tarefas de inspección ou 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 industriais xerados mediante computación espacial en gafas 3D. Fonte: Foxconn (2025)

Consideracións adicionais

A adopción destas tecnoloxías tamén introduce desafíos relacionados coa **integración de sistemas industriais con plataformas de visualización avanzada, a protección da información técnica e a fiabilidade das interfaces utilizadas en operacións críticas**. En contornos industriais, os sistemas de computación espacial deben deseñarse garantindo **precisión na representación do contorno, sincronización cos sistemas de control e protección dos datos operacionais** que se visualizan nos dispositivos. Cando se implementan adecuadamente, estas tecnoloxías poden converterse nunha ferramenta relevante para **mellorar a comprensión de sistemas complexos e apoiar a toma de decisións operativas**.

3.2.3 De vixilancia estratéxica (prioridade #3)

3.2.3.1 Intelixencia Artificial Xeral (AGI)

Descrición da tendencia

A **Intelixencia Artificial Xeral (Artificial General Intelligence, AGI)**, aínda que con múltiples concepcións na literatura, pode referirse a sistemas de intelixencia artificial capaces de **comprender, aprender e aplicar coñecemento de maneira ampla en múltiples dominios**, cun nivel de flexibilidade cognitiva comparable ao da intelixencia humana. A diferenza dos sistemas actuais de IA —que adoitan estar especializados en tarefas concretas—, a AGI implicaría a capacidade de **resolver problemas diversos, transferir aprendizaxes entre contextos distintos e adaptarse a situacións novas**

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

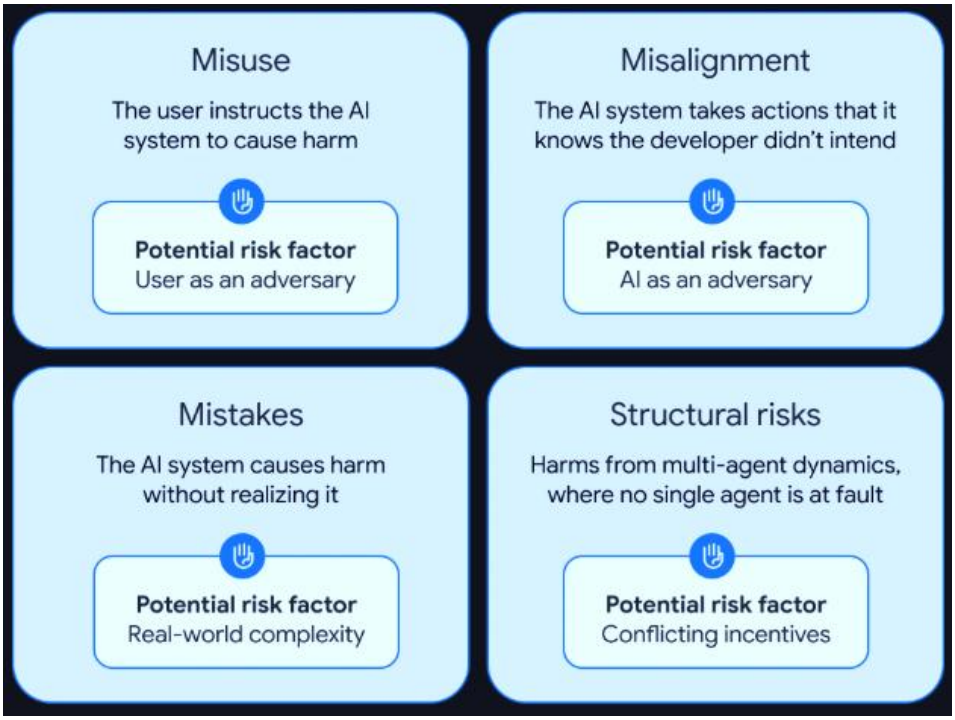
sen necesidade de reentrenamento específico. Actualmente considérase un obxectivo de investigación a medio-longo prazo no campo da IA.

Relevancia e implicacións

Aínda que a AGI se sitúa nun horizonte tecnolóxico máis afastado, a súa posible aparición podería ter **implicacións profundas na organización das actividades económicas, industriais e científicas**. Sistemas con capacidade xeral de aprendizaxe poderían asumir tarefas complexas de análise, planificación ou deseño en ámbitos como a investigación tecnolóxica, a optimización de procesos industriais ou a xestión de infraestruturas críticas. Para o ecosistema industrial galego, isto podería traducirse nunha **aceleración significativa da innovación tecnolóxica e da automatización de procesos de alto valor cognitivo**.

Consideracións adicionais

O desenvolvemento de AGI tamén suscita cuestións relevantes relacionadas coa **seguridade dos sistemas de IA, a gobernanza tecnolóxica e o impacto socioeconómico da automatización avanzada**. Entre os retos asociados inclúense a **aliñación dos sistemas de IA cos obxectivos humanos, o control de sistemas altamente autónomos e a avaliación dos riscos asociados a capacidades tecnolóxicas moi avanzadas**.



Principais riscos asociados á AGI. Fonte: Google DeepMind (2025)

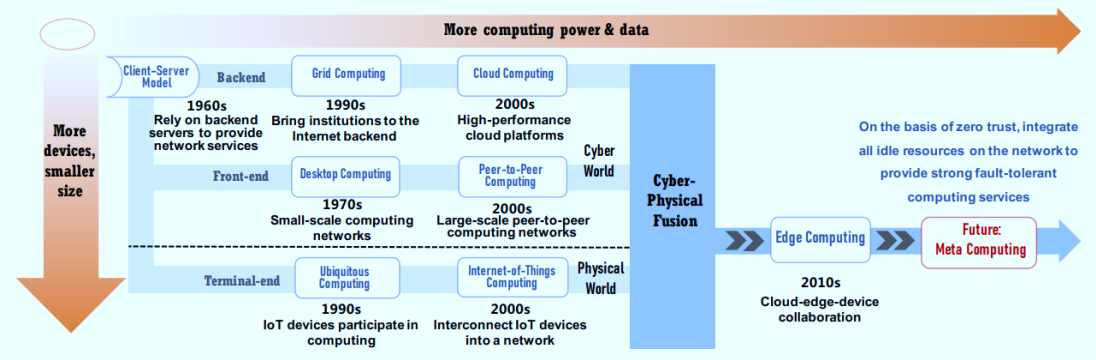
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Por este motivo, numerosos organismos e centros de investigación están a analizar os posibles escenarios de desenvolvemento da AGI e as medidas necesarias para garantir un **despregamento seguro e responsable destas tecnoloxías no futuro** [49][50].

3.2.3.2 Meta-computación (Meta Computing)

Descrición da tendencia

A **meta-computación (Meta Computing)** describe un enfoque no que os sistemas informáticos son capaces de **coordinar, xestionar e optimizar automaticamente múltiples recursos computacionais distribuídos**, incluíndo cloud, edge computing, infraestruturas locais e plataformas especializadas de procesamento [51]. Neste paradigma, as aplicacións e os sistemas de IA poden **decidir dinámicamente onde e como executar determinadas tarefas**, adaptándose á dispoñibilidade de recursos, aos requisitos de rendemento ou ás condicións operativas do sistema.



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

Relevancia e implicacións

Nun contexto de crecente complexidade tecnolóxica, no que as organizacións combinan **infraestruturas cloud, contornos industriais conectados, dispositivos IoT e sistemas de análise de datos**, a meta-computación pode facilitar unha **xestión máis eficiente da capacidade de procesamento e dos fluxos de información**. Para o tecido industrial galego, isto podería traducirse en arquitecturas tecnolóxicas capaces de **adaptar automaticamente a execución de procesos analíticos, simulacións ou sistemas de IA** segundo as condicións operativas das infraestruturas dispoñibles.

Consideracións adicionais

A evolución cara a modelos de meta-computación está ligada ao desenvolvemento de **arquitecturas distribuídas, plataformas de orquestración avanzada e sistemas de intelixencia artificial capaces de optimizar o uso de recursos computacionais**. Este

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

enfoque pode resultar especialmente relevante en contornos onde os sistemas deben combinar **procesamento en tempo real, análise avanzada de datos e integración entre múltiples plataformas tecnolóxicas**. Ao mesmo tempo, tamén require prestar atención á **seguridade das infraestruturas distribuídas, á protección dos fluxos de datos e á gobernanza das plataformas tecnolóxicas que participan no ecosistema computacional.**

3.2.3.3 Comerciantes máquina (Machine Customers & Sellers)

Descrición da tendencia

Os **comerciantes máquina** refírense a **sistemas automatizados capaces de actuar como axentes económicos en procesos de compra e venda**, executando **transaccións comerciais de forma autónoma** en nome de persoas ou organizacións. Estes sistemas, baseados en **intelixencia artificial, analítica de datos e integración con plataformas dixitais**, poden **analizar información de mercado, comparar ofertas, negociar condicións comerciais e completar operacións de compra ou venda sen intervención humana directa**.

A evolución dos **sistemas de axentes intelixentes, do comercio electrónico avanzado e da automatización empresarial** está a facilitar a aparición de **ecosistemas dixitais nos que software e sistemas intelixentes participan directamente en interaccións comerciais**, ampliando o papel dos sistemas automatizados máis alá das funcións tradicionais de recomendación ou asistencia [52].

Relevancia e implicacións

No contexto industrial e empresarial, os comerciantes máquina poden intervir **tanto en procesos de adquisición como de comercialización de produtos ou servizos**. Por unha banda, poden **identificar necesidades de subministración, analizar opcións dispoñibles e executar pedidos de forma automatizada**; por outra, poden **ofrecer produtos, adaptar prezos segundo a demanda ou responder a solicitudes comerciais en tempo real**.

Evolución prevista do modelo de cliente máquina. Fonte: Gartner (2022)

Para o **tecido industrial galego**, esta tendencia podería traducirse en **sistemas capaces de supervisar inventarios, optimizar cadeas de subministración, xestionar vendas dixitais ou interactuar con plataformas comerciais automatizadas**, permitindo **reducir tempos de resposta, mellorar a eficiencia operativa e optimizar a xestión de recursos**.

Consideracións adicionais

A aparición de comerciantes máquina introduce **novos retos relacionados coa regulación das transaccións automatizadas, a responsabilidade legal das decisións tomadas por sistemas autónomos e a seguridade das plataformas comerciais dixitais**. Ademais, a interacción entre distintos sistemas automatizados —por exemplo, entre **clientes máquina e vendedores máquina**— podería dar lugar a **ecosistemas económicos parcialmente automatizados**, nos que **negociacións e transaccións se realicen directamente entre axentes software**.

Neste escenario, as organizacións deberán **adaptarse a novas dinámicas comerciais dixitais e establecer mecanismos de supervisión que garantan transparencia, seguridade e control sobre os procesos automatizados**, especialmente en contornos nos que **software e axentes intelixentes interactúan directamente en mercados dixitais**.

3.2.3.4 Aprovisionamento autónomo (Autonomous Sourcing)

Descrición da tendencia

O **aprovisionamento autónomo** refírese ao uso de **sistemas automatizados e intelixencia artificial para identificar necesidades de subministración, seleccionar provedores e executar procesos de compra de forma autónoma**. Estes sistemas poden **analizar datos operativos, niveis de inventario, previsións de**

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

demanda ou condicións de mercado, permitindo **activar procesos de adquisición sen intervención humana directa**.

A evolución da **analítica avanzada, da intelixencia artificial aplicada á xestión empresarial e das plataformas dixitais de compras** está a permitir que determinados procesos de aprovisionamento sexan **automatizados de extremo a extremo**, dende a detección da necesidade ata a execución do pedido e o seguimento da entrega.

Relevancia e implicacións

No ámbito industrial e empresarial, o aprovisionamento autónomo pode contribuír a **optimizar a xestión de cadeas de subministración e reducir tempos de resposta nos procesos de adquisición**. Os sistemas poden **monitorizar continuamente os niveis de inventario, detectar necesidades de reposición e seleccionar automaticamente provedores segundo criterios de custo, dispoñibilidade ou calidade**. Esta tendencia podería traducirse en **sistemas capaces de xestionar automaticamente pedidos de materias primas, compoñentes ou servizos necesarios para a produción**, mellorando a **eficiencia operativa, a planificación de recursos e a resiliencia das cadeas de subministración** [53].

Consideracións adicionais

A implantación de sistemas de aprovisionamento autónomo introduce **novos retos relacionados coa gobernanza dos procesos de compra automatizados, a transparencia das decisións algorítmicas e a seguridade das plataformas dixitais de subministración**. Ademais, o uso destes sistemas pode **modificar as relacións tradicionais entre empresas e provedores**, ao integrar **plataformas dixitais, mercados electrónicos e sistemas automatizados de negociación**.

Neste contexto, será necesario establecer **mecanismos de supervisión, auditoría e control que garantan a fiabilidade das decisións automatizadas**, así como **marcos normativos que regulen a responsabilidade e a seguridade nos procesos de adquisición baseados en sistemas autónomos.**

3.2.3.5 Compañeiro cibernético (Cybernetic Teammate)

Descrición da tendencia

O **compañeiro cibernético** refírese á aparición de **sistemas de intelixencia artificial deseñados para colaborar activamente con persoas en tarefas profesionais**,

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

actuando como **asistentes avanzados capaces de participar en procesos de toma de decisións, análise de información ou execución de tarefas complexas**.

A diferenza dos sistemas tradicionais de automatización, estes sistemas están orientados a **traballar xunto aos profesionais humanos**, proporcionando **apoio cognitivo, análise de datos en tempo real e recomendacións baseadas en intelixencia artificial**. A evolución da **IA xerativa, dos modelos lingüísticos avanzados e das plataformas de colaboración dixital** está a facilitar a integración destes sistemas en contornos laborais cada vez máis complexos, que permiten optimizar os tempos de reposta (ata un 16% segundo un estudo de Harvard, á vez que mellorando a calidade das propostas formuladas) [54][55].

Relevancia e implicacións

No ámbito empresarial e industrial, os compañeiros cibernéticos poden **apoiar a profesionais en tarefas como análise de datos, xestión de coñecemento, planificación operativa ou supervisión de procesos**. Estes sistemas poden **interpretar grandes volumes de información, detectar patróns e suxerir accións**, contribuíndo a **mellorar a toma de decisións e a eficiencia organizativa**.

Para o **tecido empresarial galego**, esta tendencia podería materializarse en **sistemas de apoio á toma de decisións, asistentes intelixentes para equipos técnicos ou ferramentas de colaboración baseadas en IA**, capaces de **incrementar a produtividade e facilitar a xestión de contornos complexos como cadeas de subministración, operacións industriais ou análise de risco**.

Consideracións adicionais

A incorporación de compañeiros cibernéticos nos contornos laborais tamén introduce **novos desafíos relacionados coa confianza nos sistemas automatizados, a supervisión humana das decisións algorítmicas e a protección da información sensible utilizada por estes sistemas**. Ademais, a integración destes sistemas pode **modificar dinámicas organizativas e procesos de traballo**, requirindo **novas competencias profesionais e modelos de colaboración entre persoas e sistemas intelixentes**.

Neste contexto, será necesario establecer **marcos de gobernanza que garantan a transparencia, a seguridade e a responsabilidade no uso de sistemas de intelixencia artificial colaborativa**, asegurando que estes sistemas **complementen as**

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

capacidades humanas sen substituír os mecanismos de control e supervisión necesarios.

3.2.3.6 Descarga cognitiva (Cognitive Offloading)

Descrición da tendencia

A **descarga cognitiva** refírese ao proceso polo cal as persoas **delegan tarefas cognitivas —como lembrar información, analizar datos ou tomar decisións— en sistemas tecnolóxicos**, especialmente en ferramentas baseadas en **intelixencia artificial, asistentes dixitais e sistemas de apoio á decisión**. Este fenómeno, xa presente dende a aparición de ferramentas como buscadores ou sistemas de navegación, está a intensificarse coa expansión da **IA xerativa e dos sistemas avanzados de automatización cognitiva**.

A capacidade destes sistemas para **procesar grandes volumes de información, sintetizar coñecemento e proporcionar recomendacións en tempo real** está a permitir que determinadas tarefas intelectuais sexan externalizadas a ferramentas tecnolóxicas, modificando a forma en que as persoas interactúan coa información e toman decisións.

Relevancia e implicacións

No ámbito profesional e empresarial, a descarga cognitiva pode contribuír a **reducir a carga mental asociada á xestión de información complexa**, permitindo que os profesionais se centren en **tarefas estratéxicas ou creativas** mentres os sistemas tecnolóxicos realizan procesos de análise, filtrado ou síntese de información.

Este fenómeno na industria podería traducirse no uso de **sistemas de apoio á toma de decisións, ferramentas de análise automatizada de datos ou asistentes intelixentes para tarefas técnicas e operativas**, facilitando a **xestión de coñecemento, a análise de riscos ou a planificación de procesos**.

Consideracións adicionais

A extensión da descarga cognitiva tamén introduce **novos desafíos relacionados coa dependencia tecnolóxica, a perda potencial de habilidades cognitivas ou a confianza excesiva nos sistemas automatizados**. Ademais, o uso intensivo de sistemas baseados en IA para tarefas intelectuais pode **modificar procesos de aprendizaxe, toma de decisións e xestión do coñecemento nas organizacións**.

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

Neste contexto, será necesario desenvolver **estratexias de uso responsable destas ferramentas**, garantindo que a tecnoloxía **complemente as capacidades humanas sen substituír o pensamento crítico ou a supervisión profesional, nin degradando as cualidades mentais humanas** (lazy-thinking) [56]. A investigación recente destaca que a externalización de procesos cognitivos cara a sistemas dixitais pode mellorar a eficiencia, pero require **modelos equilibrados de colaboración entre persoas e sistemas intelixentes**.

3.2.3.7 Coñecemento fluído (Fluid Knowledge)

Descrición da tendencia

O **coñecemento fluído** refírese a un modelo emerxente de creación, distribución e uso do coñecemento no que a información **circula de maneira dinámica entre persoas, organizacións e sistemas dixitais**, adaptándose continuamente aos contextos e necesidades. Neste paradigma, o coñecemento **deixa de estar almacenado de forma estática en documentos ou repositorios** para converterse nun recurso **dinámico, distribuído e continuamente actualizado**, facilitado por tecnoloxías como **intelixencia artificial, plataformas colaborativas e sistemas avanzados de xestión da información** [57].

A expansión de ferramentas baseadas en **IA xerativa, motores de busca semánticos e sistemas de recomendación** está a permitir que o coñecemento sexa **xerado, contextualizado e adaptado en tempo real**, favorecendo novas formas de colaboración e aprendizaxe dentro das organizacións.

Relevancia e implicacións

No ámbito empresarial e industrial, o coñecemento fluído pode contribuír a **mellorar a capacidade das organizacións para acceder, interpretar e utilizar información relevante en tempo real**. Sistemas baseados en intelixencia artificial poden **integrar datos procedentes de múltiples fontes, identificar patróns e proporcionar recomendacións contextualizadas**, facilitando procesos como a **toma de decisións, a innovación ou a resolución de problemas complexos**.

Para o **tecido empresarial galego**, esta tendencia podería materializarse en **plataformas de xestión de coñecemento baseadas en IA, sistemas de documentación intelixente ou ferramentas colaborativas que permitan compartir e actualizar información de forma continua**, mellorando a **eficiencia organizativa e a transferencia de coñecemento entre equipos e organizacións**.

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

Consideracións adicionais

A adopción de modelos de coñecemento fluído tamén introduce **novos retos relacionados coa fiabilidade da información, a gobernanza do coñecemento e a protección de datos sensibles**. Ademais, a dependencia de sistemas automatizados para a xeración ou interpretación de información pode **incrementar o risco de difusión de información incorrecta ou descontextualizada**, especialmente cando os sistemas se basean en modelos de intelixencia artificial.

Neste contexto, será necesario establecer **mecanismos de validación, supervisión e gobernanza da información**, garantindo que os sistemas que facilitan o coñecemento fluído **manteñan estándares adecuados de calidade, trazabilidade e seguridade da información.**

3.2.3.8 Interfaces bidireccionais cerebro-máquina

Descrición da tendencia

As **interfaces bidireccionais cerebro-máquina** refírense a sistemas tecnolóxicos capaces de **establecer comunicación directa entre o cerebro humano e dispositivos dixitais**, permitindo **transmitir información en ambos sentidos: do cerebro ao sistema e do sistema ao cerebro**. Estas tecnoloxías combinan **neurociencia, sensores biomédicos, intelixencia artificial e sistemas de procesamento de sinais** para interpretar actividade neuronal e traducila en comandos dixitais ou, no sentido inverso, estimular o sistema nervioso mediante sinais eléctricos ou outros métodos.

A evolución recente das **tecnoloxías neurotecnolóxicas, dos sistemas de lectura neuronal non invasivos e da intelixencia artificial aplicada ao procesamento de sinais cerebrais** está a acelerar o desenvolvemento destas interfaces, abrindo novas posibilidades de interacción entre humanos e sistemas dixitais.

Relevancia e implicacións

No ámbito sanitario, estas tecnoloxías poden permitir **restaurar ou mellorar capacidades motoras ou sensoriais en persoas con lesións neurolóxicas**, facilitando a comunicación ou o control de dispositivos mediante sinais cerebrais. Noutros ámbitos, como a industria ou os servizos tecnolóxicos, as interfaces cerebro-máquina poderían **habilitar novas formas de interacción humano-máquina**, reducindo barreiras entre pensamento e acción en determinados sistemas tecnolóxicos.

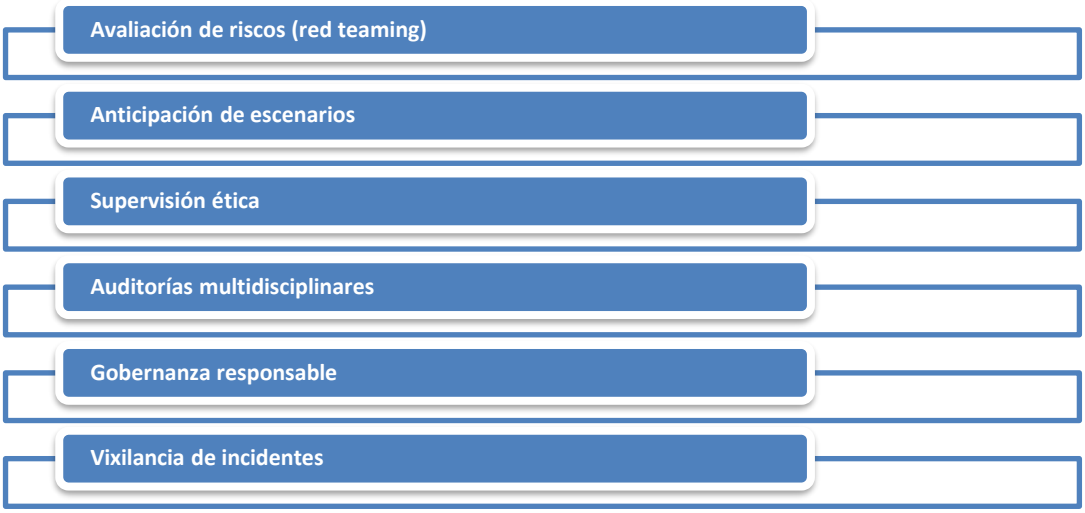
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

Consideracións adicionais

O desenvolvemento destas tecnoloxías tamén introduce **importantes cuestións éticas, legais e de seguridade**, relacionadas coa **privacidade da actividade cerebral, a protección de datos neurobiolóxicos e os posibles riscos asociados á manipulación ou acceso non autorizado a sinais neuronais**. Ademais, a integración destas interfaces en contornos tecnolóxicos avanzados pode requirir **novos marcos regulatorios e estándares de seguridade específicos para as neurotecnoloxías**.

Neste contexto, organismos internacionais e centros de investigación están a destacar a necesidade de **garantir principios de transparencia, control humano e protección da integridade cognitiva** no desenvolvemento de interfaces cerebro-máquina, especialmente a medida que estas tecnoloxías evolucionen cara a sistemas máis avanzados de interacción bidireccional.

As recomendacións específicas da OCDE (Organización para a Cooperación e o Desenvolvemento Económico) do informe anterior, son as seguintes:



Recomendacións da OCDE no ámbito da neurotecnoloxía. Fonte: OCDE (2025)

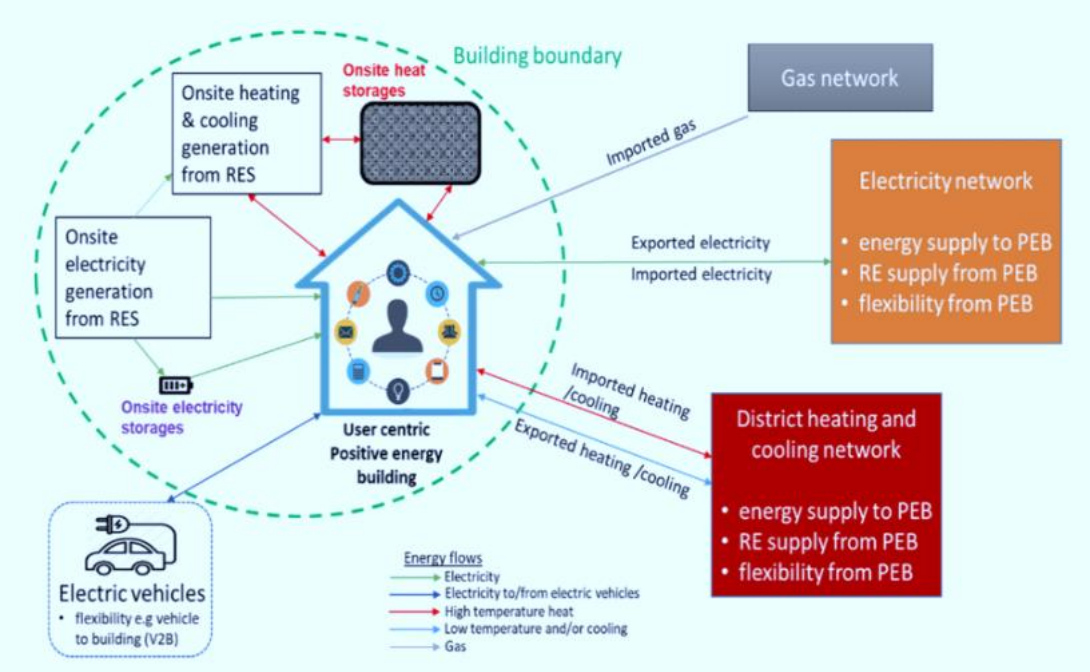
3.2.3.9 Edificios con balance positivo de recursos (Resource-Positive Buildings)

Descrición da tendencia

Os **edificios con balance positivo de recursos** son infraestruturas deseñadas para **xerar máis recursos dos que consomen ao longo do seu ciclo de vida**, especialmente en termos de **enerxía, auga ou materiais**. Este enfoque vai máis aló dos edificios enerxéticamente eficientes ou de consumo case nulo, integrando **tecnoloxías de produción renovable, sistemas avanzados de xestión enerxética e solucións 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

economía circular que permiten que os edificios contribúan activamente á sustentabilidade ambiental [58].



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

A evolución das **tecnoloxías de xeración distribuída, sensores IoT, sistemas intelixentes de xestión de edificios (BMS) e plataformas de análise de datos** está a facilitar o desenvolvemento de infraestruturas capaces de **optimizar o uso de recursos e producir excedentes enerxéticos ou ambientais**.

Relevancia e implicacións

No ámbito urbano e empresarial, os edificios con balance positivo poden contribuír a **reducir o impacto ambiental das infraestruturas, mellorar a eficiencia no uso de recursos e incrementar a resiliencia enerxética das cidades e das organizacións**. Estes sistemas poden **xerar enerxía renovable localmente, reutilizar recursos e optimizar o consumo mediante sistemas intelixentes de control e monitorización**.

Para a nosa industria, esta tendencia pode traducirse na **integración de tecnoloxías de eficiencia enerxética, autoconsumo renovable, sistemas intelixentes de xestión de edificios e solucións de economía circular**, contribuíndo á **descarbonización do parque edificatorio e á sustentabilidade das infraestruturas**.

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

Consideracións adicionais

A implantación deste modelo tamén introduce **novos desafíos relacionados coa integración tecnolóxica, a interoperabilidade dos sistemas de xestión de edificios e a ciberseguridade das infraestruturas dixitais que controlan estes sistemas**. Ademais, o incremento da conectividade e da automatización nos edificios intelixentes require **estratexias de protección fronte a riscos cibernéticos que poidan afectar aos sistemas de control ou á xestión de recursos**.

Neste contexto, entidades internacionais e iniciativas de investigación destacan a importancia de **combinar eficiencia enerxética, innovación tecnolóxica e gobernanza sostible para desenvolver edificios capaces de xerar impactos positivos no medio ambiente e nas comunidades** [59].

3.2.3.10 Avaliación de competencias na era da IA (Test for Skills in the AI Era)

Descrición da tendencia

A crecente integración da **intelixencia artificial nos procesos educativos e profesionais** está a impulsar unha transformación nos modelos de avaliación de coñecementos e habilidades. Os sistemas tradicionais, centrados principalmente na memorización de contidos, están a evolucionar cara a métodos que buscan medir **competencias aplicadas, pensamento crítico, capacidade de resolución de problemas e interacción efectiva con ferramentas baseadas en IA**. Neste contexto, están a emerxer novos enfoques de avaliación baseados en **simulacións, escenarios prácticos e análise automatizada do desempeño**, máis próximos ás situacións reais de traballo, e aliñadas coas necesidades futuras previstas no eido da empregabilidade.

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

Habilidades profesionais con maior crecemento esperado ata 2030. Fonte: WEF (2025)

Relevancia e implicacións

A adopción destes modelos de avaliación responde á necesidade de **adaptar os sistemas educativos e de formación ás novas demandas dun mercado laboral crecentemente dixitalizado**. A capacidade de **traballar con sistemas de intelixencia artificial, interpretar resultados xerados por algoritmos ou integrar ferramentas dixitais nos procesos de traballo** convértese nunha competencia clave.

Para o **ecosistema formativo e empresarial galego incluso mais aló do sector industrial**, esta tendencia podería traducirse no desenvolvemento de **novos sistemas de certificación de competencias dixitais, programas de formación adaptados á IA e ferramentas de avaliación máis dinámicas e contextualizadas**.

Consideracións adicionais

A implantación destes sistemas tamén introduce desafíos relacionados coa **equidade nos procesos de avaliación, a transparencia dos algoritmos utilizados e a protección dos datos persoais dos estudantes ou profesionais avaliados**. Ademais, será necesario garantir que os sistemas automatizados de avaliación **complementen a supervisión humana e eviten posibles sesgos algorítmicos**. Por este motivo, diferentes institucións internacionais están a analizar como **adaptar os marcos educativos e de avaliación de competencias á era da intelixencia artificial**,

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

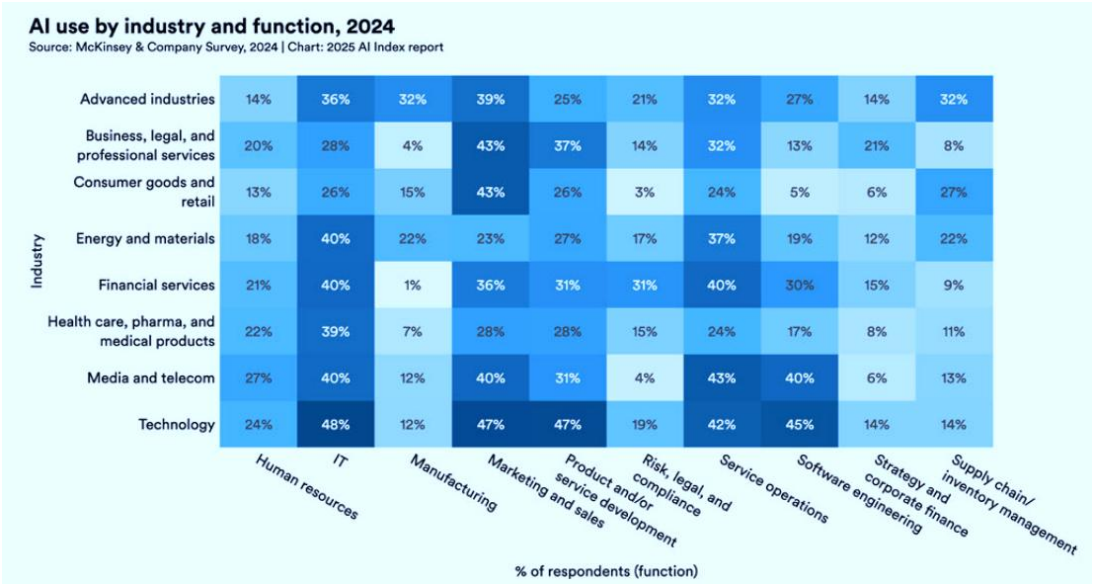
promovendo modelos que integren habilidades tecnolóxicas, cognitivas e éticas necesarias para interactuar con sistemas avanzados de IA [60].

3.2.3.11 Economía de modelos de IA (AI Model Economy)

Descrición da tendencia

A **economía de modelos de IA** refírese á aparición dun novo ecosistema económico no que **modelos de intelixencia artificial se desenvolven, comercializan, intercambian e integran como activos tecnolóxicos clave**. Neste contexto, os modelos de IA —especialmente os baseados en **modelos fundacionais e IA xerativa**— convértense nun recurso central para empresas e organizacións, que poden **crear, adaptar ou consumir modelos como servizos a través de plataformas dixitais**.

Este paradigma está impulsado pola expansión das **plataformas de computación na nube, os mercados de modelos (model marketplaces) e os ecosistemas de desenvolvemento de IA**, que permiten reutilizar modelos preentrenados e integralos rapidamente en aplicacións empresariais ou industriais, e teñen cada vez maior penetración no mercado.



Enquisa de uso da IA por industria e función en 2024. Fonte: McKinsey (2024)

Relevancia e implicacións

A economía de modelos de IA pode transformar a forma en que as organizacións **acceden ás capacidades de intelixencia artificial**, facilitando a adopción de tecnoloxías avanzadas sen necesidade de desenvolver modelos dende cero. Isto permite **acelerar a innovación, reducir custos de desenvolvemento e facilitar a integración**

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

da IA en múltiples procesos empresariais, dende a análise de datos ata a automatización de tarefas ou a interacción con clientes.

Para o **tecido empresarial galego**, esta tendencia podería favorecer o acceso a **capacidades avanzadas de IA a través de plataformas e servizos especializados**, permitindo que empresas de diferentes tamaños incorporen ferramentas baseadas en IA nos seus procesos produtivos, comerciais ou de análise.

Consideracións adicionais

O desenvolvemento deste ecosistema tamén introduce retos relacionados coa **propiedade intelectual dos modelos, a transparencia dos sistemas de IA, a seguridade das cadeas de subministración tecnolóxicas e a dependencia de plataformas tecnolóxicas globais**. Ademais, a proliferación de modelos de IA require **mecanismos de avaliación, control e gobernanza que garantan a fiabilidade, a seguridade e o uso responsable destas tecnoloxías**.

Neste contexto, organismos internacionais e centros de investigación están a analizar o impacto económico e tecnolóxico deste novo mercado de modelos de IA, destacando o seu papel na transformación dos ecosistemas de innovación dixital [61].

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

Descrición da tendencia

Durante máis de tres décadas, o deseño de interfaces de produtividade estivo baseado nun modelo centrado en **aplicacións, menús, iconas e interacción directa co software**. A expansión da **intelixencia artificial, os asistentes conversacionais e os sistemas baseados en linguaxe natural** está a impulsar un cambio significativo neste paradigma. Neste novo enfoque, os usuarios interactúan cos sistemas **mediante instrucións, contexto ou intencións**, permitindo que a IA interprete a solicitude e execute accións complexas sen necesidade de navegar por múltiples interfaces tradicionais.

Relevancia e implicacións

A evolución cara a interfaces baseadas en **interacción conversacional, automatización contextual e sistemas de axentes intelixentes** pode transformar profundamente a forma en que as persoas utilizan ferramentas dixitais. En lugar de aprender a utilizar aplicacións complexas, os usuarios poderán **expresar necesidades**

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

ou obxectivos directamente ao sistema, que se encargará de executar tarefas, integrar información de diferentes fontes ou coordinar procesos. Para o **ecosistema empresarial e tecnolóxico galego**, isto pode supoñer unha transición cara a **entornos de traballo máis automatizados, interfaces máis intuitivas e ferramentas dixitais centradas en intencións e resultados**.

Consideracións adicionais

Este cambio tamén introduce novos retos relacionados coa **usabilidade, a confianza nos sistemas automatizados e a seguridade das interaccións baseadas en IA**. A medida que os sistemas executen tarefas complexas en nome dos usuarios, será necesario garantir **transparencia nas accións realizadas polos sistemas, control humano sobre os procesos automatizados e protección da información utilizada nestas interaccións**. Expertos apuntan a que o verdadeiro futuro da UX non consiste en **mellorar pantallas individuais**, senón en **orquestrar experiencias completas do usuario ao longo do tempo**, combinando **pensamento centrado nas persoas, análise de datos e intelixencia artificial** [62].

4 Regulamentación no sector

4.1 Introdución

A dimensión regulamentaria da ciberseguridade industrial está a adquirir un peso crecente no conxunto da Unión Europea e, por extensión, tamén en Galicia. Porén, dado que este informe analizou unha grande cantidade de tendencias tecnolóxicas e de transformación do ecosistema dixital, a abordaxe detallada do marco normativo e das obrigas de cumprimento asociadas ás contornas **ICS/OT** posponse para unha edición posterior específica.

Esta decisión resulta coherente coa existencia dunha **Guía normativa de ciberseguridade industrial** xa elaborada no marco do Observatorio, que **constitúe a referencia principal para unha análise máis extensa e sistemática do panorama regulamentario actual** [20].

Con todo, resulta útil incorporar nesta edición unha visión introdutoria que permita **abrir foco sobre os principais cambios normativos e de estandarización que deberán ser vixiados nos vindeiros anos**, tanto polo sector público como polo tecido empresarial e industrial galego. A razón é clara: a presión regulamentaria xa non se limita ao cumprimento formal, senón que se está a traducir en **novas esixencias operativas, novas evidencias auditables e novos criterios de compra e relación con provedores**, con impacto directo sobre a gobernanza, a arquitectura tecnolóxica e a operación dos entornos industriais.

4.2 Principais vectores regulamentarios a vixiar

O primeiro gran eixo de seguimento é a consolidación do novo **marco europeo de ciberseguridade e resiliencia**, no que destacan tres pezas especialmente relevantes.

- En primeiro lugar, a **Directiva NIS2**, que reforza as obrigas de xestión de riscos, gobernanza, reporte de incidentes e seguridade da cadea de subministración para entidades esenciais e importantes [63].
- En segundo lugar, a **Directiva CER**, que amplía a perspectiva dende a ciberseguridade cara á **resiliencia integral de entidades críticas**, incluíndo ameazas físicas, híbridas e de continuidade de servizo [64].
- En terceiro lugar, o **Cyber Resilience Act (CRA)**, que introduce requisitos obrigatorios de seguridade para produtos con elementos dixitais e terá un efecto

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

tractor moi relevante sobre a compra, integración e operación de tecnoloxía en ambientes ICS/OT [65][66].

O segundo eixo relevante é a **aterraxe práctica deste marco no ordenamento español e na operativa das organizacións**, o que previsiblemente reforzará a esixencia efectiva sobre administracións públicas, operadores de servizos esenciais e cadeas de provedores.

- Neste contexto, cómpre seguir a evolución do **Anteproxecto de Lei de Coordinación e Gobernanza da Ciberseguridade**, orientado á transposición de NIS2 [67],
- así como o desenvolvemento do **Anteproxecto de Lei de protección e resiliencia de entidades críticas**, chamado a incorporar ao ordenamento interno os principios da Directiva CER [68].

Para Galicia, isto implicará previsiblemente unha maior demanda de **evidencias formais de gobernanza, procedementos de notificación, análise de riscos, continuidade e control de terceiros**, especialmente en sectores intensivos en compoñente OT.

O terceiro ámbito que deberá ser monitorizado con atención é o que afecta á **cadea de subministración tecnolóxica e á transparencia de compoñentes**. A tendencia regulamentaria apunta cara a unha maior esixencia en materia de **xestión de vulnerabilidades, trazabilidade técnica, relación con integradores e control de dependencias de software e hardware**, nun contexto no que o CRA, os traballos de ENISA sobre **SBOM** (Software Bill of Materials, inventario estruturado dos compoñentes de software que forman parte dunha aplicación, sistema ou produto dixital) e os estándares asociados, poden converter este tipo de evidencias nun requisito de facto para moitos procesos de compra e validación tecnolóxica [69][70][71].

Un cuarto eixo emerxente é o da **criptografía post-cuántica (PQC)** e a chamada **cripto-axilidade**, tendencia mencionada no Informe na sección previa (no grupo de prioridade #1). A Comisión Europea xa puxo en marcha unha folla de ruta específica para promover a transición coordinada cara a algoritmos resistentes á computación cuántica [72][73].

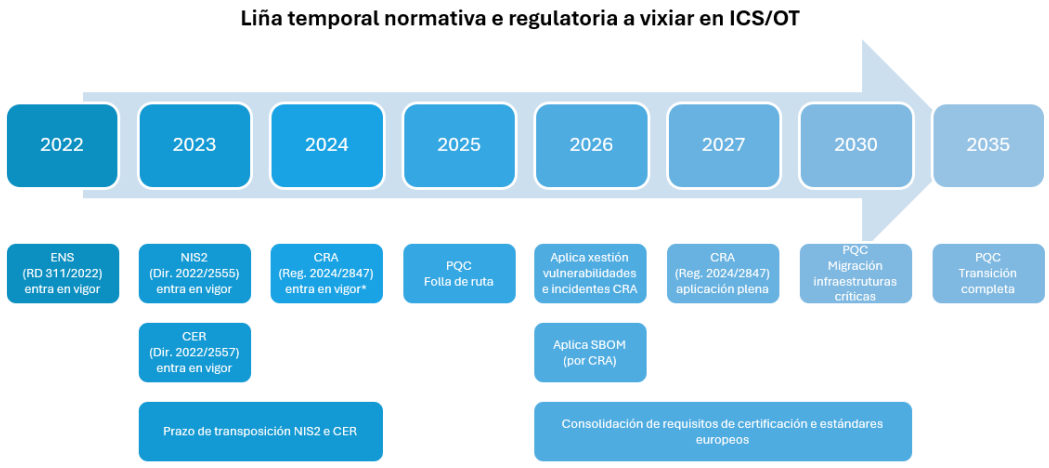
Aínda que o impacto inmediato en entornos industriais non será uniforme, este movemento normativo e técnico anticipa a necesidade de que organizacións con activos de longa vida útil —como adoita ocorrer en ICS/OT— comecen a traballar en

inventarios criptográficos, planificación de migración e revisión de dependencias tecnolóxicas críticas.

O quinto elemento a seguir é a crecente converxencia entre **regulación tecnolóxica, certificación e compra pública ou industrial**. Ademais das obrigas legais directas, todo apunta a que os próximos anos traerán un maior peso das **certificacións europeas de ciberseguridade, os estándares harmonizados e os requisitos contractuais ligados á seguridade por deseño**, incluíndo ámbitos nos que a automatización e o control industrial teñen especial relevancia [74].

Para o ecosistema galego, isto é particularmente importante porque pode condicionar non só o cumprimento, senón tamén a **capacidade de competir en cadeas de valor, contratacións públicas e proxectos industriais avanzados**.

A continuación, un resumo gráfico de todo o anterior:



Liña temporal normativa e regulamentaria a vixiar en ICS/OT (2022–2030)

4.3 Implicacións

Dende a perspectiva galega, o mais relevante non será só coñecer o marco normativo, senón **anticipar como se traducirá en requirimentos operativos concretos**. Isto afecta tanto ao sector público —no que o **ENS** segue sendo unha referencia estruturante [75]— como ás organizacións privadas que, pola súa actividade, tamaño ou criticidade, poidan quedar dentro do ámbito de aplicación de NIS2 [63] ou dos futuros desenvolvementos asociados á resiliencia de entidades críticas.

En termos prácticos, haberá que prestar especial atención á capacidade de demostrar **inventario de activos, trazabilidade, gobernanza TI-OT, procedementos 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

reporte, xestión de incidentes, relación con terceiros, continuidade e seguridade da cadea de subministración. En paralelo, a evolución dos estándares internacionais de referencia —como **NIST CSF 2.0**, os traballos sobre seguridade OT de NIST ou a serie **ISA/IEC 62443**— seguirá actuando como marco de apoio para traducir requisitos legais a controis, evidencias e follas de ruta de madurez [76][28][77].

Podemos pechar dicindo que a regulación da ciberseguridade industrial está a entrar nunha nova fase, caracterizada por unha maior interrelación entre **cumprimento, resiliencia operativa, compra tecnolóxica e gobernanza do risco**.

A presente edición non desenvolve en profundidade este ámbito por razóns de foco e extensión, pero si deixa apuntados os principais vectores que deberán ser observados con atención: **NIS2, CER, CRA, cadea de subministración e SBOM, criptografía post-cuántica, certificación europea e adaptación normativa en España e Galicia**. Estes elementos poderán constituir a base dunha futura entrega específica centrada na dimensión regulamentaria a futuro, complementaria á Guía Normativa xa dispoñible no Observatorio [20].

5 Conclusións

A análise desenvolvida neste informe permite concluír que a **ciberseguridade industrial** está a evolucionar nun contexto marcado por unha interacción cada vez máis estreita entre **transformación tecnolóxica, cambio organizativo e evolución regulamentaria**. Os contornos **ICS/OT**, historicamente máis pechados e orientados á estabilidade operativa, vense agora afectados por dinámicas moito máis amplas: incorporación de **intelixencia artificial en procesos industriais**, expansión de **modelos de automatización cognitiva e axéntica**, aparición de **novas dependencias dixitais**, uso crecente de **plataformas conectadas**, evolución da **computación distribuída**, novas formas de interacción humano-máquina e maior exposición a cambios normativos e xeopolíticos.

Neste contexto, o principal valor achegado polo informe é ofrecer unha **visión panorámica e transversal** dun escenario particularmente complexo, apoiándose en **fontes internacionais de alta relevancia** e nun exercicio de síntese orientado á utilidade práctica. En particular, a análise construída a partir do **Hype Cycle for Emerging Technologies de Gartner**, do informe **Top Strategic Predictions for 2026 and Beyond** e, de maneira especialmente relevante, do **Informe de riscos tecnolóxicos do propio Observatorio**, permite condensar nunha única peza unha lectura estruturada de sinais de cambio que, doutro xeito, aparecerían dispersos en múltiples fontes de referencia. Neste sentido, o informe non pretende substituír análises técnicas específicas e exhaustivas, senón **ordenar, contextualizar e priorizar** tendencias e vectores de cambio con potencial impacto real para Galicia.

Outra conclusión relevante é que non todas as tendencias teñen a mesma materialidade nin o mesmo horizonte de impacto. O exercicio de priorización realizado permite distinguir entre aquelas que requiren **atención inmediata**, as que deben incorporarse de maneira **programada á reflexión estratéxica e tecnolóxica**, e aquelas que convén manter en **vixilancia** por seren aínda máis incertas ou de maduración máis lenta. Esta diferenciación resulta especialmente útil nun ámbito como o da ciberseguridade industrial, no que a acumulación de sinais tecnolóxicas pode xerar ruído se non se acompaña dun criterio claro de selección e relevancia.

A lectura conxunta das tendencias analizadas mostra, ademais, que o risco industrial xa non pode entenderse unicamente dende parámetros clásicos de exposición técnica. Xunto cos retos tradicionais, emerxen con forza cuestións como a **automatización da**

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

decisión, a **gobernanza da IA**, a evolución cara a **sistemas máis autónomos**, a crecente importancia da **soberanía tecnolóxica**, os cambios nas **interfaces e modelos de interacción**, a transformación dos procesos de compra e aprovisionamento mediante sistemas intelixentes, ou a necesidade de prepararse para futuros cambios criptográficos e computacionais. Todo isto obriga a ampliar a mirada e a situar a ciberseguridade industrial tamén no terreo da **estratexia, da organización e da anticipación tecnolóxica**.

Dende a perspectiva da regulamentación, a conclusión principal é que o marco europeo e nacional está a consolidarse como un factor de transformación directa da operación industrial. A combinación de **NIS2, CER e CRA**, xunto coa evolución de cuestións como o **SBOM, a certificación europea, os estándares harmonizados ou a transición cara á criptografía post-cuántica**, apunta a un escenario no que a esixencia non será só normativa, senón tamén operativa e demostrable. Nesta parte do informe acompáñase ademais un **gráfico a modo de folla de ruta de seguimento**, pensado para visualizar de maneira sintética os **fitos máis relevantes que deberán ser monitorizados nos próximos anos** no ámbito da regulación e da estandarización aplicable a contornos ICS/OT.

Para Galicia, o informe deixa unha idea clara: a preparación ante os novos retos da ciberseguridade industrial deberá apoiarse nun **enfoque simultaneamente estratéxico, selectivo e aplicable**. Estratéxico, porque será necesario manter capacidade de observación e interpretación do que está a cambiar a escala internacional. Selectivo, porque non todas as innovacións nin todas as presións regulamentarias requiren a mesma resposta nin no mesmo momento. E aplicable, porque a utilidade final deste tipo de exercicios reside en traducir a análise en decisións realistas sobre prioridades, capacidades e follas de ruta.

En definitiva, o panorama analizado confirma que a ciberseguridade industrial debe entenderse como un punto de encontro entre **tecnoloxía, operación, regulación, resiliencia e gobernanza**. A achega deste informe consiste precisamente en proporcionar unha lectura de conxunto, ordeada e útil, que permita interpretar con maior claridade un escenario crecente en complexidade. Con iso, preténdese reforzar a capacidade do **Observatorio de Ciberseguridade Industrial de Galicia** para seguir actuando como ferramenta de apoio á decisión, de síntese de coñecemento e de orientación estratéxica para o ecosistema industrial e institucional galego.

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 análise tecnolóxica. 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 predicións estratéxicas. Recuperado de https://www.gartner.com/en/articles/strategic-predictions-for-2026

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

[20] Observatorio de Ciberseguridade Industrial de Galicia – AMTEGA (2025). *Guia normativa de ciberseguridade 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 Post-Quantum 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., Xu, 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 do Parlamento Europeo e do Consello relativa a medidas destinadas a garantir un elevado nivel común de ciberseguridade na Unión (NIS2)*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

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

[65] Unión Europea (2024). *Regulamento (UE) 2024/2847 do Parlamento Europeo e do Consello relativo aos requisitos horizontais de ciberseguridade para produtos con*

elementos dixitais (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] Goberno de España – Ministerio da Presidencia, Xustiza e Relacións coas Cortes (2025). *Anteproxecto de Lei de Coordinación e Gobernanza da Ciberseguridade (transposición da 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] Goberno de España – Ministerio do Interior (2025). *Anteproxecto de Lei de protección e resiliencia de entidades críticas (transposición da 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 da Comisión sobre unha folla de ruta coordinada para a transición cara á 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] Goberno de España (2022). *Real Decreto 311/2022, do 3 de maio, polo que se regula o Esquema Nacional de Seguridade*. 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 Ciberseguridade Industrial
Informe de tendencias e regulamento

Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Xacobeo 2027