CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial

Informe de Riscos Tecnolóxicos

Marzo 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_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

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

1 Introdución

Este informe técnico 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.

1.1 Obxectivo e alcance

O presente **Informe de riscos tecnolóxicos** do Observatorio de Ciberseguridade Industrial da AMTEGA ten como obxectivo **identificar e contextualizar** os principais riscos que poden afectar ao tecido industrial e ás infraestruturas críticas, con **foco específico nos tecnolóxicos e contornos OT/ICS** (sistemas de control industrial, automatización e operación).

En particular, o informe pretende:

- **Ofrecer unha visión agregada e comprensible** dos riscos máis relevantes que condicionan a ciberseguridade industrial na actualidade, combinando perspectivas globais (tendencias e risco sistémico) con elementos de aplicabilidade práctica.
- **Traducir riscos "macro" e emerxentes** (xeopolítica, dependencia tecnolóxica, cadeas de subministración, concentración en provedores, evolución do cibercrime, etc.) en **implicacións operativas para OT/ICS**, onde a prioridade

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

histórica de dispoñibilidade, seguridade funcional e continuidade introduce restricións específicas.

- **Incorporar o compoñente de IA** como elemento transversal: tanto polos seus usos defensivos e de optimización industrial, como polos riscos derivados do seu uso malicioso, fallos de funcionamento e posibles efectos sistémicos.
- **Aportar unha base de apoio á toma de decisións** para perfís directivos, responsables de seguridade e risco, equipos técnicos IT/OT e actores institucionais, facilitando a priorización de actuacións e investimentos.

O alcance do informe céntrase, por tanto, en:

- **Riscos, especialmente tecnolóxicos e de ciberseguridade** con impacto potencial sobre **procesos industriais, continuidade de servizo e seguridade física**, considerando tamén efectos sobre reputación, cumprimento, perdas económicas e interrupcións.
- Unha lectura aplicable ao contexto galego por afinidade sectorial (enerxía, auga, automoción, alimentación, loxística, manufactura, etc.), sen pretender ofrecer un inventario exhaustivo por planta, empresa ou instalación.

Este documento **complementa outros entregables do Observatorio**: os Informes de Ciberalertas (visión táctica e continuada de vulnerabilidades e avisos) ou os Informes de Intelixencia de Ameazas (visión máis estratéxica, por actores, campañas e evolución do adversario). O enfoque aquí é distinto: **centrado no risco** como categoría de análise e como ponte entre ameazas, vulnerabilidades, impactos e decisións.

1.2 Metodoloxía

A metodoloxía empregada combina **análise documental**, síntese comparada de fontes e **interpretación orientada a OT/ICS**, co obxecto de construír unha visión consistente e accionable.

O proceso seguido estrutúrase en catro fases principais:

1. **Delimitación do marco de análise e criterios de relevancia**
    - Definición do perímetro temático (riscos tecnolóxicos e ciberfísicos con impacto industrial).

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

- Establecemento de criterios de selección: relevancia para OT/ICS, evidencia en fontes recoñecidas, recorrencia en incidentes ou tendencias, e potencial impacto sobre continuidade e seguridade.

2. **Recollida e curación de fontes**
    - Compilación de información a partir de informes e publicacións de referencia (organismos internacionais, axencias públicas, centros nacionais de ciberseguridade, entidades do sector e fabricantes), priorizando fontes con metodoloxía explícita e datos agregados.
    - Identificación de contidos complementarios do propio Observatorio para asegurar coherencia interna.
3. **Síntese e estruturación do risco**
    - Agrupación dos riscos en bloques temáticos (panorama global, impacto económico, incidentes e ameazas emerxentes —incluíndo IA—, e dimensións de gobernanza, cumprimento e resiliencia).
    - Contextualización explícita en clave industrial: efectos sobre operación, dependencia de terceiros, limitacións de parcheo, restricións de cambios, seguridade funcional, segmentación, acceso remoto e cadea de subministración OT, etc.
4. **Validación interna e enfoque didáctico**
    - Revisión de coherencia: que os riscos descritos se conecten con impactos realistas e con medidas de mitigación (directas ou compensatorias) compatibles con OT/ICS.

1.3 Consideracións e limitacións

O informe **non substitúe** unha análise de risco específica por organización (que requiriría inventario, arquitectura, criticidade e avaliación de impactos por proceso), senón que fornece unha **base de contexto e priorización**.

As fontes empregadas son maioritariamente internacionais; con todo, a aplicabilidade ao contexto galego é elevada debido ao carácter remoto e transfronteirizo de gran parte das ameazas e á utilización de tecnoloxías e provedores comúns.

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

En materia de IA, inclúense recomendacións e riscos de carácter transversal de diversas fontes reputadas; a súa implantación debe adaptarse ao **grao de madurez** e ao **perfil de exposición** de cada contorno industrial.

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

2 Resumo executivo

Este **Informe de riscos tecnolóxicos** ofrece unha visión integrada dos principais riscos que afectan á ciberseguridade industrial e ás infraestruturas críticas, con foco en contornos **OT/ICS**. O documento **combina fontes internacionais e nacionais para describir tanto riscos estruturais e recorrentes** (segmentación deficiente, exposición de acceso remoto, xestión de vulnerabilidades, dependencias de terceiros) como **riscos emerxentes vinculados á transformación dixital e ao uso crecente de Intelixencia Artificial (IA)**, conectándoos cos impactos máis relevantes en operación: **indispoñibilidade**, degradación do proceso, custo económico e risco físico.

A lectura do informe está orientada a unha análise global. En OT/ICS, a seguridade non pode formularse só como un exercicio "IT", senón como un equilibrio continuo entre **seguridade, continuidade de operación e seguridade funcional**.

Partindo dese enfoque, o informe incorpora tamén **unha capa de risco máis ampla, máis alá do puramente tecnolóxico**. En liña coas análises de risco sistémico (por exemplo, as que populariza o **World Economic Forum**), recóllense **factores que amplifican a exposición industrial, actuales e a título predictivo: tensión xeopolítica, interrupcións de cadea de subministración, concentración de provedores, escaseza de capacidades e dependencia de servizos dixitais,** etc**.** Estes elementos non "rompen" un PLC por si sós, pero si condicionan a probabilidade, a velocidade de propagación e o custo de recuperación dun incidente, e por tanto **deben formar parte da conversa de risco a nivel directivo.**

Sobre esa base macro, o documento baixa ao chan operativo e sinala que **o risco OT é crecente e multidimensional** porque aumenta a conectividade e, con ela, a exposición a ameazas globais (cibercrime, extorsión/ransomware, espionaxe e sabotaxe), mentres persisten debilidades estruturais en inventario, xestión de configuración, accesos privilexiados e xestión do cambio**. A converxencia IT/OT e a participación de terceiros amplían aínda máis a superficie de ataque**: a **integración con sistemas corporativos, a externalización de mantemento e a dependencia de integradores e provedores introducen vías recorrentes de intrusión**, polo que se require **gobernanza**, **control contractual e deseños de conectividade minimizados e monitorizados.**

Neste escenario, **a IA aparece como elemento transversal por dous motivos**.

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

- Primeiro, porque **pode reforzar defensas e operación** (detección, correlación, apoio ao diagnóstico),
- pero tamén porque **introduce riscos novos e amplifica outros existentes.**

O informe estrutura estes riscos de IA en tres planos:

- **uso malicioso** (automatización de campañas, *phishing* máis convincente, aceleración de explotación),
- **fallos de funcionamento** (erros, deriva do modelo, decisións opacas)
- e **riscos sistémicos** (dependencias, concentración tecnolóxica e efectos en cadea).

A isto engádese un factor organizativo especialmente relevante: o **Shadow AI**, é dicir, o **uso non gobernado de ferramentas de IA por parte de empregados e equipos (incluíndo provedores)** fóra dos procedementos corporativos. En contornos industriais, o Shadow AI pode traducirse en filtración de información sensible (configuracións, diagramas, incidentes), decisións técnicas baseadas en respostas non verificadas e creación de dependencias operativas sen avaliación de risco.

A partir desta lectura, **o informe propón que a mitigación eficaz non depende de "solucións milagre", senón de fundamentos ben executados e deseñados para contención e recuperación.** Así, as **recomendacións consolidadas de fontes como NCSC, CISA, ISACA ou o fabricante Fortinet conflúen nun núcleo común**:

- **inventario e rexistro definitivo** do contorno OT;
- **segmentación** e control de conectividade;
- **eliminación de exposición OT á Internet pública** e endurecemento do acceso remoto con **mínimo privilexio** e autenticación forte;
- **xestión de vulnerabilidades** e parches baseada en risco, apoiada en **medidas compensatorias** cando a actualización inmediata non é viable;
- integración de OT en **SecOps** e en resposta a incidentes con playbooks específicos;
- e **capacidade de operación manual, illamento e continuidade** para manter seguridade funcional cando o contorno dixital está comprometido.

Para a IA en OT, o informe incorpora dúas capas complementarias de recomendacións.

- Por unha banda, os **Principios para a integración segura da IA en OT** publicados por un consorcio internacional, establecen unha folla de ruta práctica en catro bloques:

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

- **comprender a IA** (riscos únicos, ciclo de vida de desenvolvemento seguro e formación do persoal);
- **avaliar o seu uso no dominio OT** (caso de negocio, protección dos datos OT, papel dos provedores e retos de integración);
- **crear marcos de gobernanza e aseguramento** (mecanismos de gobernanza, integración cos marcos existentes, probas e avaliación, e cumprimento);
- e **incorporar supervisión e prácticas failsafe** (monitorización, supervisión e mecanismos de seguridade funcional e recuperación).

A mensaxe transversal é clara: a IA só debe introducirse cando exista un caso de uso válido e cando se poida garantir **control, trazabilidade, probas rigorosas e capacidade de reversión**.

- Por outra banda, a achega do *International AI Safety Report* inclúese de forma deliberadamente parcial e selectiva, centrada no que é máis aplicable á ciberseguridade industrial.. Deste informe destácanse cinco ideas útiles para OT/ICS:
  - os **retos técnicos e institucionais** (decisións con evidencia incompleta e responsabilidades distribuídas en cadeas de valor complexas);
  - as **prácticas de xestión do risco** (documentación, transparencia, casos de seguridade física e integración da IA na xestión de incidentes);
  - as **salvagardas técnicas e a monitorización** (avaliación adversarial/red teaming, defensa en profundidade e vixilancia en produción asumindo fallo);
  - os riscos asociados a **modelos open-weight** (maior facilidade para retirar salvagardas, modificar modelos e herdar riscos na integración);
  - e a necesidade de **resiliencia** (continuidade, coordinación e capacidade de recuperación fronte a efectos en cadea).

A incorporación de IA debe abordarse coa mesma lóxica: **valor operativo si, pero nunca a costa de aumentar a fraxilidade, reducir a capacidade de control ou degradar a seguridade funcional**.

Adicionalmente, plantéxanse **observacións específicos asociadas á cuantificación do impacto económico do risco OT** (dunha orde de magnitude de exposición de mais de trescentos mil millóns de dólares americanos)**, modelos de perdas e estimacións de redución de risco global e sectorial.**

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

Tralo anterior, analízanse a alto nivel os datos do ano pasado de incidentes en contornos industriais, e unha enquisa mundial ós xestores de empresas, para constatar que **só o 5% das mesmas teñen visibilidade con cobertura total da sua rede OT a nivel de ciberseguridade.**

Própoñense adicionalmente como gardacarrís do risco dous elementos de apoio:

- **Un modelo de goberno de ciberseguridade e resiliencia** que comprende tanto unha proposta de **estrutura organizativa canónica como as funcións de seguridade transversais asociadas** para unha organización tipo,
- A **referencia resumida do conxunto de marcos normativos e estándares recollidos na Guía Normativa de ciberseguridade Industrial** deste mesmo Observatorio.

En conxunto, o informe conclúe que o risco tecnolóxico en contornos industriais é **xestionable**, pero require disciplina e coherencia: coñecer o contorno, limitar exposición, deseñar para contención e recuperación, e establecer gobernanza que conecte persoas, procesos e tecnoloxía.

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

3 Panorama de riscos

A continuación preséntase unha visión estruturada dos principais factores que condicionan o risco tecnolóxico no eido industrial. En primeiro lugar, introdúcese un bloque de **riscos xerais**, que recolle tendencias e elementos de contexto (tecnolóxicos e tamén sistémicos) que aumentan a exposición dos contornos OT/ICS e inflúen na probabilidade de materialización das ameazas.

A continuación, analízase o **impacto económico do risco**, poñendo o foco en como os incidentes poden traducirse en custos directos e indirectos —paradas de produción, degradación operativa, recuperación, penalizacións, cumprimento e reputación— e por que isto converte a ciberseguridade industrial nun factor material para a continuidade do negocio e a toma de decisións.

3.1 Riscos xerais

3.1.1 Foro Económico Mundial (WEF)

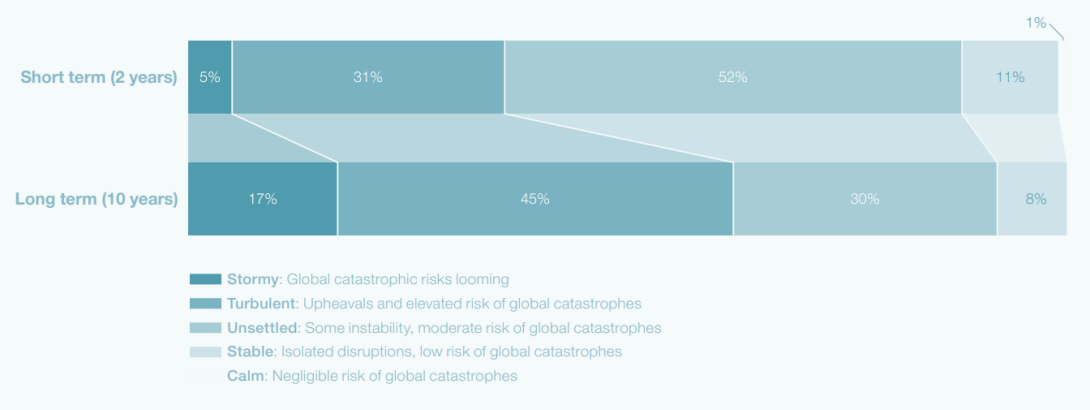
Non podemos comezar sen mencionar o **Global Risks Report 2025.** É unha publicación anual do **World Economic Forum (WEF)**, institución internacional de referencia na análise de tendencias globais que impactan sobre economías, gobernanza, tecnoloxía e sociedade [1][2].

O informe **recompila a percepción e análise de riscos a curto e longo prazo a partir de enquisas a expertos, responsables públicos, líderes empresariais e analistas de risco** a nivel mundial. A súa relevancia reside en ofrecer unha visión sistémica e prospectiva dos factores que poden comprometer a estabilidade económica, social e tecnolóxica, incluíndo aqueles con impacto directo sobre infraestruturas críticas e sistemas industriais.

Desde a perspectiva da **ciberseguridade industrial galega**, este informe constitúe unha fonte clave para contextualizar os riscos tecnolóxicos e ciberfísicos que poden afectar a sectores estratéxicos como a enerxía, a industria manufactureira, o transporte, a auga ou as telecomunicacións, todos eles fortemente dependentes de sistemas ICS/OT e de infraestruturas dixitais interconectadas.

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

Percepción global do risco: deterioración progresiva



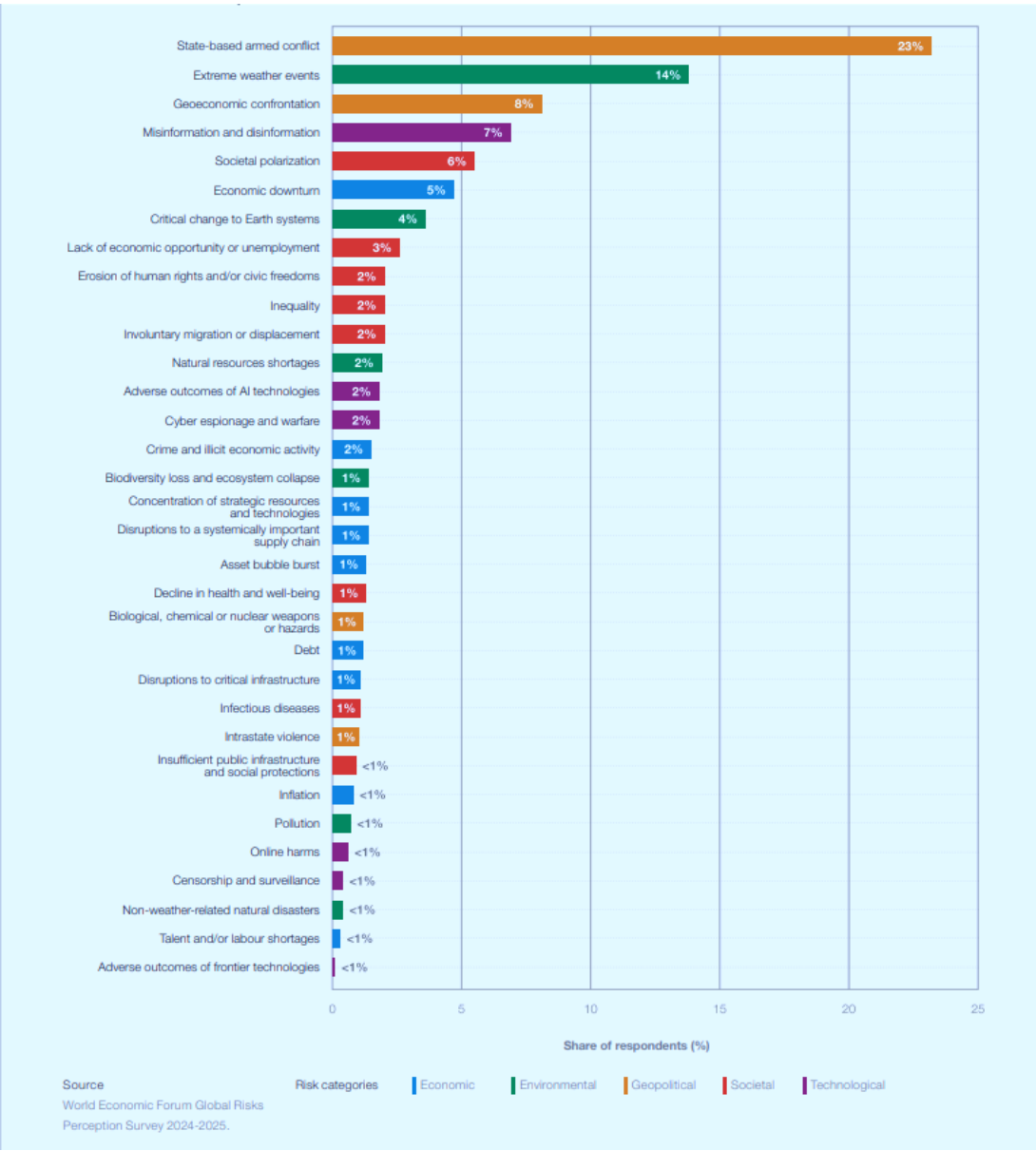
Panorama global de riscos a curto e medio prazo segundo os expertos. Fonte: WEF (2025)

O informe amosa de forma clara unha **tendencia negativa na percepción global do risco**, evidenciando que o mundo é percibido como máis inestable e exposto ca en edicións anteriores. A figura reflicte un incremento sostido da percepción de risco sistémico, asociado á combinación de crises xeopolíticas, transformación tecnolóxica acelerada e dependencia crecente de infraestruturas críticas dixitalizadas.

Para Galicia, esta tendencia global tradúcese nun aumento da exposición indirecta a riscos externos, mesmo en contornos industriais locais, debido á interdependencia con cadeas de subministración internacionais, operadores globais e tecnoloxías importadas.

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

Principais riscos globais relacionados



Riscos globais identificados. Fonte: WEF (2025)

A figura recolle a percepción dos riscos con maior capacidade de xerar unha crise material a escala global no **ano 2025** (segundo as opinións do estudio 2024-2025). Para o presente informe, interesa salientar dous elementos:

- O **peso relativo** (porcentaxe de respostas) que obteñen certos riscos tecnolóxicos, indicador da prioridade percibida.
- As **implicacións operativas en redes OT/ICS**, onde a dependencia de servizos dixitais, comunicacións e operación remota converte estes riscos en escenarios con impacto directo en continuidade, seguridade funcional e cumprimento.

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

A continuación preséntanse os **seis riscos tecnolóxicos** da imaxe anterior do WEF (marcados en morado), grupo ao que consideramos engadir por afinidade o risco de **Disrupción en infraestruturas críticas**. Incluímos a definición do Informe, posición relativa, e as posibles consecuencias para o sector industrial galego.

3.1.1.1 Desinformación ou información falsa

7% de respostas, **posto #4**.

Información falsa persistente (deliberada ou non) amplamente difundida a través de redes de medios, que despraza a opinión pública de maneira significativa cara á desconfianza nos feitos e na autoridade. Inclúe, entre outros: contido falso, impostor, manipulado e fabricado.

Pode degradar a toma de decisións en crise (p. ex., información falsa sobre cortes, verteduras, paradas programadas), **aumentar a presión pública e institucional durante incidentes e facilitar campañas de engano que acompañen intrusións** (phishing dirixido a persoal con acceso OT, falsos avisos de mantemento, suplantación de provedores).

3.1.1.2 Resultados adversos do uso da IA

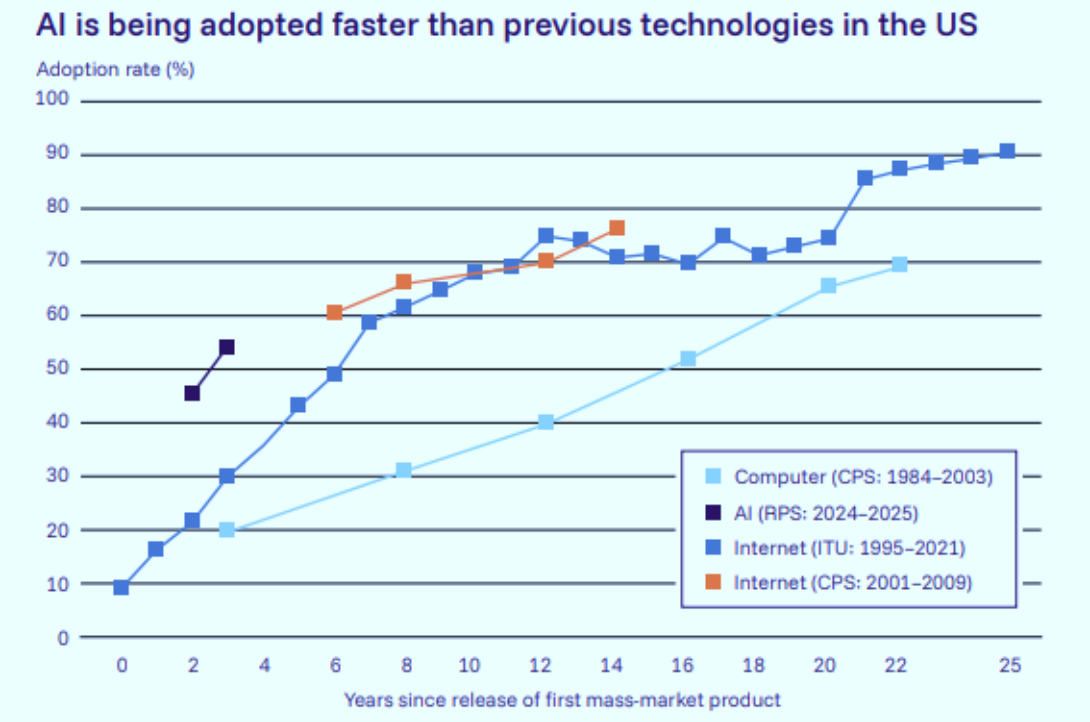
2% de respostas, **posto #13**.

Consecuencias negativas, previstas ou imprevistas, dos avances en IA e nas capacidades tecnolóxicas relacionadas (incluíndo a IA xenerativa) sobre persoas, empresas, ecosistemas e/ou economías.

A adopción de IA en monitorización, optimización de produción e detección de anomalías pode introducir fallos por modelos mal adestrados, **dependencia excesiva** de automatización, **degradación de seguridade** por datos de baixa calidade **e novos vectores** (p. ex., manipulación de datos de proceso para inducir decisións erróneas).

Hay que ter en conta que é unha tecnoloxía cuxa adopción está sendo espectacularmente rápida.

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



Velocidade de adopción da IA fronte outras tecnoloxías. Fonte: International AI Safety Report (2026)

3.1.1.3 Ciberespionaxe e guerra híbrida

2% de respostas, **posto #14**.

Uso de **armas e ferramentas de ciberseguridade por actores estatais e non estatais para obter control** sobre unha presenza dixital, **causar interrupción operativa e/ou comprometer ou danar as redes e infraestruturas** tecnolóxicas e de información dunha entidade. Inclúe: operacións cibernéticas defensivas e ofensivas que teñen lugar durante un conflito armado ou o desencadean, e ciberataques que rouban datos clasificados, sensibles ou propiedade intelectual para obter vantaxe.

Implica un **risco de intrusión orientada a intelixencia** (exfiltración de enxeñaría, planos e configuracións), **preposicionamento para sabotaxe e interrupción operativa**. En sectores industriais e infraestruturas esenciais, estes escenarios adoitan materializarse en movemento lateral IT-OT, abuso de acceso remoto e degradación de servizos de supervisión.

3.1.1.4 Disrupción en infraestruturas críticas

1% de respostas, **posto #23**.

Sobrecarga ou apagado de infraestruturas físicas e dixitais (incluíndo satélites) **ou de servizos que sustentan sistemas críticos**, incluíndo internet, telecomunicacións, servizos públicos, sistemas financeiros ou enerxía, derivados de, entre outros:

ciberataques, danos físicos intencionais ou non, episodios meteorolóxicos extremos e desastres naturais.

Xeran un **risco central para continuidade industrial: interrupcións en electricidade, telecomunicacións, servizos de internet, subministración de auga, loxística ou servizos financeiros poden provocar paradas de planta, perda de visibilidade e control, fallos en telemantemento e degradación de sistemas de seguridade**. É especialmente crítico en operación remota, integración IT-OT e dependencia de servizos satelitais e/ou de telecomunicacións.

3.1.1.5 Dano online ás persoas

1% de respostas, **posto #29**.

Erosión da protección fronte a, e/ou prevalencia de, **comportamentos daniños que supoñen unha ameaza dixital para a saúde emocional ou mental e o benestar das persoas**. Inclúe, entre outros: acoso en liña e ciberacoso.

Aínda que o impacto é máis indirecto, **pode incidir en riscos de persoas (acoso a empregados, chantaxe, exposición pública de identidades), afectar a dispoñibilidade de persoal clave e amplificar incidentes** mediante campañas de intimidación ou doxxing (revelación intencional de información persoal ou comprometedora) vinculadas a eventos industriais.

3.1.1.6 Censura e vixilancia

1% de respostas, **posto #30**.

Observación ampla e xeneralizada dun lugar ou dunha persoa e/ou supresión da comunicación, da información e das ideas, de forma física ou dixital, ata o punto de vulnerar de maneira significativa dereitos humanos e civís (por exemplo, privacidade, liberdade de palabra e liberdade de expresión).

Pode **afectar a operación industrial por restricións de comunicación e acceso a información técnica, así como por vixilancia extensiva que comprometa a privacidade e a seguridade de persoal e organizacións**. En escenarios híbridos, pode acompañarse de control da información sobre incidentes e de presión regulatoria ou xeopolítica que limite a cooperación.

3.1.1.7 Resultados adversos das tecnoloxías de fronteira

1% de respostas, **posto #30**.

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

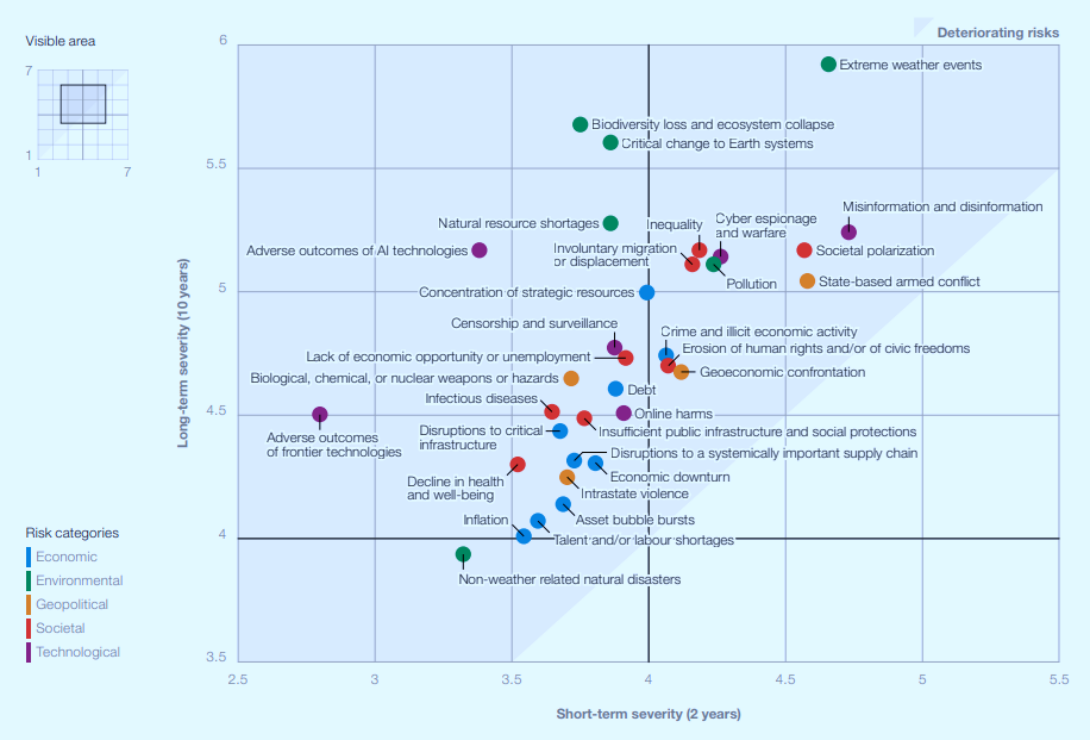
Consecuencias negativas, previstas ou imprevistas, dos avances en tecnoloxías de fronteira sobre persoas, empresas, ecosistemas e/ou economías. Inclúe, entre outros: interfaces cerebro-computador, biotecnoloxía, xeoenxeñaría e computación cuántica.

Supoñen risco de cambios disruptivos no equilibrio tecnolóxico (p. ex., impacto futuro na criptografía e na protección de comunicacións), **aparición de novas superficies de exposición e dependencia de capacidades avanzadas con gobernanza e seguridade inmaduras**. A medio prazo, **require vixilancia tecnolóxica** e avaliación de impacto en confidencialidade e integridade.

Severidade a curto e longo prazo

A figura seguinte, analiza a **severidade dos riscos no curto fronte ao longo prazo**, mostrando como algúns riscos tecnolóxicos tenden a intensificarse co paso do tempo.

Nótese que a escala de severidade é Likert de 1 a 7 (mínima a máxima).



Severidade relativa dos riscos a curto e medio prazo. Fonte: WEF (2025)

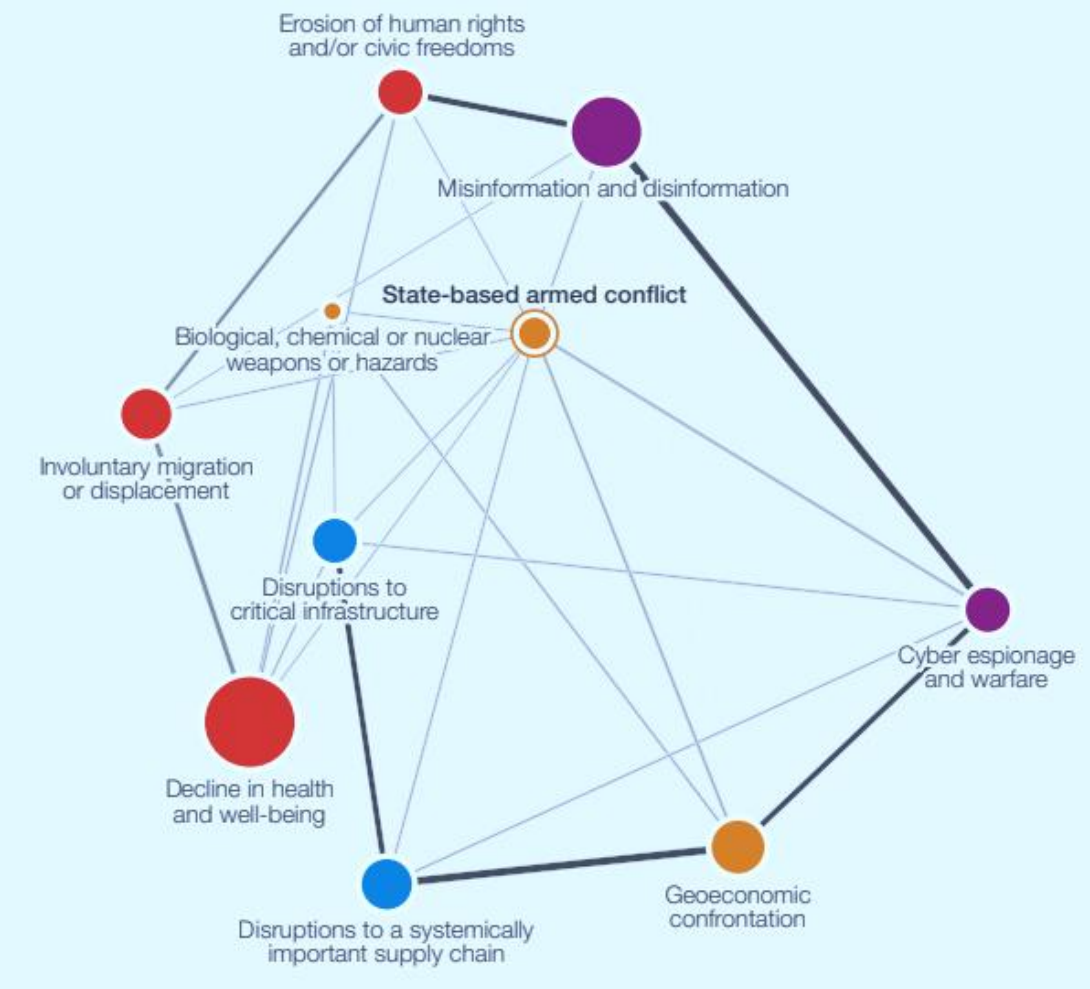
Os riscos asociados á tecnoloxía dixital, á interconectividade e ás infraestruturas críticas aparecen como moderados no curto prazo, pero con **alta severidade potencial a longo prazo**, especialmente se non se adoptan medidas estruturais de resiliencia.

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

Este enfoque **resulta clave para a planificación estratéxica en ciberseguridade industrial en Galicia**, onde moitas infraestruturas presentan ciclos de vida longos e tecnoloxías herdadas que incrementan a exposición futura.

Conflitos armados e riscos interconectados

O informe destaca a relación crecente entre **conflitos armados e riscos tecnolóxicos**, tal e como se reflicte na figura seguinte.



Relación entre conflitos armados e riscos tecnolóxicos. Fonte: WEF (2025)

Os conflitos actúan como catalizadores de ciberataques, sabotaxes dixitais e operacións híbridas que teñen como obxectivo infraestruturas críticas civís e industriais.

A experiencia recente amosa que estes riscos non permanecen confinados aos países en conflito, senón que se propagan a través do ciberespazo e das cadeas de subministración, afectando tamén a territorios como Galicia.

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

Transformación tecnolóxica acelerada

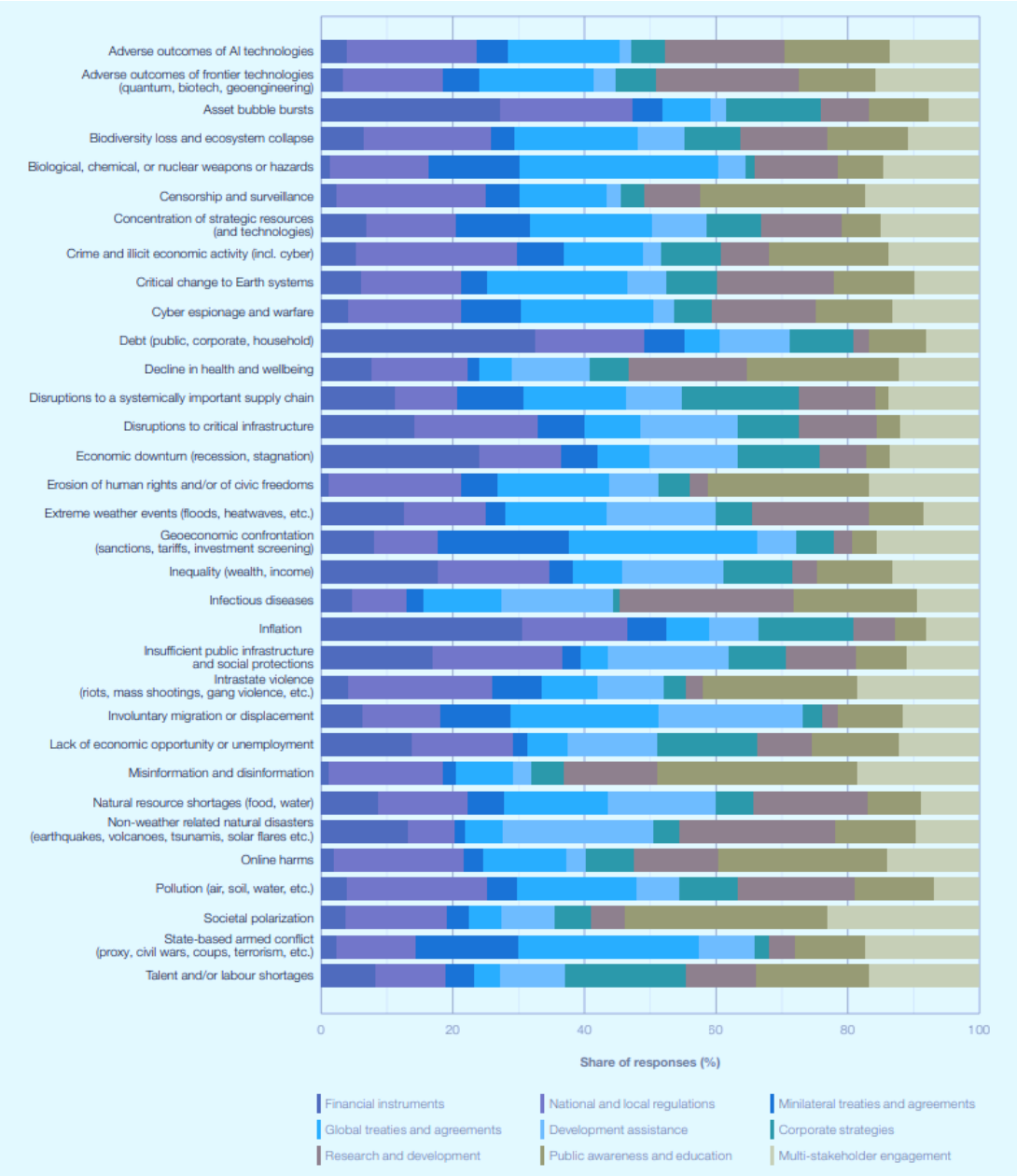
A percepción dos enquisados subliña tamén que os **cambios acelerados na tecnoloxía** están a introducir novas superficies de exposición. **A integración de sistemas industriais con plataformas dixitais**, servizos remotos, intelixencia artificial e automatización avanzada **incrementa a eficiencia, pero tamén a complexidade e o risco**.

Para o tecido industrial galego, isto implica a necesidade de integrar a ciberseguridade desde o deseño e a operación, evitando enfoques reactivos.

Propostas e implicacións

A análise da figura de **Risk governance** achega unha lectura especialmente valiosa para comprender como deben abordarse os **riscos tecnolóxicos** e o risco de **disrupción de infraestruturas críticas** desde unha perspectiva realista e operativa. A gráfica non avalía a gravidade dos riscos, senón que identifica **que enfoques teñen maior potencial para impulsar accións eficaces de redución do risco e mellora da preparación** nos vindeiros dous anos. O resultado é revelador.

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



Proposta de Risk Governance. Fonte: WEF (2025)

En primeiro lugar, obsérvase que, para a práctica totalidade dos **riscos tecnolóxicos** analizados —incluíndo **ciberespionaxe e guerra híbrida**, **resultados adversos da IA**, **tecnoloxías de fronteira**, **censura e vixilancia** ou **danos no ámbito dixital**—, **os enfoques puramente técnicos ou financeiros non son percibidos como os máis determinantes**. Pola contra, a gráfica amosa de forma consistente un maior peso da **regulación nacional e local**, da **implicación directa do sector privado**, dos **acordos multilaterais** e da **coordinación entre múltiples actores**.

Este patrón confirma que os riscos tecnolóxicos son entendidos como **riscos sistémicos de gobernanza**, e non como problemas que poidan resolverse exclusivamente

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

mediante innovación tecnolóxica, investimento en seguridade ou investigación. Desde a óptica de **OT/ICS**, esta conclusión resulta especialmente relevante: a seguridade industrial non depende só da robustez técnica dos sistemas, senón da existencia de **marcos normativos claros**, **responsabilidades ben definidas**, **cadeas de subministración seguras** e **mecanismos efectivos de coordinación público-privada**.

No caso concreto de **ciberespionaxe e ciberguerra**, a figura reflicte con claridade que os enfoques con maior potencial son os **acordos internacionais** e a **implicación do sector privado**, mentres que a investigación e desenvolvemento aparece cun peso claramente inferior. Isto reforza a idea de que estes riscos, aínda que se materializan tecnicamente en redes e sistemas, **teñen unha natureza eminentemente estratéxica e xeopolítica**. En entornos OT/ICS, isto tradúcese en escenarios de intrusión prolongada, exfiltración de información sensible ou preposicionamento para sabotaxe, fronte aos cales a capacidade de resposta local é insuficiente sen **cooperación supraterritorial e intercambio de información**.

Algo semellante ocorre cos **resultados adversos da IA** e das **tecnoloxías de fronteira**. A gráfica amosa que a **regulación**, a **concienciación** e a **participación activa do sector privado** son percibidas como máis eficaces que a propia madurez tecnolóxica. Isto suxire que estas tecnoloxías están a introducirse a un ritmo superior á capacidade de comprender e controlar os seus efectos. En sistemas industriais, esta situación pode derivar en **automatización excesiva**, **dependencia de modelos opacos** ou **decisións erróneas baseadas en datos incompletos ou manipulados**, incrementando o risco operativo e de seguridade funcional.

No que respecta a **disrupcións de infraestruturas críticas**, a gráfica presenta un patrón aínda máis significativo. Non existe un enfoque claramente dominante, senón unha distribución equilibrada entre **regulación**, **implicación do sector privado**, **investimento**, **concienciación pública** e **coordinación multiactor**. Esta dispersión reflicte a natureza **transversal, interdependente e multicausal** deste risco. As infraestruturas críticas dependen de sistemas dixitais, servizos enerxéticos, telecomunicacións e cadeas loxísticas que, ao fallar, xeran **efectos en cascada** con impacto directo sobre a operación industrial.

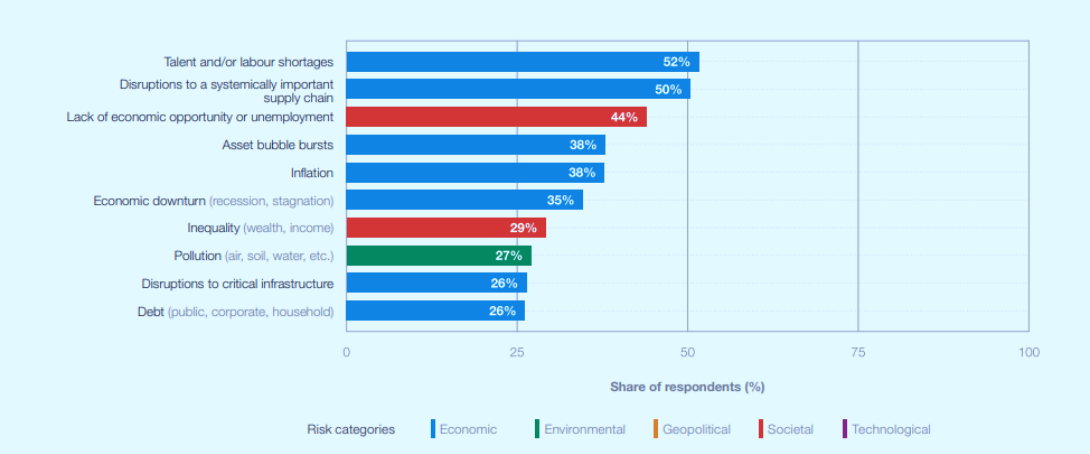
Desde a perspectiva da **ciberseguridade industrial galega**, esta lectura é especialmente relevante. Confirma que a disrupción de infraestruturas críticas **non pode mitigarse mediante unha única medida nin desde un único ámbito**, senón que

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

require unha combinación de **deseño resiliente**, **operación segura**, **gobernanza clara** e **capacidade de resposta coordinada**. A dependencia crecente de operación remota, servizos dixitais e integración IT-OT amplifica este risco, mesmo en escenarios locais afastados dos grandes focos de conflito.

En conxunto, a opinión do panel do WEF reforza unha mensaxe central que encaixa plenamente co enfoque deste Informe: **os principais riscos tecnolóxicos que afectan a OT/ICS non se reducen principalmente con máis tecnoloxía, senón con mellor gobernanza**. A ciberseguridade industrial debe entenderse como un elemento estrutural da resiliencia, no que a técnica é necesaria pero non suficiente, e no que a coordinación, a regulación e a responsabilidade compartida son factores críticos para limitar o impacto dos riscos globais sobre a realidade industrial galega.

Relacionado tamén coa Gobernanza, **a seguinte imaxe complementa esta visión, sinalando a xuizo dos expertos, que riscos poderán ser mitigados en maior medida mediante estratexias corporativas**.



Top Riscos Globais xestionables mediante estratexias corporativas. Fonte: WEF (2025)

Póñense así de manifesto as conexións entre riscos tecnolóxicos, xeopolíticos e económicos, reforzando a idea de que a ciberseguridade industrial non pode abordarse de forma illada.

O Global Risks Report 2025 confirma que os riscos tecnolóxicos e ciberfísicos xa non son escenarios excepcionais, senón elementos estruturais do contexto global. Isto implica **en Galicia** varias **necesidades a nivel colectivo e das entidades particulares**:

- Integrar a análise de riscos globais na xestión da ciberseguridade industrial local.
- Priorizar a protección e resiliencia das infraestruturas críticas.

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

- Anticipar impactos derivados de conflitos e crises externas.
- Reforzar a cooperación público-privada en materia de seguridade industrial.

3.1.2 Riscos tecnolóxicos clásicos

A análise da compañía Nozomi Networks [3] sitúa como punto de partida un feito xa estrutural: **os sistemas OT están cada vez máis conectados por IP e, en consecuencia, máis expostos a ameazas cibernéticas**, ao tempo que **se difuminan as fronteiras entre a xestión de risco TI e o risco operacional**. Neste escenario, **integrar o risco OT na estratexia corporativa de seguridade** deixa de ser unha opción e pasa a ser un requisito para protexer a continuidade operativa e a seguridade das persoas.

Dende unha perspectiva de **ciberseguridade industrial galega**, isto tradúcese nun impacto directo sobre plantas e operacións onde OT/ICS é clave (manufactura, enerxía, auga, loxística, cadeas de subministración industriais, etc.): **a exposición tecnolóxica xa non é só un risco dixital, senón un risco ciberfísico**, con potencial de indispoñibilidade, degradación de calidade e afectación á seguridade funcional.

A continuación, sintetízanse os **riscos tecnolóxicos clásicos** máis recorrentes nestes contornos, combinando o enfoque do artigo anterior, coa visión recollida en entregables previos do Laboratorio como o Informe de Ciberalertas ou Intelixencia de Ameazas [4].

3.1.2.1 Converxencia TI/OT

A converxencia tecnolóxica implica que unha intrusión inicial en TI (identidade, correo, estacións de traballo, servizos corporativos) poida **derivar en movemento lateral cara a redes de operación**, especialmente cando existen **puntos de salto TI/OT** e interdependencias fortes. O efecto práctico é unha **maior probabilidade de que ataques "clásicos" (ransomware, compromiso de credenciais, intrusións por servizos expostos) acaben impactando en operación**.

3.1.2.2 Acceso remoto

Tanto en informes sectoriais como en guías orientadas a operacións, o **acceso remoto** aparece de forma consistente como **un dos vectores máis críticos: VPNs, mantementos remotos, accesos de integradores e fabricantes, ou canles de soporte**. Este risco combínase con dous factores frecuentes en industria: **necesidade operativa real** (o acceso remoto é parte do modelo de mantemento) e **dificultade de gobernar identidades e trazabilidade** cando intervén cadea de subministración.

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

3.1.2.3 Tecnoloxía insegura

A presenza de **protocolos industriais sen cifrado nin autenticación forte por deseño** (especialmente en contornos legados) introduce riscos específicos: observación/manipulación de tráfico, suplantación e alteración de comandos ou estados de proceso. En OT isto é especialmente sensible porque a comunicación de control non é "un dato": é unha orde que actúa sobre un proceso físico.

3.1.2.4 Obsolescencia

Destacar que en OT son comúns **dispositivos legados e protocolos propietarios**, o que complica o descubrimento de activos e o perfilado de comportamento. A isto engádense ciclos de vida longos (10–25 anos), **fin de soporte** e limitacións de recursos (capacidade de cómputo e memoria) que restrinxen a incorporación de mecanismos de seguridade modernos. O resultado é un risco acumulativo: **activos críticos con exposición crecente e capacidade limitada de actualización**.

3.1.2.5 Xestión de vulnerabilidades

A xestión de vulnerabilidades en OT é descrita como un reto maior polo **volume e diversidade de dispositivos e plataformas** e porque **o parcheado non se pode automatizar como en TI**. Ademais, a práctica industrial impón fricción: paradas planificadas escasas, validacións, compatibilidades, e risco de impacto sobre a produción. Isto favorece que **vulnerabilidades coñecidas permanezan máis tempo expostas**.

3.1.2.6 Falta de visibilidade e monitorización

En OT, a **ausencia de visibilidade** (**inventario fiable**, coñecemento de protocolos industriais, cambios en lóxicas de control e configuracións) conduce á **detección tardía** e perda de oportunidade para identificar intrusións silenciosas ou manipulacións graduais. Este risco é especialmente relevante en operacións distribuídas ou con múltiples sedes, onde a heteroxeneidade e a segmentación imperfecta agravan a situación.

3.1.2.7 Arquitecturas planas

Moitas organizacións industriais parten de **redes historicamente planas e moi interconectadas, o que facilita a propagación e o movemento lateral**. En escenarios de converxencia, isto converte unha brecha inicial nun incidente máis amplo: **un evento localizado pode evolucionar cara á perda de control do proceso** se os puntos de interconexión non están ben gobernados.

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

3.1.2.8 Sensibilidade operativa

En comparación con TI, OT caracterízase por **alta sensibilidade a interrupcións**: **escaneos agresivos, reinicios non coordinados ou cambios de configuración poden provocar indispoñibilidades** ou estados non previstos. Xunto con isto, existen **dependencias complexas** (firmware, librarías, software de enxeñaría, módulos de E/S) que poden introducir risco incluso en cambios aparentemente menores. A consecuencia é que **o propio ciclo de vida tecnolóxico (cambio/actualización) se converte nun factor de risco.**

3.1.2.9 Gobernanza transversal

Finalmente, **un risco recorrente é organizativo-tecnolóxico: en OT as decisións técnicas (accesos, configuracións, actualizacións) requiren coordinación entre operación, mantemento, enxeñaría e seguridade.** Se a gobernanza é difusa, xéranse condicións para **exposición prolongada**, prácticas ad hoc e variabilidade entre plantas, o que aumenta a probabilidade de incidentes e dificulta a resposta. Falaremos desta organización posteriormente no Informe.

3.1.3 Visión de Google

As análises **Cybersecurity Forecast 2025** e **Cybersecurity Forecast 2026**, elaboradas por equipos de intelixencia e resposta a incidentes de Google (incluíndo capacidades integradas de Threat Intelligence e Mandiant), ofrecen unha lectura anticipatoria das tendencias que máis probablemente condicionarán a actividade adversaria no curto prazo e por tanto supoñen o risco mais probable [5][6].

Para este informe empregamos as dúas últimas edicións para acadar mais contexto, aínda que só se recollen os elementos **directamente aplicables á ciberseguridade industrial**, é dicir, aqueles que afectan á **continuidade operativa**, á **cadea de subministración industrial**, á **exposición TI/OT** e á **superficie de ataque típica en redes OT/ICS**.

A mensaxe común en ambos recursos é clara: a evolución do risco en 2025-2026 estará dominada por **economía do cibercrime con foco na interrupción**, por **uso intensivo de IA para escalar o engano e acelerar operacións**, e por **actividade estatal e híbrida asociada a tensións xeopolíticas**. Isto encaixa coa realidade de OT/ICS, onde o impacto final non se limita á perda de información: pode traducirse en **paradas de planta, degradación de servizos esenciais e efectos en cadea sobre produción e loxística**.

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

3.1.3.1 Cibercrime

A previsión para 2026 sinala explicitamente que o risco máis disruptivo de orixe non natural para **ICS e OT** seguirá sendo o **cibercrime**, por enriba doutras categorías. En termos industriais, isto é relevante porque o cibercrime non precisa "comprender" o proceso: abóndalle con **interromper as dependencias de negocio** que alimentan a operación.

O informe destaca un patrón especialmente crítico para industria: operacións de ransomware (bloqueo e secuestro de datos) **deseñadas para impactar software empresarial esencial** (como sistemas ERP), co obxectivo de **romper o fluxo de datos que sostén a operación OT**. Este enfoque é particularmente eficaz porque **comprometer a capa de negocio pode paralizar o ámbito industrial**, incrementando a presión para pagamentos rápidos.

3.1.3.2 Interrupción por vías indirectas

A perspectiva anterior reforza un punto clave para Galicia: a continuidade OT/ICS depende cada vez máis de servizos corporativos e de cadea de subministración dixital (planificación, compras, trazabilidade, mantemento, calidade…). Por tanto, a disrupción non require acceso directo a PLCs ou SCADA: pode materializarse mediante **interrupción de sistemas transversais** que sosteñen a operación.

3.1.3.3 Acceso remoto e "hixiene"

Sublíñase tamén recalcando a visión clásica, que prácticas deficientes, como **accesos remotos inseguros**, seguirán permitindo que **malware común** acabe penetrando en redes OT. Esta constatación é relevante para contornos industriais porque a operación real esixe acceso remoto (soporte, integradores, fabricantes), e o risco adoita concentrarse en **credenciais, sesións e canles de soporte**.

3.1.3.4 Credenciais roubadas e infostealers (malware)

As previsións do ano pasado situaban a **substracción e reutilización de credenciais** (impulsada por campañas masivas de **malware específico**) como unha tendencia central. Para OT/ICS isto implica un aumento da probabilidade de intrusión por "inicio de sesión" máis que por explotación técnica directa: un atacante con credenciais válidas pode entrar en VPNs, portais de soporte ou contornos híbridos e, dende aí, chegar a activos industriais.

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

3.1.3.5 IA como acelerador

Os dous recursos, así como o WEF, coinciden en que a IA terá un papel crecente, con especial impacto en:

- **Phishing e vishing máis verosímiles** (incluíndo **clonación de voz** e suplantación de persoal executivo ou técnico), o que incrementa o risco de acceso inicial en organizacións industriais.
- **Operacións de información** que escalan contido e perfís falsos, con efecto indirecto sobre incidentes industriais (presión social, distorsión de información crítica en crise).

As previsións de 2026 engaden un elemento novo especialmente pertinente para organizacións industriais que adoptan IA en procesos corporativos: o risco de **prompt injection**, entendido como manipulación de sistemas de IA para forzar accións non previstas, exfiltración ou sabotaxe. A medida que sistemas de IA se integren en fluxos de traballo (p.ex. análise de incidencias, xestión documental, automatización en centros de operacións), este risco introduce unha nova categoría de exposición con consecuencias potenciais sobre operación e continuidade.

3.1.3.6 Xeopolítica e análogos

No convulso mundo en que vivimos, a **xeopolítica** continuará impulsando a actividade estatal, destacando o papel persistente de Rusia e China (e tamén Irán e Corea do Norte) en operacións de espionaxe e influencia. Para 2026 compleméntase esta visión sinalando que, aínda que menos frecuentes, os ataques estatais orientados a OT seguen sendo **altamente sofisticados** e ligados a conflitos específicos.

Ademais, incorporan unha referencia relevante para OT: grupos hacktivistas pro-Rusia poden representar unha ameaza substancial e imprevisible para entornos de operación, citando como exemplo o **compromiso dunha presa en Noruega** (abril de 2025) [7]. A lectura industrial é inmediata: en escenarios de tensión xeopolítica, OT pode converterse en obxectivo por **valor simbólico, efecto social e capacidade de interrupción**.

3.1.3.7 Dispositivos de a bordo e terceiros

Destácase finalmente que certos actores aumentarán o foco en **dispositivos de a bordo** (frecuentemente sen capacidades equivalentes de detección e resposta) e en **provedores terceiros**, porque comprometer un socio pode abrir acceso a múltiples organizacións. En industria, isto é consistente coa realidade de integración e

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

mantemento: a superficie de ataque amplíase con **equipos perimetrais**, conectividade industrial e cadeas de soporte (relacionado en certa maneira coa cadena de subministro vista anteriormente).

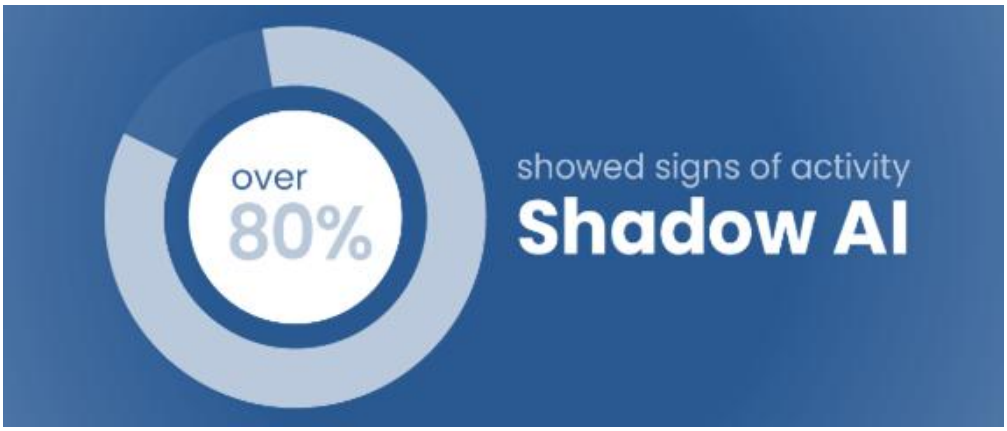
3.1.4 Uso indebido de compoñentes IT/AI

O **13º Estudo do Estado da Arte da Seguridade na Nube**, elaborado por **ISACA** e polo **capítulo español da Cloud Security Alliance (CSA Spain Chapter)** en colaboración con outros afíns [8], ofrece unha visión consolidada sobre a adopción real de servizos cloud nas organizacións e os riscos asociados á súa xestión. Aínda que o documento non está especificamente orientado a contornos industriais, **os seus achados resultan plenamente aplicables á ciberseguridade industrial**, na medida en que a nube, as ferramentas colaborativas e os servizos baseados en IA están a integrarse de forma crecente en procesos que soportan ou condicionan a operación OT.

Da revisión do estudo despréndese que, máis alá de riscos xa tratados noutras fontes (cadea de subministración, credenciais, configuracións incorrectas), **un elemento diferencial e máis relevante para este informe é a persistencia e expansión do Shadow IT e AI** (en adiante Shadow Tech cando englobe ambos), fenómeno que adquire unha nova dimensión coa popularización de **ferramentas de IA accesibles desde a nube, incluso enfoques axénticos da mesma**.

3.1.4.1 Que é o Shadow Tech

O **Shadow Tech** refírese ao **uso de aplicacións, servizos ou infraestruturas tecnolóxicas de información ou intelixencia artificial fóra do control e da gobernanza formal da organización**, normalmente sen coñecemento nin validación dos equipos de TI ou seguridade. O estudo evidencia que este fenómeno non diminúe coa madurez dixital; ao contrario, **incrementa coa facilidade de acceso a servizos cloud e SaaS**, especialmente cando achegan valor inmediato ao usuario.



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

Frecuencia de aparición de Shadow AI en organizacións. Fonte: XM Cyber (2025)

A irrupción de **ferramentas de IA xenerativa**, asistentes intelixentes, servizos de análise ou automatización na nube **intensifica este risco**, xa que permiten procesar información, xerar contido ou automatizar tarefas sen infraestrutura propia nin coñecementos técnicos avanzados. En contornos industriais, estas ferramentas poden ser empregadas para:

- Análise de incidencias ou rexistros de operación.
- Xeración de documentación técnica.
- Soporte á toma de decisións en mantemento ou produción…

Cando isto ocorre fóra de gobernanza, **datos sensibles de operación, enxeñaría ou negocio poden ser expostos a terceiros sen control nin trazabilidade**.

3.1.4.2 Implicacións específicas do Shadow Tech en contornos OT/ICS

En ciberseguridade industrial, este fenómeno presenta **características propias** que amplifican o risco:

- **Fronteira difusa entre TI e OT**: aplicacións cloud empregadas en ámbitos corporativos (planificación, mantemento, calidade) condicionan directamente a operación industrial.
- **Exposición indirecta de OT**: sen acceso directo a PLC ou SCADA, un servizo Shadow Tech pode almacenar diagramas, configuracións, informes de proceso ou credenciais.
- **Perda de visibilidade e control**: os equipos de seguridade non poden avaliar risco, aplicar políticas nin responder a incidentes sobre activos que descoñecen.
- **Cumprimento normativo comprometido**: uso non autorizado de servizos externos pode vulnerar requisitos de confidencialidade, localización de datos e seguridade esixidos por regulación sectorial.

3.1.4.3 Risco ciberfísico

A combinación de **Shadow Tech + dependencia operativa** introduce un risco cualitativamente distinto. Non se trata só de perda de datos, senón da posibilidade de:

- Manipulación indirecta da toma de decisións.
- Exposición de información que permita sabotaxe posterior.

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

- Introdución de dependencias críticas en servizos externos non avaliados.

Desde a perspectiva da ciberseguridade industrial galega, isto supón un desafío crecente: **o risco xa non reside só na rede OT, senón nas ferramentas auxiliares que condicionan como se opera, mantén e decide sobre o proceso industrial**.

3.1.4.4 O caso ClawDBot

Para ilustrar o anterior, un elemento especialmente relevante e recente é a aparición de **ferramentas útiles ou aparentemente lexítimas baseadas en IA que son adoptadas sen control nin salvagardas de seguridade**, explotando directamente o fenómeno do Shadow Tech. Un exemplo representativo é o sucedido con **ClawDBot (renomeado a Moltbot)**, un proxecto **open source en estado embrionario**, presentado como ferramenta de automatización e asistencia baseada en IA que a pesar das advertencias so seu creador Peter Steinberger, foi viralizado expoñendo a miles de particulares e organizacións a grandes riscos de seguridade [9].

Este tipo de solucións ilustra unha evolución do risco que convén matizar:

- O risco **non reside na ferramenta en si**, senón na súa **adopción sen gobernanza, control nin avaliación de seguridade**.
- No caso de ClawDBot, o propio autor **recomendaba o seu uso exclusivo por persoal experto e en contornos controlados**, advertindo do seu carácter experimental.
- A descarga e execución sen coñecemento técnico nin salvagardas introduce **exposición innecesaria a malware, roubo de información, credenciais ou acceso remoto**, entre outros.

En entornos industriais, onde o persoal técnico busca solucións rápidas para análise, diagnóstico ou documentación, **a adopción informal deste tipo de ferramentas resulta especialmente perigosa**, xa que pode operar durante longos períodos sen detección, fóra de calquera control corporativo.

3.1.5 Predicción do INCIBE-CERT

O artigo «¿Que esperar da ciberseguridade industrial en 2023?», publicado por **INCIBE-CERT (Instituto de Ciberseguridade de España)** a comezos de 2023, presenta unha serie de predicións que, malia a súa **antigüidade temporal**, continúan a ter **vixencia parcial ou plena** no contexto actual. Isto débese a que moitas delas non describen

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

fenómenos conxunturais, senón **tendencias estruturais** propias da transformación dixital industrial, da evolución do risco e do marco regulatorio [10].

Neste apartado recóllense **unicamente aquelas predicións ou riscos, non todos eles tecnolóxicos, que non se suliñan** nos apartados adxacentes, e que achegan **valor complementario** para a comprensión do risco en contornos **OT/ICS**.

3.1.5.1 Profesionalización e especialización crecente do atacante en contornos industriais

INCIBE-CERT anticipaba unha evolución cara a atacantes **máis especializados en tecnoloxías industriais**, con coñecementos específicos de procesos, protocolos e operación. Esta predición segue sendo relevante: o acceso a documentación, formación e ferramentas especializadas reduciu a barreira de entrada e favoreceu ataques máis precisos, aínda que non sempre máis sofisticados tecnicamente.

A maior risco de manipulación dirixida do proceso, **ataques máis silenciosos e mellor adaptación do atacante ás restricións operativas** industriais.

3.1.5.2 Incremento da exposición por dixitalización acelerada e presión por eficiencia

O artigo sinalaba que a presión por mellorar eficiencia, automatizar procesos e reducir custos levaría a **dixitalización acelerada**, frecuentemente sen que a seguridade avanzase ao mesmo ritmo. Esta dinámica continúa presente, especialmente en organizacións medianas e pequenas.

A introdución de tecnoloxía conectada sen avaliación de risco completa, **amplía a superficie de ataque e a dependencia crecente de sistemas dixitais** para operación crítica.

3.1.5.3 Dependencia de persoal clave e risco asociado á perda de coñecemento

INCIBE-CERT destacaba o risco asociado á **dependencia de persoal técnico moi especializado**, cuxo coñecemento non sempre está documentado nin compartido. Este risco, aínda pouco tratado noutras fontes, ten impacto directo na seguridade.

A saída, indispoñibilidade ou erro humano de persoal clave **pode derivar en configuracións inseguras, resposta tardía a incidentes ou perda de capacidade de recuperación**.

3.1.5.4 Falta de cultura de seguridade industrial como factor amplificador do risco

O artigo subliñaba que, en moitas organizacións, **a ciberseguridade industrial segue a percibirse como un problema alleo á operación diaria**. Esta falta de cultura segue sendo un elemento estrutural que amplifica outros riscos.

O seu efecto pode materializarse en **maior probabilidade de prácticas inseguras, resistencia a cambios necesarios e baixa detección temperá** de incidentes.

3.1.5.5 Incremento de incidentes híbridos con impacto físico indirecto

INCIBE-CERT anticipaba un aumento de incidentes nos que o impacto físico non é inmediato nin directo, pero aparece como consecuencia dunha cadea de eventos dixitais. Esta predición mantén plena vixencia.

Os incidentes que comezan en TI, identidade ou sistemas auxiliares poden acabar provocando paradas, degradación de servizos ou estados operativos non seguros.

3.1.5.6 Necesidade crecente de coordinación entre operación, mantemento e seguridade

Finalmente, apuntábase á **necesidade de romper silos organizativos entre áreas** técnicas. A falta de coordinación segue sendo un risco en si mesmo.

O contrario, promove a **aparición de respostas descoordinadas, cambios non comunicados e dificultades para xestionar incidentes complexos** que afectan a múltiples dominios.

3.1.6 Cadro resumo de riscos

A continuación preséntase unha **matriz resumo dos riscos identificados nos apartados previos**. Esta matriz ten como obxectivo **organizar e sintetizar os principais riscos que afectan á ciberseguridade industrial**, facilitando unha visión estruturada que permita a súa comprensión global e a posterior priorización.

O **nivel de risco asignado** a cada elemento (**alto, medio ou baixo**) ten un **carácter cualitativo e referencial**, baseado nunha valoración xeral da **probabilidade de materialización** e do **impacto potencial** en contornos **OT/ICS**. Esta estimación pretende ofrecer unha orientación inicial coherente co contexto industrial analizado, pero **non substitúe unha avaliación de risco formal**.

En consecuencia, o nivel de risco efectivo deberá ser **axustado e refinado en función do contexto organizativo concreto**, tendo en conta factores como o sector de

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

actividade, a criticidade dos procesos, o grao de dixitalización, a exposición a terceiros, a madurez da gobernanza e as capacidades reais de detección e resposta. Só mediante esta análise contextualizada é posible determinar a prioridade real de cada risco e a súa relevancia específica para unha organización determinada.

Categoría	Risco	Descrición breve	Nivel de risco
Tecnolóxico	Desinformación e información falsa	Distorsión da percepción e da toma de decisións durante incidentes industriais	Medio
Tecnolóxico	Resultados adversos do uso da IA	Automatización e analítica mal gobernadas con impacto operativo	Medio
Xeopolítico	Ciberespionaxe e guerra híbrida	Intrusións persistentes con fins de intelixencia ou sabotaxe	Alto
Tecnolóxico	Disrupción de infraestruturas críticas	Interrupción de servizos esenciais con efectos en cascada	Alto
Humano	Danos dixitais ás persoas	Acoso, chantaxe ou exposición de persoal clave	Medio

Xeopolítico	Censura e vixilancia	Restrición da comunicación e presión informativa	Baixo
Tecnolóxico	Tecnoloxías de fronteira	Cambios disruptivos con seguridade inmadura	Baixo
Organizativo	Converxencia TI/OT non gobernada	Propagación de incidentes desde TI a OT	Alto
Tecnolóxico	Acceso remoto inseguro	Compromiso vía VPNs, soporte remoto e terceiros	Alto
Tecnolóxico	Tecnoloxía industrial insegura por deseño	Protocolos e sistemas sen protección nativa	Alto
Tecnolóxico	Obsolescencia e activos legados	Exposición prolongada por ciclos de vida longos	Alto
Organizativo	Xestión deficiente de vulnerabilidades	Persistencia de fallos coñecidos en OT	Alto
Organizativo	Falta de visibilidade e monitorización OT	Detección tardía de intrusións	Alto
Organizativo	Arquitecturas de rede planas	Movemento lateral facilitado	Alto

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

Organizativo	Sensibilidade operativa a cambios	Indispoñibilidades por accións técnicas non coordinadas	Medio
Organizativo	Gobernanza transversal insuficiente	Responsabilidades difusas entre áreas	Alto
Humano	Profesionalización do atacante industrial	Ataques máis adaptados ao proceso	Medio
Estratéxico	Dixitalización acelerada sen seguridade	Incremento da superficie de ataque	Alto
Humano	Dependencia de persoal clave	Perda de coñecemento crítico	Medio
Organizativo	Falta de cultura de seguridade industrial	Normalización de prácticas inseguras	Medio
Tecnolóxico	Incidentes híbridos con impacto físico	Cadeas de eventos dixitais con efecto físico	Alto
Organizativo	Silos organizativos	Resposta ineficaz a incidentes complexos	Medio
Humano	Cibercrime orientado á interrupción	Paradas operativas como obxectivo principal	Alto

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

Organizativo	Dependencias dixitais indirectas	Paradas por fallo de sistemas corporativos	Alto
Humano	Roubo de credenciais e infostealers	Acceso por sesións válidas	Alto
Tecnolóxico	IA como acelerador do engano	Phishing e suplantación avanzada	Medio
Tecnolóxico	Prompt injection	Manipulación de sistemas baseados en IA	Medio
Xeopolítico	Hacktivismo e conflitos	Ataques simbólicos a OT	Medio
Tecnolóxico	Dispositivos de bordo expostos	Equipos perimetrais con baixa protección	Medio
Humano	Terceiros comprometidos	Acceso indirecto vía provedores	Alto
Organizativo	Shadow Tech	Uso de tecnoloxía fóra de gobernanza	Alto
Organizativo	Ferramentas de IA non gobernadas	Uso informal de software experimental	Alto
Estratéxico	Dependencia de servizos cloud non controlados	Perda de resiliencia por dependencia externa	Medio

Cadro de riscos identificados no Informe. Fonte: elaboración propia (2026)

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

3.2 Impacto económico do risco OT

A materialización dun incidente de ciberseguridade en **tecnoloxías de operación (OT/ICS)** tradúcese, en primeiro termo, en custos técnicos de contención e recuperación (análise forense, restauración de sistemas, reposición e servizos externos). Porén, o impacto económico real vén determinado, na maioría dos casos, pola **interrupción do negocio**: paradas de produción, perda de capacidade, desperdicio de produto, penalizacións contractuais, afectación a servizos esenciais e impactos en cadea sobre provedores e clientes. En moitos dos sectores estratéxicos presentes en Galicia —**industria manufactureira, enerxía, auga, portos ou loxística** por exemplo—, unha degradación temporal da operación pode converter un evento dixital nun incidente con **impacto económico ampliado**.

Nesta liña, Dragos publicou unha análise específica de risco financeiro en OT baseada en datos do mercado asegurador e en modelización do risco agregada. A comunicación pública asociada ao informe estima **máis de 300.000 millóns de dólares estadounidenses** de exposición potencial global en risco OT, cifra que busca situar o debate no plano executivo e financeiro.

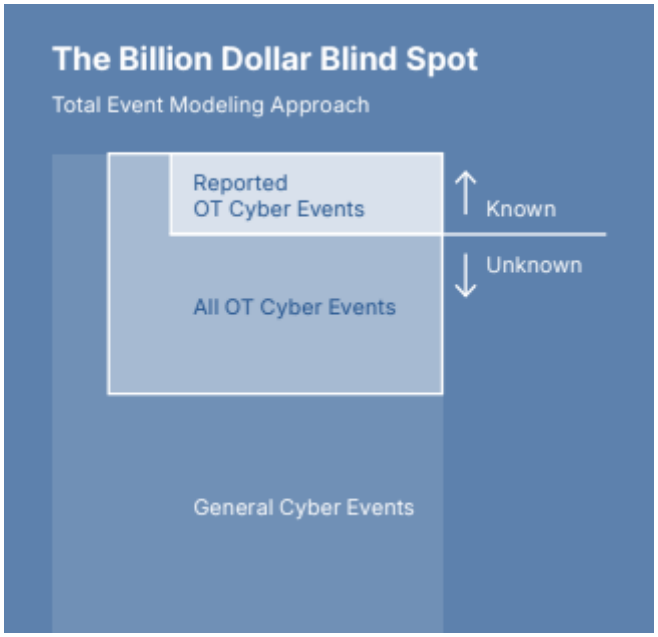
En concreto, o estudo referencia unha exposición agregada de **até 329,5 mil millóns de dólares** nun escenario de cola **1:250 (0,4% de probabilidade anual)**, e identifica **172,4 mil millóns** asociados especificamente a escenarios de **interrupción do negocio**. Para unha orde de magnitude anual "media", o informe manexa estimacións de **31,1 mil millóns** de risco anual agregado e **12,7 mil millóns** cando se consideran reclamacións asociadas a disrupcións [11][12].

Exposición agregada a risco ICS/OT. Fonte: Dragos (2025)

Como se aprecia na figura seguinte, estas cifras son **estimacións** e non un reconto exhaustivo. A razón principal non é matemática, senón empírica: **non se coñece o**

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

universo total de incidentes OT, porque unha parte significativa dos eventos **non se reportan publicamente**, non chegan a rexistrarse como reclamación aseguradora ou quedan clasificados como incidentes internos.



Clasificación de ciberincidentes OT e a efectos do estudio. Fonte: Dragos (2025)

En consecuencia, calquera análise cuantitativa que pretenda medir o risco económico global debe traballar cun **subconxunto observable** (incidentes coñecidos e datos dispoñibles) e extrapolar a exposición, incorporando a posibilidade de **subnotificación**. Esta realidade é especialmente relevante en OT/ICS, onde a prioridade operativa, a reputación e a complexidade de atribución favorecen que moitos incidentes non transcendan fóra da organización.

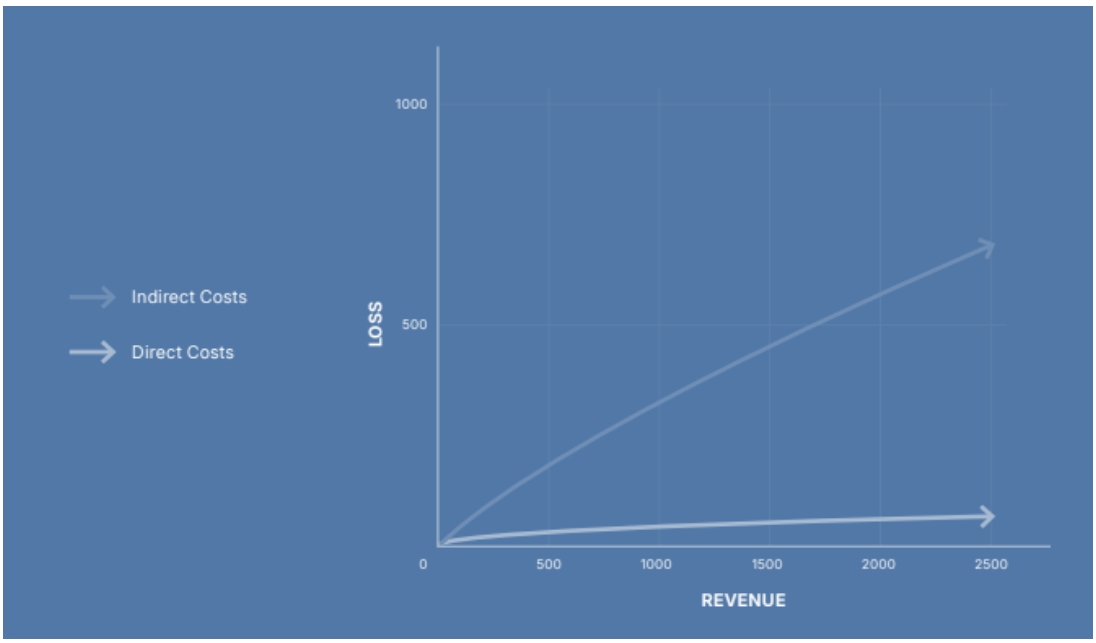
A lectura máis útil para o contexto galego non é a cifra exacta, senón o patrón que o informe enfatiza: o custo potencial en OT **non está dominado polo dano físico directo**, senón pola **perda de continuidade** e polos efectos colaterais. O documento explicita esta idea distinguindo entre:

- **custos directos** (recuperación técnica, reposición, servizos)
- e **custos indirectos** (paradas preventivas por prudencia, indispoñibilidade de sistemas de soporte, impacto contractual e efectos en cascada).

En procesos continuos (enerxía, auga) e en manufactura con cadeas axustadas (automoción, alimentación), a prudencia operativa pode implicar paradas que

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

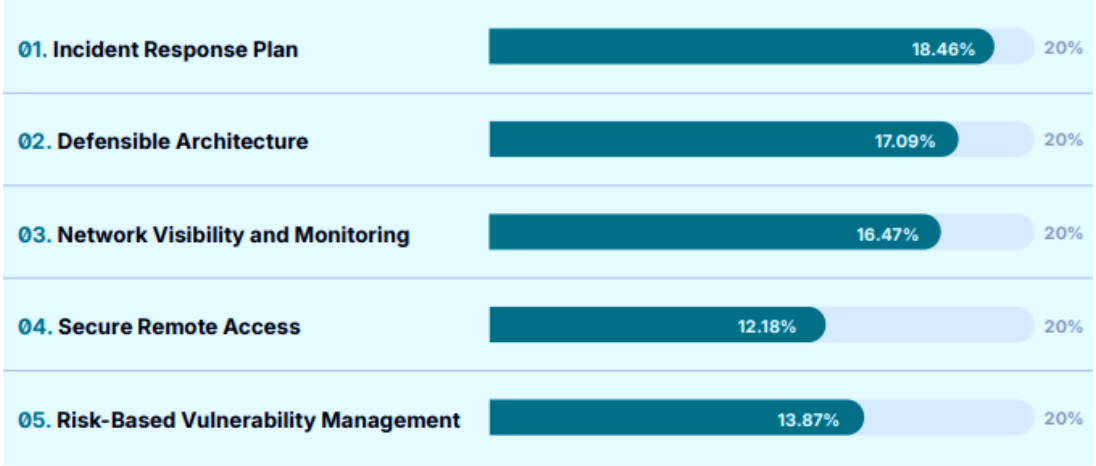
multiplican o custo final, mesmo cando o dano inicial é limitado. Como se ve na gráfica, o custo indirecto tende a dominar.



Modelo de perdas en costes directos e indirecto. Fonte: Dragos (2025)

Outro achado operativo do informe é que a redución do risco non depende por igual de todos os controis, e que existen medidas con efecto especialmente relevante para limitar perdas económicas. Dragos emprega os cinco controis críticos en ICS [13] (xa estudiados noutros Informes do Observatorio como a Guía Normativa [31]) como referencia práctica e conclúe que a **preparación e resposta a incidentes** é un dos factores con maior correlación coa redución de perdas agregadas. A modo de recordatorio, os cinco controis citados son: **plan de resposta a incidentes ICS**, **arquitectura defendible**, **visibilidade e monitorización de rede ICS/OT**, **acceso remoto seguro** e **xestión de vulnerabilidades baseada en risco**.

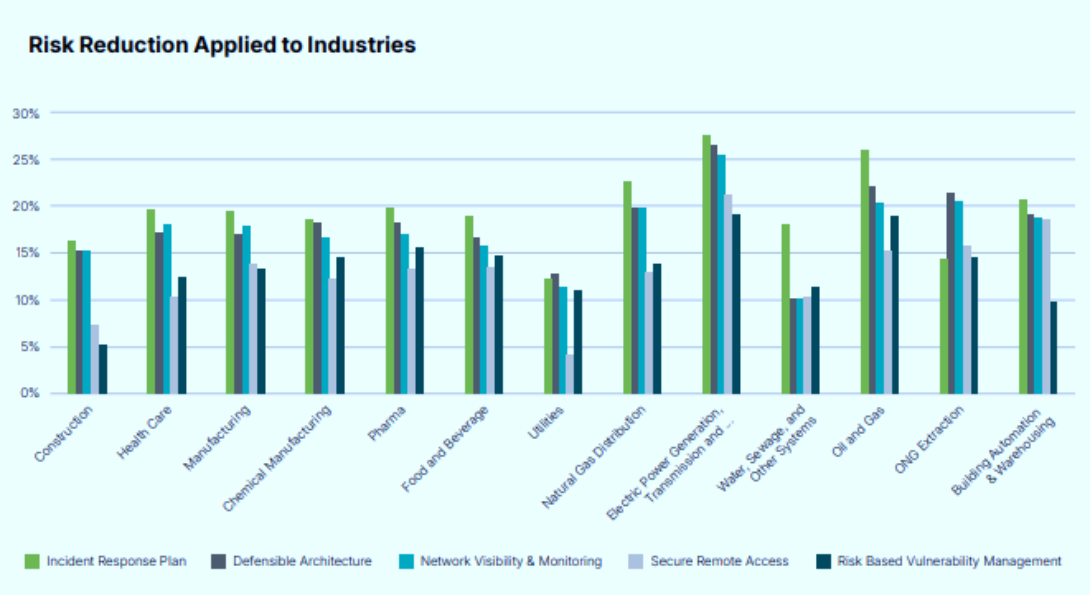
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027



Estimación de redución de niveis de risco por control crítico en ICS. Fonte: Dragos (2025)

Podemos afirmar deste xeito que **priorizar controis non só reduce probabilidade e impacto técnico, senón que reduce a exposición financeira asociada á continuidade do negocio e a custos indirectos**.

O informe tamén desagrega resultados por sector, mostrando que o peso relativo de determinados controis varía segundo a natureza da operación e a criticidade do servizo. Este punto é especialmente relevante para Galicia porque permite unha lectura sectorial inmediata: en ámbitos onde a dispoñibilidade é crítica e a recuperación é complexa, melloras en arquitectura, visibilidade e resposta poden traducirse nunha **redución estimada de perdas maior**.



Redución de risco sectorial. Fonte: Dragos (2025)

En paralelo, Dragos identifica tres retos estruturais que explican por que o risco OT estivo historicamente infravalorado:

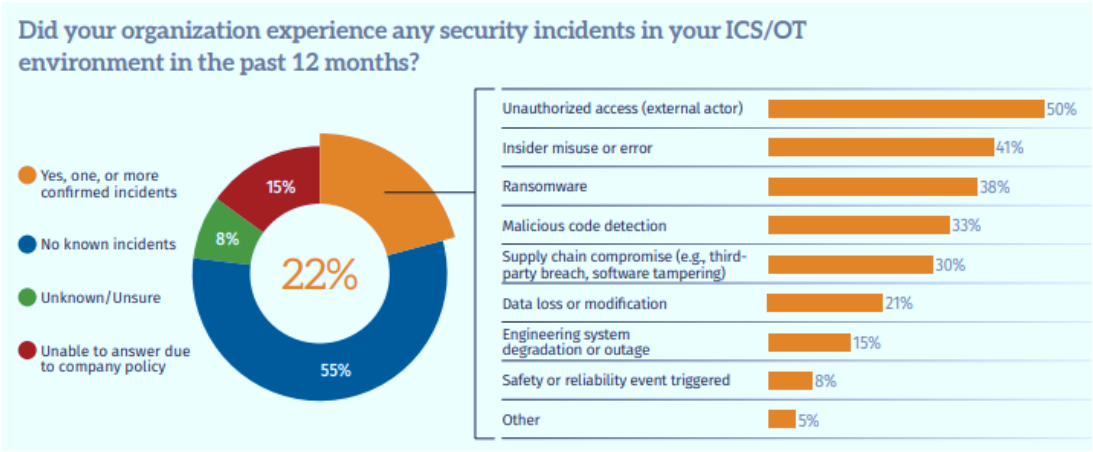
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

1. **Impacto financeiro previamente indefinido**.
2. **Dificultade para estimar o retorno do investimento (ROI)** en seguridade OT (proponse un modelo cuantitativo no Informe de Ciberalertas do Observatorio [4]).
3. **Dificultade para priorizar melloras de controis** sen evidencias independentes.

En organizacións industriais medianas, estas tres barreiras adoitan coexistir con restricións de recursos e con gobernanzas onde OT e TI non sempre están aliñadas, o que reforza a necesidade de incorporar unha lectura económica do risco.

Como lectura sintética do informe orientada a responsables de risco, xurídico e seguros, resulta útil a versión do mesmo publicada en The Policyholder Perspective [15].

Para aterrar as estimacións económicas na realidade operativa, o informe de SANS Institute de Estado da seguridade en ICS/OT 2025 [16], achega evidencias en base a enquisas sobre **tipos de incidentes habituais** e sobre **tempos do incidente**, variables que condicionan directamente o custo final.



Estatística de tipoloxía de incidentes ICS. Fonte: SANS (2025)

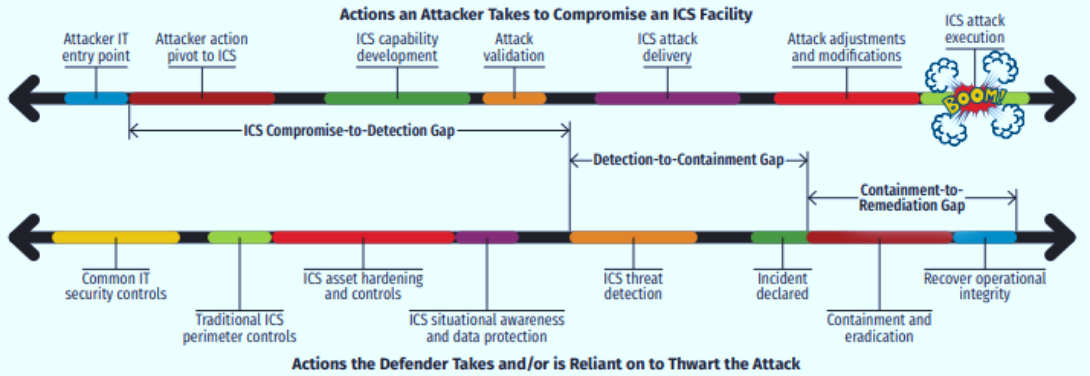
Téñase en conta que certos escenarios —por exemplo, **acceso externo non autorizado** e **ransomware**— teñen unha capacidade inmediata para derivar en interrupción operativa, mentres que outras categorías (p.ex. compromiso por terceiros) actúan como porta de entrada con efectos diferidos.

No relativo ós tempos dos incidentes, a continuación, amósanse as definicións das tres ventás temporais involucradas na mitigación dos ciberincidentes:

- Tempo entre o compromiso e a detección
- Tempo entre a detección e a contención

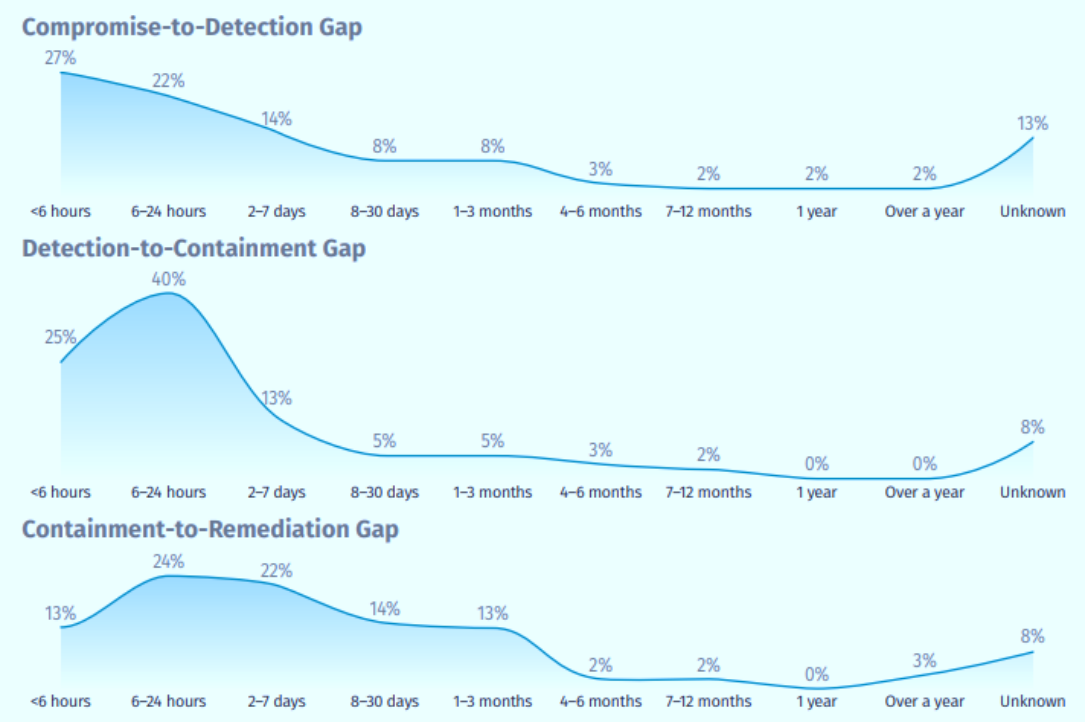
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

- Tempo entre a contención e a remediación



Tempos involucrados na mitigación dun incidente. Fonte: SANS (2025)

Estos tempos permiten ligar ciberseguridade con economía dunha maneira directa: **o custo escala co tempo**, e a remediación prolongada penaliza a continuidade e a recuperación. En OT, onde a restauración pode requirir validacións operativas e coordinación con enxeñaría, estas demoras son particularmente gravosas.



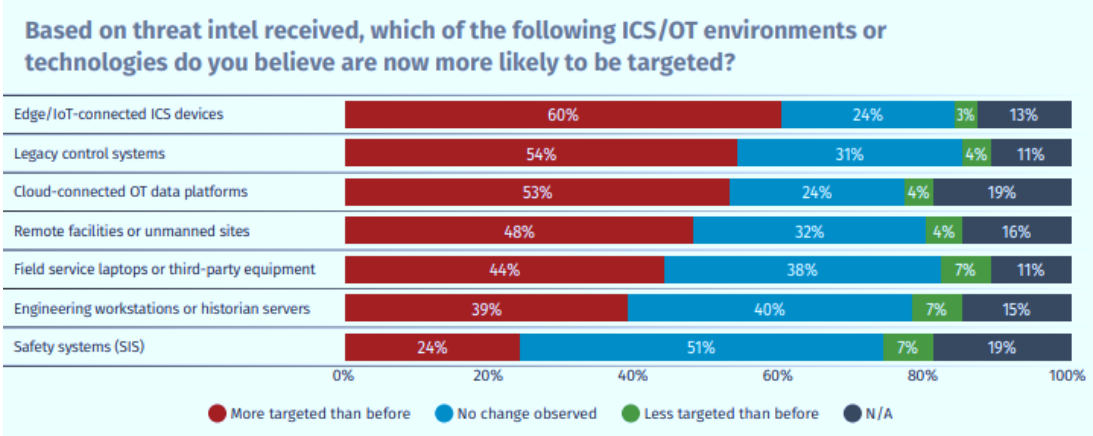
Estatisticas sobre os tempos de mitigación de incidentes. Fonte: SANS (2025)

Como se ve, **un tercio dos incidentes tardan mais dunha semana en ser detectados, en torno a un 20% tardan en conterse mais de 8 días trala detección, e mais dunha cuarta parte, son remediados en prazos superiores a un mes**.

Finalmente, as **predicións recollidas por SANS sobre ámbitos máis susceptibles de ser obxectivo dos atacantes segundo os enquisados** (destacando plataformas OT

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

conectadas á nube, sistemas legados, dispositivos de bordo/IoT industrial e instalacións remotas):



Tecnoloxías susceptibles de sufrir mais ataques segundo os enquisados. Fonte: SANS (2025)

Isto reforza a mensaxe central desta sección: a medida que aumenta a conectividade e a dependencia dixital, **o risco OT convértese nun risco económico estrutural**, e a resiliencia pasa a ser un factor de competitividade e continuidade

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

4 Incidentes e ameazas emerxentes

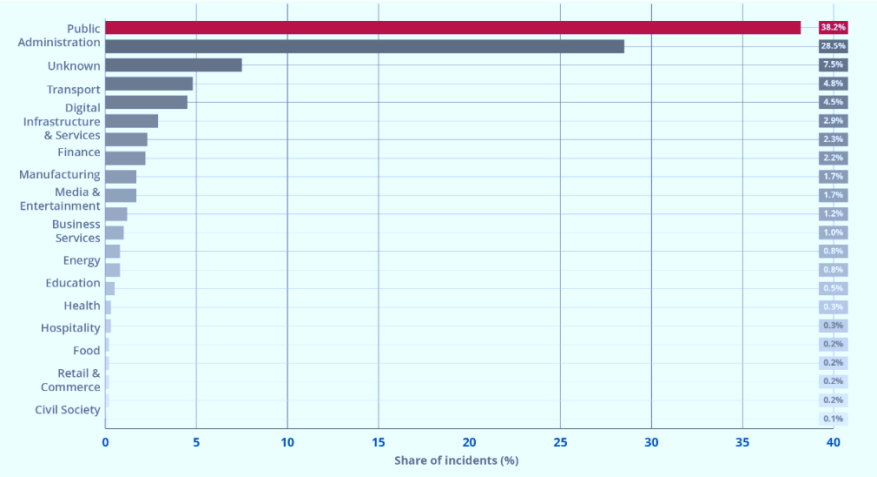
Este apartado céntrase en como o risco tecnolóxico se materializa na práctica, a través de **incidentes reais** e de patróns de ameaza predominantes no ecosistema industrial.

Sobre esa base, a sección introduce as **ameazas emerxentes** que están a redefinir a paisaxe de risco, impulsadas pola **Intelixencia Artificial**.

4.1 Incidentes e sectores afectados

Os **Informes de intelixencia de ameazas OT** do Observatorio de Ciberseguridade Industrial da Xunta de Galicia (AMTEGA) integran unha visión operativa de **incidentes con impacto en OT/ICS** e dos **sectores máis expostos**, combinando fontes europeas, repositorios de incidentes e intelixencia de fabricantes [4]. A súa lectura é particularmente útil para o contexto galego porque permite conectar patróns observados en Europa coa realidade de sectores estratéxicos do tecido produtivo: **industria manufactureira**, **enerxía e utilities**, **auga e augas residuais**, **transporte e loxística** e **agroalimentario**.

A nivel europeo, a análise sectorial recompilada no informe a partir de ENISA cuantifica a dimensión do problema de materialización de riscos: durante o período estudado, ENISA analizou **4.875 incidentes**, dos cales **o 28,5%** non puideron asociarse a un sector. Unha vez excluídos estes casos, obsérvase unha concentración clara en poucos sectores, destacando **administración pública (≈38%)**, **transporte (≈7,5%)**, **infraestruturas e servizos dixitais**, **finanzas (≈4,7%)** e **manufactura (≈2,9%)**, que conxuntamente explican unha parte maioritaria dos incidentes con sector identificado.

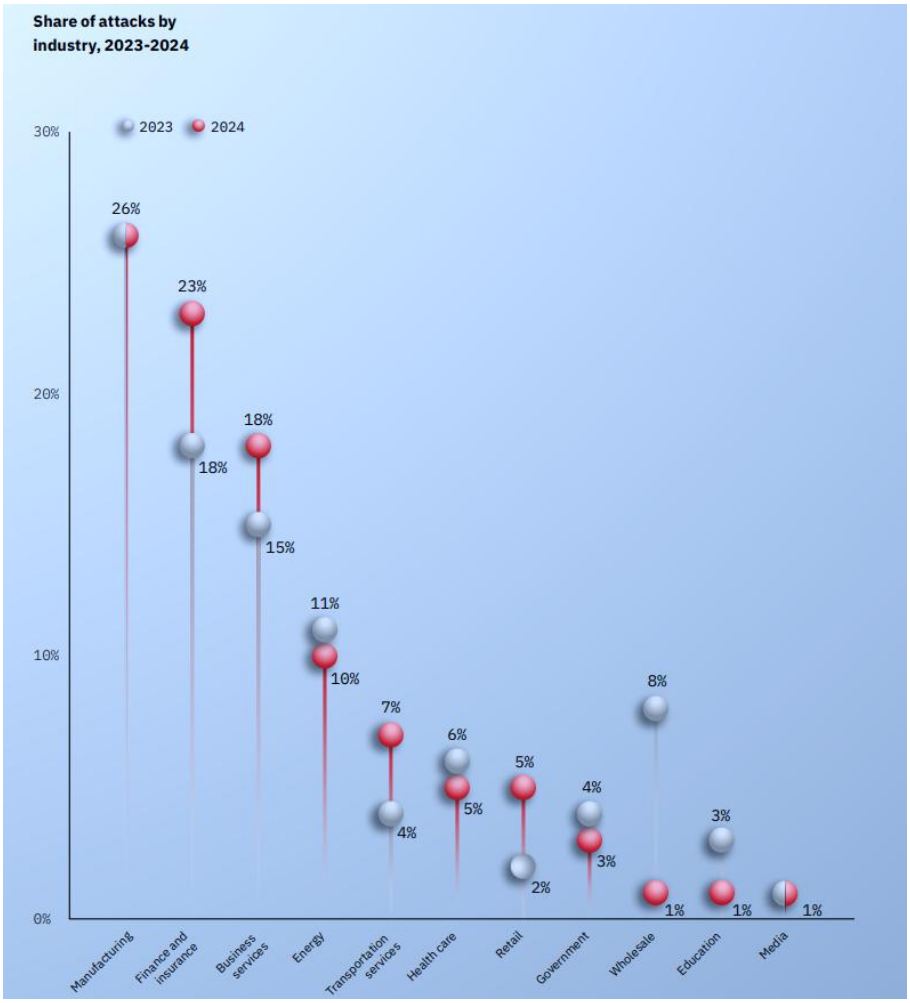


Incidentes rexistrados por sector. Fonte: ENISA (2025)

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

Para a perspectiva OT, este dato é relevante porque varios destes sectores funcionan como **dependencias críticas** da industria (comunicacións, servizos dixitais, loxística), polo que un incidente neles pode traducirse en **efectos en cascada** sobre operacións industriais.

Desde o punto de vista de cibercrime e impacto organizativo, o informe recolle tamén tendencias de intelixencia sectorial: por exemplo, segundo datos de IBM X-Force citados, **manufactura mantense como un dos sectores máis atacados (26%)**, mentres que **finanzas e seguros** concentra tamén unha porcentaxe elevada (**23%**). No eixe de impacto, destacan patróns de **captura de credenciais** e **roubo de datos**, con cifras de referencia do **29%** e **18%**, respectivamente, en incidentes analizados, reforzando unha idea clave para OT/ICS: moitas intrusións non comezan "rompendo" OT, senón **iniciando sesión** con credenciais válidas e movéndose a partir de TI cara a activos críticos.



Ratio de ciberincidentes por sector de actividade 2024 vs 2023. Fonte: IBM X-Force (2025)

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

O propio informe sintetiza exemplos de **incidentes con consecuencias operativas** en Europa durante 2024, cun patrón recorrente: compromiso inicial en **sistemas corporativos** (p.ex. ERP, servizos de identidade, plataformas de xestión), seguido de **illamento preventivo de redes** e **paradas completas de planta** durante días ou semanas. A casuística industrial europea recollida inclúe casos de manufactura con interrupción prolongada e impacto financeiro, e tamén eventos salientables no ámbito español, como un incidente no sector agroalimentario no que se afirmou acceso a sistemas tipo SCADA asociados ao tratamento de augas residuais, con parada e retorno a operación en modo manual.

Como complemento orientado á afectación real de sistemas industriais (non só a incidentes mediáticos), o informe incorpora telemetría de Kaspersky ICS-CERT para Europa (Q2 2025): aproximadamente **un de cada cinco equipos ICS** bloqueou obxectos maliciosos durante o trimestre, cun valor global arredor do **20,5%**. De especial interese para o Sur de Europa, rexión que inclúe España, sinala un **aumento continuado de ameazas procedentes do correo electrónico**, con picos próximos ao **7% de equipos ICS afectados**; isto é coherente co feito xa mencionado de que moitos compromisos en OT son consecuencia de **vectores herdados de TI** (phishing, malware xenérico, medios extraíbles, acceso remoto inseguro e movemento lateral). Ademais, o informe de incidentes de Kaspersky para Q2 2025, baseado en incidentes reportados e analizados, referencia unha mostra de **135 incidentes** no trimestre, permitindo unha lectura sectorial rápida.

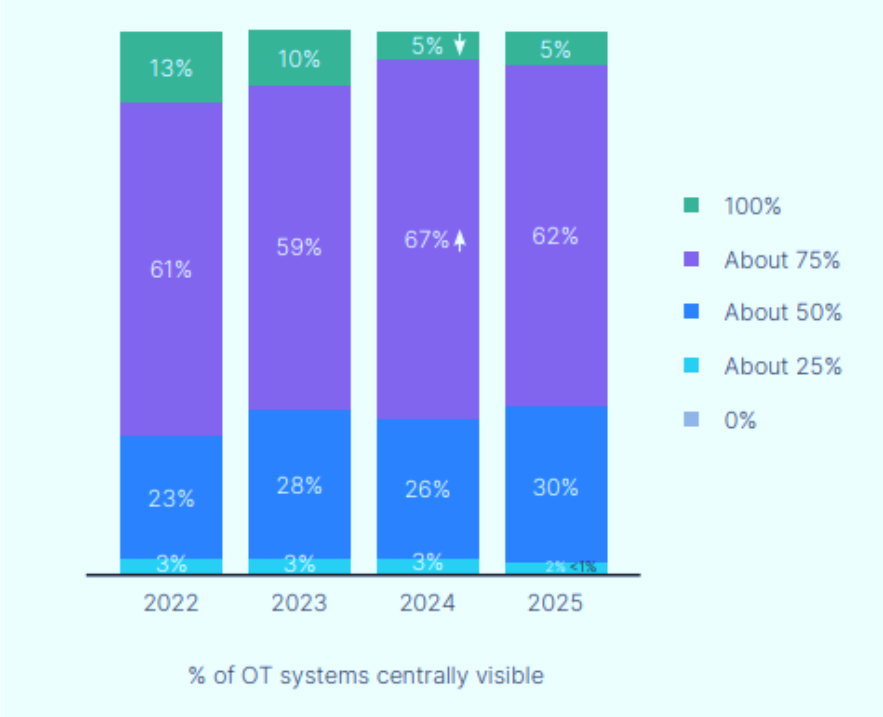
En síntese, esta evidencia sostén unha conclusión práctica para Galicia: os sectores con maior peso económico e de servizo (**manufactura, transporte/loxística, agroalimentario, enerxía e auga**) presentan unha exposición recorrente a incidentes que, aínda comezando en TI habitualmente, rematan xerando **interrupción de operación**, **degradación do servizo** e **impactos en cadea**.

En paralelo, o **2025 State of Operational Technology and Cybersecurity Report** de Fortinet achega unha lectura cuantitativa complementaria, baseada nun panel internacional [17][18]. A mostra foi elaborada mediante enquisas, acadando 558 respostas completas, procedentes de organizacións de **Enerxía/Utilities, Saúde/Farma, Transporte/Loxística, Manufactura, Químico/Petroquímico, Petróleo/Gas/Refino e Auga/Augas residuais**, tipicamente con **máis de 1.000 empregados** (con excepcións en determinados países). Os criterios de inclusión requirían que **OT estivese dentro da responsabilidade funcional**, que existise **responsabilidade de reporte sobre operacións de planta/manufactura**, e que o

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

perfil estivese **implicado en decisións de compra de ciberseguridade**; a listaxe de países incluídos contempla **España**.

Un primeiro achado crítico é a falta de **visibilidade real** das redes OT desde as operacións centrais de ciberseguridade. Como se pode apreciar, só **o 5%** das organizacións declaran **100% de visibilidade** dos seus sistemas OT.

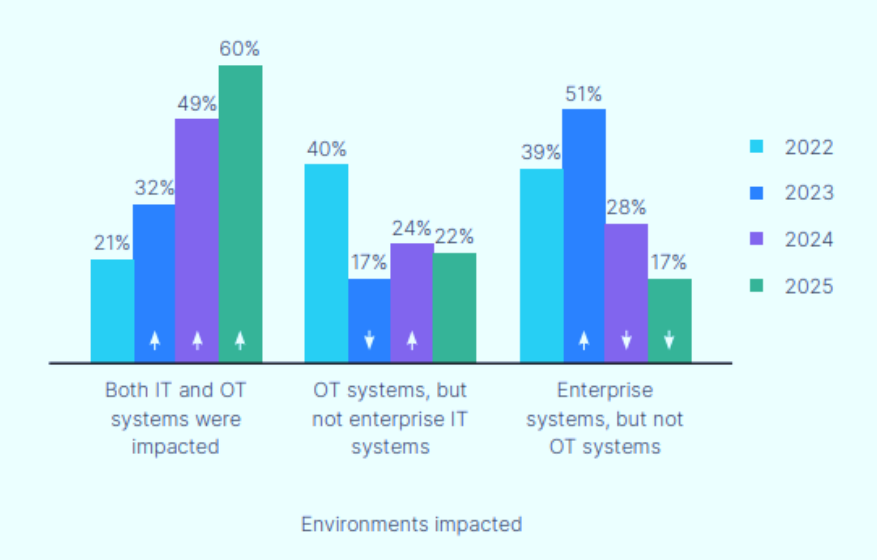


Infraestrutura OT monitorizada a nivel ciberseguridade nas empresas. Fonte: Fortinet (2025)

A maioría sitúase en coberturas parciais, co **62%** indicando arredor de **50%** de visibilidade e **o 30%** arredor de **25%**. Este dato é directamente interpretable como risco: con puntos cegos persistentes, aumenta a probabilidade de **intrusións prolongadas**, **movemento lateral non detectado** e **dificultade para delimitar alcance e impacto** cando se produce un incidente.

A segunda evidencia é que as intrusións xa non se entenden en compartimentos estancos.

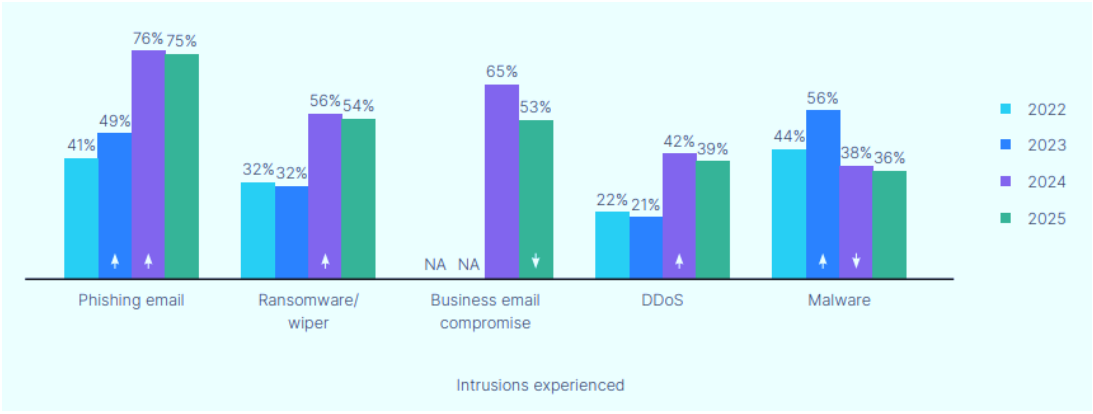
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027



Contornos impactados por intrusións o ano anterior. Fonte: Fortinet (2025)

O informe reflicte que, entre as organizacións que reportaron intrusións, en 2025 **o 60%** declarou impacto en **ambos os dominios TI e OT**. En paralelo, **o 22%** indicou afectación **só en OT**, e **o 17%** afectación **só en TI**. O propio informe matiza que parte do impacto en OT pode producirse porque elementos de TI ou conexións asociadas quedan fóra de servizo, sen que exista necesariamente infección directa dentro da rede OT. Para a análise de risco, a implicación é clara: a continuidade industrial depende de xeito incremental de **servizos dixitais compartidos**, e iso amplifica o radio de impacto.

No que atinxe a **tipos de intrusión**, o estudio mostra que as tácticas predominantes seguen sendo, en gran medida, "de TI", pero con efectos industriais: **compromiso de correo empresarial (53%)**, **malware (36%)**, **phishing por correo (75%)**, **ransomware/wiper (54%)** e **DDoS (denegación de servizo distribuida) (39%)**.

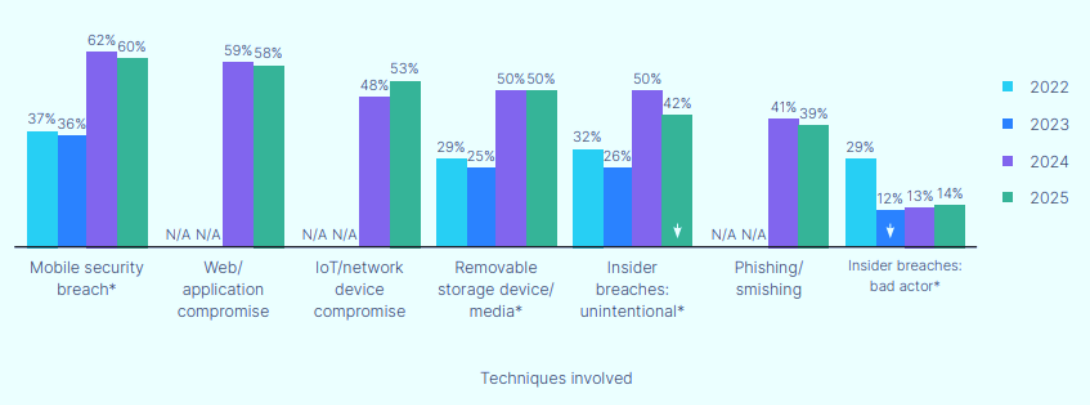


Evolución temporal dos tipos de intrusión en OT. Fonte: Fortinet (2025)

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

A lectura OT/ICS é que estes vectores poden traducirse rapidamente en **indispoñibilidade operativa** por cifrado, por perda de servizos de identidade e xestión, ou por medidas de contención que obriguen a operar de forma degradada.

Profundando neste eido, o documento caracteriza **técnicas** asociadas ás intrusións e apunta unha tendencia que incrementa a superficie de ataque industrial: **compromiso web/aplicación (58%)**, **compromiso de dispositivos IoT/de rede (14%)**, **brechas en mobilidade (60%)**, **uso de medios extraíbles (50%)** e **incidentes internos** tanto non intencionados (**42%**) como por actor malicioso (**14%**). Isto reforza que a exposición non está só en PLC/SCADA: inclúe con frecuencia **servizos web asociados**, **dispositivos de rede e acceso remoto**, **equipos móbiles en operación e mantemento** e prácticas que abren portas involuntarias ao adversario.



Evolución temporal das técnicas de ataque en OT. Fonte: Fortinet (2025)

En conxunto, a combinación das dúas fontes sostén unha conclusión coherente para Galicia: os sectores con maior criticidade económica e social son tamén os que amosan **exposición recorrente a incidentes**, e a materialización do risco adoita verse condicionada por tres factores: **converxencia TI/OT**, **visibilidade insuficiente** e **intrusións baseadas en identidade e canles habituais de TI**, que acaban tendo consecuencias operativas.

4.2 Ameazas emerxentes baseadas en IA

A aceleración recente da **intelixencia artificial (IA)** está a modificar a natureza do risco tecnolóxico: **non crea necesariamente ameazas completamente novas**, senón que **reduce barreiras de entrada** e **multiplica a velocidade, a escala e o realismo** de técnicas xa coñecidas.

O informe **Cybersecurity Forecast 2026** de Google Cloud/Mandiant xa mencionado anteriormente [6], identifica tres liñas de fondo para o curto e medio prazo: **uso da IA**

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

por parte de atacantes e defensores, **ciberdelincuencia como principal forza disruptiva**, e actividade de **actores estatais**. Aínda que o capítulo de ciberdelincuencia é amplo, a lectura máis pertinente para OT/ICS é que **o ransomware e a extorsión mediante roubo de datos seguen sendo o patrón de maior impacto económico e operativo**, con efectos en cadea que superan á vítima inicial e afectan provedores, clientes e servizos críticos.

Conclusións principais do Cybersecurity Forecast 2026. Fonte: Google/Mandiant (2025)

No que atinxe a **OT/ICS**, o mesmo informe subliña que en 2026 a ameaza disruptiva principal para sistemas industriais continuará sendo a **ciberdelincuencia**, non tanto por intrusións "puramente industriais", senón polo uso de campañas deseñadas para **danar software empresarial crítico** (por exemplo, sistemas de xestión corporativa) que sustentan a **cadea de datos imprescindible para operar OT**.

Sobre esa base, o elemento verdadeiramente diferencial é a IA como **amplificador transversal**. Pasamos a continuación a describir de xeito mais detallado este fenómeno.

- O informe prevé que o uso de IA por parte de grupos de ameaza pase de ser unha excepción a ser **a norma**, con aplicacións directas en **enxeñaría social, operacións de información e desenvolvemento de software malicioso**. Na práctica, isto tradúcese en campañas máis rápidas, máis personalizadas e máis persistentes, con capacidade de adaptar mensaxes, perfís e fluxos de ataque a cada organización e mesmo a cada persoa.
- Mencionábamos na sección 3 que unha das ameazas emerxentes máis críticas é a **inxeción de instrucións** (prompt injection, ataque que manipula un sistema

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

de IA para que **ignore as súas limitacións de seguridade** e execute ou produza saídas guiadas polo atacante). O risco aumenta na medida en que as organizacións integran modelos de IA en procesos cotiáns, con acceso a coñecemento interno, documentación ou repositorios de tickets. En clave industrial, isto pode afectar a asistentes usados para **diagnóstico de incidencias**, análise de rexistros, soporte a mantemento, xestión documental ou automatización de procedementos: se a entrada de datos incorpora contido non fiable (por exemplo, textos pegados de correos, anexos, repositorios ou incidencias), un atacante pode tentar inducir ao sistema a **exfiltrar información técnica** ou a **propoñer accións incorrectas** con impacto operativo.

- Outra área de risco emerxente é a **enxeñaría social habilitada por IA**, especialmente mediante **suplantación de voz** en chamadas (vishing) e outras formas de comunicación hiperrealistas. O informe sinala a evolución cara a clonación de voz para impersonar directivos ou persoal de TI, o que encaixa particularmente ben en escenarios industriais onde existen procesos de **acceso remoto de mantemento**, operacións con provedores e autorizacións urxentes para restauración de servizos. O efecto práctico é que a cadea de validación humana se converte no elo feble: se unha persoa con privilexios é enganada, a intrusión pode progresar ata afectar activos críticos sen explotar vulnerabilidades técnicas sofisticadas.

- A evolución cara a **axentes de IA** introduce un cambio de paradigma adicional. Cando a IA deixa de ser un asistente pasivo e pasa a executar fluxos de traballo (por exemplo, priorización de alertas, xeración de casos, recomendación de accións, automatización de respostas), xorden dous problemas:

    1. A necesidade de tratar os axentes como **actores dixitais con identidade**, permisos e trazabilidade; e

    2. O risco de que a organización delegue accións de forma implícita, xerando **privilexios acumulativos** e decisións automatizadas sen control suficiente. En OT/ICS, este escenario é particularmente delicado en actividades como **xestión de cambios**, soporte á operación e coordinación de resposta a incidentes, onde unha acción mal validada pode ter custos ciberfísicos.

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

- O fenómeno anterior conecta co risco xa observado de **IA na sombra**: o informe describe a evolución cara a **axentes na sombra**, isto é, persoas que despregan axentes autónomos para tarefas de traballo sen aprobación corporativa, creando **canles invisibles de datos**, exposición de información sensible e incumprimentos normativos. Para o tecido industrial galego, isto resulta crítico porque unha parte da información máis valiosa non está en bases de datos visibles, senón en documentos, procedementos, diagramas, rexistros de mantemento e evidencias de operación que poden acabar "aspiradas" por ferramentas non gobernadas.

Esta lectura enlaza de forma natural coa avaliación do **National Cyber Security Centre (NCSC)** do Reino Unido, autoridade técnica en ciberseguridade e parte de GCHQ (a ciberaxencia de seguridade e intelixencia británica), que analiza o impacto da IA sobre a ameaza para a seguridade da información ata 2027 [19][20]. Comentamos a continuación as principais conclusións.

- Indican que a **intelixencia artificial incrementará case con total certeza a eficacia, velocidade e escala das operacións de intrusión cibernética**, o que derivará nun **aumento da frecuencia e intensidade das ameazas** nos vindeiros anos. Este impacto non se producirá tanto pola aparición de vectores completamente novos, senón pola **evolución e reforzo das técnicas existentes (TTPs)**.
- Os actores de ameaza **xa están a empregar IA** para mellorar tarefas clave como o **recoñecemento de vítimas**, a **investigación de vulnerabilidades**, o **desenvolvemento de exploits**, a **enxeñaría social**, a **xeración básica de malware** e o **procesamento de datos exfiltrados**. Ata 2027, isto **incrementará significativamente o volume e o impacto das intrusións**, especialmente contra organizacións con niveis de seguridade desiguais.
- No curto prazo, só **actores estatais altamente capacitados** contan cos recursos, datos de adestramento e coñecemento necesarios para explotar todo o potencial da IA en operacións avanzadas. Con todo, a maioría dos grupos criminais e non estatais **optarán por reutilizar modelos comerciais e open source**, o que **reduce a barreira de entrada** e eleva as capacidades medias do ecosistema de ameaza. A proliferación de modelos abertos facilita a creación de ferramentas especializadas tanto para defensa como para ataque.

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

- Un dos desenvolvementos máis críticos identificados polo NCSC é o avance da **investigación de vulnerabilidades e desenvolvemento de exploits asistidos por IA**. A IA permitirá **identificar e explotar fallos de código e configuración con maior rapidez**, acelerando aínda máis a carreira entre divulgación de vulnerabilidades e explotación activa. O tempo entre publicación dun fallo e o seu uso en ataques **xa se reduciu a días**, e a IA **reducirao aínda máis**. Este fenómeno **incrementa de forma notable o risco para infraestruturas críticas e as súas cadeas de subministración**, especialmente para **sistemas OT con niveis de seguridade máis baixos, tecnoloxía legada e xanelas de parcheo limitadas**. En ausencia de melloras proporcionais en mitigacións, existe unha **posibilidade realista de que sistemas críticos sexan máis vulnerables a actores avanzados ata 2027**.

- En paralelo, a IA tamén **axudará aos defensores** (operadores e desenvolvedores) a mellorar a seguridade. Porén, o NCSC alerta dunha **brecha dixital crecente**: mentres algunhas organizacións poderán manter o ritmo coa defensa asistida por IA, **unha parte significativa quedará máis exposta**, incrementando a desigualdade estrutural do risco.

- O NCSC tamén prevé que os actores máis capacitados empregarán **automatización habilitada por IA para evadir detección e escalar operacións**. Aínda que **non se espera unha automatización completa de ataques avanzados de extremo a extremo** antes de 2027, si se consolidará un modelo de **"human–machine teaming"**, no que a IA automatiza partes da cadea de ataque (descubrimento de vulnerabilidades, adaptación de malware, rotación de infraestrutura), dificultando a detección e resposta sen capacidades defensivas equivalentes.

- A **proliferación de ferramentas con IA** ampliará o acceso á capacidade de intrusión a **un maior número de actores estatais e non estatais**. O sector criminal incorporará IA aos seus produtos, ofrecendo **servizos de intrusión "as a service"**, elevando o nivel de actores pouco sofisticados (novatos, mercenarios dixitais, hacktivistas) para operacións oportunistas e disruptivas.

- Outro risco salientado é o **aumento da superficie de ataque** debido á integración crecente de sistemas de IA na base tecnolóxica, especialmente en **infraestruturas críticas**. Os sistemas de IA inclúen datos, modelos, procesos de adestramento e avaliación, e tecnoloxía conectada a sistemas corporativos,

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

datos e, progresivamente, **operación OT**. Os atacantes **explotarán esta nova capa** mediante técnicas xa observadas: **prompt injection directa e indirecta**, **vulnerabilidades de software**, e **ataques á cadea de subministración**.

- O informe tamén alerta de que unha **seguridade insuficiente na IA** facilitará o seu uso malicioso por actores estatais e criminais. A presión competitiva por lanzar modelos e aplicacións ao mercado pode levar a **priorizar velocidade fronte a seguridade**, incrementando o risco de sistemas comprometidos. Isto vese agravado por **malas prácticas de xestión de datos e configuración**, como:
  - cifrado débil nas transmisións,
  - xestión deficiente de identidades e credenciais privilexiadas,
  - recollida excesiva de datos de usuario que facilita ataques dirixidos.

Finalmente, resulta útil elevar o enfoque desde a táctica á visión de risco de alto nivel que propón o **International AI Safety Report 2025**, unha revisión internacional sobre capacidades e riscos da IA de propósito xeral, liderada por Yoshua Bengio (informático canadense Premio Príncipe de Asturias e Premio Turing, considerado un dos "Padriños da IA") [21]. A organización que elabora o reporte está apoiada por múltiples países e entidades, e mais dun centenar de expertos independentes [22][23].

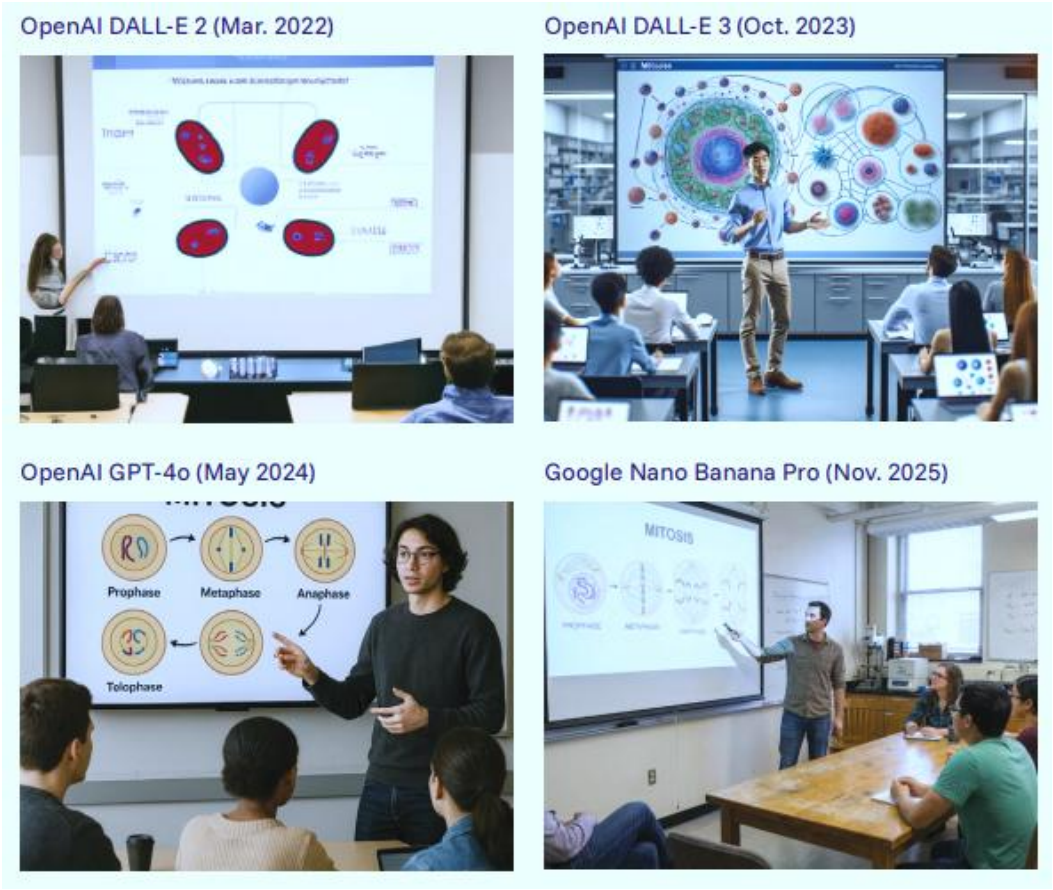
O valor deste informe para un Observatorio de ciberseguridade industrial é que ordea os riscos nunha taxonomía sinxela e accionable, especialmente útil para conectar **ameazas emerxentes baseadas en IA** con **impactos potenciais en operacións industriais (OT/ICS)**.

A análise organiza os riscos en **tres grupos —riscos por uso malicioso**, **riscos por fallos de funcionamento** e **riscos sistémicos—**. A continuación recóllense e descríbense, incorporando a lectura OT/ICS cando procede.

4.2.1 Riscos por uso malicioso

- **Contido xerado por IA e actividade criminal**: a xeración masiva de texto, audio, vídeo e imaxes realistas reduce o custo de campañas de fraude e suplantación. En OT/ICS isto tradúcese en **enxeñaría social máis convincente** (falsos procedementos, peticións urxentes de acceso remoto, cambios en configuración) que facilita acceso inicial e compromisos de credenciais. Unha mostra do vertixinoso avance neste eido a continuación:

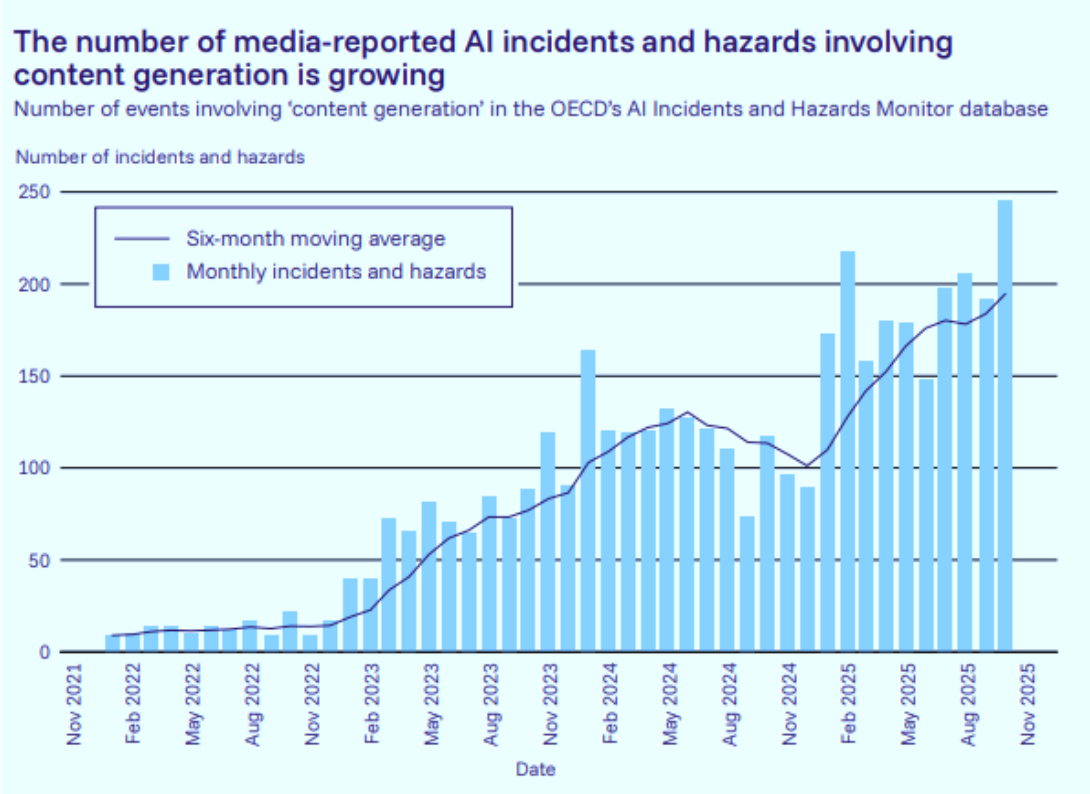
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027



Evolución da calidade das imaxes xeradas por IA. Fonte: International AI Safety Report (2026)

- **Influencia e manipulación**: a IA facilita campañas de persuasión e desinformación máis segmentadas, persistentes e difíciles de atribuír. En sectores industriais e servizos esenciais, isto pode agravar crises ao degradar a coordinación, xerar pánico ou **distorsionar información operativa** durante incidentes (por exemplo, falsas instrucións, rumores sobre indispoñibilidades, presión reputacional).

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



Evolución de incidentes xerados por IA na ODCE. Fonte: International AI Safety Report (2026)

- **Ciberataques**: a IA pode acelerar tarefas ofensivas (recoñecemento, preparación de campañas, explotación de fallos, análise de datos roubados) e aumentar a eficacia de operacións existentes. Para OT/ICS, o risco relevante é o **incremento da cadencia e da precisión** na progresión TI→OT, e a posibilidade de automatizar partes do ataque contra infraestruturas de soporte (identidade, correo, acceso remoto) que condicionan a continuidade industrial.

- **Riscos biolóxicos e químicos**: aínda que exceden o ámbito estrito da ciberseguridade, son relevantes para a seguridade industrial porque a IA pode apoiar deseño, síntese ou manipulación de substancias perigosas (impactando na área de seguridade física ou safety). A lectura OT/ICS é indirecta pero importante: instalacións químicas, farmacéuticas e de tratamento de auga poden verse afectadas por combinacións de **ameaza física + intrusión dixital**, ou por abuso de información técnica e procedementos.

4.2.2 Riscos por fallos de funcionamento

- **Desafíos de fiabilidade**: a IA pode producir respostas incorrectas, incompletas ou inconsistentes, especialmente fóra do seu dominio de adestramento. En contexto OT/ICS, onde a seguridade funcional e a continuidade son críticas, unha recomendación errónea (por exemplo, un diagnóstico de mantemento, unha

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

priorización de alarmas ou unha proposta de cambio) pode inducir **decisións operativas perigosas**.

- **Perda de control**: refírese á dificultade de asegurar que sistemas de IA —en particular cando se integran como axentes con capacidade de acción— permanezan aliñados con límites e intencións humanas. En OT/ICS isto conecta co risco de **automatización non validada**: axentes que executan tarefas (cambios, clasificación de incidencias, resposta automatizada) poden amplificar un erro ou introducir efectos non previstos se non existen autorizacións, trazabilidade e validación humana.

4.2.3 Riscos sistémicos

- **Impactos no mercado laboral**: a adopción de IA pode reconfigurar perfís e procesos, xerando transicións rápidas e tensión en competencias. Para OT/ICS, isto pode materializarse como **desequilibrios de capacidades**: aumento de demanda de perfís híbridos (operación + seguridade + IA) e risco de que a falta de persoas cualificadas degrade a capacidade de supervisión, resposta e gobernanza.
- **Riscos para a autonomía humana**: inclúe a dependencia excesiva de sistemas de IA para tomar decisións, a erosión do criterio experto e a influencia sobre eleccións e condutas. En contornos industriais, onde a autoridade operativa e os procedementos son determinantes, existe risco de **delegación implícita** e de perda de capacidade de decisión en crise, especialmente se as recomendacións dunha IA se perciben como "obxectivas" sen validación.

4.2.4 Cadro resumo de ameazas

Pechamos a sección cun **cadro resumo específico de ameazas emerxentes baseadas no uso de IA en ciberseguridade industrial**, consolidando os *puntos claves* de Google Cloud/Mandiant, NCSC e o International AI Safety Report 2025, cun enfoque específico en contornos OT/ICS. Algunha delas, solápase coa táboa análoga da sección 3.1.6.

Risco	Descrición	Impacto potencial en OT/ICS
Enxeñaría social asistida por IA	Uso de IA para crear mensaxes, chamadas ou contidos hiperrealistas (texto, voz, vídeo) orientados a enganar persoas con acceso privilexiado.	Acceso inicial non autorizado, compromiso de credenciais, habilitación de acceso remoto e progresión TI→OT.
Ransomware e extorsión amplificados por IA	Mellora da selección de vítimas, personalización de campañas e explotación de dependencias dixitais mediante IA.	Interrupción operativa, paradas de planta, impacto económico en cadea e afectación a provedores e clientes.
Contido xerado por IA e actividade criminal	Xeración masiva de contido falso para fraude, suplantación e engano sistemático.	Incremento de ataques oportunistas contra industria; erosión dos controis humanos en procesos críticos.
Influencia e manipulación	Campañas de desinformación máis segmentadas, persistentes e difíciles de atribuír grazas á IA.	Distorsión da información en crise, degradación da coordinación e presión reputacional en servizos esenciais.
Ciberataques asistidos por IA	IA como acelerador de recoñecemento, explotación, malware e análise de datos roubados.	Aumento da cadencia e precisión das intrusións, maior probabilidade de impacto operativo en OT.
Investigación de vulnerabilidades asistida por IA	Uso de IA para descubrir e explotar fallos de código e configuración con maior rapidez.	Redución drástica do tempo entre divulgación e explotación; alto risco para OT legado e con xanelas de parcheo limitadas.
Explotación acelerada de vulnerabilidades coñecidas	Automatización da identificación e explotación de fallos xa publicados.	Incremento de ataques contra sistemas non actualizados; ameaza directa a infraestruturas críticas.
Prompt injection e manipulación de sistemas de IA	Inxección de instrucións maliciosas para forzar saídas incorrectas ou exfiltración de información.	Exposición de documentación técnica e procedementos; recomendacións erróneas con impacto operativo.

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

Axentes de IA con privilexios excesivos	Axentes autónomos con capacidade de acción sen identidade clara nin control de permisos.	Automatización de cambios non validados; riscos ciberfísicos en xestión de cambios e resposta a incidentes.
IA na sombra (Shadow AI)	Uso non gobernado de ferramentas ou axentes de IA fóra do control organizativo.	Canles invisibles de saída de datos; incumprimentos normativos e perda de control sobre información OT crítica.
Automatización ofensiva habilitada por IA	Automatización parcial da cadea de ataque (recoñecemento, explotación, evasión).	Intrusións máis persistentes e difíciles de detectar; sobrecarga dos equipos de defensa OT.
Proliferación de ferramentas de ataque con IA	Comercialización de capacidades de intrusión "as a service" baseadas en IA.	Elevación do nivel medio de actores pouco sofisticados; máis ataques oportunistas contra industria.
Aumento da superficie de ataque por integración de IA	Conexión de sistemas de IA a datos corporativos e, progresivamente, á operación OT.	Novos vectores de entrada (cadea de subministración, IA comprometida) con acceso indirecto a OT.
Fallos de fiabilidade da IA	Respostas incorrectas, incompletas ou inconsistentes fóra do dominio de adestramento.	Decisións operativas perigosas, mala priorización de alarmas e impacto en seguridade funcional.
Perda de control sobre sistemas de IA	Dificultade de garantir límites, intencións e comportamento esperado dos sistemas de IA.	Automatización non validada; amplificación de erros con consecuencias operativas e físicas.
Riscos biolóxicos e químicos asistidos por IA	Apoio da IA ao deseño ou manipulación de substancias perigosas.	Relevancia indirecta en sectores químico, farmacéutico e auga; ameaza combinada física + dixital.
Impactos no mercado laboral industrial	Reconfiguración rápida de perfís e competencias pola adopción de IA.	Déficit de perfís híbridos OT+seguridade+IA; perda de capacidade de supervisión e resposta.

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

Riscos para a autonomía humana	Dependencia excesiva da IA e erosión do criterio experto.	Delegación implícita en situacións críticas e perda de capacidade de decisión en crise.
Brecha dixital na defensa asistida por IA	Desigualdade entre organizacións que poden adoptar defensa con IA e as que non.	Aumento estrutural da exposición en industria mediana e infraestruturas con menor madurez.
Mala seguridade por deseño en sistemas de IA	Priorizar velocidade de lanzamento fronte á seguridade; malas prácticas de datos e identidade.	Compromiso de sistemas de IA conectados a OT; escalado de intrusións e filtración de datos críticos.

Cadro de riscos baseados no uso da IA do Informe. Fonte: elaboración propia (2026)

Podemos concluír que a IA non debe tratarse só como tecnoloxía, senón como un **factor transversal de risco** que afecta persoas, procesos e tecnoloxía. Por iso, as recomendacións de securización deben combinar **gobernanza** (uso permitido, xestión de datos e identidades, control de provedores), **controles técnicos** (tolerancias, rexistros, illamento, permisos mínimos) e **validación operativa**, tal e como se desenvolverá no apartado correspondente de recomendacións.

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

5 Goberno da ciberseguridade e resiliencia

Sirva como introdución deste apartado, o artigo publicado por **Industrial Cyber** que aborda unha cuestión clave e recorrente na ciberseguridade industrial: a existencia dunha **debilidade estrutural na forma en que as organizacións industriais gobernan, xestionan e comunican os incidentes de seguridade en contornos OT/ICS**, nun contexto no que as ameazas evolucionan máis rápido ca os modelos organizativos tradicionais [24].

Neste sentido, o artigo serve como punto de partida para reflexionar sobre a necesidade de evolucionar cara a modelos máis integrados e resilientes, sobre os que, posteriormente, **se proporán unha serie de recomendacións exemplificativas extraídas da literatura especializada**, orientadas a reforzar a capacidade real de xestión do risco en ciberseguridade industrial.

O escrito sinala que a **notificación e xestión formal de incidentes de ciberseguridade en contornos OT/ICS continúa sendo unha debilidade estrutural**, especialmente en organizacións industriais que operan con **modelos de gobernanza herdados**, deseñados para entornos TI máis estáticos e previsibles. Mentres as ameazas evolucionan en velocidade, escala e impacto, **os mecanismos de reporte, escalado e aprendizaxe organizativa non avanzan ao mesmo ritmo**.

Un dos puntos centrais é que **moitos incidentes OT non se reportan ou se reportan de forma incompleta**, ben por temor a impacto reputacional, por falta de obrigas claras, ou porque **non se recoñecen como incidentes de ciberseguridade**, senón como fallos operativos ou técnicos. Isto provoca unha **infrarrepresentación do risco real**, dificulta a análise agregada e limita a capacidade do sector para aprender de eventos previos, como xa adiantabamos no informe de Dragos.

O artigo destaca tamén que a **converxencia TI/OT** incrementou a frecuencia de incidentes con impacto operativo, pero **a gobernanza segue fragmentada**: TI adoita xestionar a seguridade da información e OT a continuidade do proceso, sen mecanismos eficaces de coordinación cando un incidente afecta a ambos dominios. Como consecuencia, **as decisións de reporte, resposta e comunicación tómase tarde ou de forma desaliñada**.

Outro aspecto relevante é a **dependencia de tecnoloxías legadas e cadeas de subministración complexas**, que dificulta a atribución, a avaliación de impacto e a

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

comunicación externa. En moitos casos, a falta de visibilidade sobre activos OT e sobre a progresión dun ataque fai que **a organización non teña certeza suficiente para activar procedementos formais de notificación**.

Ponse así mesmo o foco no **desfase entre as novas obrigas regulatorias emerxentes** (especialmente en infraestruturas críticas) e a realidade operativa das organizacións industriais. A ausencia de procesos maduros de reporte e de métricas compartidas supón un risco adicional: **o incumprimento non é só normativo, senón tamén estratéxico**, ao impedir unha xestión do risco baseada en evidencias.

Sosteñen os autores que **mellorar a notificación de incidentes OT non é un exercicio administrativo**, senón un **factor clave de resiliencia**. Sen datos fiables, oportunos e comparables, as organizacións industriais seguirán reaccionando de forma illada, mentres as ameazas —cada vez máis automatizadas e asistidas por IA— **superan os modelos de gobernanza tradicionais**.

A partir desta análise, recóllese unha conclusión de fondo: **a xestión eficaz dos riscos en entornos OT non pode basearse exclusivamente en controis técnicos illados**, senón que require **construír unha organización cunha gobernanza clara, unha estrutura definida e funcións de seguridade adaptadas á criticidade da operación**. Profundaremos agora nestes dous eidos, baseándonos en elaboración propia e as fontes da literatura de goberno e seguridade da información propostas [25][26][27][28].

5.1 Estrutura organizativa

A **gobernanza** dun **Programa de Seguridade da Información** constitúen un **hixiénico organizativo imprescindible** para xestionar de forma consistente os riscos aos que están sometidas as organizacións industriais galegas, **sexan estes tecnolóxicos, operativos, regulatorios ou reputacionais**.

Resulta necesario dispoñer dunha **estrutura clara de gobernanza**, cunha **asignación explícita de responsabilidades**, **funcións de seguridade ben definidas** e **mecanismos de coordinación e supervisión ao máximo nivel**, que permitan identificar, avaliar, priorizar e tratar os riscos de forma continuada e aliñada cos obxectivos de negocio. A aproximación proposta —baseada na implicación da alta dirección, na independencia das funcións de control, na separación e coordinación entre IT/OT e Seguridade, e na implantación dun conxunto coherente de capacidades ao longo de todo o ciclo de vida do risco— **non o elimina, pero reduce de maneira estrutural**

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

a incerteza e a exposición, converténdose nun requisito previo para calquera estratexia eficaz de resiliencia industrial.

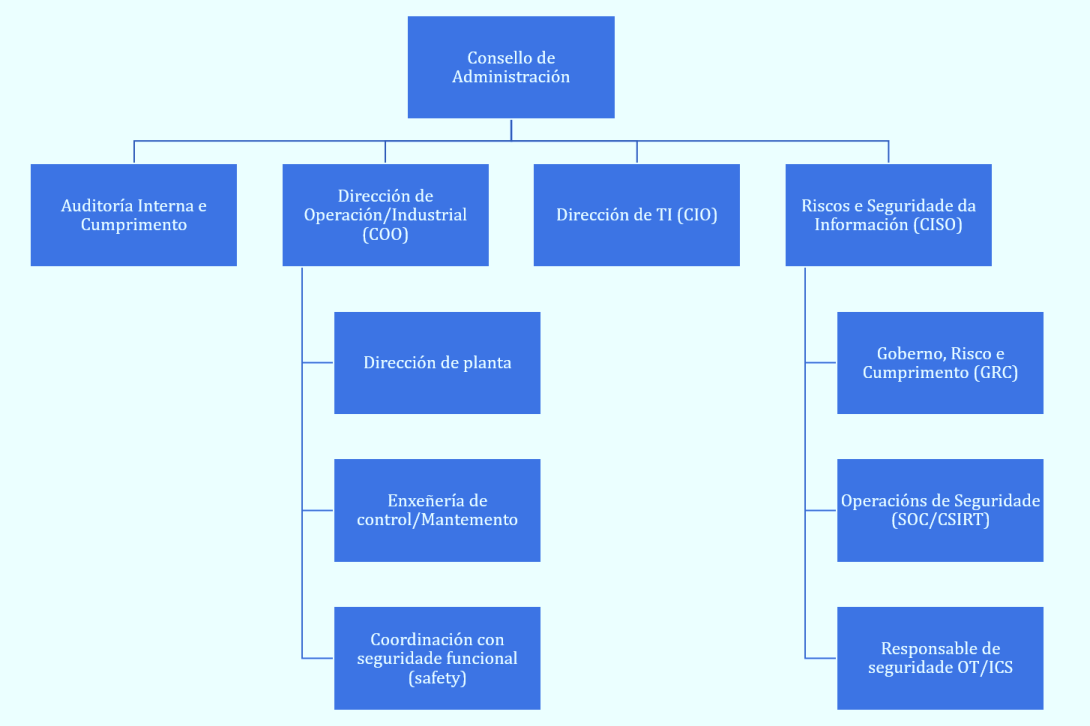
Tendo en mente este marco, **propóñense unha serie de recomendacións exemplificativas extraídas da literatura especializada**, co obxectivo de ilustrar como adaptar estes principios a diferentes realidades organizativas do ámbito industrial galego.

5.1.1 Estrutura global

Cómpre deixar claro, en primeiro lugar, que **non existe unha forma de organización canónica** que sexa óptima en todos os escenarios e para calquera entidade, nin tampouco isto implica que non existan outras alternativas que poidan funcionar adecuadamente. Con todo, si se observa que existen **determinadas prácticas** que, en termos xerais, adoitan ofrecer bos resultados.

En todo caso, para unha estrutura xerárquica determinada, debe existir un **goberno axeitado**, unha **asunción clara de responsabilidades** e unha **comunicación efectiva entre áreas**, de maneira que se asegure que cada función se desempeña con éxito tanto a nivel interno de cada equipo como no conxunto da organización.

Vexamos, a continuación, unha posible proposta de organización.



Organigrama proposto para o goberno da seguridade IT/OT. Fonte: elaboración propia (2026)

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

5.1.2 Consello de Administración / Comité executivo

Na cúspide sitúase o **Consello de Administración (ou Comité executivo)**, responsable último do **goberno, supervisión e rendición de contas** sobre a operación e sobre o **Programa de seguridade**. A súa función non se limita á aprobación orzamentaria: implica **definir a dirección estratéxica**, establecer o **apetito de risco**, aprobar políticas e criterios de priorización, e asegurar que existen capacidades reais para **previr, detectar, responder e recuperarse** de incidentes.

Nunha organización con OT, esta supervisión debe cubrir explicitamente:

- **Protección de activos críticos**, incluíndo activos industriais e infraestruturas de soporte.
- **Continuidade do negocio e resiliencia operativa**, asumindo que un incidente pode derivar en parada, operación degradada ou impacto en servizos esenciais.
- **Cumprimento e evidencia de control**, garantindo trazabilidade das decisións e dos cambios que afectan á operación.

5.1.3 Auditoría interna e cumprimento

A área de **Auditoría interna e cumprimento** debe depender exclusivamente do Consello/Comité e manter **independencia xerárquica absoluta**, co mandato de avaliar e mellorar a eficacia do sistema de control interno. En entornos con componente OT/ICS, isto require capacidade para auditar non só TI, senón tamén operación: **xestión de accesos remotos industriais**, **xestión de cambios en sistemas de control**, **segmentación e arquitectura de rede OT**, **inventarios de activos**, **rexistros e trazas**, ou **gobernanza de provedores industriais**.

5.1.4 Operacións industriais (OT)

A **Dirección de Operacións/Industrial (COO)**, xunto coas **Direccións de Planta**, constitúe o **eixe central da gobernanza OT**, ao asumir a responsabilidade directa sobre a **continuidade operativa**, a **seguridade do proceso industrial** e a execución diaria das operacións. Este ámbito complétase coa **Enxeñaría de control e Mantemento**, como función técnica clave responsable do **deseño, configuración, operación e mantemento** dos sistemas de automatización e control industrial ao longo de todo o seu ciclo de vida.

De maneira complementaria, a **Seguridade funcional (safety)** forma parte esencial desta gobernanza, ao ser a función encargada de garantir a protección de persoas,

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

instalacións e procesos fronte a riscos ciberfísicos. A súa integración coas operacións industriais é imprescindible para asegurar que as decisións técnicas e organizativas non comprometan os niveis de seguridade esixidos polo proceso nin introduzan riscos adicionais durante cambios, incidencias ou situacións de operación degradada.

Para que a xestión do risco en contornos **OT/ICS** sexa **realista, efectiva e executable**, resulta imprescindible que no ámbito de Operacións estean claramente definidos os seguintes elementos:

- A **propiedade de activos e sistemas industriais** (asset owners / system owners), asignada a responsables de **Operacións** ou de **Enxeñaría de control/Mantemento** segundo corresponda, para dominios como **SCADA, PLC, historiadores, redes industriais, estacións de enxeñaría, HMI, sistemas instrumentados de seguridade** e plataformas auxiliares, garantindo responsables identificables para a toma de decisións e a aceptación do risco.
- Un **proceso formal de xestión de cambios**, liderado desde **Operacións** e **Enxeñaría de control/Mantemento**, e **coordinado coa función de ciberseguridade e coa seguridade funcional (safety)**, que equilibre de forma explícita **seguridade, dispoñibilidade e seguridade do proceso**. Este proceso debe incluír avaliación previa de risco, probas técnicas, definición de ventás de intervención, validación en produción e rexistro documental.
- Un **mecanismo claro de toma de decisións ante compromisos ou equilibrios entre seguridade, dispoñibilidade e seguridade funcional**, que permita escalar adecuadamente aquelas situacións nas que o impacto potencial supere o ámbito da planta, involucrando cando sexa necesario á **Dirección de Operacións/Industrial** e ao **nivel executivo**.

Esta estrutura garante que a seguridade en OT non se xestione de forma allea á operación, senón **plenamente integrada nos procesos industriais**, coa participación activa de **Operacións, Enxeñaría de control/Mantemento e Seguridade funcional**, e coa coordinación necesaria co resto das funcións corporativas implicadas.

5.1.5 TI corporativa

A **TI corporativa** (CIO ou función equivalente) mantén as responsabilidades de deseño e operación de sistemas corporativos, infraestrutura local e en nube, soporte e xestión de provedores tecnolóxicos. En organizacións industriais, TI é tamén unha dependencia crítica da operación: **identidade**, **correo**, **directorio**, **redes**, **acceso remoto** e

plataformas corporativas condicionan a continuidade industrial e poden actuar como vía de progresión cara a OT en movementos laterais.

Por iso, a coordinación TI–OT debe estar institucionalizada mediante **procedementos compartidos**, canles de escalado e trazabilidade de decisións, evitando que dependa só de relacións informais.

5.1.6 Ciberseguridade e xestión de riscos tecnolóxicos

A función de **ciberseguridade e xestión de riscos tecnolóxicos** debe manter **independencia** e capacidade efectiva de priorización, co reporte adecuado ao nivel executivo. A estrutura recomendable combina:

- **Goberno, risco e cumprimento (GRC)**: xestión do risco tecnolóxico (incluíndo OT), risco de provedores e cadea de subministración, corpo normativo interno, indicadores e reporte, e formación.
- **Operacións de seguridade**: monitorización, resposta a incidentes, xestión de vulnerabilidades e ameazas e coordinación con provedores de servizo.
- En entornos OT/ICS é recomendable así mesmo unha función específica: o/a **Responsable de Seguridade OT/ICS**, que garante que políticas, controis e operacións de seguridade son aplicables á realidade industrial e que existe coordinación diaria coa planta. Esta función debe ter **dependencia funcional do CISO** e coordinación operativa con **Operacións/Plantas**, especialmente en ámbitos como xestión de cambios, acceso remoto, monitorización e resposta, etc.

5.1.7 Coordinación TI–OT–Seguridade

A **coordinación entre TI, OT e ciberseguridade é crítica porque a protección e a continuidade dependen de infraestruturas compartidas e de respostas coordinadas**. En particular, a resposta a incidentes en OT require conter e recuperar sen comprometer a seguridade funcional nin a continuidade do proceso. Por este motivo, recoméndase institucionalizar un **mecanismo estable de coordinación** (por exemplo, un comité técnico TI–OT–Seguridade ou unha oficina de programa), con participación de Operacións/Planta, para asegurar **visibilidade mutua**, **priorización consistente** e **execución segura** de cambios e medidas.

5.2 Funcións de seguridade

A continuación preséntase unha **proposta de funcións de seguridade** orientada a organizacións industriais, co obxectivo de cubrir de maneira coherente todo o **ciclo de vida do risco**, desde a súa identificación ata a recuperación tras un incidente. Esta proposta parte dunha visión integral da seguridade, na que a **seguridade da información**, a **continuidade operativa** e a **protección dos procesos industriais** se abordan de forma conxunta, evitando unha aproximación restrinxida exclusivamente ao ámbito TI.

Como marco de referencia conceptual emprégase o **NIST Cybersecurity Framework (NIST CSF)**, un estándar internacional amplamente adoptado que estrutura as capacidades de ciberseguridade arredor de cinco funcións nucleares: **Identificar, Protexer, Detectar, Responder e Recuperar**. Estas funcións non describen solucións técnicas concretas, senón **capacidades organizativas e operativas** que deben estar presentes en calquera modelo de seguridade maduro [29][30].

Funcións NIST CSF 2.0. Fonte: NIST (2024)

As funcións de seguridade que se describen a continuación inspíranse nestas cinco funcións do NIST CSF, que se toman como referencia común, pero preséntanse cunha **visión orientada ao negocio e á operación industrial**, de maneira que resulten comprensibles e aplicables ao contexto real das organizacións con activos **OT/ICS**. Esta aproximación ten en conta os riscos, limitacións e particularidades identificadas nas seccións previas do informe.

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

O **NIST CSF**, así como a súa aplicación específica a contornos industriais e infraestruturas críticas, abórdase con maior detalle na **Guía Normativa do Observatorio de Ciberseguridade Industrial da AMTEGA** [31], que complementa este informe cunha análise máis profunda dos requisitos, boas prácticas e marcos de referencia aplicables.

Seguidamente descríbese o conxunto de **funcións de seguridade propostas**, indicando de forma implícita a súa correspondencia coas capacidades de **Identificación, Protección, Detección, Resposta e Recuperación** do NIST CSF. Tal e como se expón, as cinco funcións nucleares do marco atópanse cubertas, cun enfoque adaptado á realidade das organizacións industriais.

Funciones do Programa de Seguridade e relación co NIST CSF. Fonte: elaboración propia (2026)

Indícase tamén na figura a responsabilidade de cada función.

- Nome de cor branca: área de Xestión do Risco (GRC).
- Cor gris: área de Operacións de Seguridade.

Pasemos agora a describir cada función de xeito individual.

5.2.1 Xestión do risco tecnolóxico e operativo

A **xestión do risco tecnolóxico e operativo** encárgase de identificar, analizar, avaliar e facer seguimento dos riscos que afectan á organización, tanto no ámbito das **tecnoloxías da información (TI)** como nos **entornos operativos industriais**

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

(OT/ICS). Trátase dun compoñente transversal e estruturante do modelo de gobernanza, desde o cal se realizan revisións **como mínimo anuais**, así como análises **ad hoc** cando se producen cambios relevantes no contexto tecnolóxico, operativo, regulatorio ou de ameaza.

Estes análises poden conducirse empregando metodoloxías recoñecidas, como **ISO/IEC 27005**, **ISO 31000** ou outras aproximacións equivalentes, adaptadas á realidade industrial. O seu obxectivo é facilitar unha visión estruturada do risco que permita o **seguimento por parte dun comité de revisión do risco tecnolóxico**, no que deben estar representadas as áreas de **Operacións (OT)**, **TI**, **Xestión de Riscos**, **Ciberseguridade**, **Negocio** e, cando corresponda polo impacto potencial, o **nivel executivo ou Consello**. Será este último quen adopte as decisións de maior impacto mediante **procesos formais de aprobación e aceptación do risco**.

De forma habitual, os riscos son **identificados, avaliados, priorizados, tratados e monitorizados** a través dun rexistro centralizado, que pode xestionarse mediante plataformas especializadas de **gobernanza, risco e cumprimento (eGRC)** ou, en organizacións con menor madurez, mediante ferramentas máis sinxelas. En calquera caso, o obxectivo é garantir un **seguimento sistemático dos riscos** e proporcionar información relevante aos distintos **stakeholders**, de maneira que se manteña un nivel de **incerteza suficientemente baixo** para cumprir os obxectivos estratéxicos, operativos e de continuidade da organización.

Manterase un **rexistro de riscos permanentemente actualizado**, no que cada risco contará cun **propietario claramente identificado** (Operacións, TI ou Negocio) responsable de executar os plans de tratamento acordados. A función de **Ciberseguridade ou Xestión do Risco Tecnolóxico**, segundo a estrutura organizativa, asumirá a coordinación global do proceso e a propiedade daqueles riscos **transversais**, non asociados a un servizo, activo ou planta concreta, incluíndo os que afectan simultaneamente a múltiples dominios TI e OT.

Para a correcta implantación desta función, existen unha serie de aspectos clave que deben definirse de maneira explícita:

- A **delimitación do alcance** do proceso de xestión do risco, incluíndo sistemas, procesos, activos industriais e cadeas de subministración relevantes.
- A definición do **apetito de risco** da organización, aprobado ao nivel executivo, especialmente no relativo a continuidade operativa, seguridade do proceso e impacto en servizos esenciais.

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

- O acordo sobre a **metodoloxía de identificación, avaliación e tratamento dos riscos**, adaptada á realidade TI e OT.
- A **asignación clara de roles e responsabilidades**, incluíndo propietarios de risco e mecanismos de escalado.
- O **modelo de toma de decisións**, diferenciando entre riscos aceptables a nivel operativo e aqueles que requiren aprobación executiva.

Adicionalmente, a función debe aliñarse cos **principios de actuación establecidos na norma ISO 31000 de Xestión do Risco**, que constitúen unha guía sólida para unha xestión eficaz e sostible. Estes principios inclúen:

- **Xestión integrada**: a xestión do risco non é unha actividade illada, senón que debe estar integrada nos procesos da organización, desde a planificación estratéxica ata a execución operativa, a xestión de proxectos e a definición de políticas e procedementos.
- **Estruturada e exhaustiva**: o proceso debe seguir unha aproximación sistemática que permita obter resultados coherentes e comparables no tempo.
- **Adaptada ao contexto**: o marco de referencia e os procesos deben axustarse continuamente ao contexto interno e externo da organización, tendo en conta a súa realidade industrial, o seu sector e os seus obxectivos.
- **Inclusiva**: deben participar de maneira oportuna os distintos grupos de interese, garantindo decisións informadas, un nivel adecuado de concienciación e unha conexión real co negocio e coa operación.
- **Dinámica**: a xestión do risco debe basearse en información histórica, situacións actuais e expectativas futuras, incorporando a evolución das ameazas e do contexto tecnolóxico.
- **Atención aos factores humanos e culturais**: os comportamentos, percepcións e sesgos das persoas inflúen directamente na xestión do risco, polo que deben ser considerados de forma explícita.
- **Mellora continua**: o proceso debe optimizarse de maneira constante, incorporando a experiencia adquirida, o feedback dos incidentes e a evolución das boas prácticas.

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

En conxunto, esta función permite establecer unha **base sólida para a toma de decisións informadas**, asegurando que os riscos tecnolóxicos e operativos en contornos **OT/ICS** se xestionan de forma sistemática, proporcionada e aliñada coa estratexia e coa continuidade da organización.

5.2.2 Arquitectura de seguridade (TI e OT/ICS)

A función de **Arquitectura de seguridade** abrangue todo o relativo á **xestión, operación e representación formal** (deseños, diagramas, táboas, modelos e especificacións) dos compoñentes de seguridade dunha organización. O seu obxectivo é describir de maneira estruturada as **funcións, a estrutura e as interrelacións** entre os distintos controis, servizos e produtos de seguridade, garantindo unha visión coherente e consistente tanto en contornos **TI** como **OT/ICS**.

En organizacións industriais, esta función resulta especialmente crítica, xa que a arquitectura debe equilibrar **seguridade, dispoñibilidade e seguridade do proceso**, tendo en conta limitacións tecnolóxicas, dependencias de fabricantes, ciclos de vida longos e a necesidade de evitar impactos non desexados na operación.

Arquitectura de redes

A arquitectura de redes encárgase de asegurar que toda a **documentación asociada a dispositivos, redes, comunicacións e cableado** se atopa permanentemente **actualizada, accesible ao persoal autorizado** e revisada de forma periódica polos responsables correspondentes. Sempre que sexa posible, esta xestión debe apoiarse en **ferramentas específicas** de documentación e xestión de rede.

Os dispositivos de rede —como **routers, switches, firewalls, balanceadores, pasarelas industriais e dispositivos de comunicación OT**— deben estar correctamente configurados, prestando especial atención a aspectos como:

- **Bastionado e configuración segura**.
- **Rexistro e almacenamento seguro de eventos de seguridade**.
- **Xeración de alertas e excepcións** ante comportamentos anómalos.
- **Integración cos mecanismos de control de acceso e xestión de identidades**.

Debe implementarse unha **segmentación adecuada da rede**, especialmente relevante en contornos industriais, mantendo un esquema que diferencie claramente:

- **Zona non segura**, que inclúe Internet e servizos de terceiros non controlados pola organización.
- **DMZ (zona desmilitarizada)**, que permite comunicacións controladas entre a zona non segura e os sistemas internos.
- **Zona de confianza**, de acceso restrinxido, que permite principalmente conexións saíntes e conexións entrantes moi controladas desde a DMZ.
- **Zona restrinxida ou OT**, que non permite comunicación directa coa DMZ nin coa zona non segura, e só admite conexións internas estritamente necesarias e documentadas.

No caso de **conexións externas** (provedores autorizados, mantemento remoto ou persoal desprazado), deben empregarse solucións como **VPN con autenticación forte** (OTP, certificados, tokens, etc.) ou contornos de acceso controlado (clientes lixeiros, escritorios virtuais), mantendo sempre un **inventario actualizado de conexións remotas, usuarios e permisos asociados**.

Seguridade de redes Wi-Fi

Como boa práctica, as redes **Wi-Fi de invitados** deben estar completamente **segmentadas**, sen acceso a recursos corporativos nin industriais. En contornos industriais, ademais, recoméndase **ocultar routers e cableado**, así como axustar a potencia das antenas para evitar que o sinal supere o perímetro das instalacións.

A rede Wi-Fi corporativa debe empregar **protocolos e mecanismos de autenticación robustos**, e manter unha configuración bastionada, incluíndo a desactivación de funcionalidades innecesarias, a protección fronte a cambios non autorizados e a revisión periódica dos parámetros de seguridade.

Xestión de cambios en arquitectura de seguridade

No ámbito da arquitectura de seguridade, a **xestión de cambios** refírese especificamente a modificacións que poden afectar á postura de seguridade de sistemas TI e OT, tales como:

- Actualizacións e modificacións de software, incluídos parches.
- Cambios en parámetros de configuración e táboas de control.
- Modificacións na estrutura da información (bases de datos, ficheiros, rexistros).
- Cambios en procedementos operativos e de usuario.

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

- Correccións de emerxencia.
- Cambios en infraestruturas, equipos e redes.

Estes cambios deben revisarse e aprobarse mediante un **procedemento formal**, normalmente apoiado por un **Change Advisory Board (CAB)**, no que participen **TI, Operacións e Ciberseguridade**, e no que, en contornos OT, debe considerarse tamén a **seguridade funcional (safety)**. Ademais, debe existir un procedemento específico para **cambios de emerxencia**, garantindo sempre a trazabilidade e a avaliación posterior do impacto.

Xestión de activos

A **xestión de activos hardware e software** é un requisito básico para a seguridade. Debe manterse un **inventario protexido e actualizado** que inclúa tanto activos TI como OT, facilitando a posterior aplicación de controis de seguridade, a xestión de vulnerabilidades e a resposta a incidentes.

En contornos industriais, este inventario debe recoller tamén información sobre **criticidade operativa**, localización, dependencia de provedores, versións de firmware e relacións con outros sistemas.

Copias de seguridade

Debe realizarse unha **copia de seguridade da información esencial**, incluíndo datos de negocio, sistemas e servizos críticos, cunha periodicidade acorde aos **obxectivos de recuperación** a nivel de tempos e puntos de información previos **(RTO/RPO)** definidos pola organización.

A práctica habitual é empregar **estratexias de respaldo en capas**, que permitan restaurar rapidamente a información crítica e recuperar progresivamente o resto. Dado o risco crecente de **ransomware**, é imprescindible contar cunha estratexia de protección de copias que inclúa, por exemplo, **segmentación de rede**, almacenamento illado ou destinos alternativos, así como **cifrado das copias** para evitar accesos non autorizados.

Protección de endpoints (TI e OT)

As **estacións de traballo e endpoints** deben adquirirse a provedores homologados, probarse antes da súa posta en servizo, contar con acordos de mantemento e empregar **configuracións técnicas estándar**. En entornos OT, isto inclúe estacións de enxeñaría, HMI e equipos de operación.

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

Os endpoints deben estar protexidos fronte a accesos non autorizados mediante:

- **Mecanismos de bloqueo automático por inactividade**.
- **Controis de acceso adecuados**.
- **Cortalumes persoais e cifrado da información sensible**.

Os sistemas de protección fronte a malware deben estar instalados, activos e configurados para analizar memoria, ficheiros, medios extraíbles, correo electrónico e descargas, proporcionando alertas, corentena e eliminación segura, sen permitir a desactivación non autorizada nin afectar á operación estándar.

No caso de **servidores e sistemas críticos**, deberán configurarse segundo **liñas base documentadas**, como as guías de bastionado do **Center for Internet Security (CIS)** [32], tendo en conta as limitacións propias de OT. Como mínimo, debe considerarse:

- Desactivación ou restrición de servizos innecesarios.
- Restrición do acceso a utilidades críticas e á configuración.
- Aplicación controlada de parches e actualizacións de seguridade.

Uso de Internet

O acceso a Internet debe estar **restrinxido por usuarios e funcionalidades**, apoiado por **políticas de uso aceptable** e accións de concienciación. A organización debe coñecer as súas conexións primarias e secundarias a Internet, quen está autorizado a acceder e que **controles tecnolóxicos** existen para inspeccionar, filtrar e actuar sobre tráfico sospeitoso (proxies, filtrado web, WAF, etc.).

En contornos OT, o acceso directo a Internet debe ser **excepcional**, estar xustificado e documentado, e canalizarse sempre a través de mecanismos de control específicos.

Controis xerais de seguridade

Os **controis xerais de seguridade** inclúen políticas, procedementos e mecanismos técnicos destinados a protexer a **confidencialidade, integridade e dispoñibilidade** da información e dos procesos. Entre os marcos de referencia dispoñibles, os **Controis Críticos de Seguridade do CIS** constitúen unha guía práctica e concisa, estruturada en 18 dominios que cobren desde a xestión de activos ata a protección de datos e copias de seguridade [33]. Moitos outros marcos e estándares recóllense na Guía Normativa do Observatorio [31].

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

Un aspecto crítico é o **deseño de novos sistemas ou a evolución dos existentes**. Os controis de seguridade deben considerarse desde as fases iniciais, avaliando a súa viabilidade e impacto. Cando non sexa posible implantalos, deberá tomarse unha **decisión baseada en risco**, optando por omitir, pospoñer ou compensar os controis mediante medidas alternativas, documentando sempre esta decisión.

Neste proceso deben analizarse, entre outros aspectos:

- Os **fluxos de información previstos**, incluíndo entradas, saídas, almacenamento e interconexións con outros sistemas.
- A totalidade de **controis de seguridade necesarios** para protexer a información e os procesos.
- Os controis específicos esixidos polos **procesos de negocio e operación industrial** soportados.
- A forma e o lugar onde aplicar os controis, mediante unha **arquitectura de seguridade documentada**.
- A revisión dos deseños para garantir o cumprimento dos requisitos.
- A documentación explícita daqueles controis que non cumpran plenamente os criterios establecidos.

En conxunto, a función de Arquitectura de Seguridade proporciona a **base técnica e organizativa** para unha protección eficaz e sostible dos sistemas **TI e OT/ICS**, garantindo que a seguridade se integra desde o deseño e se mantén de forma coherente ao longo do tempo.

5.2.3 Cumprimento normativo e regulatorio

O **National Institute of Standards and Technology (NIST)** define unha política de seguridade da información como un *"conxunto de directivas, regulamentos, normas e prácticas que prescriben como unha organización xestiona, protexe e distribúe a información"*. Esta definición resulta plenamente aplicable aos contornos **OT/ICS**, coa particularidade de que a información e os sistemas que a procesan están directamente ligados á operación de procesos físicos críticos.

As políticas de seguridade constitúen o **nivel máis alto da xerarquía normativa interna** para a implantación de Programas de Xestión da Seguridade. Trátase de documentos de alto nivel, de carácter xeral, que establecen que activos deben ser

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

protexidos e baixo que principios, sen entrar nun excesivo detalle operativo. No ámbito OT, estas políticas deben reflectir explicitamente prioridades como a **seguridade funcional, a dispoñibilidade e a continuidade da operación**, por riba doutras consideracións habituais en contornos IT.

Estas políticas definen os **obxectivos estratéxicos de seguridade** e establecen o marco para os niveis inferiores, materializados mediante estándares, procedementos, instrucións técnicas, guías operativas e liñas base específicas para sistemas industriais. A súa función é servir de referencia para deseñar e implantar os controis de seguridade de forma coherente e aliñada co risco.

Aínda sendo documentos xerais, as políticas deben **adaptarse ao contexto operativo da organización**, ao seu sector industrial, ao nivel de criticidade dos procesos e ao seu marco regulatorio. Idealmente, deben ser **atemporais**, de xeito que non dependan de tecnoloxías concretas, senón de principios estables que guíen a toma de decisións ao longo do tempo. En contornos OT/ICS, isto é especialmente relevante debido aos longos ciclos de vida dos sistemas industriais.

Neste marco, adoitan existir políticas e procedementos específicos para ámbitos como:

- boas prácticas de seguridade en contornos industriais,
- control de accesos físicos a instalacións e zonas críticas,
- control de accesos lóxicos a sistemas OT,
- xestión de usuarios e contas con privilexios,
- políticas de contratación e formación de persoal con acceso a sistemas críticos,
- xestión de provedores e da cadea de subministración industrial,
- clasificación e tratamento da información técnica e operativa,
- xestión de incidentes de seguridade con impacto operacional ou de seguridade física.

Os **requisitos legais e regulatorios** deben ser recoñecidos e asumidos pola capa de dirección, así como polo resto de actores implicados na seguridade, incluíndo operacións, mantemento, enxeñaría e IT. No ámbito OT, este recoñecemento resulta clave para garantir que as decisións técnicas e operativas non entren en conflito coas obrigas normativas.

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

Debe establecerse, ademais, un **proceso formal para garantir o cumprimento dos requisitos legais e regulamentarios aplicables á seguridade**, incluíndo:

- Normativa específica de seguridade da información e ciberseguridade (como ISO/IEC 27001, ENS, NIS2, IEC 62443, ou NIST SP 800-82) [31],
- Lexislación xeral con impacto na seguridade (protección de datos, propiedade intelectual, responsabilidade corporativa),
- Regulación sectorial aplicable ás infraestruturas críticas ou servizos esenciais (enerxía, auga, transporte, saúde, financeiro, etc.).

Aínda que non pertence estritamente á disciplina clásica da Seguridade da Información —e adoita recaer baixo a responsabilidade de IT ou de operacións— é imprescindible considerar o **impacto dos eventos disruptivos na dispoñibilidade dos procesos industriais**. Por este motivo, resulta esencial unha colaboración estreita entre OT, IT e o resto das áreas da organización para a elaboración dun **Plan de Continuidade de Negocio (PCN)** e, cando proceda, de plans de recuperación específicos para sistemas industriais.

Os PCN en contornos OT deben incluír, como mínimo:

- A lista priorizada de servizos e procesos industriais a recuperar,
- Tarefas e procedementos de resposta e recuperación,
- Responsables claramente asignados,
- Dependencias críticas (enerxía, comunicacións, provedores externos).

Estes plans deben ser **probados periodicamente**, mediante exercicios ou simulacións, co obxectivo de validar a súa viabilidade real e identificar melloras. En determinados casos, pode ser necesario recorrer a **terceiros especializados** para garantir a recuperación da operación dentro dos tempos máximos aceptables (RTO, Recovery Time Objective), especialmente cando os procesos industriais teñen unha tolerancia moi baixa á interrupción.

De novo, este ámbito require unha **toma de decisións baseada en risco**, de maneira que o alcance do plan, o nivel de detalle e o investimento asociado se axusten ás expectativas realistas de impacto e ás consecuencias dun fallo operativo.

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

5.2.4 Formación e concienciación

Os controis automáticos de Seguridade da Información **non eliminan a necesidade de formar ás persoas**. Por unha banda, a xestión eficaz da seguridade require expertise especializado; pola outra, para un adversario adoita ser máis sinxelo **inducir a erro a un usuario mediante enxeñaría social** para que realice unha acción en seu beneficio que superar barreiras técnicas avanzadas. Por este motivo, considérase tradicionalmente ás persoas como "o elo máis feble da cadea da ciberseguridade".

En contornos **OT/ICS**, esta realidade é aínda máis crítica, xa que unha acción aparentemente menor (por exemplo, a conexión dun dispositivo non autorizado ou a execución dun ficheiro) pode ter **impacto directo na seguridade física, na dispoñibilidade do proceso ou na continuidade do servizo**. Resulta, polo tanto, imprescindible implantar un **programa robusto de formación (cualificación) e concienciación**, adaptado ao contexto industrial.

Aspectos clave do programa:

- **Avaliación de necesidades**

  Existen ferramentas automáticas que, mediante enquisas estruturadas, permiten obter *feedback* sobre o nivel de coñecemento e percepción do risco. Esta información pode complementarse con entrevistas a perfís clave (persoal de operación, mantemento, enxeñaría, mandos intermedios) e a empregados en xeral, co obxectivo de identificar carencias específicas en OT/ICS.

- **Programación de campañas**

  Unha boa práctica en materia de concienciación consiste en combinar:

  - sesións anuais obrigatorias (cando así o esixa a normativa aplicable),
  - cunha **campaña trimestral continuada ao longo dun período aproximado de tres anos**.

  Estas campañas deben priorizar as áreas nas que se detecte un maior nivel de risco segundo as avaliacións realizadas, procurando, non obstante, cubrir progresivamente todos os colectivos. Poden deseñarse campañas selectivas ou personalizadas por obxectivo (operadores, persoal de mantemento, enxeñaría, IT/OT), **evitando a sobrecarga** do persoal con excesivas interaccións.

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

Recoméndase coordinar previamente con **Xestión de Persoas e a Área Legal**, para garantir que non existan solapamentos con outras iniciativas formativas corporativas que poidan xerar fatiga ou conflito.

Nos plans anuais, os elementos críticos serán:

- o deseño e creación de contidos adaptados ao contexto OT (carteis, píldulas *online*, comunicados, ciberexercicios, simulacións),
- unha comunicación eficaz e o compromiso dos interlocutores clave,
- e a **medición da efectividade** das campañas mediante indicadores obxectivos (participación, resultados de probas, redución de incidentes atribuíbles a erro humano).

5.2.5 Protección de datos e Privacidade

Esta función encárgase do **goberno e da xestión do ciclo de vida dos datos sensibles**: que datos existen, onde se almacenan, como se transmiten, quen accede a eles e que actuacións deben realizarse no caso de accesos indebidos, exfiltracións ou fugas non intencionadas. Todo isto debe facerse en **estreita colaboración coa área Legal e co DPO (Delegado de Protección de Datos)**, cando exista. Inclúe datos de clientes, provedores e empregados, así como información técnica e operativa relevante en contornos OT.

Non se trata unicamente de boas prácticas voluntarias: as **regulacións vixentes esíxeno** (por exemplo, RGPD e LOPD-GDD), incluso en organizacións industriais nas que o foco principal non sexa o tratamento masivo de datos persoais [31].

Principais aspectos a considerar:

- **Clasificación da información**

  A información debe clasificarse segundo a súa tipoloxía e criticidade para as operacións do negocio, valorando o impacto derivado dunha perda de confidencialidade, integridade ou dispoñibilidade. Esta clasificación debe aplicarse a:

  - documentación electrónica e en papel,
  - aplicacións de negocio,
  - sistemas OT/ICS,

- redes, postos de traballo e contornos en desenvolvemento, contemplando tamén como resolver posibles conflitos de clasificación.

Non é un proceso trivial. A aproximación recomendada é **comezar por un ámbito reducido** (por exemplo, un departamento ou proceso crítico) e ir ampliando progresivamente en círculos concéntricos. Cada conxunto de datos debe ter sempre un **responsable (*owner*)**, encargado de asignar e revisar os niveis de seguridade.

Un esquema típico de clasificación contempla catro niveis:

- **C-1. Restrinxida** (máxima criticidade: plans estratéxicos, M&A, información moi sensible).
- **C-2. Confidencial** (acceso limitado a un ámbito interno reducido).
- **C-3. Interna** (uso exclusivo de persoal interno).
- **C-4. Pública**.

Unha vez implantado o modelo, a información debe **etiquetarse, almacenarse, procesarse e compartirse** conforme ao seu nivel. Existen ferramentas que permiten identificar automaticamente a clasificación e, por exemplo, cifrar correos electrónicos con información de nivel elevado. Isto implica etiquetado, rexistro, formación, posibles adaptacións contractuais e a aplicación de controis como **DLP (Data Loss Prevention)**.

Un enfoque baseado en risco recomenda **concentrar maiores recursos** alí onde reside a información clasificada como máis crítica, mediante medidas como segmentación de rede, monitorización avanzada ou controis reforzados en sistemas OT.

- **Requisitos de confidencialidade, integridade e dispoñibilidade**

  En contornos industriais, a prioridade de negocio adoita centrarse na **dispoñibilidade**. Por iso resulta esencial implantar segmentación, redundancia e estratexias de copia de seguridade adaptadas a OT, sen descoidar os requisitos de confidencialidade e integridade.

- **Criptografía / cifrado**

  A criptografía permite garantir confidencialidade, integridade e non repudio. Unha xestión eficaz das claves criptográficas debe cubrir:

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

- xeración segura,
- distribución segura,
- almacenamento, recuperación e renovación de claves caducadas,
- revogación en caso de compromiso ou cambio de función do propietario,
- recuperación de claves perdidas ou danadas,
- copia de seguridade e arquivo con mantemento do historial,
- definición de datas de activación e desactivación,
- restrición do acceso só a persoal autorizado.

Debe terse en conta a protección dos datos **en repouso, en tránsito e en uso**, incluíndo os endpoints e sistemas industriais.

- **Normas de tratamento da información en soporte electrónico**

  Ademais do cifrado, é necesario protexer a información sensible almacenada en soportes electrónicos (discos duros, medios extraíbles) mediante prácticas como:

  - borrado seguro de soportes reutilizables,
  - almacenamento conforme ás recomendacións do fabricante,
  - rexistro e autorización das transferencias de datos,
  - control dos soportes que saen fóra do contorno habitual,
  - eliminación da información antes de enviar equipos a mantemento ou destrución.

- **Soporte legal**

  Esta función debe apoiar ao **DPO e á área Legal** en todo o relativo a comunicacións con clientes e/ou Autoridades de Control, especialmente en caso de **brechas de seguridade**, garantindo unha resposta coordinada, conforme á normativa e dentro dos prazos establecidos.

5.2.6 Xestión de Identidades e Accesos (IAM)

A **Xestión de Identidades e Accesos (IAM)** refírese ao goberno e á xestión da provisión, modificación e retirada dos mecanismos de autenticación e control de acceso de

usuarios, entidades técnicas e procesos, incluídos aqueles propios de contornos **OT/ICS**. Un dos puntos tradicionalmente máis febles atópase na xestión do ciclo de vida do persoal, especialmente nos **cambios de posto, mobilidade interna ou saídas da organización**, onde adoitan persistir accesos innecesarios.

Existen múltiples solucións técnicas (autenticación multifactor, passkeys, cloud brokers, **SSO**, portais de self-service para reseteo de credenciais, etc.). Resulta eficiente empregar **Directorios centralizados** (como Directorio Activo) e aplicacións compatibles con **LDAP**, sempre que sexa viable tamén en contornos industriais. O foco principal debe situarse nos **administradores, superusuarios e perfís con acceso á información ou sistemas máis sensibles**, especialmente en operacións industriais.

Aspectos clave de IAM:

- **Acceso baseado en funcións (RBAC)**

  Os permisos deben asignarse sempre en base a **roles**, nunca mediante personalizacións individuais. Deben observarse estritamente os principios de **mínimo privilexio** e **segregación de funcións**, particularmente relevantes en OT para evitar que unha única conta poida operar, modificar e auditar un mesmo proceso crítico.

- **Autenticación**
  Baseada en credenciais (usuario e contrasinal), idealmente reforzada cun **segundo factor de autenticación** (tokens, certificados ou biometría cando proceda). Deben establecerse políticas de:

  - lonxitude e complexidade mínimas,
  - eliminación de contrasinais administrativas por defecto,
  - convencións de nomes de usuario que eviten duplicidades,
  - reforzo específico para accesos remotos a contornos OT.
    Os sistemas federados modernos incrementan a seguridade ao automatizar a autenticación, esixindo unha **identificación inicial máis robusta**.

- **Xestión de credenciais**

  Inclúe o almacenamento seguro de identidades, contrasinais, tokens e certificados. Sempre que sexa posible, recoméndase a **centralización** para

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

simplificar a xestión e o proceso de autenticación, avaliando o uso de **SSO** e directorios corporativos en aplicacións industriais compatibles.

- **Supervisión e monitorización**

  A monitorización dos intentos de autenticación e dos accesos a información sensible é crítica. Pode realizarse mediante un **SIEM**, permitindo detectar patróns anómalos (horarios inusuais, orixes xeográficas inesperadas, IP/MAC non habituais). É tan importante definir correctamente as **regras de alerta** como garantir a súa xestión efectiva.

- **Mantemento de contas de usuario**

  As ferramentas de xestión deben permitir asociar un usuario a unha ou varias contas e revisar os seus privilexios ao longo do tempo. Os riscos habituais son a **acumulación de permisos** tras cambios de posto e a **non desactivación** das contas tras baixas voluntarias ou forzosas. Deben existir procesos claros, preferiblemente automatizados, para revisións periódicas.

5.2.7 Xestión de ameazas e vulnerabilidades

En ciberseguridade, unha **ameaza** é un evento ou axente externo con capacidade para causar dano ou comprometer a seguridade dun sistema ou rede. Pode ter orixe humana, técnica ou ambiental (malware, ataques dirixidos, fallos de hardware/software, desastres naturais, etc.).

Unha **vulnerabilidade**, pola súa banda, é unha debilidade nun sistema que pode ser explotada por unha ameaza. Pode deberse a erros de deseño, configuracións incorrectas, ausencia de parches ou mecanismos de control insuficientes.

En resumo: **a ameaza é o axente**, a **vulnerabilidade é a fenda**. A existencia dunha vulnerabilidade non implica necesariamente un incidente, pero **toda ameaza precisa dunha vulnerabilidade para materializarse**.

Esta función é responsabilidade do **equipo de Operacións de Seguridade**, asumindo que non existen contornos 100 % seguros. As vulnerabilidades poden identificarse mediante:

- escáneres automáticos,
- análise de rexistros de seguridade (intentos de acceso fallidos, caídas de servizos, borrados anómalos),

- probas de intrusión controladas.

As vulnerabilidades deben tratarse **por orde de prioridade segundo o risco**, dentro dun programa sistemático e documentado.

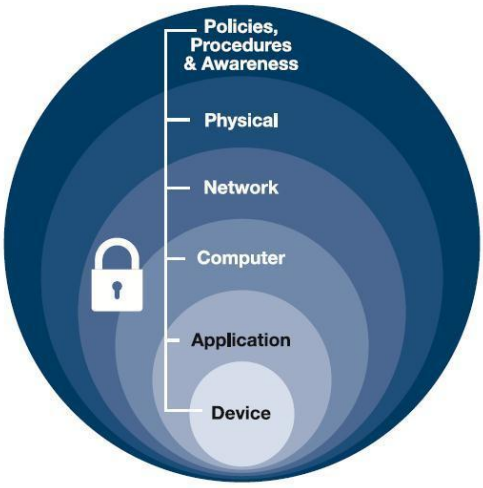
Os rexistros de eventos de seguridade deben analizarse de forma **continua e automatizada**, incluíndo:

- procesamento e correlación de eventos relevantes,
- interpretación de comportamentos anómalos,
- resposta coordinada ante eventos críticos, derivando a información ao equipo de xestión de incidentes.

Aspectos clave:

- definición de **regras de correlación** e playbooks asociados,
- establecemento dun **proceso de xestión de parches**, adaptado a OT: aprobación formal polo owner do sistema, probas previas, contornos de test cando sexa posible, e avaliación do impacto operativo.
  Os cambios adoitan realizarse en **xanelas de mantemento**, salvo parches críticos, que deben contar cun **procedemento de emerxencia** (idealmente <24 h).

Adicionalmente, é imprescindible dispoñer de **solucións antimalware** en *endpoints*, servidores e pasarelas. Máis que apostar por mecanismos excesivamente sofisticados, recoméndase un enfoque de **defensa en profundidade**.



Esquema de defensa en profundidade. Fonte: OpenPracticeLabrary (2022)

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

A defensa en profundidade baséase na combinación de múltiples capas de protección complementarias:

- políticas e procedementos,
- formación e concienciación,
- controis físicos,
- protección perimetral e de rede (cortafogos, NDR, CPS PP, IDS/IPS, segmentación, *honeypots*..),
- controis a nivel de aplicación e dispositivo (DLP, cifrado, EDR, HIDS).

Este enfoque é eficaz, comprensible a nivel organizativo e **suficiente sen recorrer a solucións extremadamente complexas ou custosas**, que non están exentas de riscos.

5.2.8 Resposta a incidentes de seguridade

Un **incidente de ciberseguridade** é unha violación —ou ameaza inminente de violación— das políticas de seguridade, de uso aceptable ou das prácticas estándar. A súa xestión debe estar **perfectamente documentada e procedementada**, permitindo unha resposta coherente e unha recuperación áxil.

O **Plan de Resposta a Incidentes de Seguridade** é o documento central das Operacións de Seguridade. Inclúe enfoques, métricas, contactos, secuencias de actuación, escalados, métodos de notificación e listas de comprobación. O proceso simplificado, estrutúrase en catro fases:

1. **Iniciación / triaxe**

   Determínanse que alertas ou eventos activan o proceso e que accións iniciais se executan. Unha alerta pode xerar un evento, que á súa vez se converta nun incidente. Avalíase a prioridade e a necesidade de apoio de terceiros.

2. **Contención**

   Identifícanse os **IoC (indicadores de compromiso)** para determinar o alcance: *hosts* afectados, contas comprometidas, datos impactados. Implántanse medidas para limitar a propagación e reducir o impacto, avaliando novamente o apoio externo se procede.

3. **Erradicación**

   O equipo de Seguridade, en coordinación con IT/OT, lidera as accións técnicas:

bloqueo de portos, illamento de sistemas, scripts de limpeza, retirada de accesos indebidos, etc.

4. **Recuperación**

   O equipo de Seguridade fornece información forense para restaurar os servizos. Identifícase a **causa raíz** e formúlanse recomendacións: cambios de arquitectura, melloras de procesos, parcheado adicional ou despregue de novos controis para evitar recorrencias, a modo de mellora continua.

Os **roles e responsabilidades** deben estar claramente definidos para evitar confusións en situacións de crise. Resulta imprescindible **practicar escenarios de incidente** mediante exercicios periódicos, especialmente en contornos OT/ICS onde o tempo de resposta é crítico.

6 Marcos normativos e cumprimento

Os marcos normativos, estándares e regulacións en materia de ciberseguridade industrial constitúen un **elemento fundamental para a mitigación do risco** en contornos OT/ICS. O seu principal valor reside en proporcionar un conxunto estruturado de **boas prácticas recoñecidas**, que axudan ás organizacións a abordar a seguridade desde unha perspectiva integral: organizativa, procedemental e técnica.

A través destes marcos establécense criterios claros sobre **como gobernar a seguridade**, como definir responsabilidades, como xestionar procesos críticos (accesos, cambios, incidentes, continuidade) e que **controles físicos e lóxicos** deben implantarse para reducir a probabilidade e o impacto de incidentes. A súa aplicación non garante a eliminación do risco, pero si permite **reducilo a niveis aceptables**, dotando ademais á organización dun marco común para a toma de decisións baseada en risco.

Co obxectivo de profundar neste ámbito, o Observatorio desenvolveu o entregable específico **Guía Normativa do Observatorio**, ao que se convida expresamente ao lector a acudir para un tratamento exhaustivo e detallado [31]. Esta guía está concibida como un documento de referencia práctica e estrutúrase en tres grandes bloques de contido, mais un elemento auxiliar:

- Normativa española aplicable á industria e ás infraestruturas críticas.
- Marco normativo e regulatorio da Unión Europea.
- Estándares e marcos internacionais de referencia.
- Guía de implantación práctica orientada a contornos OT/ICS.

A continuación preséntase unha síntese de alto nivel dos tres primeiros epígrafes, co obxectivo de contextualizar o seu alcance e utilidade.

6.1 Normativa española

Na **Guía Normativa do Observatorio** a normativa nacional preséntase como un conxunto de referencias de obrigado cumprimento (ou de aplicación práctica moi frecuente) que determinan "o chan mínimo" regulatorio para moitas organizacións, incluídas as que operan contornos OT/ICS [31]. En concreto, inclúense:

- **Esquema Nacional de Seguridade (ENS)**: é o marco normativo español que fixa principios básicos, requisitos mínimos e medidas de seguridade para os

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

sistemas, datos e servizos no ámbito do sector público e dos seus provedores. Serve para establecer unha referencia común e auditable de controis (organizativos, operativos e técnicos) e para orientar a xestión do risco e a categorización de sistemas.

- **Lei 12/2018 e Real Decreto 43/2021 (transposición e desenvolvemento da Directiva NIS 2016/1148)**: é o paquete normativo que trasladou á normativa española as obrigas de seguridade e notificación de incidentes para **operadores de servizos esenciais** e **provedores de servizos dixitais**. Serve para obrigar a implantar medidas de xestión de riscos e establecer canles e prazos de reporte e supervisión, ata que a transposición de NIS2 en España a substitúa/modifique.
- **Lei de Protección de Infraestruturas Críticas (Lei PIC)**: é a norma nacional orientada á protección das infraestruturas críticas mediante a planificación, coordinación e obrigas de seguridade asociadas (incluíndo figuras, plans e medidas de protección). Serve para **asegurar a continuidade e a protección de servizos esenciais fronte a ameazas**, incluídas as ciberameazas con impacto operacional.
- **Estratexia Nacional de Ciberseguridade (2019) e Plan Nacional de Ciberseguridade**: son instrumentos estratéxicos que definen **liñas de acción, prioridades e coordinación institucional en materia de ciberseguridade**. Serven para orientar políticas públicas e reforzar capacidades (prevención, detección, resposta e cooperación), actuando como marco director para plans e iniciativas sectoriais.
- **Lei Orgánica 3/2018 (LOPD-GDD) e obrigas asociadas (incluíndo AIPD/EIPD)**: é a **norma española que desenvolve e complementa a protección de datos persoais no marco do RGPD**. Serve para establecer deberes e garantías no tratamento de datos persoais (dereitos dos interesados, obrigas para entidades, avaliacións de impacto cando proceda), algo relevante tamén en contornos industriais cando existen datos persoais en sistemas corporativos ou en procesos dixitalizados que converxen con OT.

Este bloque nacional **define obrigas e expectativas auditables** que condicionan a gobernanza, a xestión do risco e a implantación de controis en organizacións industriais, especialmente cando prestan servizos esenciais, operan infraestruturas críticas ou manexan datos persoais.

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

6.2 Normativa da Unión Europea

O bloque europeo recolle os instrumentos que elevan e harmonizan o nivel de ciberseguridade e resiliencia no conxunto da UE, e que impactan directamente nos sectores industriais e nas infraestruturas críticas [31]. Inclúense:

- **Directiva NIS2 (Directiva (UE) 2022/2555)**: é a norma europea que establece un **alto nivel común de ciberseguridade para unha ampla lista de entidades esenciais e importantes, con obrigas reforzadas de gobernanza, xestión de riscos e notificación de incidentes**, así como un réxime de supervisión e sancións. Serve para profesionalizar e homoxeneizar a xestión do risco ciber en sectores críticos, reforzando tamén a coordinación e a cooperación a nivel europeo. A guía incorpora, ademais, a referencia á **CCN-STIC 892 (PCE-NIS2)** como apoio práctico ao cumprimento e menciona o marco de transposición en España.
- **CRA (Cyber Resilience Act)**: é unha regulación europea orientada a mellorar a **ciberresiliencia dos produtos con elementos dixitais ao longo do seu ciclo de vida.** Serve para introducir requisitos de seguridade "por deseño e por defecto" e obrigas para fabricantes e cadea de subministración, reducindo risco sistémico por vulnerabilidades en compoñentes e produtos empregados tamén en contornos industriais.
- **CER (Critical Entities Resilience)**: é o **marco europeo centrado na resiliencia das entidades críticas fronte a riscos, incluíndo a dimensión ciber e a continuidade de servizo**. Serve para reforzar a preparación e resiliencia operacional, complementando a visión de ciberseguridade con obrigas e expectativas de continuidade e xestión de crises en sectores esenciais.

O bloque europeo actúa como **impulsor de madurez e harmonización**, elevando obrigas de xestión do risco, gobernanza e resiliencia que as organizacións industriais deben traducir a políticas, procedementos e controis efectivos.

6.3 Estándares e marcos internacionais

Os marcos e estándares internacionais funcionan como a capa que facilita pasar do "que debo cumprir" ao "como o implanto", proporcionando boas prácticas estruturadas e, no caso de OT/ICS, orientación moi aplicable a controis técnicos e operativos [31]. Inclúense:

- **ISO/IEC 27001**: é o estándar internacional para implantar un **Sistema de Xestión da Seguridade da Información (SXSI/ISMS)**, con enfoque de mellora continua. Serve para establecer gobernanza, procesos, análise e tratamento do risco, é un marco auditable/certificable para xestionar a seguridade de maneira sistemática.
- **NIST CSF (Cybersecurity Framework)**: é un **marco de boas prácticas estruturado en funcións (identificar, protexer, detectar, responder, recuperar) e perfís de implantación**. Serve para ordenar programas de ciberseguridade, avaliar situación actual vs. obxectivo e definir follas de ruta de mellora, cunha linguaxe moi utilizada a nivel internacional.
- **CIS Controls**: é un **conxunto priorizado de controis/salvagardas de ciberseguridade, organizado para facilitar unha implantación progresiva** por nivel de madurez. Serve para seleccionar medidas de alto impacto e baixo "ruído", apoiar análises de brecha e estruturar plans de acción realistas, tamén como ponte entre requisitos e evidencias.
- **ISA/IEC 62443**: é a **familia de normas máis específica e completa** para a ciberseguridade de **sistemas de automatización e control industrial (IACS/OT/ICS)**. Serve para definir requisitos e controis por dominios (organización, procesos, sistemas e compoñentes), apoiar deseños "defendibles" e, cando aplica, habilitar esquemas de avaliación e certificación en contornos industriais.
- **SANS ICS Top 5 Controls**: é unha **selección de controis críticos priorizados especificamente para ICS.** Serve para **orientar de forma moi pragmática a implantación de medidas de alto retorno en contornos OT**, especialmente cando hai limitacións de recursos ou necesidade de resultados rápidos.

Como complemento, a guía tamén introduce a conveniencia de empregar **modelos de madurez** (p.ex., C2M2, CSET) para avaliar capacidades e planificar melloras máis aló do "check" de cumprimento. Serve para converter o cumprimento nunha folla de ruta realista de evolución e resiliencia.

De novo, aconsellamos ó lector revisar a Guía Normativa con tranquilidade [31].

7 Controis e boas prácticas

Como xa se mencionou en diversas ocasións, a mitigación dos riscos tecnolóxicos asociados á ciberseguridade en contornos industriais **non depende dunha única medida nin dunha tecnoloxía concreta**, senón da aplicación coherente dun conxunto de **controles organizativos, procedementais e técnicos**, priorizados en función do risco e adaptados ás particularidades dos sistemas OT/ICS.

Os informes previos do **Observatorio de Ciberseguridade Industrial** sentaron xa unha base de recomendacións prácticas, orientadas á realidade operativa das organizacións industriais [4].

Neste sentido, os informes e guías elaborados por organismos públicos, axencias nacionais de ciberseguridade, entidades de referencia internacional e fabricantes especializados, constitúen unha fonte esencial de boas prácticas contrastadas, que se recollerán a continuación de xeito sintético nesta sección. Lóxicamente dada a sua relevancia, hai solape parcial entre as fontes.

Veremos as directrices publicadas por **organismos como o National Cyber Security Centre inglés [34], a Cybersecurity and Infrastructure Security Agency americana [35] ou a ISACA (Information Systems Audit and Control Association) [36]**.

Resulta tamén relevante **a contribución de fabricantes especializados** como Fortinet, a través do seu State of OT Cybersecurity Report 2025 xa citado, que ofrecía datos empíricos sobre tendencias de ataque, debilidades recorrentes e controis con maior impacto real en contornos industriais [17].

Adicionalmente, o uso crecente da **Intelixencia Artificial**, tanto por defensores como por adversarios, introduce novos riscos que deben ser xestionados de forma específica. Para este ámbito, empregaremos como referencia unha guía cocreada pola **CISA e o Australian Cyber Security Centre (ACSC)** [37], en colaboración con múltiples axencias gobernamentais e centros nacionais de ciberseguridade (entre eles a National Security Agency americana [38], o Canadian Centre for Cyber Security [39], o National Cyber Security Centre británico xa presentado, o Bundesamt für Sicherheit in der Informationstechnik alemán [40] ou os NCSC de Países Baixos e Nova Zelandia [41][42]). Esta guía establece principios para un **uso seguro, responsable e resiliente da IA**, tamén aplicables a contornos industriais.

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

Finalmente, estas recomendacións complétanse coa análise de riscos emerxentes recollida no **International AI Safety Report**, xa tratado neste informe, que achega unha visión prospectiva sobre ameazas sistémicas, riscos de abuso e impactos potenciais da IA en infraestruturas críticas e sistemas ciberfísicos [23].

En conxunto, estas fontes permiten construír un **catálogo coherente de medidas de seguridade aplicables**, fundamentado en evidencias, aliñado co estado da ameaza real e orientado á redución efectiva do risco tecnolóxico no ámbito industrial.

7.1 NCSC

As seguintes recomendacións sintetizan as principais liñas de boas prácticas publicadas polo **National Cyber Security Centre (NCSC)** do Reino Unido en materia de seguridade OT. A sección baséase, por unha banda, no artigo divulgativo sobre a importancia de comprender o contorno OT como primeiro paso para mellorar a ciberseguridade, e por outra, na colección completa de guías de Operational Technology, que constitúe un corpo coherente de orientación práctica para organizacións industriais [43][44].

7.1.1 Arquitectura OT

Segundo a guía do NCSC, a creación e mantemento dunha visión definitiva da arquitectura OT baséase en **cinco principios explícitos**, que deben aplicarse de forma sistemática:

- **Definir procesos para establecer e manter o rexistro definitivo do contorno OT**, asegurando que existe unha fonte autorizada e coherente de información.
- Establecer un **programa de xestión da información OT**, que determine como se recompila, mantén, protexe e utiliza a información técnica e operativa.
- **Identificar e categorizar os activos OT** para soportar decisións informadas baseadas en risco, tendo en conta criticidade e impacto.
- **Identificar e documentar a conectividade dentro do sistema OT**, incluíndo fluxos de datos, interdependencias e puntos de interconexión.
- **Identificar e documentar os riscos de terceiros** que afectan ao sistema OT, incluíndo provedores, mantemento e accesos externos.

Estes principios teñen como obxectivo garantir que a organización **comprende realmente o seu contorno OT** antes de aplicar medidas técnicas de protección.

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

7.1.2 Conectividade segura OT

Defenden que a conectividade en contornos industriais debe deseñarse e xestionarse de acordo con oito principios explícitos, que equilibran necesidade operativa e risco:

- **Balancear o risco e as oportunidades**: avaliar conscientemente que beneficios aporta cada conexión fronte ao risco adicional que introduce no contorno OT.
- **Limitar a exposición da conectividade**: reducir ao mínimo necesario o número de conexións e os puntos accesibles desde outros dominios.
- **Centralizar e estandarizar as conexións de rede**: empregar arquitecturas coherentes, evitando excepcións e conexións ad hoc difíciles de controlar.
- **Empregar protocolos estandarizados e seguros**: priorizar protocolos coñecidos, documentados e con capacidades de seguridade fronte a solucións propietarias opacas.
- **Endurecer o perímetro OT**: protexer os límites do sistema industrial mediante controis técnicos adecuados ao risco.
- **Limitar o impacto dun posible compromiso**: deseñar a conectividade asumindo que pode producirse un fallo ou intrusión.
- **Garantir que toda a conectividade está rexistrada e monitorizada**: dispoñer de visibilidade continua sobre as comunicacións OT.
- **Establecer un plan de illamento**: definir con antelación como desconectar ou illar partes do sistema OT en caso de incidente.

O propósito destes principios é **permitir a conectividade necesaria para a operación**, reducindo á vez a superficie de ataque e facilitando a detección, contención e recuperación fronte a incidentes.

Hai que destacar que o NCSC achega un exemplo prácticos que permite aplicar estes principios, na mesma fonte referida.

7.1.3 Uso de terminais de acceso privilexiado

Segundo a guía específica do NCSC sobre **PAW (Privileged Access Workstations) en contornos OT**, o uso de estacións de traballo privilexiadas debe basearse en oito principios explícitos:

- **Establecer a estratexia de PAW da organización**: definir claramente o alcance, obxectivos e casos de uso da PAW dentro do ecosistema OT.
- **Deseñar a solución PAW para que sexa usable e segura**: equilibrar requisitos de seguridade cun uso práctico para os equipos técnicos.
- **Establecer unha base de confianza**: garantir a integridade da PAW mediante arranque seguro, configuración controlada e cadea de confianza.
- **Escalar a solución**: deseñar a PAW para que poida ampliarse a medida que crecen os requisitos operativos e organizativos.
- **Reducir a superficie de ataque**: minimizar software, servizos e capacidades dispoñibles na PAW.
- **Illar actividades de alto risco da PAW**: evitar que tarefas perigosas comprometan o contorno privilexiado.
- **Implantar monitorización protectora**: rexistrar e supervisar o uso da PAW para detectar usos indebidos ou anómalos.
- **Controlar os datos que entran e saen da solución PAW**: evitar fugas de información ou introdución de código malicioso.

Estes principios teñen como finalidade **protexer as credenciais e accións privilexiadas**, reducindo o risco de compromiso dos sistemas OT.

7.1.4 SCADAs na nube

A guía do NCSC sobre **SCADAs aloxados en nube** aborda este modelo como unha evolución emerxente, con distintos graos de adopción e madurez no ámbito OT. Non se limita a recomendar ou desaconsellar a súa adopción, senón que **propón unha análise reflexiva previa á toma de decisións.**

O despregue de SCADA en cloud pode abranguer escenarios moi diversos, desde o procesamento e enriquecemento de datos operativos ata arquitecturas máis avanzadas nas que é posible o control remoto de activos físicos. En todos os casos, o NCSC subliña que a decisión debe tomarse a partir dunha **avaliación de riscos rigorosa**, na que a ciberseguridade sexa un elemento central.

Migrar SCADA á nube non supón un simple cambio de localización da infraestrutura, senón que **altera profundamente os límites tradicionais de seguridade**, **os modelos de conectividade e os mecanismos de control de acceso**. Sistemas historicamente

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

illados pasan a depender de conexións a Internet e de modelos de responsabilidade compartida cos provedores de cloud.

Neste contexto, resulta imprescindible garantir que a conectividade continúa sendo **limitada, controlada e monitorizada**, mantendo niveis de protección equivalentes ou superiores aos dos despregues tradicionais. O NCSC recomenda, ademais, complementar esta orientación coa súa **guía xeral de seguridade en cloud** [45], dado que moitos principios aplicables a IT tamén son relevantes en contornos SCADA modernos.

O obxectivo final desta guía é axudar ás organizacións a **determinar a idoneidade real** dunha solución SCADA en cloud en función do seu contexto operativo, do nivel de risco asumible e das capacidades de seguridade dispoñibles.

7.1.5 Comunidades de interese ICS

O **Industrial Control Systems Community of Interest (ICS CoI)** é unha iniciativa promovida polo NCSC que serve como exemplo de **comunidade nacional de referencia** para mellorar a seguridade e a resiliencia das infraestruturas críticas no Reino Unido.

Trátase dun foro no que participan profesionais do propio NCSC, operadores e propietarios de activos, fabricantes de sistemas ICS, investigadores en seguridade, administracións públicas, reguladores e ámbito académico. A comunidade está gobernada por un comité director que marca a orientación estratéxica e promove a colaboración entre os distintos actores.

O ICS CoI combina a elaboración de orientación técnica sobre problemas concretos coa **concienciación e capacitación** de perfís que se incorporan ao ámbito OT, contribuíndo a reducir a fenda de capacidades existente. Conta con máis de 500 membros activos e organiza sesións periódicas de intercambio de coñecemento.

Aínda que é un exemplo específico do Reino Unido, este modelo é **perfectamente extrapolable** a outros ámbitos. A nivel europeo ou nacional poden identificarse iniciativas semellantes, como grupos de traballo impulsados por **ENISA**, comunidades técnicas arredor de **CERT/CSIRT nacionais** (por exemplo, CCN-CERT en España) ou foros sectoriais promovidos por asociacións industriais e organismos de ciberseguridade.

A participación en comunidades deste tipo permite reforzar a **intelixencia colectiva**, compartir leccións aprendidas e mellorar a preparación fronte a incidentes OT.

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

7.2 CISA

A **Cybersecurity and Infrastructure Security Agency (CISA)** dos Estados Unidos publicou unha guía específica centrada nas mitigacións elementais para reducir as ciberameazas en contornos de **Operational Technology (OT)**.

O enfoque da CISA é eminentemente práctico e priorizado: non pretende cubrir todo o espectro posible de controis, senón identificar aquelas medidas fundamentais que, aplicadas de forma consistente, **reducen de maneira significativa a superficie de ataque e o impacto dos incidentes** en sistemas industriais.

A folla informativa identifica **cinco mitigacións primarias** que as organizacións con OT/ICS deberían priorizar para reducir a exposición fronte a campañas que apuntan especificamente a sistemas OT conectados a Internet:

- **Eliminar conexións OT á Internet pública**: os dispositivos OT adoitan carecer de mecanismos de autenticación e autorización robustos e son doadamente localizables a través de buscas de portos en rangos IP públicos. A recomendación céntrase en identificar activos expostos e eliminar exposicións non intencionadas.
- **Cambiar inmediatamente contrasinais por defecto e empregar contrasinais fortes e únicos**: a actividade observada polos organismos autores inclúe o abuso de credenciais por defecto ou doadamente adiviñables (incluíndo o uso de ferramentas open source). A medida é especialmente crítica en dispositivos expostos que poden afectar procesos OT.
- **Asegurar o acceso remoto ás redes OT**: cando o acceso remoto sexa imprescindible, recoméndase pasar a conexións sobre redes privadas (evitando exposición pública), empregar VPN e reforzar a autenticación con contrasinal forte e **Factor de Autenticación Múltiple (MFA) resistente ao *phishing***. Tamén se enfatiza documentar/configurar o acceso remoto con **mínimo privilexio** e desactivar contas inactivas.
- **Segmentar as redes IT e OT**: introducir segmentación e, cando aplique, unha DMZ para o intercambio de datos de control coa rede corporativa reduce o impacto potencial e diminúe o risco de interrupción das operacións OT.
- **Practicar e manter a capacidade de operar manualmente os sistemas OT**: a posibilidade de volver a controis manuais para restaurar operacións tras un incidente é vital. Recoméndase probar de forma rutineira plans de continuidade

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

e recuperación, mecanismos *de* fallo seguro, capacidades de illamento, copias de seguridade de software e sistemas en reserva.

Adicionalmente, a guía recomenda **coordinarse regularmente con provedores terceiros**, integradores de sistemas e fabricantes, xa que configuracións inseguras poden introducirse durante operacións habituais ou derivar de configuracións por defecto, e a súa corrección reduce vulnerabilidades non intencionadas.

7.3 Fortinet

O informe **State of OT Cybersecurity 2025 de Fortinet** ofrece unha visión baseada en datos empíricos recollidos a partir de enquisas globais, telemetría e experiencia directa en contornos industriais [17].

A continuación preséntanse as principais boas prácticas para contornos OT identificadas por este fabricante. Lóxicamente pola natureza da entidade, presentan certo sesgo cara a recomendación de solución específicas de ciberseguridade.

- **Implantar segmentación de rede en contornos OT**: a segmentación é a base dun contorno OT endurecido. Mediante a creación de zonas e segmentos con políticas de control estritas en todos os puntos de acceso, redúcese drasticamente a capacidade dun atacante para moverse lateralmente. Os estándares como ISA/IEC 62443 reforzan este enfoque, promovendo a separación entre redes IT e OT e entre diferentes dominios OT.
- **Mellorar a visibilidade e aplicar controis compensatorios sobre os activos OT:** unha vez establecida a segmentación inicial, as organizacións poden ampliar a visibilidade do tráfico e do comportamento dos activos OT. Isto permite identificar dispositivos vulnerables e aplicar controis compensatorios deseñados para contornos sensibles, como políticas baseadas en protocolos industriais, análise de comunicacións sistema-a-sistema ou monitorización específica de endpoints OT.
- **Incorporar intelixencia de ameazas e servizos de seguridade específicos para OT**: a seguridade OT require coñecemento actualizado das ameazas reais que afectan a estes contornos. O fabricante destaca a necesidade de empregar intelixencia de ameazas e servizos de seguridade con contido específico OT, capaces de detectar variantes de ataque e comportamentos maliciosos dirixidos a protocolos e dispositivos industriais.

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

- **Integrar OT nas operacións de seguridade (SecOps) e na planificación de resposta a incidentes**: as organizacións deben avanzar cara a modelos de **IT-OT SecOps**, nos que os contornos industriais se integren plenamente nos centros de operacións de seguridade e nos plans de resposta a incidentes. Isto require playbooks específicos OT e unha colaboración estreita entre equipos de seguridade, operacións e produción, tendo en conta o impacto físico e operativo dun incidente.
- **Adoptar un enfoque de plataforma para a arquitectura global de seguridade:** a proliferación de solucións puntuais de distintos fabricantes incrementa a complexidade e a carga operativa. Recoméndase un enfoque de plataforma que permita consolidar capacidades para IT e OT, mellorar a integración entre ferramentas e habilitar respostas máis rápidas e automatizadas fronte ás ameazas, reducindo á vez a carga sobre equipos con recursos limitados.

En conxunto, estas recomendacións reforzan a idea de que a ciberseguridade OT efectiva require **visibilidade, integración e simplificación arquitectónica**, aliñadas cunha comprensión clara do risco e das limitacións operativas dos entornos industriais.

7.4 ISACA

Este apartado baséase nun artigo de opinión elaborado por un **experto certificado de ISACA**, publicado nos seus canais oficiais, pero que **non constitúe unha posición normativa nin oficial da asociación**.

A análise aborda a ciberseguridade industrial desde unha perspectiva de **gobernanza, xestión do risco e control**, complementaria ás guías máis técnicas. No artigo Common cybersecurity risks to ICS/OT systems, ISACA identifica un conxunto de riscos recorrentes en contornos industriais e formula recomendacións prácticas orientadas a reducir a súa probabilidade e impacto, tendo en conta as limitacións operativas propias de OT [47].

- **Establecer e manter un inventario completo de activos ICS/OT**: implantar procesos formais para identificar, clasificar e manter actualizado o inventario de sistemas, dispositivos, software e comunicacións OT, como base para a xestión do risco e a toma de decisións informadas.
- **Definir e gobernar adecuadamente a conectividade IT/OT:** deseñar arquitecturas claras, aplicar segmentación de rede e limitar as

interconexións ao estritamente necesario, asegurando que todas as conexións estean documentadas, controladas e monitorizadas.

- **Aplicar unha xestión rigorosa de identidades e accesos privilexiados:** implantar o principio de mínimo privilexio, eliminar contas compartidas, revisar periodicamente os accesos e empregar mecanismos de autenticación reforzada, incluíndo accesos de terceiros a contornos OT.
- **Adoptar unha xestión de vulnerabilidades e parches baseada en risco:** priorizar a corrección de vulnerabilidades segundo o impacto operativo e de seguridade, complementando o parcheado con controis compensatorios cando as limitacións técnicas ou operativas impidan a actualización inmediata.
- **Desenvolver capacidades específicas de resposta a incidentes ICS/OT:** elaborar e probar plans de resposta e recuperación adaptados a contornos industriais, garantindo a coordinación entre seguridade, operacións e dirección, e priorizando a seguridade física e a continuidade do servizo.
- **Impulsar unha cultura de ciberseguridade integrada na operación industrial**: establecer programas de formación e concienciación dirixidos a operadores, enxeñeiros e persoal de mantemento, reforzando a responsabilidade compartida na protección dos sistemas ICS/OT.

De novo subliñar a coincidencia en grande medida con recomendacións previas, como as do NCSC. En conxunto, ISACA recomenda tratar a ciberseguridade industrial como un **elemento de gobernanza e risco empresarial**, integrando persoas, procesos e tecnoloxía nun enfoque coherente e sostible.

7.5 Uso de IA en OT

A integración de capacidades de Intelixencia Artificial (IA) en contornos OT/ICS pode achegar melloras de eficiencia, mantemento preditivo, optimización operativa e apoio á toma de decisións. Porén, tamén introduce **novas superficies de ataque**, dependencias tecnolóxicas e riscos específicos (por exemplo, deriva do modelo, problemas de explicabilidade, novas vías de exfiltración de datos ou impactos sobre a seguridade funcional).

En xeral, podemos ver á luz deste informe da Cloud Security Alliance [49] como as organizacións aínda non están preparadas a nivel procedemental para o emprego regulado desta tecnoloxía emerxente:

Enquisa de políticas e guías para desenvolvemento e uso seguro da IA. Fonte: CSA (2025)

7.5.1 Integración segura de IA en OT

As seguintes recomendacións sintetizan, de xeito práctico e accionable, os **principios** recollidos na guía **Principles for the Secure Integration of Artificial Intelligence in Operational Technology** creado de forma coral por varios organismos internacionais de ciberseguridade [48], e estruturados nos **catro bloques** do propio documento. O reporte é denso, polo que se recomenda acudir á fonte para un entendemento exhaustivo.

7.5.1.1 Principio 1 — Comprender a IA

7.5.1.1.1 Comprender os riscos únicos da IA e o impacto potencial en OT

- **Tratar a IA como un compoñente ciberfísico**, avaliando impactos non só de confidencialidade, senón tamén de **dispoñibilidade e seguridade funcional** (paradas innecesarias, alarmística incorrecta, cambios de lóxica de control, etc.).
- **Anticipar riscos de calidade e centralización de datos**: os modelos dependen de datos de adestramento e operación (sensórica, telemetría, históricos). A dificultade de obter datos normalizados en OT e a tentación de centralizalos poden **incrementar o risco** e dar máis contexto ao adversario.
- **Considerar a deriva do modelo (model drift)**: cambios de proceso, condicións de operación ou equipamentos poden degradar a precisión co tempo; isto pode levar a **falsos positivos/negativos** e decisións operativas incorrectas.

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

- **Recoñecer limitacións de explicabilidade**: se non se entende por que o sistema recomenda unha acción, aumenta o tempo de recuperación e a complexidade de troubleshooting, e complica auditorías e cumprimento.

7.5.1.1.2 Comprender o ciclo de vida de desenvolvemento seguro dun sistema de IA

- **Exixir prácticas de seguridade "secure-by-design" e "secure-by-default"** para a IA, incluíndo requisitos de seguridade dende o deseño, validación e mantemento.
- **Incorporar ameazas específicas de IA ao modelado de ameazas**, como entradas adversariais e envelenamento de datos.
- **Validar e refinar modelos de forma continua en contornas simuladas/non produtivas** antes de despregamentos e cambios relevantes, para reducir risco operacional.

7.5.1.1.3 Formar ao persoal sobre IA

- **Capacitar a operadores, enxeñaría e seguridade** sobre como funciona a IA, os seus límites e os riscos máis relevantes en OT.
- **Reducir a dependencia e o "automation bias"**: establecer criterios para que o persoal cuestione recomendacións e saiba cando escalar, deter ou volver a operación manual.
- **Preparar ao persoal para interpretar erros e alarmas**: a IA pode incrementar carga cognitiva se xera alertas incorrectas; a formación debe incluír procedementos de verificación e reacción.

7.5.1.2 Principio 2 — Considerar o uso de IA no dominio OT

7.5.1.2.1 Considerar o caso de negocio OT para o uso de IA

- **Xustificar o uso por obxectivos OT reais** (seguridade, fiabilidade, continuidade, eficiencia), evitando despregamentos "por moda".
- **Aplicar unha decisión baseada en risco**: avaliar se os beneficios superan os novos riscos e custos (ciberseguridade, seguridade funcional, mantemento, dependencia do provedor).

7.5.1.2.2 Xestionar os riscos de seguridade dos datos OT para sistemas de IA

- **Protexer datos OT ao longo de todo o ciclo** (en repouso, en tránsito e en uso), porque a IA amplifica o valor e o volume de datos.

- **Aplicar control de acceso e cifrado**, e reforzar gobernanza de datos cando a IA consome datos sensibles ou operativos.
- **Minimizar exposición ao mover datos fóra de OT**: favorecer patróns de transferencia controlados e auditables (por exemplo, movemento "push" de resumos/atributos) fronte a accesos persistentes de entrada.

7.5.1.2.3 Comprender o rol dos provedores OT na integración de IA

- **Esixir evidencias de seguridade do provedor** (auditorías, avaliacións de risco, probas) e claridade contractual sobre responsabilidades.
- **Asegurar soporte e supervisión ao longo do ciclo de vida** (procura, deseño, despregamento, operación e mantemento), incluíndo cando o provedor participe na vixilancia ou actualización do modelo.

7.5.1.2.4 Avaliar retos na integración IA–OT

- **Planificar integración técnica e operativa** (protocolos, dependencias de versións, requisitos de infraestrutura, latencias, limitacións en tempo real).
- **Evitar que a IA se converta nunha "ponte" permanente cara OT**: manter segmentación e separación por zonas, e deseñar conectividade de forma minimizada e controlada.

7.5.1.3 Principio 3 — Establecer marcos de gobernanza e aseguramento da IA

7.5.1.3.1 Establecer mecanismos de gobernanza para IA en OT

- **Crear políticas, procedementos e estruturas de responsabilidade** para decisións e riscos asociados á IA.
- **Implicar stakeholders clave**: dirección (incluíndo CISO), expertos OT/IT/IA, equipos de ciberseguridade e provedores cando corresponda.
- **Implantar gobernanza de datos estrita** (cifrado, control de acceso e analítica de comportamento de usuario), e **definir roles e responsabilidades** para evitar confusión (e risco de responsabilidade) ante incidentes.
- **Realizar auditorías e probas de cumprimento regulares**, e **validación/verificación continua** do rendemento do sistema conforme a obxectivos e requisitos.

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

7.5.1.3.2 Integrar a IA nos marcos existentes de seguridade e ciberseguridade

- **Incorporar avaliacións da IA aos procesos actuais de risco, mitigación e monitorización**, incluíndo xestión de vulnerabilidades e requisitos regulatorios aplicables á infraestrutura crítica.
- **Aplicar controis robustos** (cifrado, control de acceso, detección de intrusións) e reforzar trazabilidade:
  - recoller logs do fluxo de datos e accesos dos endpoints de IA
  - controlar e monitorizar saídas de datos por activo e identidade
  - integrar con DLP para inspección de prompts e saídas cando aplique
- **Engadir intelixencia e modelado de ameaza específico de IA**: incorporar TTPs (Técnicas, Tácticas e Procedementos) relacionados con IA e empregar matrices/recursos orientados a IA cando se analicen escenarios.

7.5.1.3.3 Realizar probas e avaliación exhaustivas da IA

- **Comezar probas en infraestrutura de test**, permitindo iteracións rápidas (probas de baixa fidelidade ao inicio).
- **Evolucionar cara probas máis realistas en contornas non produtivas** (incluíndo hardware-in-the-loop cando aplique) antes de calquera paso a produción.
- **Evitar exposición de datos de produción en contornas non produtivas**, mantendo prácticas tradicionais de protección de datos.

7.5.1.3.4 Navegar consideracións regulatorias e de cumprimento para IA en OT

- **Recoñecer retos específicos**: ausencia de estándares orientados a OT, dificultade de auditoría/explicabilidade e encaixe con certificacións de seguridade.
- **Revisar estándares técnicos de IA aplicables e en evolución**, avaliando a súa pertinencia no dominio OT.
- **Validar continuamente que o rendemento cumpre requisitos estritos OT** (seguridade funcional e operación), e **definir limiares de degradación** para volver a operación sen IA cando as saídas non cumpran os niveis de seguridade/precisión.

7.5.1.4 Principio 4 — Integrar supervisión e prácticas de seguridade funcional e fallo seguro

7.5.1.4.1 Establecer mecanismos de monitorización e supervisión da IA en OT

- **Inventariar compoñentes de IA e dependencias asociadas** (o que depende do modelo e do seu output) como base para o control.
- **Rexistrar e monitorizar entradas e saídas**, e manter un **estado coñecido bo** (ou limiares de comportamento seguro) que permita detectar desviacións e decidir cando restaurar dende copia/backup.
- **Introducir á persoa ("human-in-the-loop") en decisións críticas**:
    - para sistemas pasivos, integrar recomendacións en procesos de xestión do cambio
    - para sistemas activos que afectan ao control, engadir puntos de intervención humana mediante limiares de seguridade, sinais alternativos ou cambios de estado
- **Revisar de forma regular con stakeholders** (operación, gobernanza e provedores) resultados, incidencias e melloras.
- **Actualizar modelos de ameaza e vixiar manipulación**: monitorizar anomalías, entradas adversariais e indicios de envelenamento, e refinar modelos con novos datos OT para reducir falsos positivos/negativos.
- **Explorar mecanismos de explicabilidade e transparencia** (XAI) cando sexa viable, priorizando a capacidade de auditoría e seguridade en OT.
- **Preservar segmentación mediante deseños de conectividade seguros**: favorecer arquitecturas "push"/brokered, e cando haxa transferencia a redes de negocio empregar patróns unidireccionais e buffers auditados, evitando camiños persistentes cara OT.

7.5.1.4.2 Integrar mecanismos "failsafe" e de recuperación segura

- **Establecer mecanismos de fallo seguro** para que a IA "falle adecuadamente" sen interromper operacións críticas.
- **Incorporar novos estados de fallo da IA** aos procesos existentes de seguridade funcional e resposta a incidentes, definindo como **bypassear, substituír ou retirar** o compoñente de IA.

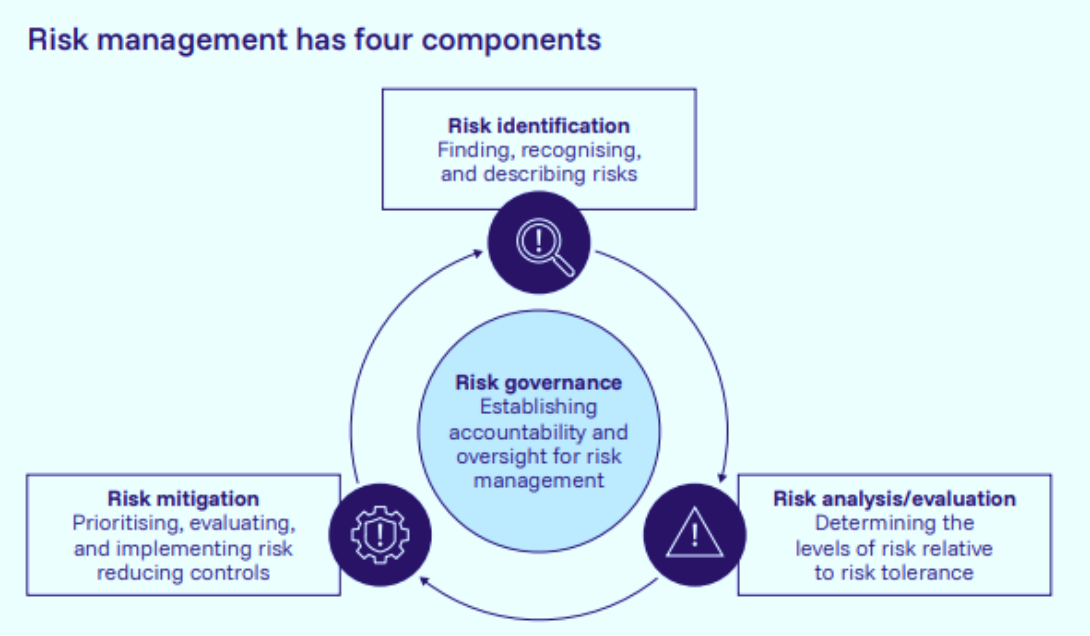
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

- **Deseñar procedementos de seguridade funcional que teñan en conta a IA**: adaptar estados e procedementos por sector para contemplar a integración e o uso seguro.
- **Actualizar o plan de resposta a incidentes** con pasos específicos para actividade maliciosa contra a IA e para fallos do sistema de IA, asumindo que o risco non pode reducirse a cero.

7.5.2 International AI Safety Report 2026

O **International AI Safety Report 2026** xa mencionado con anterioridade previamente é un informe internacional de síntese que recompila e organiza o coñecemento existente sobre capacidades, riscos e xestión do risco en IA de propósito xeral [23].

Como se pode apreciar, a metodoloxía que propoñen de xestión do risco en IA está aliñada coa visión canónica habitual.



Metodoloxía proposta para a xestión de riscos no uso da IA. Fonte: International AI Safety Report (2026)

A orientación do reporte é transversal (sociedade, economía, gobernanza e tecnoloxía) e non está escrita especificamente para OT/ICS. Por este motivo, a contribución a nivel de recomendacións que se incorpora neste informe é **parcial e selectiva**: céntrase unicamente nos elementos das seccións que poden ser máis afíns á **ciberseguridade industrial, ás infraestruturas críticas e aos sistemas ciberfísicos**, facendo una interpretación do informe a nivel de xestión do risco, para levalo ó terreo mais operativo. Para un tratamento completo e literal, recoméndase revisar a fonte orixinal.

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

7.5.2.1 Retos técnicos e institucionais

- **Tomar decisións con evidencia incompleta (dilema da evidencia)**: en ámbitos críticos (enerxía, auga, industria), pode ser necesario establecer controis e gobernanza antes de dispor de probas definitivas sobre capacidades e riscos futuros. Isto favorece enfoques de **precaución, escalado progresivo e revisión continua**.
- **Dificultade de avaliación e atribución**: os riscos asociados a IA poden ser difíciles de observar e medir en contornos reais, especialmente cando a IA se integra en cadeas longas (provedores → integradores → operadores). Isto reforza a necesidade de **trazabilidade, rexistro e compartición estruturada de información**.
- **Brechas de coordinación e incentivos**: cando existen múltiples actores, as responsabilidades poden diluírse. Para OT/ICS, isto tradúcese en reforzar **contratos, responsabilidades e mecanismos de aseguramento** ao longo da cadea de subministración.

7.5.2.2 Prácticas de xestión do risco

- **Transparencia e documentación de risco**: adoptar prácticas de documentación (informes de transparencia, rexistros de avaliación e mitigación, etc.) para soportar decisións e auditoría. En contornos industriais, isto é clave para demostrar **dilixencia debida** en sistemas que poden afectar seguridade e continuidade.
- **Notificación e xestión de incidentes**: integrar IA nos fluxos existentes de xestión de incidentes, incluíndo criterios de reporte, análise post-incidente e leccións aprendidas.
- **Compromiso da dirección e incentivos**: cultura, liderado e incentivos condicionan o éxito da mitigación. Para OT, isto implica que a integración de IA debe ter **patrocinio executivo**, responsabilidades claras e obxectivos que prioricen seguridade e resiliencia sobre só eficiencia.
- **"Safety cases" e análise de risco residual**: empregar enfoques estruturados (avaliación previa, mitigación, red teaming, análise de risco residual) antes e durante o despregue, particularmente en operacións críticas.

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

7.5.2.3 Salvagardas técnicas e monitorización

- **Defensa en profundidade como patrón de referencia**: as salvagardas deben combinarse por capas (procesos, avaliación, controis técnicos, monitorización), evitando depender dunha única medida.
- **Avaliación e *red teaming***: empregar probas adversariais e avaliacións para descubrir fallos antes do despregue e ante cambios relevantes. En OT, isto debe facerse en contornos de proba/simulación para non comprometer a operación.
- **Monitorización en produción e detección temperá**: asumir que as medidas poden fallar e, por tanto, reforzar a monitorización, a detección de anomalías e os mecanismos de resposta.
- **Limitacións da verificación formal en produción**: o informe indica que certas técnicas avanzadas (p.ex. verificación formal) aínda teñen adopción limitada en sistemas reais; en consecuencia, convén priorizar combinacións pragmáticas de **avaliación + monitorización + contención**.

7.5.2.4 Modelos de pesos abertos (open-weight)

Os **modelos open-weight** son modelos de IA cuxos **pesos (parámetros aprendidos)** se publican e poden descargarse para **executalos e modificalos localmente**, sen depender do provedor orixinal. A este respecto, sínalase o seguinte:

- **Equilibrar beneficios e riscos**: os modelos de pesos abertos facilitan investigación e innovación, pero tamén poden permitir a eliminación máis doada de salvagardas e dificultan a monitorización do seu uso.
- **Risco de modificación maliciosa**: o informe sinala que actores maliciosos poden axustar modelos para usos daniños, retirar mecanismos de seguridade ou desfacer axustes de seguridade previos.
- **Risco herdado na integración**: os desenvolvedores e operadores que integran modelos open-weight herdan posibles debilidades (incluíndo vulnerabilidades a ataques adversariais) e poden ter máis difícil distribuír correccións de forma universal.
- **Implicación para OT/ICS**: cando se empreguen modelos open-weight en casos con impacto operacional, recoméndase reforzar:
    - avaliación previa e probas adversariais,

- control de actualizacións e versións,
- illamento e limitación de privilexios,
- e unha estratexia de reversión/retirada rápida.

7.5.2.5 Construír resiliencia social

- **Resiliencia como complemento ás salvagardas**: o informe define resiliencia como a capacidade de resistir, absorber, recuperar e adaptarse a shocks e danos; subliña que algunhas fallas emerxen só en despregamentos reais e poden ter efectos en cadea.
- **Resiliencia aplicada a infraestrutura crítica**: para contornos industriais, isto tradúcese en fortalecer capacidades de:
  - continuidade operativa e recuperación,
  - coordinación público-privada,
  - compartición de información en tempo real,
  - e exercicios/escenarios de crise.
- **A IA tamén pode reforzar a defensa**: o informe menciona usos defensivos como detección de anomalías a gran escala, clasificación de malware e prevención de phishing. En contornos OT, estes usos deben implementarse con gobernanza, control de datos e supervisión, para non crear novas dependencias fráxiles.
- **Xestión do equilibrio ofensiva-defensiva**: recoñécese que mellorar capacidades defensivas con IA pode ter efectos secundarios (aceleración de capacidades ofensivas). Para operadores industriais, isto reforza a importancia de **avaliación continua**, segmentación e deseño para contención.

8 Conclusións

O presente **Informe de riscos tecnolóxicos** confirma unha realidade xa observada noutros entregables do Observatorio: a progresiva dixitalización industrial e a converxencia IT/OT incrementan de forma sostida a superficie de exposición, mentres a ameaza evoluciona cara a modelos mais rápidos, mais automatizados e cunha orientación crecente ao **impacto operativo**. A consecuencia práctica é clara: en contornos OT/ICS, a ciberseguridade debe formularse como **xestión do risco ciberfísico**, onde dispoñibilidade e seguridade funcional condicionan que controis son viables, cando poden implantarse e como se verifica a súa eficacia.

Desde unha perspectiva estratéxica, o informe mostra que **o risco non é exclusivamente tecnolóxico**. Factores sistémicos —como a **tensión xeopolítica, a dependencia de cadeas de subministración e a concentración de provedores**— amplifican a exposición e dificultan a recuperación cando se produce un incidente. Este contexto reforza a **necesidade de integrar a ciberseguridade industrial na gobernanza corporativa e institucional**, asumindo que o risco é **transfronteirizo** e que a resiliencia require coordinación con terceiros e co ecosistema.

No plano operativo, os patróns recorrentes que explican boa parte dos incidentes son coñecidos e, por tanto, mitigables: falta de visibilidade e inventario, conexións excesivas, accesos remotos insuficientemente controlados, xestión desigual de vulnerabilidades e unha integración incompleta de OT nos procesos de detección e resposta. Isto suxire unha prioridade inequívoca: antes de adoptar capacidades "avanzadas", **cómpre consolidar unha base defensiva sólida baseada en segmentación, control estrito de conectividade, autenticación e privilexios, monitorización e capacidade de contención.**

A incorporación de **Intelixencia Artificial introduce un cambio cualitativo**. Por unha banda, pode reforzar capacidades defensivas e operativas; por outra, **habilita novas ameazas (automatización de recoñecemento e explotación, *phishing* máis efectivo) e engade riscos por fallos de funcionamento e riscos sistémicos**. En particular, o informe salienta dous puntos de atención: a **necesidade de gobernanza e supervisión** (para evitar decisións opacas ou degradación silenciosa do rendemento) e o **risco organizativo asociado á Shadow AI**, que pode provocar filtración de información sensible e dependencias tecnolóxicas non avaliadas.

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

As recomendacións sintetizadas ao longo do documento converxen nunha mensaxe común: **a mitigación eficaz do risco en OT/ICS require un enfoque de defensa en profundidade e unha aplicación disciplinada de controis, priorizados en función do risco e adaptados ás restricións da planta**. Isto inclúe coñecer e documentar o contorno (rexistro definitivo), reducir exposición (eliminar conexións innecesarias e endurecer acceso remoto), limitar propagación (segmentación e illamento), mellorar detección (monitorización e correlación adaptadas a OT) e asegurar recuperación (operación manual, plans de illamento, continuidade e probas regulares).

No caso específico da IA en OT, o informe conclúe que a adopción debe seguir unha lóxica de caso de negocio + risco, apoiada en principios de integración segura (formación, ciclo de vida seguro, protección de datos OT, gobernanza, probas rigorosas e mecanismos para fallar de xeito seguro). De maneira complementaria, a visión do International AI Safety Report reforza a necesidade de **combinar salvagardas técnicas con prácticas de xestión do risco** (transparencia, avaliación adversarial, monitorización en produción e resiliencia), prestando especial atención aos modelos open-weight cando se integren en ámbitos con impacto operacional.

Finalmente, este informe pecha cunha **conclusión de carácter programático: a mellora da ciberseguridade industrial é un proceso continuo que require coherencia entre persoas, procesos e tecnoloxía.** O valor do Observatorio reside precisamente en facilitar esa coherencia mediante intelixencia compartida, seguimento de alertas e vulnerabilidades, orientación normativa e síntese de boas prácticas accionables, entre outras. En consecuencia, **recoméndase empregar este documento como base de priorización e complementalo cos demais entregables (ciberalertas, intelixencia de ameazas, guía normativa ou tendencias)** para **converter a análise en planificación e acción sostible.**

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

Bibliografía

[1] World Economic Forum (WEG) (1971). *Sitio web oficial do Foro Económico Mundial.* Recuperado de https://www.weforum.org/

[2] World Economic Forum (2025). *Global Risks Report 2025.* Recuperado de https://www.weforum.org/publications/global-risks-report-2025/

[3] Nozomi Networks (2025). *OT Cybersecurity Risk Management for CISOs*. Recuperado de https://www.nozominetworks.com/blog/ot-cybersecurity-risk-management-for-cisos

[4] Observatorio de Ciberseguridade Industrial de Galicia (2025). *Informes de Ciberalertas e Intelixencia de Ameazas.* Recuperados de https://ciberseguridadegalicia.gal/es

[5] Google Cloud Threat Intelligence (2024). *Cybersecurity Forecast 2025*. Recuperado de https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025

[6] Google Cloud (2025). *Cybersecurity Forecast 2026*. Recuperado de https://services.google.com/fh/files/misc/cybersecurity-forecast-2026-en.pdf

[7] Escudo Digital (2025). *Un ciberataque logra hackear unha presa e deixala aberta durante horas*. Recuperado de https://www.escudodigital.com/ciberseguridad/un-ciberataque-logra-hackear-una-presa-y-dejarla-abierta-durante-horas.html

[8] ISMS Forum (2025). *13º Estudo do Estado da Arte da Seguridade na Nube*. Recuperado de https://www.ismsforum.es/ficheros/descargas/291225sotafinal1767006346.pdf

[9] Acuvity (2026). *The ClawDBot Dumpster Fire: 72 Hours That Exposed Everything Wrong With AI Security*. Recuperado de https://acuvity.ai/the-clawdbot-dumpster-fire-72-hours-that-exposed-everything-wrong-with-ai-security/

[10] INCIBE-CERT (2023). *¿Que esperar da ciberseguridade industrial en 2023?* Recuperado de https://www.incibe.es/incibe-cert/blog/que-esperar-de-la-ciberseguridad-industrial-en-2023

[11] Dragos (2025). *New Dragos Report Estimates Over $300 Billion in Potential Global OT Cyber Risk Exposure*. Recuperado de https://www.dragos.com/resources/press-

release/new-dragos-report-estimates-over-300-billion-in-potential-global-ot-cyber-risk-exposure

[12] Dragos (2025). *2025 OT Security Financial Risk Report*. Recuperado de https://www.dragos.com/2025-ot-security-financial-risk-report

[13] SANS Institute (2022). *Five ICS Cybersecurity Critical Controls*. Recuperado de https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

[14] Ciberseguridade Galicia - AMTEGA (2026). Portal oficial de ciberseguridade de Galicia. Recuperado de https://ciberseguridadegalicia.gal/gl

[15] McMahan, E. e Scott, L.-M. (2025). *Billions at Stake: The Growing Financial Impact of Operational Technology Cyber Risk*. Recuperado de https://www.policyholderperspective.com/post/102lp90/billions-at-stake-the-growing-financial-impact-of-operational-technology-cyber-r

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

[17] Fortinet (2025). *State of Operational Technology and Cybersecurity*. Recuperado de https://www.fortinet.com/resources/reports/state-ot-cybersecurity

[18] Fortinet (2025). *Fortinet Report: OT Cybersecurity Risk Elevates Within Executive Leadership Ranks*. Recuperado de https://www.fortinet.com/tw/corporate/about-us/newsroom/press-releases/2025/fortinet-report-ot-cybersecurity-risk-elevates-within-executive-leadership-ranks

[19] National Cyber Security Centre (NCSC) (2016). *National Cyber Security Centre — Sitio web oficial*. Recuperado de https://www.ncsc.gov.uk/

[20] National Cyber Security Centre (NCSC) (2025). *Impact of AI on cyber threat from now to 2027*. Recuperado de https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

[21] Wikipedia (2025). *Yoshua Bengio*. Recuperado de https://es.wikipedia.org/wiki/Yoshua_Bengio

[22] International AI Safety Report (2026). *International AI Safety Report — Sitio web oficial*. Recuperado de https://internationalaisafetyreport.org/

[23] International AI Safety Report (2026). *International AI Safety Report 2026*. Recuperado de https://internationalaisafetyreport.org/sites/default/files/2026-02/international-ai-safety-report-2026.pdf

[24] Industrial Cyber (2025). *OT cybersecurity reporting remains a structural weakness as threats outpace legacy governance models*. Recuperado de https://industrialcyber.co/features/ot-cybersecurity-reporting-remains-a-structural-weakness-as-threats-outpace-legacy-governance-models/

[25] Brotby, K. (2009). *Information Security Governance: A Practical Development and Implementation Approach*. Wiley.

[26] Calder, A. e Watkins, S. (2015). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. Kogan Page Publishers.

[27] Davies, J. (2016). *Performing Information Governance: A Step-by-step Guide to Making Information Governance Work*. IBM Press.

[28] Gentile, M., Collette, R. e D. August, T. (2005). *The CISO Handbook: A Practical Guide to Securing Your Company*. CRC Press. Recuperado de https://www.amazon.es/CISO-Handbook-Protecting-Facilities-Information/dp/0849319528

[29] NIST (2024). *O NIST publica a versión 2.0 do seu marco histórico de ciberseguridade*. Recuperado de https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[30] NIST (2024). *NIST Cybersecurity Framework, versión 2.0*. Recuperado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[31] Observatorio de Ciberseguridade Industrial de Galicia (2025). *Guía normativa de ciberseguridade industrial*. Recuperados de https://ciberseguridadegalicia.gal/es

[32] Center for Internet Security (CIS) (2000). *CIS Benchmarks™ – Guías de boas prácticas para a configuración segura de sistemas*. Recuperado de: https://www.cisecurity.org/cis-benchmarks

[33] Center for Internet Security (CIS) (2008). *CIS Critical Security Controls® – Controis prioritarios de ciberseguridade*. Recuperado de: https://www.cisecurity.org/controls

[34] National Cyber Security Centre (NCSC) (2016). *Guidance and best practices for industrial and operational technology security*. Recuperado de: https://www.ncsc.gov.uk

[35] Cybersecurity and Infrastructure Security Agency (CISA) (2018). *Industrial Control Systems Cybersecurity Guidance*. Recuperado de: https://www.cisa.gov/ics

[36] ISACA (Information Systems Audit and Control Association) (1969). *Sitio oficial*. Recuperado de: https://www.isaca.org

[37] Cybersecurity and Infrastructure Security Agency (CISA); Australian Cyber Security Centre (ACSC) (2025). *Principles for the Secure Integration of Artificial Intelligence in Operational Technology.* Recuperado de: https://www.cisa.gov/resources-tools/resources/principles-secure-integration-artificial-intelligence-operational-technology

[38] National Security Agency (NSA) (1952). *Sitio oficial*. Recuperado de: https://www.nsa.gov

[39] Canadian Centre for Cyber Security (2018). *Sitio oficial*. Recuperado de: https://www.cyber.gc.ca

[40] Bundesamt für Sicherheit in der Informationstechnik (BSI) (1991). *Sitio oficial*. Recuperado de: https://www.bsi.bund.de

[41] National Cyber Security Centre Netherlands (NCSC-NL) (2012). *Sitio oficial*. Recuperado de: https://www.ncsc.nl

[42] National Cyber Security Centre New Zealand (NCSC-NZ) (2011). *Sitio oficial*. Recuperado de: https://www.ncsc.govt.nz

[43] National Cyber Security Centre (NCSC) (2025). *Understanding your OT environment: the first step to stronger cyber security*. Recuperado de: https://www.ncsc.gov.uk/blog-post/understanding-ot-environment-1step-stronger-cyber-security

[44] National Cyber Security Centre (NCSC) (2024). *Operational Technology – Collection of guidance*. Recuperado de: https://www.ncsc.gov.uk/collection/operational-technology

[45] National Cyber Security Centre (NCSC) (2023). *Cloud Security – Collection of guidance*. Recuperado de: https://www.ncsc.gov.uk/collection/cloud

[46] Cybersecurity and Infrastructure Security Agency (CISA) (2025). *Primary Mitigations to Reduce Cyber Threats to Operational Technology*. Recuperado de: https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

[47] ISACA. (2023). *Common cybersecurity risks to ICS/OT systems*. Recuperado de: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/common-cybersecurity-risks-to-ics-ot-systems

[48] CISA (2025). *Principles for the Secure Integration of Artificial Intelligence in Operational Technology*. Recuperado de https://www.cisa.gov/resources-tools/resources/principles-secure-integration-artificial-intelligence-operational-technology

[49] Cloud Security Alliance. (2024). *The State of AI Security and Governance*. Recuperado de: https://cloudsecurityalliance.org/artifacts/the-state-of-ai-security-and-governance

Glosario

ACSC (Australian Cyber Security Centre)

Centro nacional de ciberseguridade de Australia. Publica guías e avisos, e colabora con outras axencias internacionais na definición de boas prácticas, incluíndo recomendacións para integrar IA e seguridade en contornos OT.

AIPD / EIPD (Avaliación de Impacto na Protección de Datos)

Análise sistemática para identificar e mitigar riscos sobre a privacidade e os dereitos das persoas ao tratar datos persoais, especialmente cando se empregan tecnoloxías ou tratamentos de alto risco.

AMTEGA (Axencia para a Modernización Tecnolóxica de Galicia)

Organismo da Xunta de Galicia responsable da modernización tecnolóxica e da coordinación de iniciativas de ciberseguridade no ámbito autonómico.

Antimalware

Conxunto de mecanismos e solucións para detectar, bloquear e eliminar software malicioso en endpoints, servidores ou pasarelas.

Auditoría interna

Función independente que verifica a eficacia dos controis e procesos de seguridade e cumprimento, avaliando evidencias e recomendando melloras.

Bastionado (hardening)

Proceso de endurecemento dun sistema mediante configuración segura, desactivación de servizos innecesarios e aplicación de boas prácticas para reducir a superficie de ataque.

Biometría

Método de autenticación baseado en características físicas ou comportamentais (p.ex. impresión dixital). Úsase como factor adicional cando é compatible e está ben gobernado.

BSI (Bundesamt für Sicherheit in der Informationstechnik)

Axencia federal alemá de seguridade da información. Publica guías e orientacións técnicas, incluíndo contidos sobre seguridade e risco en tecnoloxías emerxentes.

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

CAB (Change Advisory Board)

Comité ou órgano de xestión do cambio que revisa e aproba cambios en sistemas, especialmente relevante en OT para equilibrar continuidade operativa, seguridade e seguridade funcional.

Cadea de subministración

Conxunto de provedores, integradores e dependencias tecnolóxicas que poden introducir risco (vulnerabilidades, accesos, software/firmware) en sistemas industriais.

C2M2 (Cybersecurity Capability Maturity Model)

Modelo de madurez para avaliar e mellorar capacidades de ciberseguridade, especialmente útil para planificar evolución por fases.

CER (Critical Entities Resilience)

Marco regulatorio europeo orientado a reforzar a resiliencia de entidades críticas fronte a riscos, incluíndo aqueles con compoñente tecnolóxico e ciberfísico.

CERT (Computer Emergency Response Team)

Equipo especializado na xestión e coordinación de incidentes, análise técnica e emisión de alertas e recomendacións.

CCN-CERT

Centro de resposta a incidentes do Centro Criptolóxico Nacional (España). Publica guías e avisos, e coordina a resposta a incidentes no ámbito público e sectores vinculados.

CCN-STIC

Serie de guías técnicas do CCN-CERT (España) para apoiar a implantación de controis, cumprimento e boas prácticas de seguridade.

CIO (Chief Information Officer)

Responsable executivo de tecnoloxía da información. En contornos con converxencia TI–OT, é clave para aliñar arquitectura, operación e investimentos con requisitos de seguridade.

CISA (Cybersecurity and Infrastructure Security Agency)

Axencia federal dos EUA que publica guías e avisos para infraestruturas críticas, incluíndo mitigacións primarias para reducir ameazas en contornos OT.

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

CIS (Center for Internet Security)

Organización que publica Benchmarks e Controls (Controis CIS), amplamente empregados como referencia de boas prácticas e liñas base de configuración.

CISO (Chief Information Security Officer)

Responsable executivo de seguridade da información e ciberseguridade. Coordina estratexia, risco, controis e resposta a incidentes, incluíndo a integración TI–OT cando aplica.

ClawDBot / Moltbot

Exemplo de ferramenta baseada en IA difundida de forma viral, asociada ao risco de Shadow Tech cando se adoptan solucións sen gobernanza nin salvagardas.

Cloud

Modelo de provisión de servizos TIC baixo demanda (infraestrutura, plataformas ou aplicacións). En OT pode introducir novas dependencias e riscos de conectividade, datos e responsabilidade compartida.

COO (Chief Operating Officer)

Responsable executivo de operacións. En industria, é un stakeholder crítico porque os incidentes cibernéticos poden impactar directamente a continuidade e o rendemento operativo.

Conectividade OT

Conxunto de conexións e fluxos de comunicación dentro do sistema OT e entre OT e outros dominios (p.ex. IT, terceiros). A súa minimización e control son críticos para reducir exposición.

CRA (Cyber Resilience Act)

Regulamento europeo para mellorar a ciberresiliencia de produtos con elementos dixitais, esixindo seguridade por deseño e por defecto e obrigas ao longo do ciclo de vida.

CSIRT (Computer Security Incident Response Team)

Equipo de resposta a incidentes (sinónimo próximo a CERT), centrado en detección, análise, contención e coordinación da recuperación.

CSA (Cloud Security Alliance)

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

Organización internacional centrada en boas prácticas de seguridade na nube e gobernanza asociada, incluíndo análises sobre seguridade e gobernanza de IA.

CSET (Cyber Security Evaluation Tool)

Ferramenta de avaliación (CISA) para analizar postura de ciberseguridade e controis, utilizada como apoio a diagnósticos e melloras, incluíndo ámbitos industriais.

DDoS (Distributed Denial of Service)

Ataque distribuído de denegación de servizo que busca saturar servizos ou redes para provocar indispoñibilidade.

Defensa en profundidade

Estratexia que combina múltiples capas de controis (organizativos, físicos e técnicos) para previr, detectar e mitigar ataques, evitando depender dun único mecanismo.

Directorio Activo (Active Directory)

Servizo de directorio de Microsoft para xestionar identidades, grupos e políticas. Úsase habitualmente como base para SSO, LDAP e gobernanza de accesos.

DMZ (Zona desmilitarizada)

Zona intermedia de rede para expor servizos controlados e separar dominios (p.ex. IT e OT), reducindo risco de acceso directo a sistemas críticos.

DLP (Data Loss Prevention)

Controis e ferramentas para previr exfiltración ou fuga de datos, mediante políticas, inspección de contido e control de canles de saída.

DoS (Denial of Service)

Ataque de denegación de servizo que busca interromper a dispoñibilidade dun sistema ou servizo, normalmente por saturación de recursos.

DPO (Data Protection Officer)

Delegado/a de Protección de Datos, responsable de asesorar e supervisar cumprimento en materia de protección de datos e privacidade.

EDR (Endpoint Detection and Response)

Capacidade de detección e resposta en endpoints mediante telemetría, análise e accións de contención, útil tamén en contornas híbridas TI/OT cando é compatible.

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

ENISA

Axencia da Unión Europea para a Ciberseguridade. Publica orientación, informes e recomendacións para mellorar capacidades e resiliencia a nivel europeo.

ENS (Esquema Nacional de Seguridade)

Marco español que establece principios e requisitos para protexer información e servizos no sector público e entidades vinculadas, con impacto sobre gobernanza e controis.

Envelenamento de datos

Ataque contra sistemas de IA que introduce ou modifica datos para degradar o rendemento do modelo ou inducir saídas incorrectas, con risco operativo en OT.

Entradas adversariais

Técnicas que manipulan entradas a un modelo de IA para provocar erros de clasificación ou comportamento non desexado, mesmo sen modificar o modelo.

ERP (Enterprise Resource Planning)

Sistemas corporativos de planificación e xestión (finanzas, compras, loxística, produción) cuxo compromiso pode paralizar operación industrial ao romper fluxos de datos e procesos.

Escala Likert

Escala de valoración por niveis (p.ex. 1–7) empregada en enquisas para estimar percepcións de severidade, probabilidade ou impacto.

Failsafe

Deseño de fallo seguro: mecanismos para que un sistema pase a un estado seguro ante erros, anomalías ou perda de confianza, priorizando continuidade e seguridade funcional.

Formación e concienciación

Programa de capacitación e sensibilización para reducir erros humanos, mellorar prácticas e reforzar cultura de seguridade, clave tamén en OT.

GCHQ (Government Communications Headquarters)

Organismo británico de intelixencia e seguridade, no que se integra o NCSC como autoridade técnica en ciberseguridade.

GRC (Goberno, risco e cumprimento)

Disciplina que integra gobernanza, xestión do risco e cumprimento normativo. En OT/ICS abrangue risco tecnolóxico, provedores, políticas, métricas e reporte.

HIDS (Host-based Intrusion Detection System)

Sistema de detección de intrusións a nivel de host que supervisa eventos e integridade local para identificar actividade sospeitosa.

HMI (Human-Machine Interface)

Interface home-máquina usada por operadores para supervisar e controlar procesos industriais. A súa protección é crítica pola visibilidade e control que proporciona.

IAM (Identity and Access Management)

Goberno e xestión do ciclo de vida de identidades, autenticación e autorización, incluíndo provisión, modificación e retirada de accesos.

IA (Intelixencia Artificial)

Conxunto de técnicas que permiten a sistemas realizar tarefas cognitivas (análise, predición, xeración). En OT pode aportar eficiencia, pero tamén introduce novos riscos.

IA xenerativa

Subcampo da IA capaz de xerar texto, imaxes ou código. Pode mellorar produtividade, pero tamén facilitar fraude, *phishing* e filtración de información (incluíndo Shadow AI).

IACS (Industrial Automation and Control Systems)

Termo equivalente/próximo a ICS, centrado en automatización e control industrial e nos seus compoñentes e interdependencias.

ICS (Industrial Control Systems)

Conxunto de sistemas e dispositivos empregados para monitorizar e controlar procesos industriais, incluíndo PLC, SCADA e HMI.

ICS-CERT

Denominación empregada por certos equipos/capacidades especializadas en resposta e análise en contornos ICS; no informe tamén aparece como referencia a telemetría e informes sectoriais.

IEC 62443 (ISA/IEC 62443)

Conxunto de estándares internacionais para seguridade de sistemas de automatización e control industrial, con enfoque por requisitos e niveis de seguridade.

INCIBE-CERT
Equipo de resposta a incidentes e emisión de alertas do INCIBE (Instituto Nacional de Ciberseguridade de España), con contidos específicos para ciberseguridade industrial.

Infostealer
Tipo de malware orientado ao roubo de información (credenciais, cookies, datos) que pode facilitar acceso inicial e movemento lateral.

Integración IT/OT (converxencia TI–OT)

Proceso polo que sistemas de operación industrial se conectan ou interaccionan con sistemas corporativos, aumentando eficiencia pero tamén superficie de ataque.

IoC (Indicadores de compromiso)

Evidencias técnicas dun posible compromiso (hashes, IPs, dominios, rutas, patróns de log) usadas para detección e resposta a incidentes.

IP (Internet Protocol)

Protocolo base de comunicación en redes. A súa xestión e segmentación é relevante para controlar conectividade e exposición de sistemas OT.

IDS (Intrusion Detection System)

Sistema de detección de intrusións que monitoriza tráfico ou eventos para identificar actividade maliciosa; pode existir en rede (NIDS) ou en host (HIDS).

ISACA
Asociación internacional de profesionais de auditoría, risco e seguridade. Publica orientación e análise desde unha óptica de gobernanza e control.

ISMS / SXSI (Sistema de Xestión da Seguridade da Información)
Conxunto de políticas, procesos e controis para xestionar a seguridade da información de forma sistemática e auditable, normalmente aliñado con ISO/IEC 27001.

ISO/IEC 27001

Estándar internacional para sistemas de xestión de seguridade da información (ISMS), que define requisitos para gobernanza, controis e mellora continua.

ISO27002

Código de boas prácticas asociado a ISO/IEC 27001 que detalla controis recomendados para a seguridade da información.

IPS (Intrusion Prevention System)

Sistema de prevención de intrusións que, ademais de detectar, pode bloquear ou mitigar tráfico malicioso en tempo real.

LDAP (Lightweight Directory Access Protocol)

Protocolo para acceso a servizos de directorio (identidades, grupos, permisos). Útil para centralizar autenticación e autorización en contornas con múltiples aplicacións.

LOPD-GDD

Lei Orgánica española de Protección de Datos e garantía dos dereitos dixitais, complementaria ao RGPD e relevante para tratamentos e gobernanza de datos.

MAC (Media Access Control)

Identificador dunha interface de rede. Pode empregarse en políticas de rede e control de acceso, aínda que non é un control de seguridade suficiente por si só.

Malware

Software malicioso deseñado para danar, interromper ou comprometer sistemas (p.ex. ransomware, infostealers).

MFA (Multi-Factor Authentication)

Autenticación multifactor que combina dous ou máis factores (contrasinal + token/OTP, biometría, certificado), reducindo risco por roubo de credenciais.

Mínimo privilexio

Principio polo que as contas e procesos deben ter só os permisos imprescindibles para a súa función, limitando o impacto dun compromiso.

Modelado de ameazas

Proceso de identificar activos, superficies de ataque, ameazas e mitigacións dun sistema, para deseñar controis de forma preventiva.

Model drift (deriva do modelo)

Degradación progresiva do rendemento dun sistema de IA debido a cambios nos datos, proceso ou contorno, podendo causar decisións incorrectas en OT.

Modelos de pesos abertos (open-weight)

Modelos de IA cuxos pesos se publican e poden executarse/modificarse localmente, o que facilita innovación pero tamén pode permitir retirar salvagardas e incrementar risco.

Monitorización

Recollida e análise continua de eventos e tráfico para detectar anomalías, compromisos e degradacións, adaptada ás particularidades de OT/ICS.

NCSC (National Cyber Security Centre, UK)

Centro nacional británico de ciberseguridade (parte de GCHQ) que publica guías prácticas para OT, conectividade segura e arquitectura.

NCSC-NL (National Cyber Security Centre Netherlands)

Centro nacional de ciberseguridade dos Países Baixos. Publica guías e participa en iniciativas internacionais, incluíndo recomendacións de seguridade en IA.

NCSC-NZ (National Cyber Security Centre New Zealand)

Centro nacional de ciberseguridade de Nova Zelandia. Emite guías e participa en colaboracións internacionais en materia de ciberseguridade e IA.

NDR (Network Detection and Response)

Capacidades para detectar e responder a actividade maliciosa en rede mediante análise de tráfico e comportamento.

NIS / NIS2

Directivas europeas sobre seguridade de redes e sistemas de información. NIS2 reforza requisitos de xestión do risco, reporte de incidentes e cadea de subministración.

NIST

Instituto Nacional de Estándares e Tecnoloxía (EUA). Publica estándares e guías de referencia en seguridade, incluíndo orientación para sistemas industriais.

NIST CSF (Cybersecurity Framework)

Marco de boas prácticas de NIST estruturado en funcións (identificar, protexer, detectar, responder, recuperar) para xestión do risco de ciberseguridade.

NIST SP 800-82

Guía de NIST para seguridade de sistemas de control industrial, con recomendacións específicas para arquitectura, riscos e controis en OT/ICS.

NSA (National Security Agency)

Axencia estadounidense con papel destacado en seguridade e criptografía; participa en colaboracións internacionais sobre recomendacións e boas prácticas de seguridade.

Operación manual

Capacidade de operar procesos industriais mediante procedementos manuais cando sistemas dixitais fallan ou se consideran non fiables, clave para continuidade e seguridade funcional.

OT (Operational Technology)

Sistemas e dispositivos que monitorizan e controlan procesos físicos. Prioriza dispoñibilidade e seguridade operacional fronte a confidencialidade.

OTP (One-Time Password)

Contrasinal dun só uso empregado como segundo factor en autenticación, normalmente xerado por token, app ou hardware.

Passkey

Mecanismo de autenticación moderno baseado en criptografía de clave pública (xeralmente FIDO2/WebAuthn) que reduce dependencia de contrasinais reutilizables.

PAW (Privileged Access Workstation)

Estación de traballo privilexiada e endurecida para tarefas administrativas sensibles, destinada a protexer credenciais e accións de alto impacto.

Parcheado virtual (virtual patching)

Medida compensatoria que bloquea explotacións a nivel de rede ou aplicación (p.ex. IPS/WAF) cando non é viable aplicar o parche no activo vulnerable de inmediato.

PCE-NIS2 (CCN-STIC 892)

Guía do CCN-CERT que actúa como apoio práctico ao cumprimento de NIS2 en España, axudando a mapear obrigas a medidas e evidencias.

PCN (Plan de Continuidade de Negocio)

Plan que define servizos prioritarios, tarefas, responsables e procedementos para manter/restaurar operación tras incidentes disruptivos.

Phishing

Técnica de enxeñaría social que busca enganar ás persoas para obter credenciais ou executar accións maliciosas, relevante como vector inicial que pode afectar OT por converxencia.

PIC (Lei de Protección de Infraestruturas Críticas)

Normativa española orientada á protección e planificación de seguridade de infraestruturas críticas, reforzando coordinación e obrigas para garantir continuidade de servizos esenciais.

PLC (Programmable Logic Controller)

Controlador lóxico programable empregado para automatizar procesos industriais. A súa indispoñibilidade ou modificación pode ter impacto operativo e físico.

Playbook

Procedemento operativo (frecuentemente en SecOps/SOC) que define pasos de resposta a alertas ou incidentes, facilitando actuación consistente e reproducible.

Privacidade

Conxunto de principios e medidas para garantir un tratamento adecuado de datos persoais, minimizando riscos legais e reputacionais.

Prompt injection (inxección de instrucións)

Ataque que manipula un sistema de IA para ignorar limitacións e executar instrucións do atacante, podendo causar exfiltración ou recomendacións perigosas.

RBAC (Role-Based Access Control)

Modelo de control de acceso baseado en roles, asignando permisos por función e facilitando mínimo privilexio e segregación de funcións.

Ransomware

Malware que cifra sistemas ou datos para extorsionar mediante rescate; en OT pode provocar paradas e impactos económicos significativos.

Resiliencia (ciberresiliencia)

Capacidade de resistir, absorber, recuperar e adaptarse tras incidentes. En OT inclúe contención, operación manual, continuidade e recuperación probada.

RGPD

Regulamento Xeral de Protección de Datos da UE, marco principal de privacidade e protección de datos persoais.

ROI (Return on Investment)

Indicador que estima o retorno dun investimento. En ciberseguridade OT úsase para xustificar medidas, aínda que require modelos que capten impacto por indispoñibilidade e risco ciberfísico.

RPO (Recovery Point Objective)

Obxectivo de punto de recuperación: cantidade máxima de perda de datos aceptable medida no tempo, clave no deseño de copias de seguridade.

RTO (Recovery Time Objective)

Obxectivo de tempo de recuperación: tempo máximo aceptable para restaurar un servizo tras un incidente, determinando prioridades e recursos.

SaaS (Software as a Service)

Modelo cloud no que aplicacións se consumen como servizo. Pode acelerar Shadow Tech e introducir riscos de datos e dependencia de terceiros.

SANS

Organización de formación e investigación en seguridade que publica guías e recomendacións, incluíndo contidos específicos para sistemas industriais.

SCADA (Supervisory Control and Data Acquisition)

Sistema para supervisión e control a nivel de planta ou infraestrutura distribuída, agregando telemetría e permitindo operación remota.

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

SecOps

Integración de seguridade nas operacións diarias (detección, resposta, automatización), buscando coordinación entre equipos e ciclos de mellora continua.

Segregación de funcións

Principio que separa responsabilidades críticas (p.ex. aprobación, execución, revisión) para reducir risco de abuso e erros.

Seguridade funcional (safety)

Disciplina orientada a garantir que sistemas industriais operan de forma segura e previsíbel, reducindo risco de danos físicos; debe considerarse xunto á ciberseguridade.

Segmentación de rede

División dunha rede en segmentos/zonas con políticas de acceso e filtrado para limitar movemento lateral e reducir impacto dun compromiso.

Shadow AI

Uso de tecnoloxía e/ou ferramentas de IA fóra da gobernanza formal (sen aprobación nin controis), incrementando risco de filtración de datos e exposición indirecta de OT.

SIEM (Security Information and Event Management)

Plataforma para recoller, normalizar e correlacionar eventos de seguridade, xerando alertas e facilitando investigación.

SOC (Security Operations Center)

Equipo/función que monitoriza seguridade, xestiona alertas e coordina resposta a incidentes, idealmente integrando visibilidade TI e OT.

SSO (Single Sign-On)

Mecanismo que permite autenticación única para múltiples servizos, mellorando experiencia e control cando se combina con MFA e gobernanza de identidades.

Token

Dispositivo ou mecanismo lóxico empregado para autenticación (p.ex. xeración de OTP) ou para representar credenciais/certificados.

UE (Unión Europea)

Marco institucional e regulatorio europeo que impulsa directivas e regulamentos relevantes (p.ex. NIS2, CER, CRA) e coordinación en ciberseguridade.

VPN (Virtual Private Network)

Tecnoloxía para crear un túnel cifrado de acceso remoto. Útil para terceiros e mantemento, pero debe reforzarse con MFA e control estrito de privilexios.

Vishing

Variante de phishing baseada en chamadas de voz, a miúdo amplificada por clonación/suplantación, usada para obter credenciais ou inducir accións.

WAF (Web Application Firewall)

Cortafogos de aplicación web que filtra e bloquea ataques contra aplicacións; pode empregarse como medida compensatoria en certos escenarios.

WEF (World Economic Forum)

Foro Económico Mundial. Publica análises de risco global (Global Risks Report) que axudan a contextualizar riscos sistémicos con impacto en infraestruturas críticas.

XAI (Explainable AI)

Conxunto de técnicas para mellorar a explicabilidade da IA, facilitando auditoría, confianza e identificación de erros, especialmente relevante en decisións críticas.

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

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial
Informe de Riscos Tecnolóxicos

AMTEGA – Xunta de Galicia 2026

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