CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Informe de Riesgos Tecnológicos

Marzo 2026

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

Edita: Xunta de Galicia
Agencia para la Modernización Tecnológica de Galicia (AMTEGA)

Lugar: Santiago de Compostela
Año: 2026

Índice

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

1 Introducción

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

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

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

1.1 Objetivo y alcance

El presente **Informe de Riesgos Tecnológicos** del Observatorio de Ciberseguridad Industrial de la AMTEGA tiene como objetivo **identificar y contextualizar** los principales riesgos que pueden afectar al tejido industrial y a las infraestructuras críticas, con **foco específico en los tecnológicos y entornos OT/ICS** (sistemas de control industrial, automatización y operación).

En particular, el informe pretende:

- **Ofrecer una visión agregada y comprensible** de los riesgos más relevantes que condicionan la ciberseguridad industrial en la actualidad, combinando perspectivas globales (tendencias y riesgo sistémico) con elementos de aplicabilidad práctica.
- **Traducir riesgos "macro" y emergentes** (geopolítica, dependencia tecnológica, cadenas de suministro, concentración en proveedores, evolución del cibercrimen, etc.) en **implicaciones operativas para OT/ICS**, donde la

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

prioridad histórica de disponibilidad, seguridad funcional y continuidad introduce restricciones específicas.

- **Incorporar el componente de IA** como elemento transversal: tanto por sus usos defensivos y de optimización industrial, como por los riesgos derivados de su uso malicioso, fallos de funcionamiento y posibles efectos sistémicos.
- **Aportar una base de apoyo a la toma de decisiones** para perfiles directivos, responsables de seguridad y riesgo, equipos técnicos IT/OT y actores institucionales, facilitando la priorización de actuaciones e inversiones.

El alcance do informe se centra, por tanto, en:

- **Riesgos, especialmente tecnológicos y de ciberseguridad** con impacto potencial sobre **procesos industriales, continuidad de servicio y seguridad física**, considerando también efectos sobre reputación, cumplimiento, pérdidas económicas e interrupciones.
- Una lectura aplicable al contexto gallego por afinidad sectorial (energía, agua, automoción, alimentación, logística, manufactura, etc.), sin pretender ofrecer un inventario exhaustivo por planta, empresa o instalación.

Este documento **complementa otros entregables del Observatorio**: los Informes de Ciberalertas (visión táctica y continuada de vulnerabilidades y avisos) o los Informes de Inteligencia de Amenazas (visión más estratégica, por actores, campañas y evolución del adversario). El enfoque aquí es distinto: **centrado en el riesgo** como categoría de análisis y como puente entre amenazas, vulnerabilidades, impactos y decisiones.

1.2 Metodología

La metodología empleada combina **análisis documental**, se sabe comparada de fuentes e **interpretación orientada a OT/ICS**, al objeto de construir una visión consistente y accionable.

El proceso seguido se estructura en cuatro fases principales:

1. **Delimitación del marco de análisis y criterios de relevancia**
    - Definición del perímetro temático (riesgos tecnológicos y ciberfísicos con impacto industrial).

- Establecimiento de criterios de selección: relevancia para OT/ICS, evidencia en fuentes reconocidas, recurrencia en incidentes o tendencias, y potencial impacto sobre continuidad y seguridad.

2. **Recogida y curación de fuentes**
    - Compilación de información a partir de informes y publicaciones de referencia (organismos internacionales, agencias públicas, centros nacionales de ciberseguridad, entidades del sector y fabricantes), priorizando fuentes con metodología explícita y datos agregados.
    - Identificación de contenidos complementarios del propio Observatorio para asegurar coherencia interna.
3. **Síntesis y estructuración del riesgo**
    - Agrupación de los riesgos en bloques temáticos (panorama global, impacto económico, incidentes y amenazas emergentes —incluyendo IA—, y dimensiones de gobernanza, cumplimiento y resiliencia).
    - Contextualización explícita en clave industrial: efectos sobre operación, dependencia de terceros, limitaciones de parcheo, restricciones de cambios, seguridad funcional, segmentación, acceso remoto y cadena de suministro OT, etc.
4. **Validación interna y enfoque didáctico**
    - Revisión de coherencia: que los riesgos descritos se conecten con impactos realistas y con medidas de mitigación (directas o compensatorias) compatibles con OT/ICS.

1.3 Consideraciones y limitaciones

El informe **no sustituye** un análisis de riesgo específico por organización (que requeriría inventario, arquitectura, criticidad y evaluación de impactos por proceso), sino que abastece una **base de contexto y priorización**.

Las fuerzas empleadas son mayoritariamente internacionales; con todo, la aplicabilidad al contexto gallego es elevada debido al carácter remoto y transfronterizo de gran parte de las amenazas y a la utilización de tecnologías y proveedores comunes.

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, se incluyen recomendaciones y riesgos de carácter transversal de diversas fuentes reputadas; su implantación debe adaptarse al **grado de madurez y** al **perfil de exposición** de cada entorno industrial.

2 Resumen ejecutivo

Este **Informe de riesgos tecnológicos** ofrece una visión integrada de los principales riesgos que afectan a la ciberseguridad industrial y a las infraestructuras críticas, con foco en entornos **OT/ICS**. El documento **combina fuentes internacionales y nacionales para describir tanto riesgos estructurales y recurrentes** (segmentación deficiente, exposición de acceso remoto, gestión de vulnerabilidades, dependencias de terceros) como **riesgos emergentes vinculados a la transformación digital y al uso creciente de Inteligencia Artificial (IA)**, conectándolos con los impactos más relevantes en operación: **indisponibilidad**, degradación del proceso, coste económico y riesgo físico.

La lectura del informe está orientada a un análisis global. En OT/ICS, la seguridad no puede formularse sólo como un ejercicio "IT", sino como un equilibrio continuo entre **seguridad, continuidad de operación y seguridad funcional**.

Partiendo de ese enfoque, el informe incorpora también **una capa de riesgo más amplia, más allá del puramente tecnológico**. En línea con los análisis de riesgo sistémico (por ejemplo, las que populariza el **World Economic Forum**), se recogen **factores que amplifican la exposición industrial, actuales y a título predictivo: tensión geopolítica, interrupciones de cadena de suministro, concentración de proveedores, escasez de capacidades y dependencia de servicios digitales,** etc**.** Estos elementos no "rompen" un PLC por sí solos, pero sí condicionan la probabilidad, la velocidad de propagación y el coste de recuperación de un incidente, y por tanto **deben formar parte de la conversación de riesgo a nivel directivo.**

Sobre esa base macro, el documento baja al suelo operativo y señala que **el riesgo OT y creciente y multidimensional** porque aumenta la conectividad y, con ella, la exposición a amenazas globales (cibercrimen, extorsión/ransomware, espionaje y sabotaje), mientras persisten debilidades estructurales en inventario, gestión de configuración, accesos privilegiados y gestión del cambio**. La convergencia IT/OT y la participación de terceros amplían aún más la superficie de ataque**: la **integración con sistemas corporativos, la externalización de mantenimiento y la dependencia de integradores y proveedores introducen vías recurrentes de intrusión**, por lo que se requiere **gobernanza**, **control contractual y diseños de conectividad minimizados y monitorizados.**

En este escenario, **la IA aparece como elemento transversal por dos motivos**.

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

- Primero, porque **puede reforzar defensas y operación** (detección, correlación, apoyo al diagnóstico),
- pero también porque **introduce riesgos nuevos y amplifica otros existentes.**

El informe estructura estos riesgos de IA en tres planos:

- **uso malicioso** (automatización de campañas, *phishing* más convincente, aceleración de explotación),
- **fallos de funcionamiento** (errores, deriva del modelo, decisiones opacas)
- y **riesgos sistémicos** (dependencias, concentración tecnológica y efectos en cadena).

A esto se añade un factor organizativo especialmente relevante: el **Shadow AI**, es decir, el **uso no gobernado de herramientas de IA por parte de empleados y equipos (incluyendo proveedores)** fuera de los procedimientos corporativos. En entornos industriales, el Shadow AI puede traducirse en filtración de información sensible (configuraciones, diagramas, incidentes), decisiones técnicas basadas en respuestas no verificadas y creación de dependencias operativas sin evaluación de riesgo.

A partir de esta lectura, **el informe propone que la mitigación eficaz no depende de "solucións milagre", sino de fundamentos bien ejecutados y diseñados para contención y recuperación.** Así, las **recomendaciones consolidadas de fuentes como NCSC, CISA, ISACA o el fabricante Fortinet confluyen en un núcleo común**:

- **inventario y registro definitivo** del entorno OT;
- **segmentación** y control de conectividad;
- **eliminación de exposición OT a Internet pública** y endurecimiento del acceso remoto con **mínimo privilegio** y autenticación fuerte;
- **gestión de vulnerabilidades** y parches basada en riesgo, apoyada en **medidas compensatorias** cuando la actualización inmediata no es viable;
- integración de OT en **SecOps** y en respuesta a incidentes con playbooks específicos;
- y **capacidad de operación manual, aislamiento y continuidad** para mantener seguridad funcional cuando el entorno digital está comprometido.

Para la IA en OT, el informe incorpora dos capas complementarias de recomendaciones.

- Por una banda, los **Principios para la integración segura de la IA en OT** publicados por un consorcio internacional, establecen una hoja de ruta práctica en cuatro bloques:

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

  - **comprender la IA** (riesgos únicos, ciclo de vida de desarrollo seguro y formación del personal);
  - **avaliar y su uso en el dominio OT** (caso de negocio, protección dos datos OT, papel dos proveedores y retos de integración);
  - **crear marcos de gobernanza y aseguramiento** (mecanismos de gobernanza, integración con los marcos existentes, pruebas y evaluación, y cumplimiento);
  - e **incorporar supervisión y prácticas failsafe** (monitorización, supervisión y mecanismos de seguridad funcional y recuperación).

  El mensaje transversal es claro: la IA sólo debe introducirse cuando exista un caso de uso válido y cuando pueda garantizarse **control, trazabilidad, pruebas rigurosas y capacidad de reversión**.

- Por otro lado, la aportación del *International AI Safety Report* se incluye de forma deliberadamente parcial y selectiva, centrada en lo que es más aplicable a la ciberseguridad industrial. De este informe se destacan cinco ideas útiles para OT/ICS:
  - los **retos técnicos e institucionales** (decisiones con evidencia incompleta y responsabilidades distribuidas en cadenas de valor complejas);
  - las **prácticas de gestión del riesgo** (documentación, transparencia, casos de seguridad física e integración de la IA en la gestión de incidentes);
  - las **salvaguardias técnicas y la monitorización** (evaluación adversarial/red teaming, defensa en profundidad y vigilancia en producción asumiendo fallo);
  - los riesgos asociados a **los modelos de peso abierto** (mayor facilidad para eliminar salvaguardas, modificar modelos y heredar riesgos en la integración);
  - y la necesidad de **resiliencia** (continuidad, coordinación y capacidad de recuperación frente a efectos en cadena).

La incorporación de IA debe abordarse con la misma lógica: **valor operativo sí, pero nunca a costa de aumentar la fragilidad, reducir la capacidad de control o degradar la seguridad funcional**.

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

Adicionalmente, se plantean **observaciones específicas asociadas a la cuantificación del impacto económico del riesgo OT** (de una orden de magnitud de exposición de más de trescientos mil millones de dólares americanos)**, modelos de pérdidas y estimaciones de reducción de riesgo global y sectorial.**

Tras lo anterior, se analizan el alto nivel los datos del año pasado de incidentes en entornos industriales, y una encuesta mundial a los gestores de empresas, para constatar que **sólo el 5% de las mismas tienen visibilidad con cobertura total de su red OT a nivel de ciberseguridad.**

Se puede adicionalmente como guardacarriles del riesgo dos elementos de apoyo:

- **Un modelo de gobierno de ciberseguridad y resiliencia** que comprende tanto una propuesta de **estructura organizativa canónica como las funciones de seguridad transversales asociadas** para una organización tipo,
- La **referencia resumida del conjunto de marcos normativos y estándares recogidos en la Guía Normativa de ciberseguridad Industrial** de este mismo Observatorio.

En conjunto, el informe concluye que el riesgo tecnológico en entornos industriales **es gestionable**, pero requiere disciplina y coherencia: conocer el entorno, limitar exposición, diseñar para contención y recuperación, y establecer gobernanza que conecte personas, procesos y tecnología.

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

3 Panorama de riesgo

A continuación, se presenta una visión estructurada de los principales factores que condicionan el riesgo tecnológico en el campo industrial. En primer lugar, se introduce un bloque de **riesgos generales**, que recoge tendencias y elementos de contexto (tecnológicos y también sistémicos) que aumentan la exposición de los entornos OT/ICS e influyen en la probabilidad de materialización de las amenazas.

A continuación, se analiza **el impacto económico del riesgo**, poniendo el foco en como los incidentes pueden traducirse en costes directos e indirectos —paradas de producción, degradación operativa, recuperación, penalizaciones, cumplimiento y reputación— y porque ello convierte la ciberseguridad industrial en un factor material para la continuidad del negocio y la toma de decisiones.

3.1 Riesgos generales

3.1.1 Foro Económico Mundial (WEF)

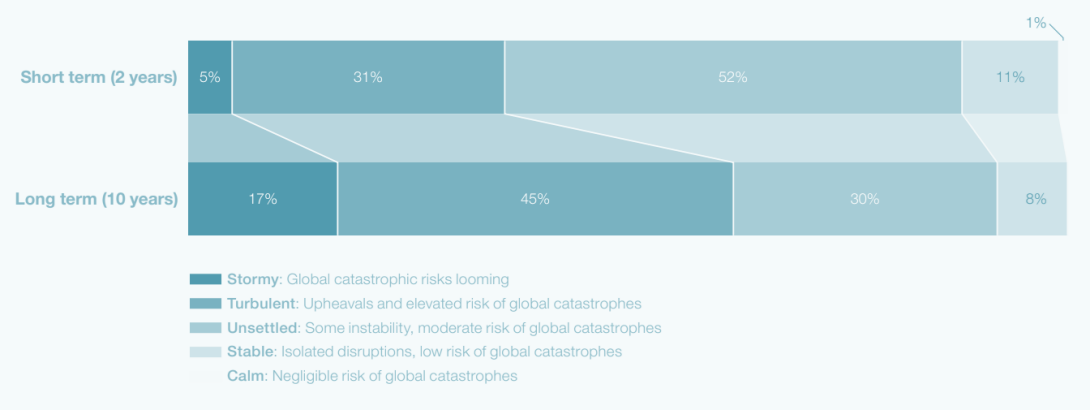
No podemos comenzar sin mencionar el **Global Risks Report 2025.** Es una publicación anual del **World Economic Forum (WEF)**, institución internacional de referencia en el análisis de tendencias globales que impactan sobre economías, gobernanza, tecnología y sociedad [1][2].

El informe **recopila la percepción y análisis de riesgos a corto y largo plazo a partir de encuestas a expertos, responsables públicos, líderes empresariales y analistas de riesgo** a nivel mundial. Su relevancia reside en ofrecer una visión sistémica y perspectiva de los factores que pueden comprometer la estabilidad económica, social y tecnológica, incluyendo aquellos con impacto directo sobre infraestructuras críticas y sistemas industriales.

Desde la perspectiva de la **ciberseguridad industrial gallega**, este informe constituye una fuente clave para contextualizar los riesgos tecnológicos y ciberfísicos que pueden afectar a sectores estratégicos como la energía, la industria manufacturera, el transporte, el agua o telecomunicaciones, todos ellos fuertemente dependientes de sistemas ICS/OT y de infraestructuras digitales interconectadas.

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

Percepción global del riesgo: deterioración progresiva



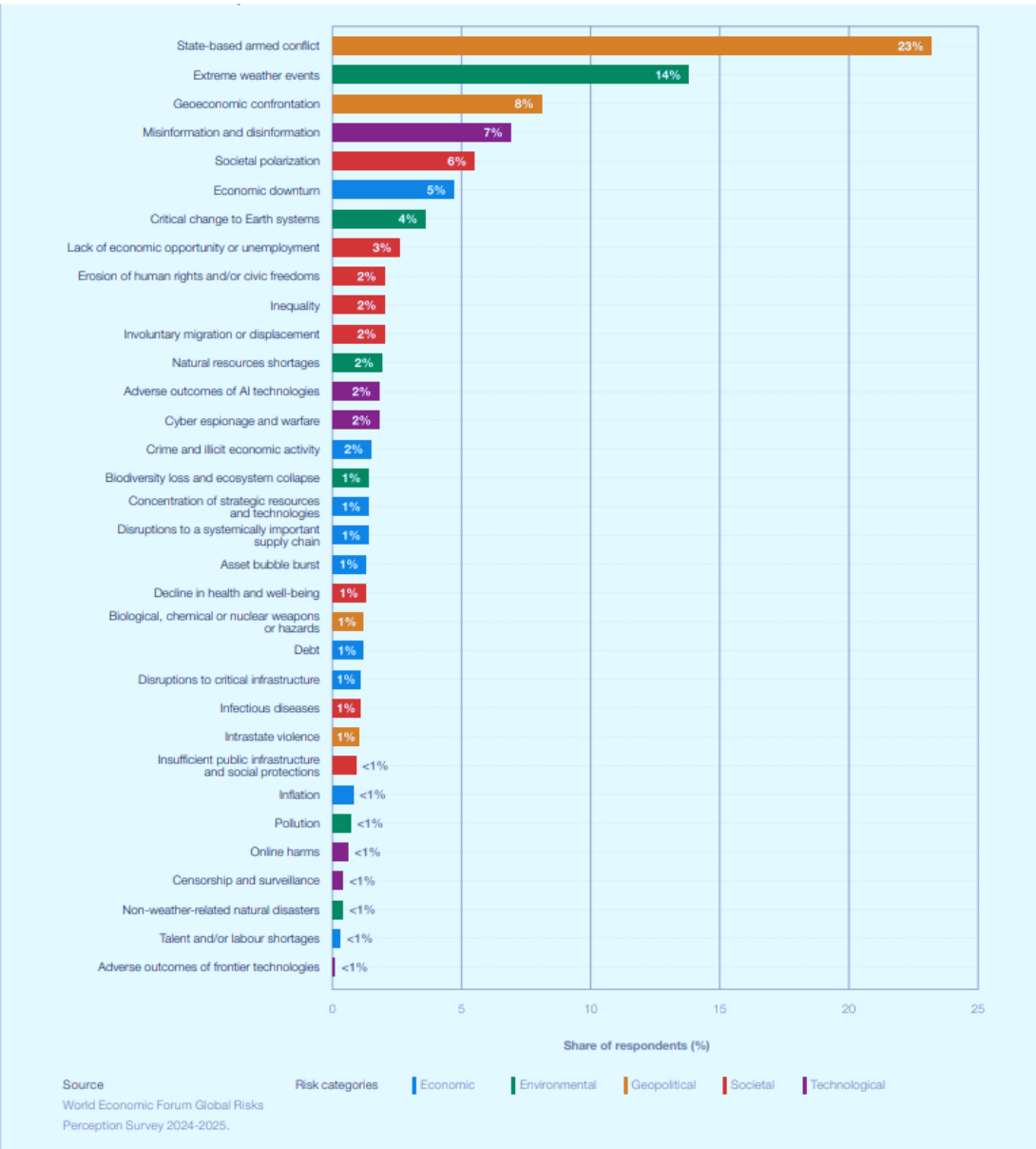
Panorama global de riesgos a corto y medio plazo según los expertos. Fuente: WEF (2025)

El informe muestra de forma clara una **tendencia negativa en la percepción global del riesgo**, evidenciando que el mundo es percibido como más inestable y ha expuesto en ediciones anteriores. La figura refleja un incremento sostenido de la percepción de riesgo sistémico, asociado a la combinación de crisis geopolíticas, transformación tecnológica acelerada y dependencia creciente de infraestructuras críticas digitalizadas.

Para Galicia, esta tendencia global se traduce en un aumento de la exposición indirecta a riesgos externos, incluso en entornos industriales locales, debido a la interdependencia con cadenas de suministro internacionales, operadores globales y tecnologías importadas.

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

Principales riesgos globales relacionados



Riesgos globales identificados. Fuente: WEF (2025)

La figura recoge la percepción de los riesgos con mayor capacidad de generar una crisis material a escala global en el año **2025** (según las opiniones del estudio 2024-2025). Para el presente informe, interesa destacar dos elementos:

- El **peso relativo** (porcentaje de respuestas) que obtienen ciertos riesgos tecnológicos, indicador de la prioridad percibida.
- Las **implicaciones operativas en redes OT/ICS**, donde la dependencia de servicios digitales, comunicaciones y operación remota convierte estos riesgos en escenarios con impacto directo en continuidad, seguridad funcional y cumplimiento.

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

A continuación, se presentan los **seis riesgos tecnológicos** de la imagen anterior del WEF (marcados en morado), grupo al que consideramos añadir por afinidad el riesgo de **Disrupción en infraestructuras críticas**. Incluimos la definición del Informe, posición relativa, y las posibles consecuencias para el sector industrial gallego.

3.1.1.1 Desinformación o información falsa

7% de respuestas, **puesto #4**.

Información falsa persistente (deliberada o no) ampliamente difundida a través de redes de medios, que desplaza la opinión pública de manera significativa hacia la desconfianza en los hechos y en la autoridad. Incluye, entre otros: contenido falso, impostor, manipulado y fabricado.

Puede degradar la toma de decisiones en crisis (p. ex., información falsa sobre cortes, vertidos, paradas programadas), **aumentar la presión pública e institucional durante incidentes y facilitar campañas de engaño que acompañen intrusiones** (phishing dirigido a personal con acceso OT, falsos avisos de mantenimiento, suplantación de proveedores).

3.1.1.2 Consecuencias adversas del uso de IA

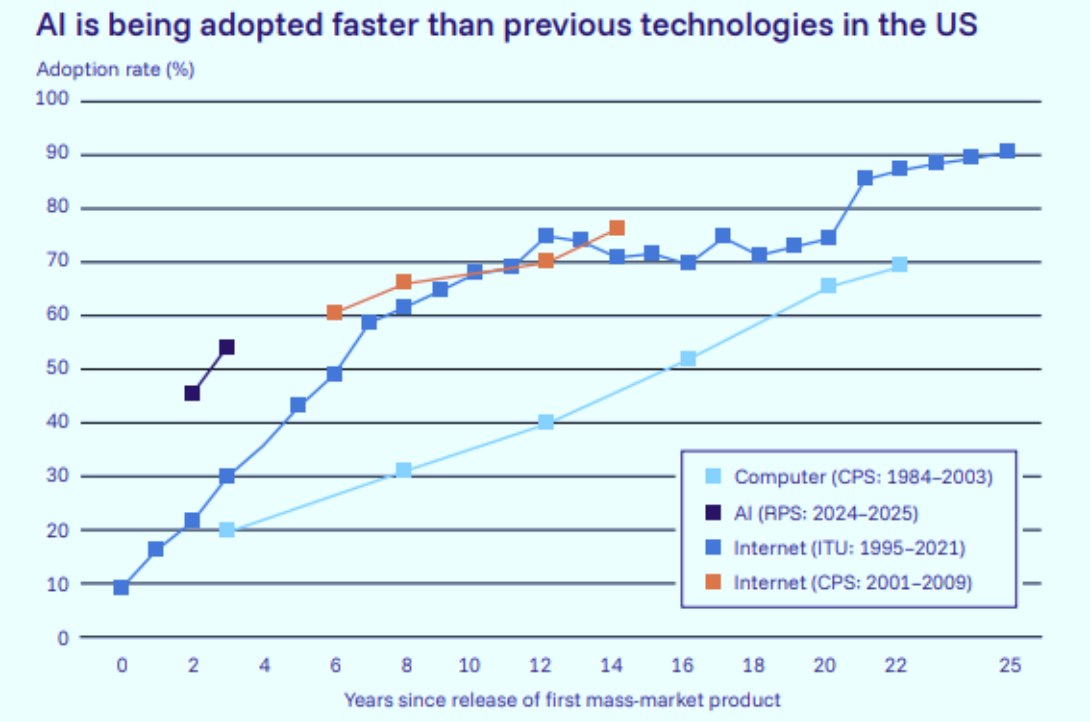
2% de las respuestas, **puesto #13**.

Consecuencias negativas, previstas o imprevistas, de los avances en IA y en las capacidades tecnológicas relacionadas (incluyendo la IA generativa) sobre personas, empresas, ecosistemas y/o economías.

La adopción de IA en monitorización, optimización de producción y detección de anomalías puede introducir fallos por modelos mal adiestrados, **dependencia excesiva** de automatización, **degradación de seguridad** por datos de baja calidad y nuevos **vectores** (p. ej., manipulación de datos de proceso para inducir decisiones erróneas).

Hay que tener en cuenta que es una tecnología cuya adopción está siendo espectacularmente rápida.

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



Velocidad de adopción de la IA frente a otras tecnologías. Fuente: International AI Safety Report (2026)

3.1.1.3 Ciberespionaje y guerra híbrida

2% de las respuestas, **puesto #14**.

Uso de **armas y herramientas de ciberseguridad por actores estatales y no estatales para obtener control** sobre una presencia digital, **causar interrupción operativa y/o comprometer o dañar las redes e infraestructuras** tecnológicas y de información de una entidad. Incluye: operaciones cibernéticas defensivas y ofensivas que tienen lugar durante un conflicto armado o el desencadenamiento, y ciberataques que roban datos clasificados, sensibles o propiedad intelectual para obtener ventaja.

Implica un **riesgo de intrusión orientada a la inteligencia** (exfiltración de ingeniería, planos y configuraciones), **preposicionamiento para sabotaje e interrupción operativa**. En sectores industriales e infraestructuras esenciales, estos escenarios adoptan materializarse en movimiento lateral IT-OT, abuso de acceso remoto y degradación de servicios de supervisión.

3.1.1.4 Disrupción en infraestructuras críticas

1% de las respuestas, **puesto #23**.

Sobrecarga o apagado de infraestructuras físicas y digitales (incluyendo satélites) **o de servicios que sustentan sistemas críticos**, incluyendo internet, telecomunicaciones, servicios públicos, sistemas financieros o energía, derivados de,

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

entre otros: **ciberataques, daños físicos intencionales o no, episodios meteorológicos extremos y desastres naturales.**

Generan un **riesgo central para continuidad industrial: interrupciones en electricidad, telecomunicaciones, servicios de internet, suministro de agua, logística o servicios financieros pueden provocar paradas de planta, pérdida de visibilidad y control, fallos en telemantenimiento y degradación de sistemas de seguridad**. Es especialmente crítico en operación remota, integración IT-OT y dependencia de servicios satelitales y/o de telecomunicaciones.

3.1.1.5 Daño online a las personas

1% de las respuestas, **puesto #29**.

Erosión de la protección frente a, y/o prevalencia de, **comportamientos dañinos que suponen una amenaza digital para la salud emocional o mental y el bienestar de las personas**. Incluye, entre otros: acoso en línea y ciberacoso.

Aunque el impacto es más indirecto, **puede incidir en riesgos de personas (acoso a empleados, chantaje, exposición pública de identidades), afectar a la disponibilidad de personal clave y amplificar incidentes** mediante campañas de intimidación o doxxing (revelación intencional de información personal o comprometedora) vinculadas a eventos industriales.

3.1.1.6 Censura y vigilancia

1% de las respuestas, **puesto #30**.

Observación amplia y generalizada de un lugar o de una persona y/o supresión de la comunicación, de la información y de las ideas, de forma física o digital, hasta el punto de vulnerar de manera significativa derechos humanos y civiles (por ejemplo, privacidad, libertad de palabra y libertad de expresión).

Puede **afectar a la operación industrial por restricciones de comunicación y acceso a información técnica, así como por vigilancia extensiva que comprometa la privacidad y la seguridad de personal y organizaciones**. En escenarios híbridos, puede acompañarse de control de la información sobre incidentes y de presión regulatoria o geopolítica que limite la cooperación.

3.1.1.7 Resultados adversos de las tecnologías de frontera

1% de las respuestas, **puesto #30**.

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

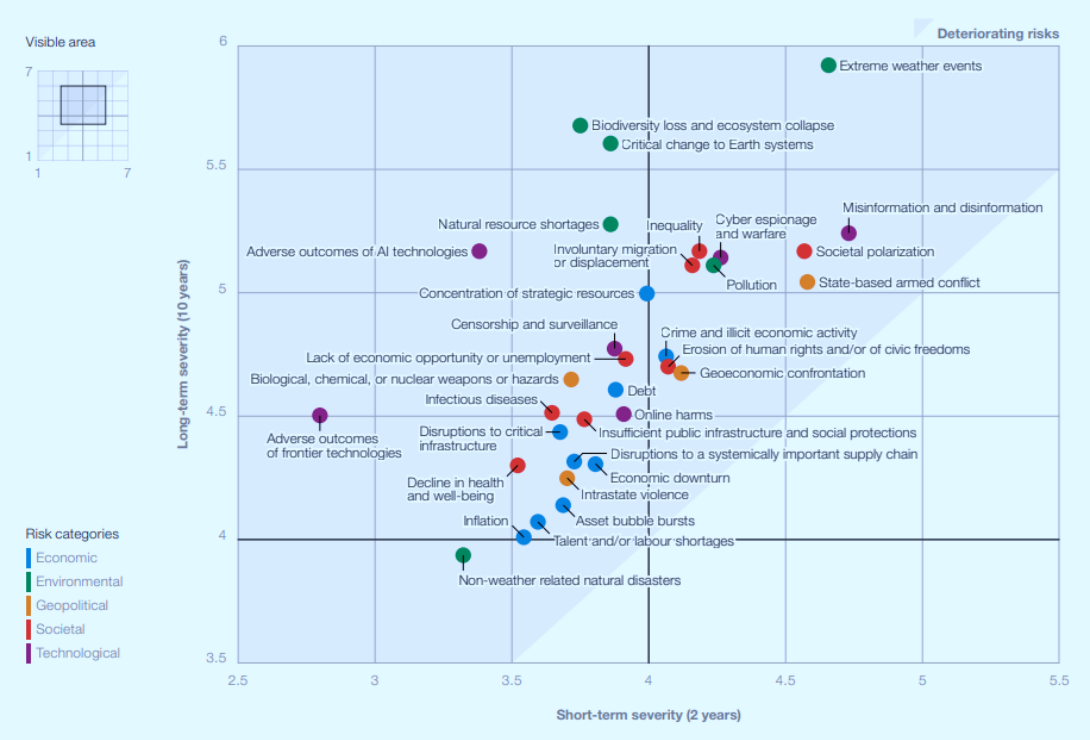
Consecuencias negativas, previstas o imprevistas, de los avances en tecnologías de frontera sobre personas, empresas, ecosistemas y/o economías. Incluye, entre otros: interfaces cerebro-computador, biotecnología, geoingeniería y computación cuántica.

Suponen riesgo de cambios disruptivos en el equilibrio tecnológico (p. ej., impacto futuro en la criptografía y en la protección de comunicaciones), **aparición de nuevas superficies de exposición y dependencia de capacidades avanzadas con gobernanza y seguridad inmaduras**. A medio plazo, **requiere vigilancia tecnológica** y evaluación de impacto en confidencialidad e integridad.

Gravedad a corto y largo plazo

La figura siguiente, analiza **la severidad de los riesgos en el corto frente a lo largo plazo**, mostrando como algunos riesgos tecnológicos tienden a intensificarse con el paso del tiempo.

Ten en cuenta que la escala de severidad es Likert del 1 al 7 (mínimo a máximo).



Gravedad relativa de los riesgos a corto y medio plazo. Fuente: WEF (2025)

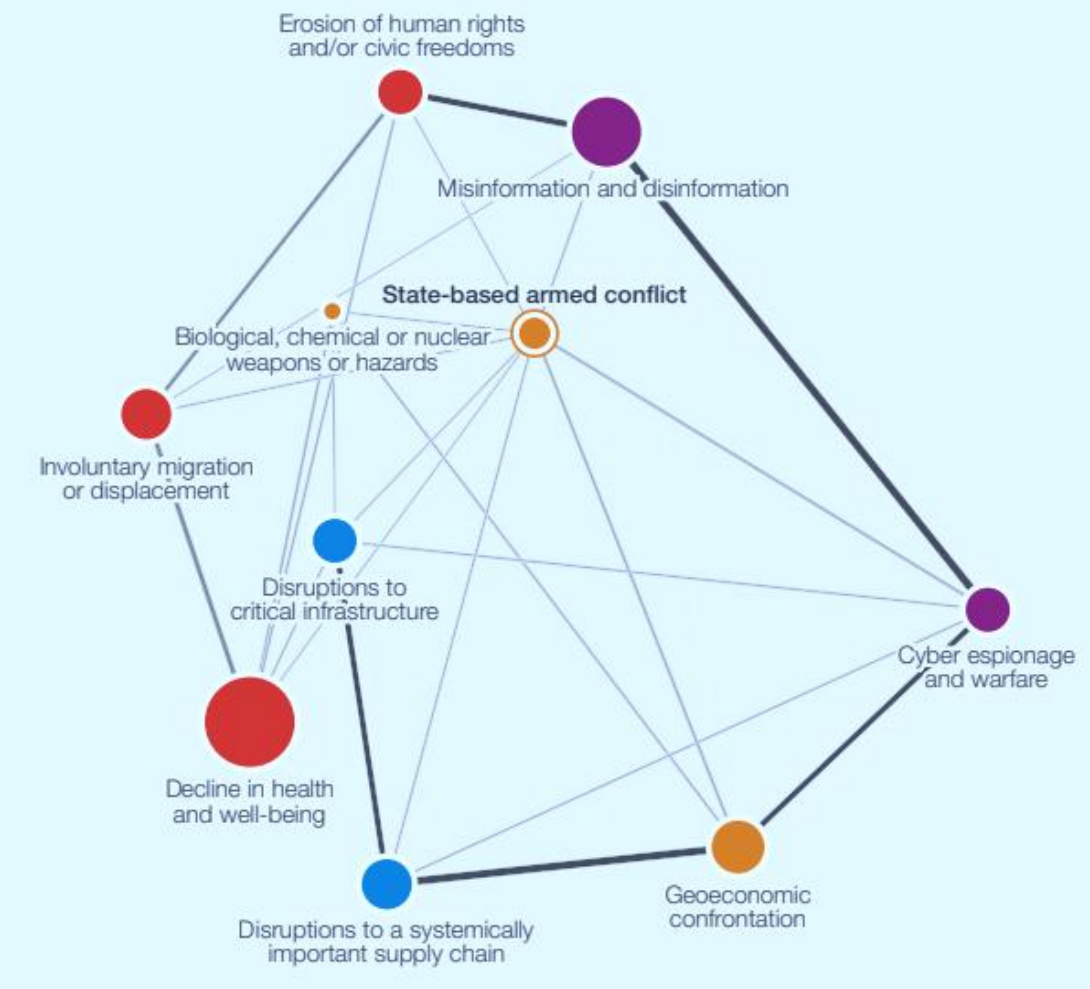
Los riesgos asociados a la tecnología digital, la interconectividad y las infraestructuras críticas aparecen como moderados en el corto plazo, pero con **alta severidad potencial a largo plazo**, especialmente si no se adoptan medidas estructurales de resiliencia.

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 la planificación estratégica en ciberseguridad industrial en Galicia**, donde muchas infraestructuras presentan ciclos de vida largos y tecnologías heredadas que incrementan la exposición futura.

Conflictos armados y riesgos interconectados

El informe destaca la relación creciente entre **conflictos armados y riesgos tecnológicos**, tal y como se refleja en la figura siguiente.



Relación entre conflictos armados y riesgos tecnológicos. Fuente: WEF (2025)

Los conflictos actúan como catalizadores de ciberataques, sabotajes digitales y operaciones híbridas que tienen como objetivo infraestructuras críticas civiles e industriales.

La experiencia reciente muestra que estos riesgos no permanecen confinados a los países en conflicto, sino que se propagan a través del ciberespacio y de las cadenas de suministro, afectando también 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 tecnológica acelerada

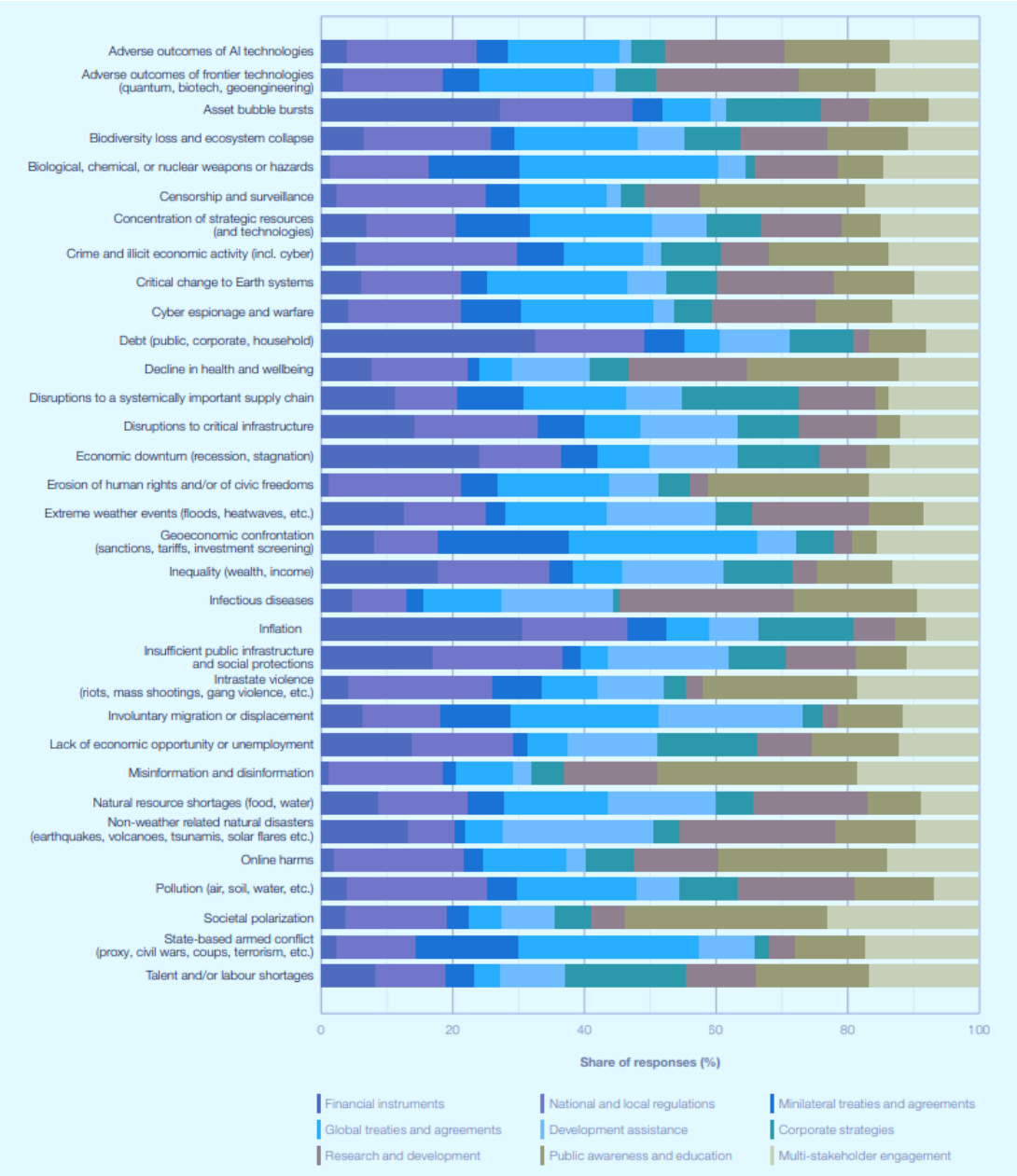
La percepción de los encuestados subraya también que los **cambios acelerados en la tecnología** están introduciendo nuevas superficies de exposición. **La integración de sistemas industriales con plataformas digitales**, servicios remotos, inteligencia artificial y automatización avanzada **incrementa la eficiencia, pero también la complejidad y el riesgo**.

Para el tejido industrial gallego, esto implica la necesidad de integrar la ciberseguridad desde el diseño y la operación, evitando enfoques reactivos.

Propuestas e implicaciones

El análisis de la figura de **Risk governance** aporta una lectura especialmente valiosa para comprender cómo deben abordarse los **riesgos tecnológicos y** el riesgo de **disrupción de infraestructuras críticas** desde una perspectiva realista y operativa. La gráfica no avalía la huella de los riesgos, sino que identifica **que enfoques tienen mayor potencial para impulsar acciones eficaces de reducción del riesgo y mejora de la preparación** en los próximos dos años. El resultado es revelador.

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



Propuesta de Risk Governance. Fuente: WEF (2025)

En primer lugar, se observa que, para la práctica totalidad de los **riesgos tecnológicos** analizados —incluyendo **ciberespionaje y guerra híbrida**, **resultados adversos de la IA**, **tecnologías de frontera**, **censura y vigilancia** o **daños en el ámbito digital**—, **los enfoques puramente técnicos o financieros no son percibidos como los más determinantes**. Por el contrario, la gráfica muestra de forma consistente un mayor peso de la **regulación nacional y local**, **de la implicación directa del sector privado**, de los **acuerdos multilaterales y** de la **coordinación entre múltiples actores**.

Este patrón confirma que los riesgos tecnológicos son entendidos como **riesgos sistémicos de gobernanza**, y no como problemas que puedan resolverse

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

exclusivamente mediante innovación tecnológica, inversión en seguridad o investigación. Desde la óptica de **OT/ICS**, esta conclusión resulta especialmente relevante: la seguridad industrial no depende sólo de la robustez técnica de los sistemas, sino de la existencia de **marcos normativos claros**, **responsabilidades bien definidas**, **cadenas de suministro seguras** y **mecanismos efectivos de coordinación público-privada**.

En el caso concreto de **ciberespionaje y ciberguerra**, la figura refleja con claridad que los enfoques con mayor potencial son los **acuerdos internacionales y la implicación del sector privado**, mientras que la investigación y desarrollo aparece con un peso claramente inferior. Esto refuerza la idea de que estos riesgos, aunque se materializan técnicamente en redes y sistemas, **tienen una naturaleza eminentemente estratégica y geopolítica**. En entornos OT/ICS, esto se traduce en escenarios de intrusión prolongada, exfiltración de información sensible o preposicionamiento para sabotaje, frente a los que la capacidad de respuesta local es insuficiente sin **cooperación supraterritorial e intercambio de información**.

Algo semejante ocurre con los **resultados adversos de la IA** y de las **tecnologías de frontera**. La gráfica muestra que **la regulación**, **la concienciación** y **la participación del sector privado** son percibidas como más eficaces que la propia madurez tecnológica. Esto sugiere que estas tecnologías están introduciendo a un ritmo superior a la capacidad de comprender y controlar sus efectos. En sistemas industriales, esta situación puede derivar en **automatización excesiva**, **dependencia de modelos opacos** o **decisiones erróneas basadas en datos incompletos o manipulados**, incrementando el riesgo operativo y de seguridad funcional.

En lo que respecta las **disrupciones de infraestructuras críticas**, la gráfica presenta un patrón aún más significativo. No existe un enfoque claramente dominante, sino una distribución equilibrada entre **regulación**, **implicación del sector privado**, **inversión**, **concienciación pública** y **coordinación multiactor**. Esta dispersión refleja la naturaleza **transversal, interdependiente y multicausal** de este riesgo. Las infraestructuras críticas dependen de sistemas digitales, servicios energéticos, telecomunicaciones y cadenas logísticas que, al fallar, generan **efectos en cascada** con impacto directo sobre la operación industrial.

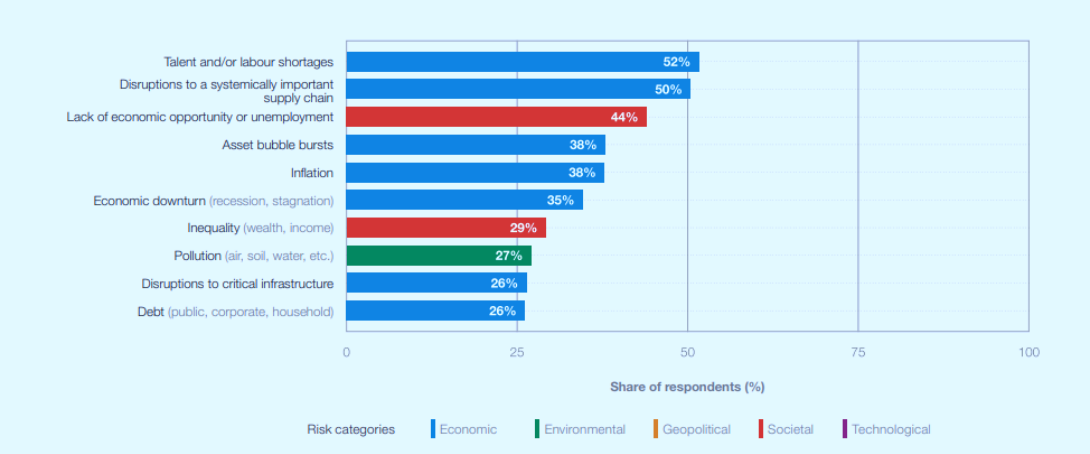
Desde la perspectiva de la **ciberseguridad industrial gallega**, esta lectura es especialmente relevante. Confirma que la disrupción de infraestructuras críticas **no puede mitigarse mediante una única medida ni desde un único ámbito**, sino que

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

requiere una combinación de **diseño resiliente**, **operación segura**, **gobernanza clara y capacidad de respuesta coordinada**. La dependencia creciente de operación remota, servicios digitales e integración IT-OT amplifica este riesgo, incluso en escenarios locales alejando de los grandes focos de conflicto.

En conjunto, la opinión del panel del WEF refuerza un mensaje central que encaja plenamente con el enfoque de este Informe: **los principales riesgos tecnológicos que afectan a la OT/ICS no se reducen principalmente con más tecnología, sino con mejor gobernanza**. La ciberseguridad industrial debe entenderse como un elemento estructural de la resiliencia, en el que la técnica es necesaria pero no suficiente, y en el que la coordinación, la regulación y la responsabilidad compartida son factores críticos para limitar el impacto de los riesgos globales sobre la realidad industrial gallega.

Relacionado también con la Gobernanza, **la siguiente imagen complementa esta visión, señalando a juicio de los expertos, que riesgos podrán ser mitigados en mayor medida mediante estrategias corporativas**.



Top Riesgos Globales gestionables mediante estrategias corporativas. Fuente: WEF (2025)

Se ponen así de manifiesto las conexiones entre riesgos tecnológicos, geopolíticos y económicos, reforzando la idea de que la ciberseguridad industrial no puede abordarse de forma aislada.

El Global Risks Report 2025 confirma que los riesgos tecnológicos y ciberfísicos ya no son escenarios excepcionales, sino elementos estructurales del contexto global. Esto implica **en Galicia** varias **necesidades a nivel colectivo y de las entidades particulares**:

- Integrar el análisis de riesgos globales en la gestión de la ciberseguridad industrial local.

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

- Priorizar la protección y resiliencia de las infraestructuras críticas.
- Anticipando los impactos derivados de conflictos y crisis externas.
- Reforzar la cooperación público-privada en materia de seguridad industrial.

3.1.2 Riesgos tecnológicos clásicos

El análisis de la compañía Nozomi Networks [3] se sitúa como punto de partida un hecho ya estructural: **los sistemas OT están cada vez más conectados por IP y, en consecuencia, más expuestos a amenazas cibernéticas, al tiempo** que **se difuminan las fronteras entre la gestión de riesgo TI y el riesgo operacional**. En este escenario, **integrar el riesgo OT en la estrategia corporativa de seguridad** deja de ser una opción y pasa a ser un requisito para proteger la continuidad operativa y la seguridad de las personas.

Desde una perspectiva de **ciberseguridad industrial gallega**, esto se traduce en un impacto directo sobre plantas y operaciones donde OT/ICS es clave (manufactura, energía, agua, logística, cadenas de suministro industriales, etc.): la **exposición tecnológica ya no es sólo un riesgo digital, sino un riesgo ciberfísico**, con potencial de indisponibilidad, degradación de calidad y afectación a la seguridad funcional.

A continuación, se sintetizan los **riesgos tecnológicos clásicos** más recurrentes en estos entornos, combinando el enfoque del artículo anterior, con la visión contemplada en entregables previos del Laboratorio como el Informe de Ciberalertas o Inteligencia de Amenazas [4].

3.1.2.1 Convergencia TI/OT

La convergencia tecnológica implica que una intrusión inicial en TI (identidad, correo, estaciones de trabajo, servicios corporativos) **pueda derivar en movimiento lateral hacia redes de operación**, especialmente cuando existen **puntos de salto TI/OT** e interdependencias fuertes. El efecto práctico es una **mayor probabilidad de que ataques "clásicos" (ransomware, compromiso de credenciales, intrusiones por servicios expuestos) acaben impactando en operación**.

3.1.2.2 Acceso remoto

Tanto en informes sectoriales como en guías orientadas a operaciones, **el acceso remoto** aparece de forma consistente como **uno de los vectores más críticos: VPNs, mantenimientos remotos, accesos de integradores y fabricantes, o canales de soporte**. Este riesgo se combina con dos factores frecuentes en industria: **necesidad**

operativa real (el acceso remoto es parte del modelo de mantenimiento) y **dificultad de gobernar identidades y trazabilidad** cuando interviene cadena de suministro.

3.1.2.3 Tecnología insegura

La presencia de **protocolos industriales sin cifrado ni autenticación fuerte por diseño** (especialmente en entornos legados) introduce riesgos específicos: observación/manipulación de tráfico, suplantación y alteración de comandos o estados de proceso. En OT esto es especialmente sensible porque la comunicación de control no es "un dato": es una orden que actúa sobre un proceso físico.

3.1.2.4 Obsolescencia

Destacar que en OT son comunes **dispositivos legados y protocolos propietarios**, lo que complica el descubrimiento de activos y el perfilado de comportamiento. A esto se añaden ciclos de vida largos (10–25 años), **fin de soporte** y limitaciones de recursos (capacidad de cómputo y memoria) que restringen la incorporación de mecanismos de seguridad modernos. El resultado es un riesgo acumulativo: **activos críticos con exposición creciente y capacidad limitada de actualización**.

3.1.2.5 Gestión de vulnerabilidades

La gestión de vulnerabilidades en OT es descrita como un reto mayor por el **volumen y diversidad de dispositivos y plataformas** y porque **el parcheado no se puede automatizar como en TI**. Además, la práctica industrial impone fricción: paradas planificadas escasas, convalidaciones, compatibilidades, y riesgo de impacto sobre la producción. Esto favorece que **vulnerabilidades conocidas permanezcan más tiempo expuestas**.

3.1.2.6 Falta de visibilidad y monitorización

En OT, la **ausencia de visibilidad** (**inventario fiable**, conocimiento de protocolos industriales, cambios en lógicas de control y configuraciones) conduce a la **detección tardía y** pérdida de oportunidad para identificar intrusiones silenciosas o manipulaciones graduales. Este riesgo es especialmente relevante en operaciones distribuidas o con múltiples sedes, donde la heterogeneidad y la segmentación imperfecta agravan la situación.

3.1.2.7 Arquitecturas planas

Muchas organizaciones industriales parten de **redes históricamente planas y muy interconectadas, lo que facilita la propagación y el movimiento lateral**. En

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

escenarios de convergencia, esto convierte una brecha inicial en un incidente más amplio: **un evento localizado puede evolucionar hacia la pérdida de control del proceso** si los puntos de interconexión no están bien gobernados.

3.1.2.8 Sensibilidad operativa

En comparación con TI, OT se caracteriza por **alta sensibilidad a interrupciones**: **escaneos agresivos, reanudaciones no coordinados o cambios de configuración pueden provocar indisponibilidades** o estados no previstos. Junto con esto, existen **dependencias complejas** (firmware, librerías, software de ingeniería, módulos de E/S) que pueden introducir riesgo incluso en cambios aparentemente menores. La consecuencia es que el **propio ciclo de vida tecnológico (cambio/actualización) se convierte en un factor de riesgo.**

3.1.2.9 Gobernanza transversal

Finalmente, **un riesgo recurrente es organizativo-tecnológico: en OT las decisiones técnicas (accesos, configuraciones, actualizaciones) requieren coordinación entre operación, mantenimiento, ingeniería y seguridad.** Si la gobernanza es difusa, se generan condiciones para **exposición prolongada**, prácticas ad hoc y variabilidad entre plantas, lo que aumenta la probabilidad de incidentes y dificulta la respuesta. Hablaremos de esta organización posteriormente en el Informe.

3.1.3 Visión de Google

Los análisis **Cybersecurity Forecast 2025** y **Cybersecurity Forecast 2026**, elaborados por equipos de inteligencia y respuesta a incidentes de Google (incluyendo capacidades integradas de Threat Intelligence y Mandiant), ofrecen una lectura anticipatoria de las tendencias que más probablemente condicionarán la actividad adversaria en el corto plazo y por tanto suponen el riesgo más probable [5][6].

Para este informe empleamos las dos últimas ediciones para alcanzar más contexto, aunque sólo se recogen los elementos **directamente aplicables a la ciberseguridad industrial,** es decir, aquellos que afectan a la **continuidad operativa**, a la **cadena de suministro industrial**, a la **exposición TI/OT** y la **superficie de ataque típico en redes OT/ICS**.

El mensaje común en ambos recursos es claro: la evolución del riesgo en 2025-2026 estará dominada por **economía del cibercrimen con foco en la interrupción**, por **uso intensivo de IA para escalar el engaño y acelerar operaciones**, y por **actividad estatal e híbrida asociada a tensiones geopolíticas**. Ello encaja con la realidad de

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

OT/ICS, donde el impacto final no se limita a la pérdida de información: puede traducirse en **paradas de planta, degradación de servicios esenciales y efectos en cadena sobre producción y logística**.

3.1.3.1 Ciberdelito

La previsión para 2026 señala explícitamente que el riesgo más disruptivo de origen no natural para **ICS y OT** seguirá **siendo el cibercrimen**, por encima de otras categorías. En términos industriales, esto es relevante porque el cibercrimen no precisa "comprender" el proceso: abandona con **interrumpir las dependencias de negocio** que alimentan la operación.

El informe destaca un patrón especialmente crítico para industria: operaciones de ransomware (bloqueo y secuestro de datos) **diseñadas para impactar software empresarial esencial** (como sistemas ERP), con el objetivo de **romper el flujo de datos que sostiene la operación OT**. Este enfoque es particularmente eficaz porque **comprometer la capa de negocio puede paralizar el ámbito industrial**, incrementando la presión para pagos rápidos.

3.1.3.2 Interrupción por vías indirectas

La perspectiva anterior refuerza un punto clave para Galicia: la continuidad OT/ICS depende cada vez más de servicios corporativos y de cadena de suministro digital (planificación, compras, trazabilidad, mantenimiento, calidad...). Por tanto, la disrupción no requiere acceso directo a PLCs o SCADA: puede materializarse mediante **interrupción de sistemas transversales** que sostienen la operación.

3.1.3.3 Acceso remoto e "higiene"

Se subraya también recalcando la visión clásica, que prácticas deficientes, como **accesos remotos inseguros**, seguirán permitiendo que **malware común** acabe penetrando en redes OT. Esta constatación es relevante para entornos industriales porque la operación real exige acceso remoto (soporte, integradores, fabricantes), y el riesgo adopta concentrarse en **credenciales, sesiones y canales de soporte**.

3.1.3.4 Credenciales robadas y robos de información (malware)

Las previsiones del año pasado ubicaban la **sustracción y reutilización de credenciales** (impulsada por campañas masivas de **malware específico**) como una tendencia central. Para OT/ICS esto implica un aumento de la probabilidad de intrusión por "inicio de sesión" más que por explotación técnica directa: un atacante con

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

credenciales válidas puede entrar en VPNs, portales de soporte o entornos híbridos y, desde ahí, llegar a activos industriales.

3.1.3.5 La IA como acelerador

Los dos recursos, así como el WEF, coinciden en que la IA tendrá un papel creciente, con especial impacto en:

- **Phishing y vishing más verosímiles** (incluyendo **clonación de voz** y suplantación de personal ejecutivo o técnico), lo que incrementa el riesgo de acceso inicial en organizaciones industriales.
- **Operaciones de información** que escalan contenido y perfiles falsos, con efecto indirecto sobre incidentes industriales (presión social, distorsión de información crítica en crisis).

Las previsiones de 2026 añaden un elemento nuevo especialmente pertinente para organizaciones industriales que adoptan IA en procesos corporativos: el riesgo de **prompt injection**, entendido como manipulación de sistemas de IA para forzar acciones no previstas, exfiltración o sabotaje. A medida que sistemas de IA se integren en flujos de trabajo (p.ej. análisis de incidencias, gestión documental, automatización en centros de operaciones), este riesgo introduce una nueva categoría de exposición con consecuencias potenciales sobre operación y continuidad.

3.1.3.6 Geopolítica y análogos

En el convulso mundo en el que vivimos, **la geopolítica** continuará impulsando la actividad estatal, destacando el papel persistente de Rusia y China (y también Irán y Corea del Norte) en operaciones de espionaje e influencia. Para 2026 se completa esta visión señalando que, aunque menos frecuentes, los ataques estatales orientados a OT siguen siendo **altamente sofisticados** y ligados a conflictos específicos.

Además, incorporan una referencia relevante para OT: grupos hacktivistas pro-Rusia pueden representar una amenaza sustancial e imprevisible para entornos de operación, citando como ejemplo el **compromiso de una presa en Noruega** (abril de 2025) [7]. La lectura industrial es inmediata: en escenarios de tensión geopolítica, OT puede convertirse en objetivo por **valor simbólico, efecto social y capacidad de interrupción**.

3.1.3.7 Dispositivos a bordo y de terceros

Se destaca finalmente que ciertos actores aumentarán el foco en **dispositivos de a bordo** (frecuentemente sin capacidades equivalentes de detección y respuesta) y en **proveedores terceros**, porque comprometer un socio puede abrir acceso a múltiples organizaciones. En industria, esto es consistente con la realidad de integración y mantenimiento: la superficie de ataque se amplía con **equipos perimetrales**, conectividad industrial y cadenas de soporte (relacionado en cierta manera con la cadena de suministro vista anteriormente).

3.1.4 Uso indebido de componentes IT/AI

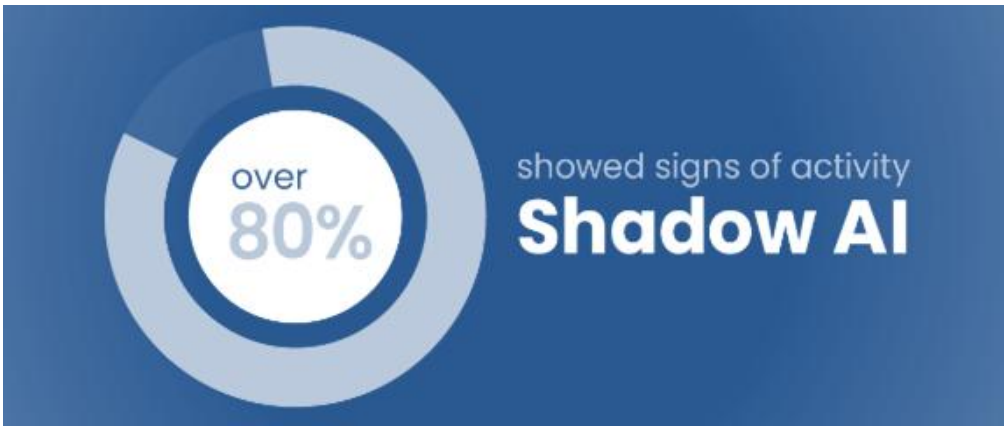
El **13º Estudio del Estado del Arte de la Seguridad en la Nube**, elaborado por **ISACA** y por el **capítulo español de la Cloud Security Alliance (CSA Spain Chapter)** en colaboración con otros afines [8], ofrece una visión consolidada sobre la adopción real de servicios cloud en las organizaciones y los riesgos asociados a su gestión. Aunque el documento no está específicamente orientado a entornos industriales, **sus aportes resultan plenamente aplicables a la ciberseguridad industrial**, en la medida en que la nube, las herramientas colaborativas y los servicios basados en IA están integrarse de forma creciente en procesos que soportan o condicionan la operación OT.

De la revisión del estudio se desprende que, más allá de riesgos ya tratados en otras fuerzas (cadena de suministro, credenciales, configuraciones incorrectas), **un elemento diferencial y más relevante para este informe es la persistencia y expansión del Shadow IT y AI** (en adelante Shadow Tech cuando englobe ambos), fenómeno que adquiere una nueva dimensión con la popularización de herramientas **de IA accesibles desde la nube, incluso enfoques agénticos de la misma**.

3.1.4.1 ¿Qué es Shadow Tech?

El **Shadow Tech** se refiere al **uso de aplicaciones, servicios o infraestructuras tecnológicas de información o inteligencia artificial fuera del control y de la gobernanza formal de la organización**, normalmente sin conocimiento ni convalidación de los equipos de TI o seguridad. El estudio evidencia que este fenómeno no disminuye con la madurez digital; al contrario, **incrementa con la facilidad de acceso a servicios cloud y SaaS**, especialmente cuando aportan valor inmediato al 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 organizaciones. Fuente: XM Cyber (2025)

La irrupción de **herramientas de IA generativa**, asistentes inteligentes, servicios de análisis o automatización en la nube **intensifica este riesgo**, ya que permiten procesar información, generar contenido o automatizar tareas sin infraestructura propia ni conocimientos técnicos avanzados. En entornos industriales, estas herramientas pueden ser empleadas para:

- Análisis de incidencias o registros de operación.
- Generación de documentación técnica.
- Soporte a la toma de decisiones en mantenimiento o producción...

Cuando ello ocurre fuera de gobernanza, **datos sensibles de operación, ingeniería o negocio pueden ser expuestos a terceros sin control ni trazabilidad**.

3.1.4.2 Implicaciones específicas del Shadow Tech en entornos OT/ICS

En ciberseguridad industrial, este fenómeno presenta **características propias** que amplifican el riesgo:

- **Frontera difusa entre TI y OT**: aplicaciones cloud empleadas en ámbitos corporativos (planificación, mantenimiento, calidad) condicionan directamente la operación industrial.
- **Exposición indirecta de OT**: sin acceso directo a PLC o SCADA, un servicio Shadow Tech puede almacenar diagramas, configuraciones, informes de proceso o credenciales.
- **Pérdida de visibilidad y control**: los equipos de seguridad no pueden evaluar riesgo, aplicar políticas ni responder a incidentes sobre activos que desconocen.

- **Cumplimiento normativo comprometido**: uso no autorizado de servicios externos puede vulnerar requisitos de confidencialidad, localización de datos y seguridad exigidos por regulación sectorial.

3.1.4.3 Riesgo ciberfísico

La combinación de **Shadow Tech + dependencia operativa** introduce un riesgo cualitativamente distinto. No se trata sólo de pérdida de datos, sino de la posibilidad de:

- Manipulación indirecta de la toma de decisiones.
- Exposición de información que permita sabotaje posterior.
- Introducción de dependencias críticas en servicios externos no evaluados.

Desde la perspectiva de la ciberseguridad industrial gallega, esto supone un desafío creciente: el **riesgo ya no reside sólo en la red OT, sino en las herramientas auxiliares que condicionan como se opera, mantiene y decide sobre el proceso industrial**.

3.1.4.4 El caso ClawDBot

Para ilustrar lo anterior, un elemento especialmente relevante y reciente es la aparición de **herramientas útiles o aparentemente legítimas basadas en IA que son adoptadas sin control ni salvaguardias de seguridad**, explotando directamente el fenómeno del Shadow Tech. Un ejemplo representativo es lo sucedido con **ClawDBot (renombrado a Moltbot)**, un proyecto **open source en estado embrionario**, presentado como herramienta de automatización y asistencia basada en IA que a pesar de las advertencias su creador Peter Steinberger, fue viralizado exponiendo a miles de particulares y organizaciones a grandes riesgos de seguridad [9].

Este tipo de soluciones ilustra una evolución del riesgo que conviene matizar:

- El riesgo **no reside en la herramienta en sí**, sino en su **adopción sin gobernanza, control ni evaluación de seguridad**.
- En el caso de ClawDBot, el propio autor **recomendaba su uso exclusivo por personal experto y en entornos controlados**, advirtiendo de su carácter experimental.
- La descarga y ejecución sin conocimiento técnico ni salvaguardias introduce **exposición innecesaria a malware, robo de información, credenciales o acceso remoto**, entre otros.

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

En entornos industriales, donde el personal técnico busca soluciones rápidas para análisis, diagnóstico o documentación, la **adopción informal de este tipo de herramientas resulta especialmente peligrosa**, ya que puede operar durante largos períodos sin detección, fuera de cualquier control corporativo.

3.1.5 Predicciones del INCIBE-CERT

El artículo «¿Que esperar de la ciberseguridad industrial en 2023?», publicado por **INCIBE-CERT (Instituto de Ciberseguridad de España)** a comienzos de 2023, presenta una serie de predicciones que, a pesar de su **antigüedad temporal**, siguen teniendo **vigencia parcial o plena** en el contexto actual. Esto se debe a que muchas de ellas no describen fenómenos coyunturales, sino **tendencias estructurales** propias de la transformación digital industrial, de la evolución del riesgo y del marco regulatorio [10].

En este apartado se recogen **únicamente aquellas predicciones o riesgos, no todos ellos tecnológicos, que no se subrayan** en los apartados adyacentes, y que aportan **valor complementario** para la comprensión del riesgo en entornos **OT/ICS**.

3.1.5.1 Profesionalización y especialización creciente del atacante en entornos industriales

INCIBE-CERT anticipaba una evolución hacia atacantes **más especializados en tecnologías industriales**, con conocimientos específicos de procesos, protocolos y operación. Esta predicción sigue siendo relevante: el acceso a la documentación, formación y herramientas especializadas ha reducido la barrera de entrada y favoreció ataques más precisos, aunque no siempre más sofisticados técnicamente.

El mayor riesgo de manipulación dirigida del proceso, **ataques más silenciosos y mejor adaptación del atacante a las restricciones operativas** industriales.

3.1.5.2 Incremento de la exposición por digitalización acelerada y presión por eficiencia

El artículo señalaba que la presión por mejorar eficiencia, automatizar procesos y reducir costes llevaría la **digitalización acelerada**, frecuentemente sin que la seguridad haya avanzado al mismo ritmo. Esta dinámica continúa presente, especialmente en organizaciones medianas y pequeñas.

La introducción de tecnología conectada sin evaluación de riesgo completa, **amplía la superficie de ataque y la dependencia creciente de sistemas digitales** para operación crítica.

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

3.1.5.3 Dependencia de personal clave y riesgo asociado a la pérdida de conocimiento

INCIBE-CERT destacaba el riesgo asociado a la **dependencia de personal técnico muy especializado**, cuyo conocimiento no siempre está documentado ni compartido. Este riesgo, aún poco tratado en otras fuerzas, tiene impacto directo en la seguridad.

La salida, indisponibilidad o error humano de personal clave puede **derivar en configuraciones inseguras, respuesta tardía a incidentes o pérdida de capacidad de recuperación**.

3.1.5.4 La falta de una cultura de seguridad industrial como factor amplificador de riesgos

El artículo subrayaba que, en muchas organizaciones, **la ciberseguridad industrial sigue percibiendo como un problema ajeno a la operación diaria**. Esta falta de cultura sigue siendo un elemento estructural que amplifica otros riesgos.

Su efecto puede materializarse en **mayor probabilidad de prácticas inseguras, resistencia a cambios necesarios y baja detección temprana** de incidentes.

3.1.5.5 Incremento de incidentes híbridos con impacto físico indirecto

INCIBE-CERT anticipaba un aumento de incidentes en los que el impacto físico no es inmediato ni directo, pero aparece como consecuencia de una cadena de eventos digitales. Esta predicción mantiene plena vigencia.

Los incidentes que comienzan en TI, identidad o sistemas auxiliares pueden acabar provocando paradas, degradación de servicios o estados operativos no seguros.

3.1.5.6 Necesidad creciente de coordinación entre operación, mantenimiento y seguridad

Finalmente, se apuntaba a la **necesidad de romper silos organizativos entre áreas** técnicas. A falta de coordinación sigue siendo un riesgo en sí mismo.

Lo contrario, promueve la **aparición de respuestas descoordinadas, cambios no comunicados y dificultades para gestionar incidentes complejos** que afectan a múltiples dominios.

3.1.6 Cuadro resumen de riesgos

A continuación, se viene una **matriz resumen de los riesgos identificados en los apartados previos**. Esta matriz tiene como objetivo **organizar y sintetizar los**

principales riesgos que afectan a la ciberseguridad industrial, facilitando una visión estructurada que permita su comprensión global y la posterior priorización.

El **nivel de riesgo asignado** a cada elemento (**alto, medio o bajo**) tiene un **carácter cualitativo y referencial**, basado en una valoración general de la **probabilidad de materialización** y del **impacto potencial** en entornos **OT/ICS**. Esta estimación pretende ofrecer una orientación inicial coherente con el contexto industrial analizado, pero **no sustituye una evaluación de riesgo formal**.

En consecuencia, el nivel de riesgo efectivo deberá ser **ajustado y refinado en función del contexto organizativo concreto**, teniendo en cuenta factores como el sector de actividad, la criticidad de los procesos, el grado de digitalización, la exposición a terceros, la madurez de la gobernanza y las capacidades reales de detección y respuesta. Sólo mediante este análisis contextualizado es posible determinar la prioridad real de cada riesgo y su relevancia específica para una organización determinada.

Categoría	Riesgo	Descripción breve	Nivel de riesgo
Tecnológico	Desinformación e información falsa	Distorsión de la percepción y de la toma de decisiones durante incidentes industriales	Medio
Tecnológico	Consecuencias adversas del uso de IA	Automatización y analítica mal gobernadas con impacto operativo	Medio
Geopolítico	Ciberespionaje y guerra híbrida	Intrusiones persistentes con fines de inteligencia o sabotaje	Alto

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

Tecnológico	Disrupción de infraestructuras críticas	Interrupción de servicios esenciales con efectos en cascada	Alto
Humano	Daños digitales a las personas	Acoso, chantaje o exposición de personal clave	Medio
Geopolítico	Censura y vigilancia	Restricción de la comunicación y presión informativa	Bajo
Tecnológico	Tecnologías de frontera	Cambios disruptivos con seguridad inmadura	Bajo
Organizativo	Convergencia TI/OT no gobernada	Propagación de incidentes desde TI a OT	Alto
Tecnológico	Acceso remoto inseguro	Compromiso vía VPNs, soporte remoto y terceros	Alto
Tecnológico	Tecnología industrial insegura por diseño	Protocolos y sistemas sin protección nativa	Alto
Tecnológico	Obsolescencia y activos legados	Exposición prolongada por ciclos de vida largos	Alto

Organizativo	Gestión deficiente de vulnerabilidades	Persistencia de fallos conocidos en OT	Alto
Organizativo	Falta de visibilidad y monitorización OT	Detección tardía de intrusiones	Alto
Organizativo	Arquitecturas de redes planas	Movimiento lateral facilitado	Alto
Organizativo	Sensibilidad operativa al cambio de divisas	Indisponibilidades por acciones técnicas no coordinadas	Medio
Organizativo	Gobernanza transversal insuficiente	Responsabilidades difusas entre áreas	Alto
Humano	Profesionalización del atacante industrial	Ataques más adaptados al proceso	Medio
Estratégico	Digitalización acelerada sin seguridad	Incremento da superficie de ataque	Alto
Humano	Dependencia de personal clave	Pérdida de conocimiento crítico	Medio
Organizativo	Falta de cultura de seguridad industrial	Normalización de prácticas inseguras	Medio
Tecnológico	Incidentes híbridos con impacto físico	Cadenas de eventos digitales con efecto físico	Alto

Organizativo	Silos organizativos	Respuesta ineficaz a incidentes complejos	Medio
Humano	Cibercrimen orientado a la interrupción	Paradas operativas como objetivo principal	Alto
Organizativo	Dependencias digitales indirectas	Paradas por fallo de sistemas corporativos	Alto
Humano	Robo de credenciales y robos de información	Acceso por sesiones válidas	Alto
Tecnológico	La IA como acelerador de engaño	Phishing y suplantación avanzada	Medio
Tecnológico	Inyección rápida	Manipulación de sistemas basados en IA	Medio
Geopolítico	Hacktivismo y conflictos	Ataques con tokens en OT	Medio
Tecnológico	Dispositivos a bordo expuestos	Equipos perimetrales con baja protección	Medio
Humano	Terceros comprometidos	Acceso indirecto vía proveedores	Alto
Organizativo	Tecnología Sombra	Uso de tecnología fuera de gobernanza	Alto

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

Organizativo	Herramientas de IA non gobernadas	Uso informal de software experimental	Alto
Estratégico	Dependencia de servicios cloud no controlados	Perdida de resiliencia por dependencia externa	Medio

Cuadro de riesgos identificados en el Informe. Fuente: elaboración propia (2026)

3.2 Impacto económico del riesgo de OT

La materialización de un incidente de ciberseguridad en **tecnologías de operación (OT/ICS)** se traduce, en primer término, en costes técnicos de contención y recuperación (análisis forense, restauración de sistemas, reposición y servicios externos). Sin embargo, el impacto económico real viene determinado, en la mayoría de los casos, por la **interrupción del negocio**: paradas de producción, pérdida de capacidad, desperdicio de producto, penalizaciones contractuales, afectación a servicios esenciales e impactos en cadena sobre proveedores y clientes. En muchos de los sectores estratégicos presentes en Galicia —**industria manufacturera, energía, agua, puertos o logística,** por ejemplo—, una degradación temporal de la operación puede convertir un evento digital en un incidente con **impacto económico ampliado**.

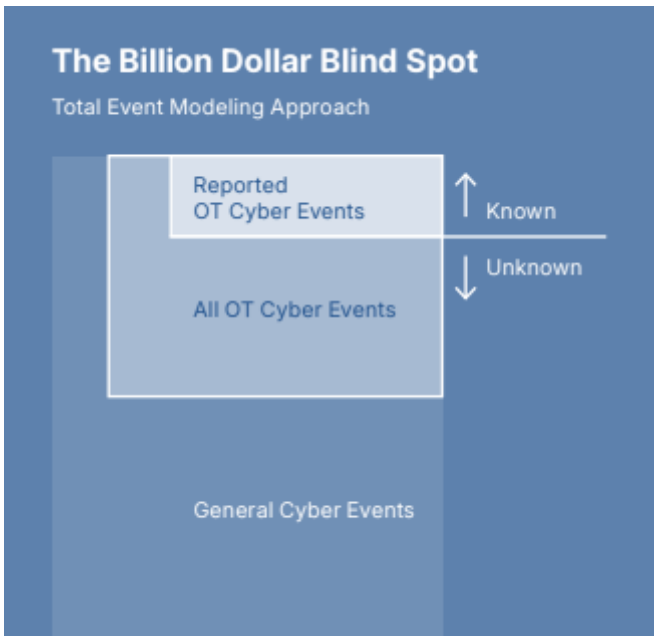
En esta línea, Dragos publicó un análisis específico de riesgo financiero en OT basada en datos del mercado asegurador y en modelización del riesgo agregada. La comunicación pública asociada al informe estima **más de 300.000 millones de dólares estadounidenses** de exposición potencial global en riesgo OT, cifra que busca situar el debate en el plano ejecutivo y financiero.

En concreto, el estudio referencia una exposición agregada de **hasta 329,5 mil millones de dólares** en un escenario de cola **1:250 (0,4% de probabilidad anual)**, e identifica **172,4 mil millones** asociados específicamente a escenarios de **interrupción del negocio**. Para una orden de magnitud anual "media", el informe maneja estimaciones de **31,1 mil millones** de riesgo anual agregado y **12,7 mil millones** cuando se consideran reclamaciones asociadas a disrupciones [11][12].

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

Exposición agregada al riesgo ICS/OT. Fuente: Dragos (2025)

Como se aprecia en la figura siguiente, estas cifras son **estimaciones** y no un recuento exhaustivo. La razón principal no es matemática, sino empírica: **no se conoce el universo total de incidentes OT**, porque una parte significativa de los eventos **no se reportan públicamente**, no llegan a registrarse como reclamación aseguradora o quedan clasificados como incidentes internos.



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

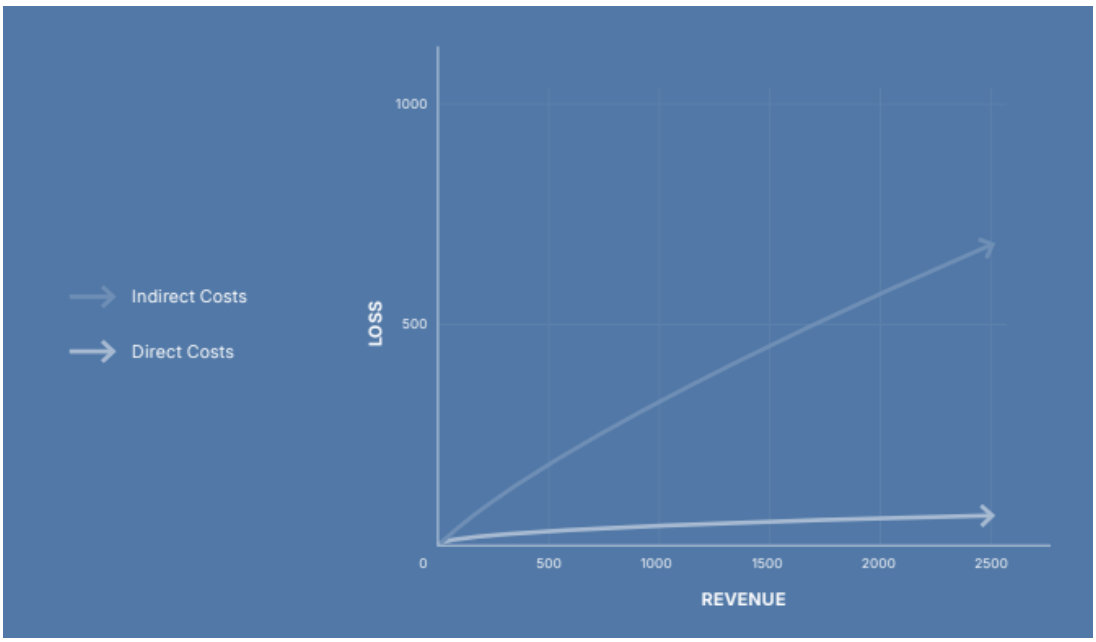
En consecuencia, cualquier análisis cuantitativo que pretenda medir el riesgo económico global debe trabajar con un **subconjunto observable** (incidentes conocidos y datos disponibles) y extrapolar la exposición, incorporando la posibilidad de **subnotificación**. Esta realidad es especialmente relevante en OT/ICS, donde la prioridad operativa, la reputación y la complejidad de atribución favorecen que muchos incidentes no trasciendan fuera de la organización.

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

La lectura más útil para el contexto gallego no es la cifra exacta, sino el patrón que el informe enfatiza: el coste potencial en OT **no está dominado por el daño físico directo**, sino por la pérdida **de continuidad** y por los efectos colaterales. El documento explicita esta idea distinguiendo entre:

- **costes directos** (recuperación técnica, reposición, servicios)
- y **costes indirectos** (paradas preventivas por prudencia, indisponibilidad de sistemas de soporte, impacto contractual y efectos en cascada).

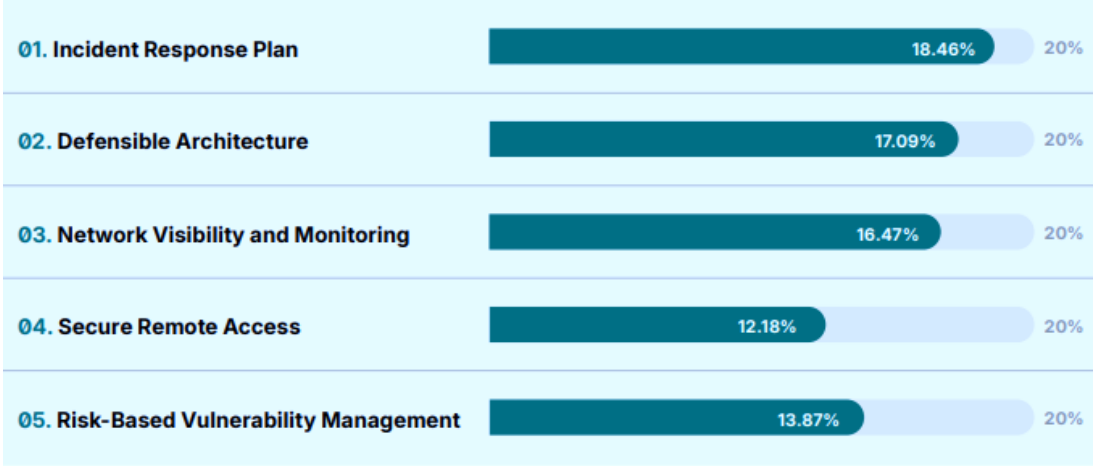
En procesos continuos (energía, agua) y en manufactura con cadenas ajustadas (automoción, alimentación), la prudencia operativa puede implicar paradas que multiplican el coste final, incluso cuando el daño inicial es limitado. Como se ve en la gráfica, el coste indirecto tiende a dominar.



Modelo de perdidas en costes directos e indirecto. Fuente: Dragos (2025)

Otro hallazgo operativo del informe es que la reducción del riesgo no depende por igual de todos los controles, y que existen medidas con efecto especialmente relevante para limitar pérdidas económicas. Dragos emplea los cinco controles críticos en ICS [13] (ya estudiados en otros Informes del Observatorio como la Guía Normativa [31]) como referencia práctica y concluye que la **preparación y respuesta a incidentes** es uno de los factores con mayor correlación con la reducción de pérdidas agregadas. A modo de recordatorio, los cinco controles citados son: **plan de respuesta a incidentes ICS**, **arquitectura defendible**, **visibilidad y monitorización de red ICS/OT**, **acceso remoto seguro y gestión de vulnerabilidades basada en riesgo**.

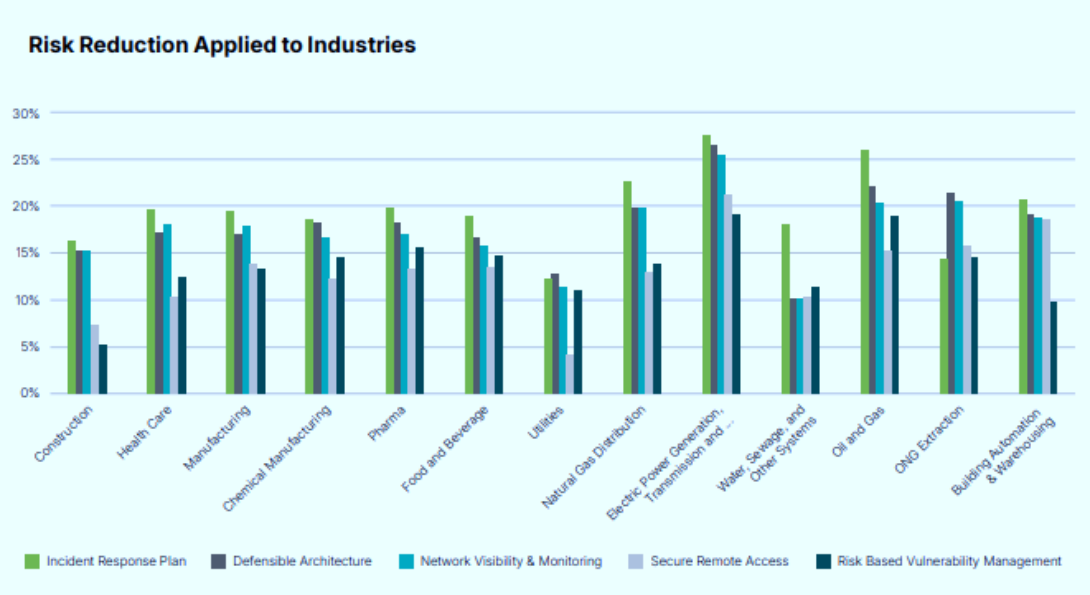
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027



Estimación de reducción de niveles de riesgo por control crítico en ICS. Fuente: Dragos (2025)

Podemos afirmar de este modo que **priorizar controles no sólo reduce probabilidad e impacto técnico, sino que reduce la exposición financiera asociada a la continuidad del negocio y a costes indirectos**.

El informe también desglosa resultados por sector, mostrando que el peso relativo de determinados controles varía según la naturaleza de la operación y la criticidad del servicio. Este punto es especialmente relevante para Galicia porque permite una lectura sectorial inmediata: en ámbitos donde la disponibilidad es crítica y la recuperación es compleja, mejoras en arquitectura, visibilidad y respuesta pueden traducirse en **una reducción estimada de pérdidas mayor**.



Reducción de riesgo sectorial. Fuente: Dragos (2025)

En paralelo, Dragos identifica tres retos estructurales que explican por qué el riesgo OT estuvo históricamente infravalorado:

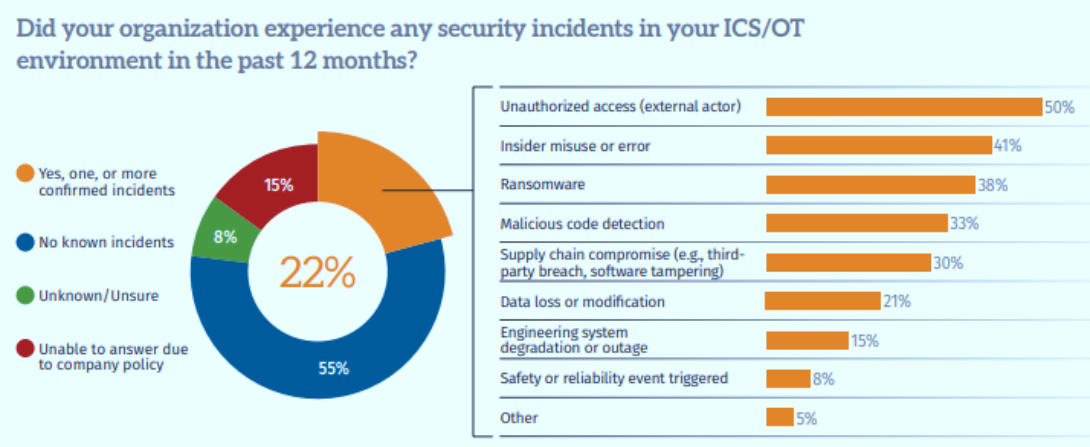
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

1. **Impacto financiero previamente indefinido**.
2. **Dificultad para estimar el retorno de la inversión (ROI)** en seguridad OT (se propone un modelo cuantitativo en el Informe de Ciberalertas del Observatorio [4]).
3. **Dificultad para priorizar mejoras de controles** sin evidencias independientes.

En organizaciones industriales medianas, estas tres barreras adoptan coexistir con restricciones de recursos y con gobernanzas donde OT y TI no siempre están alineadas, lo que refuerza la necesidad de incorporar una lectura económica del riesgo.

Como lectura sintética del informe orientada a responsables de riesgo, jurídico y seguros, resulta útil la versión del mismo publicada en The Policyholder Perspective [15].

Para aterrizar las estimaciones económicas en la realidad operativa, el informe de SANS Institute de Estado de la seguridad en ICS/OT 2025 [16], aporta evidencias en base a encuestas sobre **tipos de incidentes habituales** y sobre **tiempos del incidente**, variables que condicionan directamente el coste final.



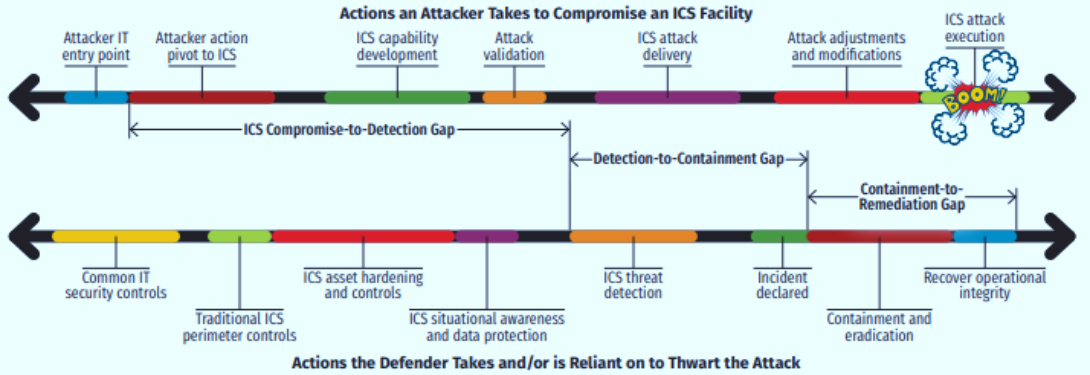
Estadística de tipología de incidentes ICS. Fuente: SANS (2025)

Se tenga en cuenta que ciertos escenarios —por ejemplo, **acceso externo no autorizado** y **ransomware**— tienen una capacidad inmediata para derivar en interrupción operativa, mientras que otras categorías (p.ej. compromiso por terceros) actúan como puerta de entrada con efectos diferidos.

En lo relativo a los tiempos de los incidentes, a continuación, se muestran las definiciones de las tres ventanas temporales involucradas en la mitigación de los ciberincidentes:

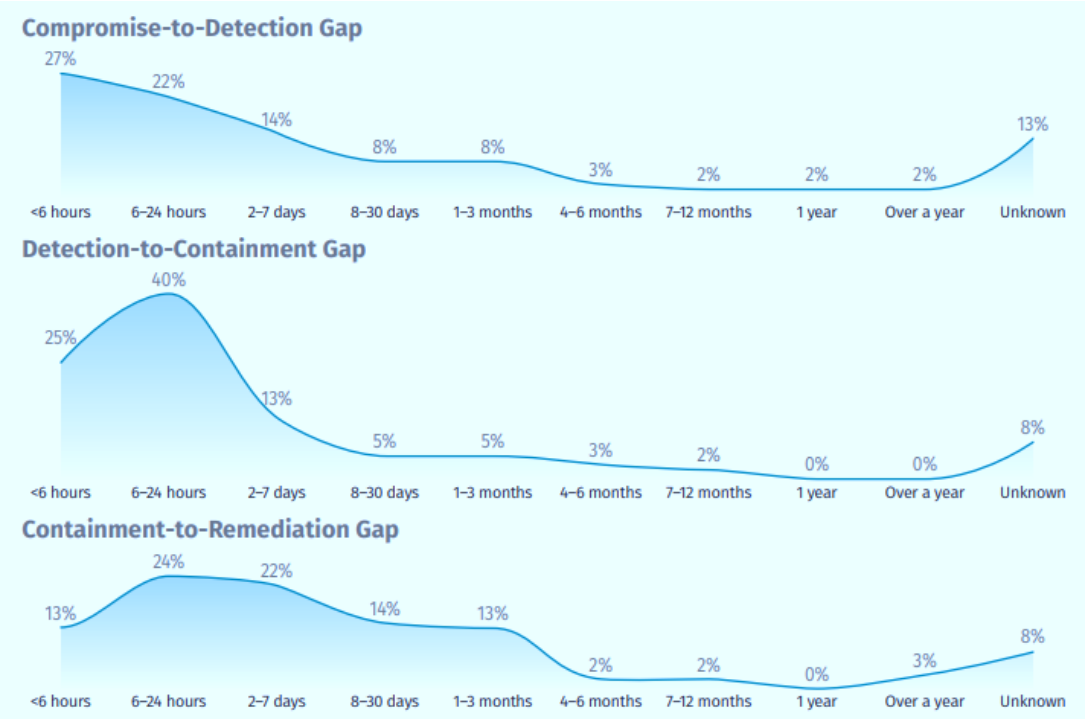
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

- Tiempo entre el compromiso y la detección
- Tiempo entre la detección y la contención
- Tiempo entre la contención y la remediación



Tiempos involucrados en la mitigación de un incidente. Fuente: SANS (2025)

Estos tiempos permiten ligar ciberseguridad con economía de una manera directa: el **coste escala con el tiempo**, y la remediación prolongada penaliza la continuidad y la recuperación. En OT, donde la restauración puede requerir convalidaciones operativas y coordinación con ingeniería, estas demoras son particularmente gravosas.

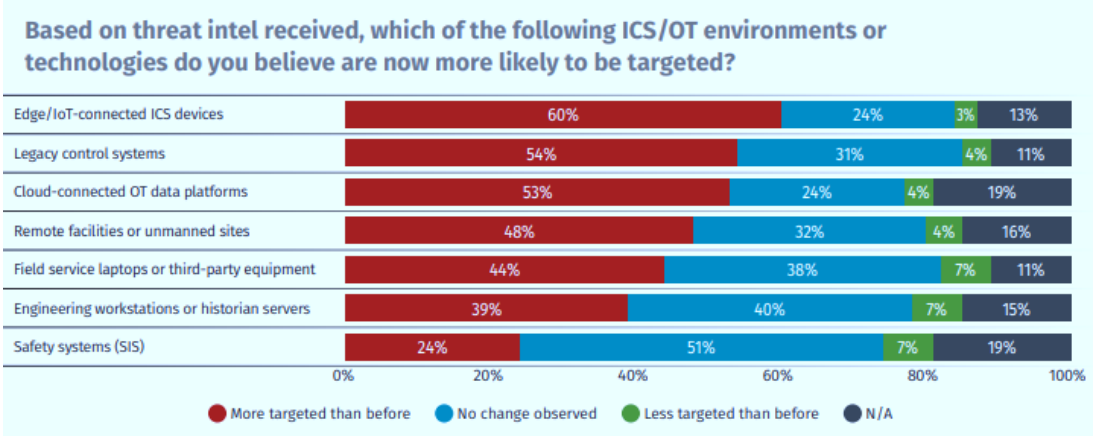


Estadísticas sobre los tiempos de mitigación de incidentes. Fuente: SANS (2025)

Como se ve, **un tercio de los incidentes tardan más de una semana en ser detectados, en torno a un 20% tardan en contenerse más de 8 días tras la detección, y de una cuarta parte, son remediados en plazos superiores a un mes**.

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

Finalmente, **las predicciones recogidas por SANS sobre ámbitos más susceptibles de ser objetivo de los atacantes según los encuestados** (destacando plataformas OT conectadas a la nube, sistemas legados, dispositivos de borde/IoT industrial e instalaciones remotas):



Tecnologías susceptibles de sufrir más ataques según los encuestados. Fuente: SANS (2025)

Ello refuerza el mensaje central de esta sección: a medida que aumenta la conectividad y la dependencia digital, el **riesgo OT se convierte en un riesgo económico estructural**, y la resiliencia pasa a ser un factor de competitividad y continuidad

4 Incidentes y amenazas emergentes

Este apartado se celebra en cómo el riesgo tecnológico se materializa en la práctica, a través de **incidentes reales** y de patrones de amenaza predominantes en el ecosistema industrial.

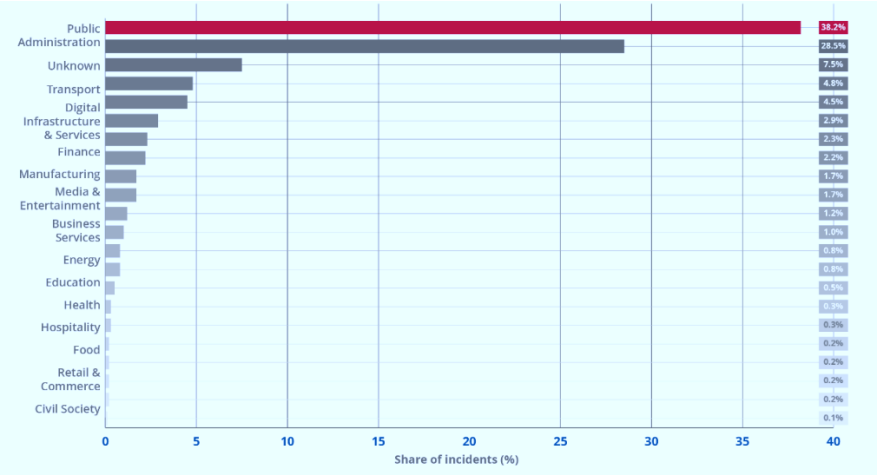
Sobre esa base, la sección introduce las **amenazas emergentes** que están redefiniendo el paisaje de riesgo, impulsadas por la **Inteligencia Artificial**.

4.1 Incidentes y sectores afectados

Los **informes de inteligencia de amenazas OT** del Observatorio de Ciberseguridad Industrial de la Xunta de Galicia (AMTEGA) integran una visión operativa de **incidentes con impacto en OT/ICS** y de los **sectores más expuestos**, combinando fuentes europeas, repositorios de incidentes e inteligencia de fabricantes [4]. Su lectura es particularmente útil para el contexto gallego porque permite conectar patrones observados en Europa con la realidad de sectores estratégicos del tejido productivo: **industria manufacturera**, **energía y utilities**, **agua y aguas residuales**, **transporte y logística** y **agroalimentario**.

A nivel europeo, el análisis sectorial recopilado en el informe a partir de ENISA cuantifica la dimensión del problema de materialización de riesgos: durante el período estudiado, ENISA analizó **4.875 incidentes**, de los cuales **el 28,5%** no pudieron asociarse a un sector. Una vez excluidos estos casos, se observa una concentración clara en pocos sectores, destacando **administración pública (≈38%)**, **transporte (≈7,5%)**, **infraestructuras y servicios digitales**, **finanzas (≈4,7%)** y **manufactura (≈2,9%)**, que conjuntamente explican una parte mayoritaria de los incidentes con sector identificado.

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

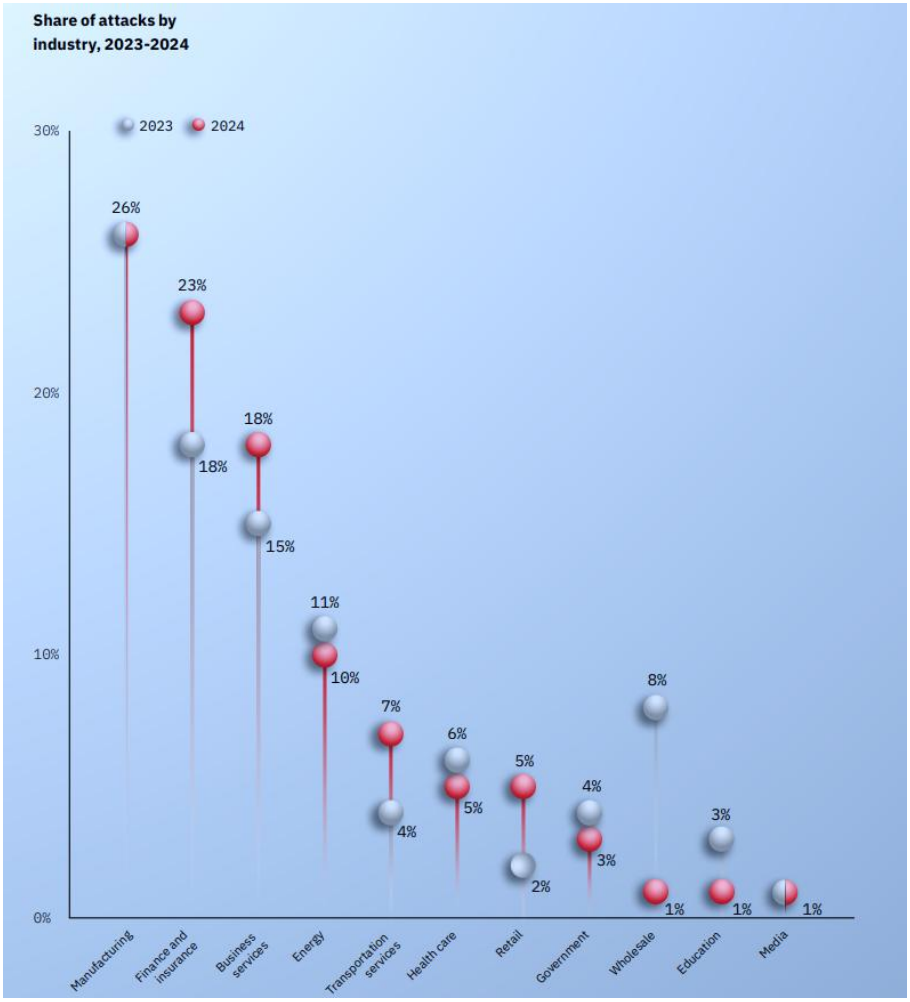


Incidentes registrados por sector. Fuente: ENISA (2025)

Para la perspectiva OT, este dato es relevante porque varios de estos sectores funcionan como **dependencias críticas** de la industria (comunicaciones, servicios digitales, logística), por lo que un incidente en ellos puede traducirse en **efectos en cascada** sobre operaciones industriales.

Desde el punto de vista de cibercrimen e impacto organizativo, el informe recoge también tendencias de inteligencia sectorial: por ejemplo, según datos de IBM XForce citados, **manufactura se mantiene como uno de los sectores más atacados (26%)**, mientras que **finanzas y seguros** concentra también un porcentaje elevado (**23%**). En el eje de impacto, destacan patrones de **captura de credenciales** y **robo de datos**, con cifras de referencia del **29%** y **18%**, respectivamente, en incidentes analizados, reforzando una idea clave para OT/ICS: muchas intrusiones no comienzan "rompiendo" OT, sino **iniciando sesión** con credenciales válidas y moviéndose a partir de TI hacia activos críticos.

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



Ratio de incidentes cibernéticos por sector de actividad 2024 frente a 2023. Fuente: IBM X-Force (2025)

El propio informe sintetiza ejemplos de **incidentes con consecuencias operativas** en Europa durante 2024, con un patrón recurrente: compromiso inicial en **sistemas corporativos** (p.ej. ERP, servicios de identidad, plataformas de gestión), seguido de **aislamiento preventivo de redes** y **paradas completas de planta** durante días o semanas. La casuística industrial europea recogida incluye casos de manufactura con interrupción prolongada e impacto financiero, y también eventos destacables en el ámbito español, como un incidente en el sector agroalimentario en el que se afirmó acceso a sistemas tipo SCADA asociados al tratamiento de aguas residuales, con parada y retorno la operación en modo manual.

Como complemento orientado a la afectación real de sistemas industriales (no sólo a incidentes mediáticos), el informe incorpora telemetría de Kaspersky ICSCERT para Europa (Q2 2025): aproximadamente **uno de cada cinco equipos ICS** bloqueó objetos maliciosos durante el trimestre, con un valor global en torno al **20,5%**. De especial interés para el Sur de Europa, región que incluye España, señala un **aumento**

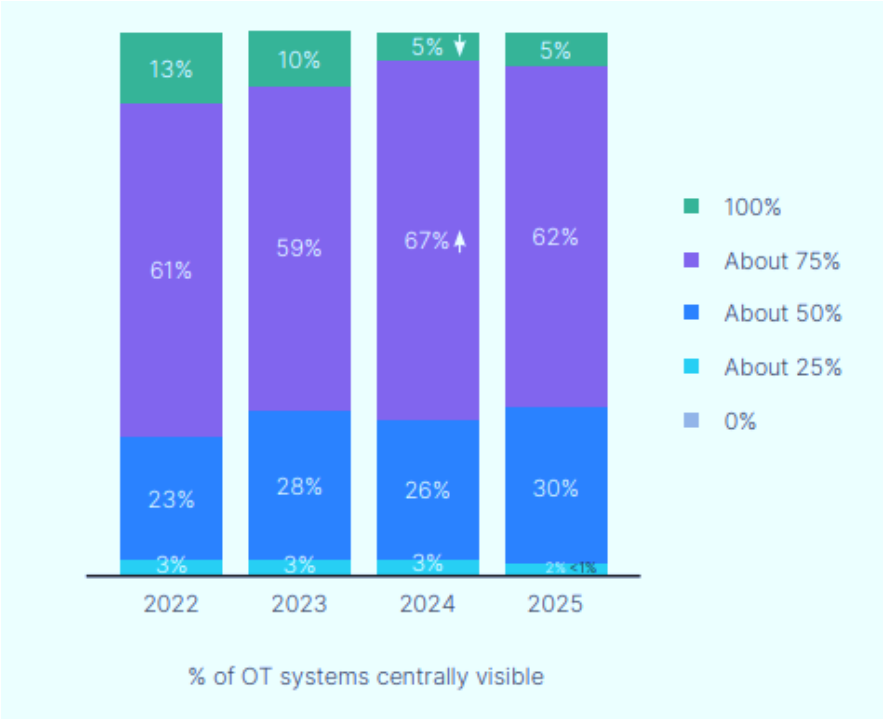
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

continuado de amenazas procedentes del correo electrónico, con picos cercanos al **7% de equipos ICS afectados;** esto es coherente con el hecho ya mencionado de que muchos compromisos en OT son consecuencia de **vectores heredados de TI** (phishing, malware genérico, medios extraíbles, acceso remoto inseguro y movimiento lateral). Además, el informe de incidentes de Kaspersky para Q2 2025, basado en incidentes reportados y analizados, referencia una muestra de **135 incidentes** en el trimestre, permitiendo una lectura sectorial rápida.

En síntesis, esta evidencia sostiene una conclusión práctica para Galicia: los sectores con mayor peso económico y de servicio (**manufactura, transporte/logística, agroalimentario, energía y agua**) presentan una exposición recurrente a incidentes que, aun comenzando en TI habitualmente, terminan generando **interrupción de operación**, **degradación del servicio** e **impactos en cadena**.

En paralelo, el **2025 State of Operational Technology and Cybersecurity Report** de Fortinet aporta una lectura cuantitativa complementaria, basada en un panel internacional [17][18]. La muestra fue elaborada mediante encuestas, alcanzando 558 respuestas completas, procedentes de organizaciones de **Energía/Utilities, Salud/Farma, Transporte/Logística, Manufactura, Químico/Petroquímico, Petróleo/Gas/Refino y Agua/Aguas residuales**, típicamente con **más de 1.000 empleados** (con excepciones en determinados países). Los criterios de inclusión requerían que **OT estuviera dentro de la responsabilidad funcional**, que haya existido **responsabilidad de reporte sobre operaciones de planta/manufactura**, y que el perfil estuviera **implicado en decisiones de compra de ciberseguridad**; el listado de países incluidos contempla **España**.

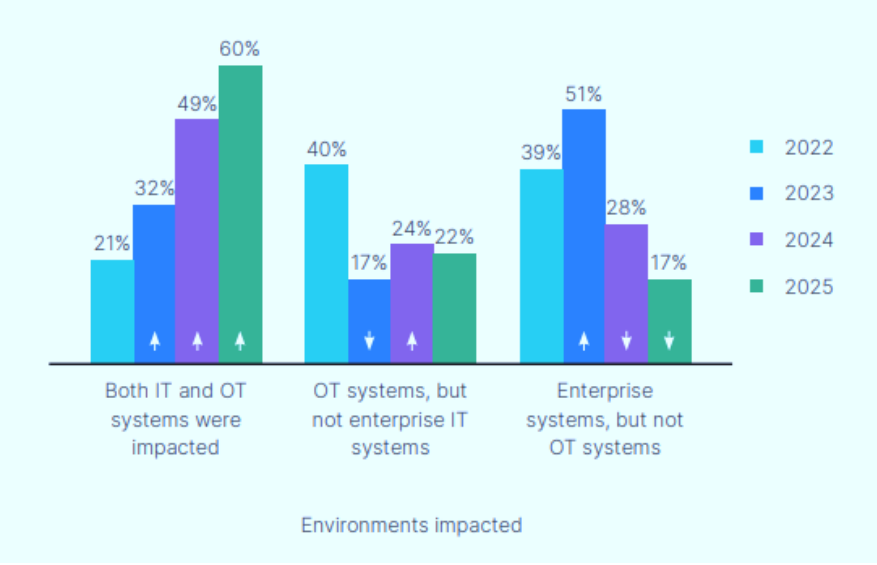
Un primer hallazgo crítico es la falta de **visibilidad real** de las redes OT desde las operaciones centrales de ciberseguridad. Como se puede apreciar, sólo el **5% de** las organizaciones declaran **100% de visibilidad de** sus sistemas OT.



Infraestructura OT monitorizada a nivel de ciberseguridad en las empresas. Fuente: Fortinet (2025)

La mayoría se sitúa en coberturas parciales, con el **62%** indicando alrededor de **50%** de visibilidad y **el 30%** en torno a **25%**. Este dato es directamente interpretable como riesgo: con puntos ciegos persistentes, aumenta la probabilidad de **intrusiones prolongadas**, **movimiento lateral no detectado y dificultad para delimitar alcance e impacto** cuando se produce un incidente.

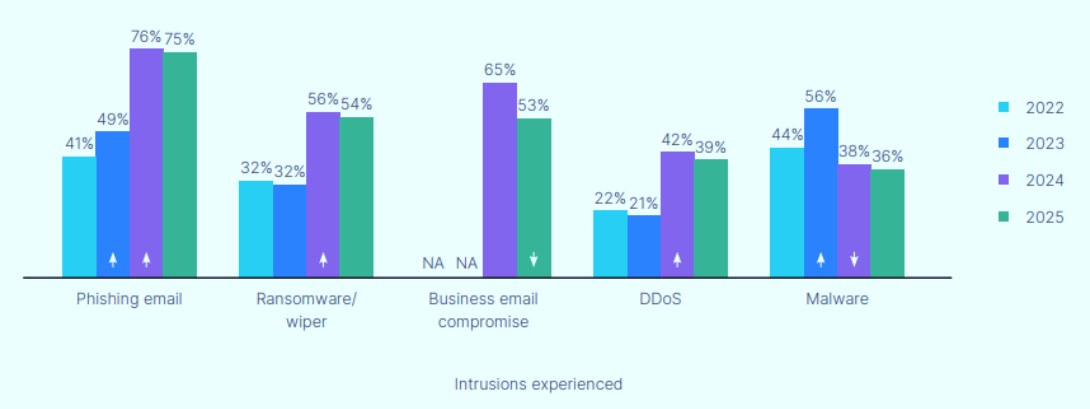
La segunda evidencia es que las intrusiones ya no se entienden en compartimentos estancos.



Entornos impactados por intrusiones el año anterior. Fuente: Fortinet (2025)

El informe refleja que, entre las organizaciones que reportaron intrusiones, en 2025 el **60%** declaró impacto en **ambos dominios TI y OT**. En paralelo, **el 22%** indicó que **solo en OT**, y **el 17%** afectación **solo en TI**. El propio informe matiza que parte del impacto en OT puede producirse porque elementos de TI o conexiones asociadas quedan fuera de servicio, sin que exista necesariamente infección directa dentro de la red OT. Para el análisis de riesgo, la implicación es clara: la continuidad industrial depende de forma incremental de **servicios digitales compartidos**, y eso amplifica el radio de impacto.

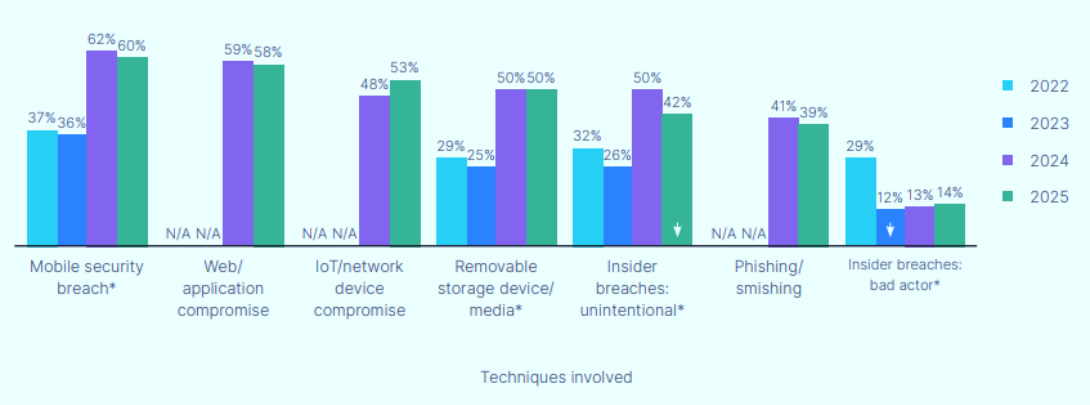
En cuanto a **tipos de intrusión**, el estudio muestra que las tácticas predominantes siguen siendo, en gran medida, "de TI", pero con efectos industriales: **compromiso de correo empresarial (53%)**, **malware (36%)**, **phishing por correo (75%)**, **ransomware/wiper (54%)** y **DDoS (denegación de servicio distribuida) (39%)**.



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

La lectura OT/ICS es que estos vectores pueden traducirse rápidamente en **indisponibilidad operativa** por cifrado, por pérdida de servicios de identidad y gestión, o por medidas de contención que obliguen a operar de forma degradada.

Profundando en este campo, el documento caracteriza **técnicas** asociadas a las intrusiones y apunta una tendencia que incrementa la superficie de ataque industrial: **compromiso web/aplicación (58%)**, **compromiso de dispositivos IoT/de red (14%)**, **brechas en movilidad (60%)**, **uso de medios extraíbles (50%)** e **incidentes internos** tanto no intencionados (**42%**) como por actor malicioso (**14%**). Esto refuerza que la exposición no está sólo en PLC/SCADA: incluye con frecuencia **servicios web asociados**, **dispositivos de red y acceso remoto**, **equipos móviles en operación y mantenimiento y** prácticas que abren puertas involuntarias al adversario.



Evolución temporal de las técnicas de ataque en OT. Fuente: Fortinet (2025)

En conjunto, la combinación de las dos fuentes sostiene una conclusión coherente para Galicia: los sectores con mayor criticidad económica y social son también los que muestran **exposición recurrente a incidentes**, y la materialización del riesgo adopta verse condicionada por tres factores: **convergencia TI/OT**, **visibilidad insuficiente** e **intrusiones basadas en identidad y canales habituales de TI**, que acaban teniendo consecuencias operativas.

4.2 Amenazas emergentes basadas en IA

La aceleración reciente de la **inteligencia artificial (IA)** está modificando la naturaleza del riesgo tecnológico: **no crea necesariamente amenazas completamente nuevas**, sino que **reduce barreras de entrada** y **multiplica la velocidad, a escala y el realismo** de técnicas ya conocidas.

El informe **Cybersecurity Forecast 2026** de Google Cloud/Mandiant ya mencionado anteriormente [6], identifica tres líneas de fondo para el corto y medio plazo: **uso de la IA por parte de atacantes y defensores**, **ciberdelincuencia como principal fuerza disruptiva**, y actividad de **actores estatales**. Aunque el capítulo de ciberdelincuencia es amplio, la lectura más pertinente para OT/ICS **es que el ransomware y la extorsión mediante robo de datos siguen siendo el patrón de mayor impacto económico y operativo**, con efectos en cadena que superan a la víctima inicial y afectan a proveedores, clientes y servicios críticos.

Conclusiones principales del Cybersecurity Forecast 2026. Fuente: Google/Mandiant (2025)

En cuanto al **OT/ICS**, el mismo informe subraya que en 2026 la amenaza disruptiva principal para sistemas industriales continuará siendo la **ciberdelincuencia**, no tanto por intrusiones "puramente industriales", sino por el uso de campañas diseñadas para dañar **software empresarial crítico** (por ejemplo, sistemas de gestión corporativa) que sustentan la **cadena de datos imprescindible para operar OT**.

Sobre esa base, el elemento verdaderamente diferencial es la IA como **amplificador transversal**. Pasamos a continuación a describir de forma más detallada este fenómeno.

- El informe prevé que el uso de IA por parte de grupos de amenaza pase de ser una excepción a ser **la norma**, con aplicaciones directas en **ingeniería social, operaciones de información y desarrollo de software malicioso**. En la práctica, esto se traduce en campañas más rápidas, más personalizadas y persistentes, con capacidad de adaptar mensajes, perfiles y flujos de ataque a cada organización e incluso a cada persona.
- Mencionábamos en la sección 3 que una de las amenazas emergentes más críticas es **la inyección de instrucciones** (prompt injection, ataque que manipula un sistema de IA para que **ignore sus limitaciones de seguridad y** ejecute o produzca salidas guiadas por el atacante). El riesgo aumenta en la medida en que las organizaciones integran modelos de IA en procesos cotidianos, con acceso a conocimiento interno, documentación o repositorios de tickets. En clave industrial, esto puede afectar a asistentes usados para **diagnóstico de incidencias**, análisis de registros, soporte a mantenimiento,

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

gestión documental o automatización de procedimientos: si la entrada de datos incorpora contenido no fiable (por ejemplo, textos pegados de correos, anexos, repositorios o incidencias), un atacante puede intentar inducir al sistema a **exfiltrar información técnica** o a **proponer acciones incorrectas** con impacto operativo.

- Otra área de riesgo emergente es **la ingeniería social habilitada por IA**, especialmente mediante **suplantación de voz** en llamadas (vishing) y otras formas de comunicación hiperrealistas. El informe señala la evolución hacia la clonación de voz para impersonar directivos o personal de TI, lo que encaja particularmente bien en escenarios industriales donde existen procesos de **acceso remoto de mantenimiento**, operaciones con proveedores y autorizaciones urgentes para restauración de servicios. El efecto práctico es que la cadena de convalidación humana se convierte en el ello fehaciente: si una persona con privilegios es engañada, la intrusión puede progresar hasta afectar activos críticos sin explotar vulnerabilidades técnicas sofisticadas.

- La evolución hacia **agentes de IA** introduce un cambio de paradigma adicional. Cuando la IA deja de ser un asistente pasivo y pasa a ejecutar flujos de trabajo (por ejemplo, priorización de alertas, generación de casos, recomendación de acciones, automatización de respuestas), surgen dos problemas:

    1. La necesidad de tratar los agentes como **actores digitales con identidad**, permisos y trazabilidad; y

    2. El riesgo de que la organización delegue acciones de forma implícita, generando **privilegios acumulativos y** decisiones automatizadas sin control suficiente. En OT/ICS, este escenario es particularmente delicado en actividades como **gestión de cambios**, soporte a la operación y coordinación de respuesta a incidentes, donde una acción mal validada puede tener costes ciberfísicos.

- El fenómeno anterior conecta con el riesgo ya observado de **IA en la sombra**: el informe describe la evolución hacia **agentes en la sombra**, esto es, personas que despliegan agentes autónomos para tareas de trabajo sin aprobación corporativa, creando **canales invisibles de datos**, exposición de información sensible e incumplimientos normativos. Para el tejido industrial gallego, esto resulta crítico porque una parte de la información más valiosa no está en bases de datos visibles, sino en documentos, procedimientos, diagramas, registros de

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

mantenimiento y evidencias de operación que pueden acabar "aspiradas" por herramientas no gobernadas.

Esta lectura enlaza de forma natural con la evaluación del **National Cyber Security Centre (NCSC)** del Reino Unido, autoridad técnica en ciberseguridad y parte de GCHQ (la ciberagencia de seguridad e inteligencia británica), que analiza el impacto de la IA sobre la amenaza para la seguridad de la información hasta 2027 [19][20]. Comentamos a continuación las principales conclusiones.

- Indican que la **inteligencia artificial incrementará casi con total certeza la eficacia, velocidad y escala de las operaciones de intrusión cibernética**, lo que derivará en un **aumento de la frecuencia e intensidad de las amenazas** en los próximos años. Este impacto no se producirá tanto por la aparición de vectores completamente nuevos, sino por la **evolución y refuerzo de las técnicas existentes (TTPs)**.

- Los actores de amenaza **ya están empleando IA** para mejorar tareas clave como el **reconocimiento de víctimas**, la **investigación de vulnerabilidades**, **el desarrollo** de exploits, **la ingeniería social**, **la generación básica de malware y el procesamiento de datos exfiltrados**. Hasta 2027, esto **incrementará significativamente el volumen y el impacto de las intrusiones**, especialmente contra organizaciones con niveles de seguridad desiguales.

- En el corto plazo, sólo **actores estatales altamente capacitados** cuentan con los recursos, datos de adiestramiento y conocimiento necesarios para explotar todo el potencial de la IA en operaciones avanzadas. Con todo, la mayoría de los grupos criminales y no estatales **optarán por reutilizar modelos comerciales y open source**, lo que **reduce la barrera de entrada** y eleva las capacidades medias del ecosistema de amenaza. La proliferación de modelos abiertos facilita la creación de herramientas especializadas tanto para defensa como para ataque.

- Uno de los desarrollos más críticos identificados por el NCSC es el avance de la **investigación de vulnerabilidades y desarrollo de exploits asistidos por IA**. La IA permitirá **identificar y explotar fallos de código y configuración con mayor rapidez**, acelerando aún más la carrera entre divulgación de vulnerabilidades y explotación activa. El tiempo entre publicación de un fallo y su uso en ataques **ya se ha reducido a días**, y la IA **lo reducirá aún más**. Este fenómeno **incrementa de forma notable el riesgo para infraestructuras**

críticas y sus cadenas de suministro, especialmente para **sistemas OT con niveles de seguridad más bajos, tecnología legada y energías de parcheo limitadas**. En ausencia de mejoras proporcionales en mitigaciones, existe una **posibilidad realista de que sistemas críticos sean más vulnerables a actores avanzados hasta 2027**.

- En paralelo, la IA también **ayudará a los defensores** (operadores y desarrolladores) a mejorar la seguridad. Sin embargo, el NCSC alerta de una **brecha digital creciente**: mientras algunas organizaciones podrán mantener el ritmo con la defensa asistida por IA, **una parte significativa quedará más expuesta**, incrementando la desigualdad estructural del riesgo.
- El NCSC también prevé que los actores más capacitados emplearán **automatización habilitada por IA para evadir detección y escalar operaciones**. Aunque **no se espera una automatización completa de ataques avanzados de extremo a extremo** antes de 2027, si se consolidará un modelo de **"human–machine teaming"**, en el que la IA automatiza partes de la cadena de ataque (descubrimiento de vulnerabilidades, adaptación de malware, rotación de infraestructura), dificultando la detección y respuesta sin capacidades defensivas equivalentes.
- La **proliferación de herramientas con IA** ampliará el acceso a la capacidad de intrusión a **un mayor número de actores estatales y no estatales**. El sector criminal incorporará IA a sus productos, ofreciendo **servicios de intrusión "las asociaciones a service"**, elevando el nivel de actores poco sofisticados (novatos, mercenarios digitales, hacktivistas) para operaciones oportunistas y disruptivas.
- Otro riesgo destacado es el **aumento de la superficie de ataque** debido a la integración creciente de sistemas de IA en la base tecnológica, especialmente en **infraestructuras críticas**. Los sistemas de IA incluyen datos, modelos, procesos de adiestramiento y evaluación, y tecnología conectada a sistemas corporativos, datos y, progresivamente, **operación OT**. Los atacantes **explotarán esta nueva capacidad** de técnicas ya observadas: **Prompt injection directa e indirecta**, **vulnerabilidades de software**, y **ataques a la cadena de suministro**.
- El informe también alerta de que una **seguridad insuficiente en la IA** facilitará su uso malicioso por actores estatales y criminales. La presión competitiva por lanzar modelos y aplicaciones al mercado puede llevar a **priorizar velocidad**

frente a seguridad, incrementando el riesgo de sistemas comprometidos. Esto se ve agravado por **malas prácticas de gestión de datos y configuración**, como:

- cifrado débil en las transmisiones,
- gestión deficiente de identidades y credenciales privilegiadas,
- recogida excesiva de datos de usuario que facilita ataques dirigidos.

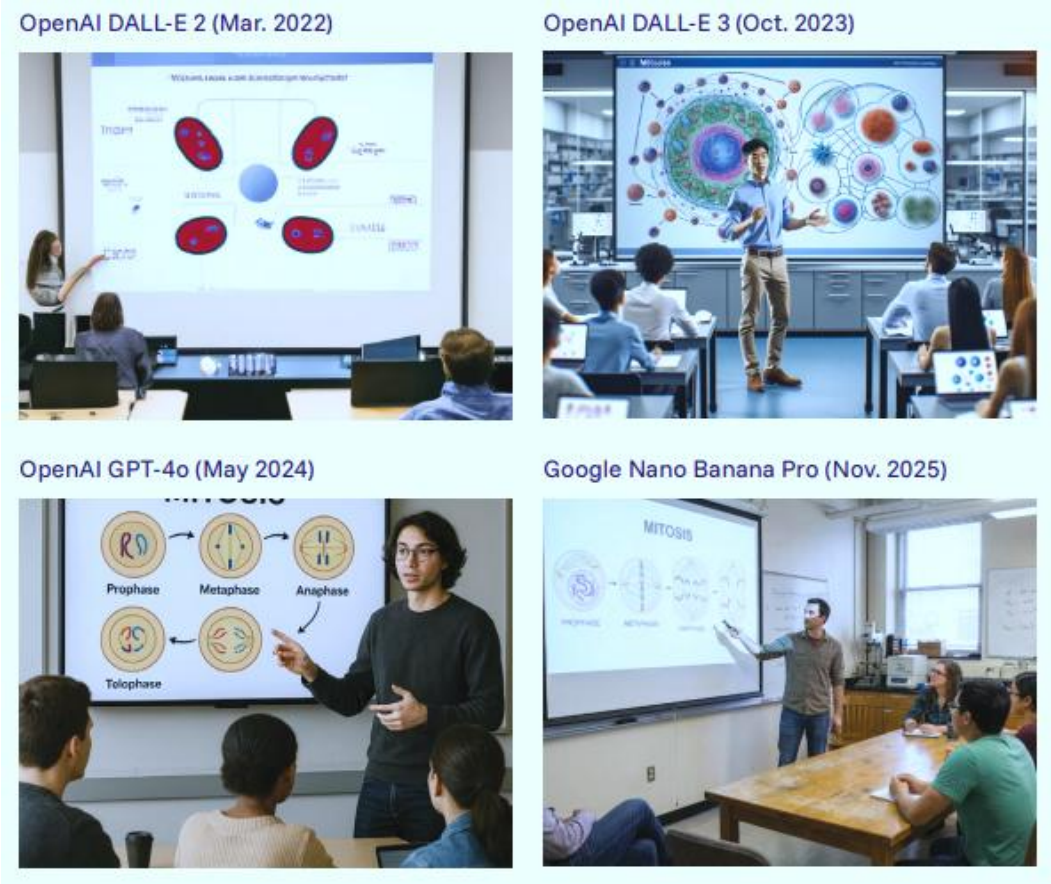
Finalmente, resulta útil elevar el enfoque desde la táctica a la visión de riesgo de alto nivel que propone el **International AI Safety Report 2025**, una revisión internacional sobre capacidades y riesgos de la IA de propósito general, liderada por Yoshua Bengio (informático canadiense Premio Príncipe de Asturias y Premio Turing, considerado uno de los "Padrinos de la IA") [21]. La organización que elabora el reporte está apoyada por múltiples países y entidades, y de un centenar de expertos independientes [22][23].

El valor de este informe para un Observatorio de Ciberseguridad Industrial es que ordena los riesgos en una taxonomía sencilla y accionable, especialmente útil para conectar **amenazas emergentes basadas en IA** con **impactos potenciales en operaciones industriales (OT/ICS)**.

El análisis organiza los riesgos en **tres grupos —riesgos por uso malicioso**, **riesgos por fallos de funcionamiento** y **riesgos sistémicos—**. A continuación, se recogen y se describen, incorporando la lectura OT/ICS cuando procede.

4.2.1 Riesgos de uso malicioso

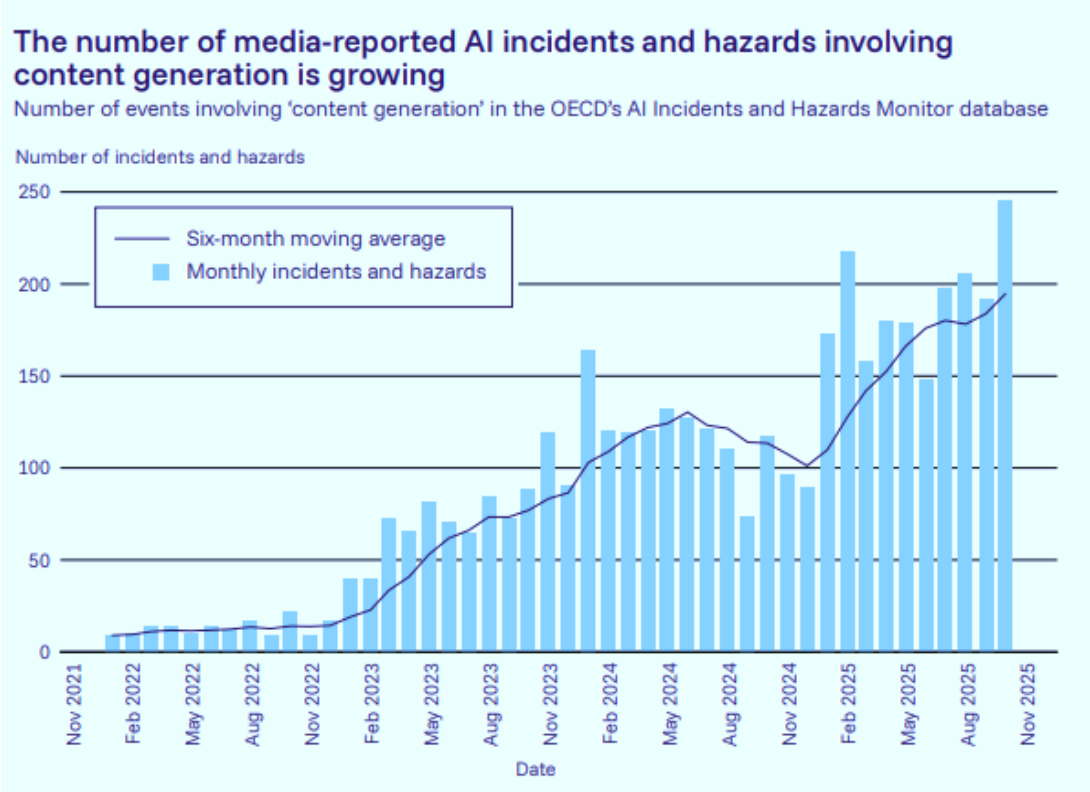
- **Contenido generado por IA y actividad criminal**: la generación masiva de texto, audio, vídeo e imágenes realistas reduce el coste de campañas de fraude y suplantación. En OT/ICS esto se traduce en **ingeniería social más convincente** (falsos procedimientos, peticiones urgentes de acceso remoto, cambios en configuración) que facilita acceso inicial y compromisos de credenciales. Una muestra del vertiginoso avance en este campo a continuación:



Evolución de la calidad de las imágenes generadas por IA. Fuente: International AI Safety Report (2026)

- **Influencia y manipulación**: la IA facilita campañas de persuasión y desinformación más segmentadas, persistentes y difíciles de atribuir. En sectores industriales y servicios esenciales, ello puede agravar crisis al degradar la coordinación, generar pánico o **distorsionar información operativa** durante incidentes (por ejemplo, falsas instrucciones, rumores sobre indisponibilidades, 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 generados por IA en la ODCE. Fuente: International AI Safety Report (2026)

- **Ciberataques**: la IA puede acelerar tareas ofensivas (reconocimiento, preparación de campañas, explotación de fallos, análisis de datos robados) y aumentar la eficacia de operaciones existentes. Para OT/ICS, el riesgo relevante **es el incremento de la cadencia y de la precisión** en la progresión TI→OT, y la posibilidad de automatizar partes del ataque contra infraestructuras de soporte (identidad, correo, acceso remoto) que condicionan la continuidad industrial.

- **Riesgos biológicos y químicos**: aunque exceden del ámbito estricto de la ciberseguridad, son relevantes para la seguridad industrial porque la IA puede apoyar diseño, síntesis o manipulación de sustancias peligrosas (impactando en el área de seguridad física o safety). La lectura OT/ICS es indirecta pero importante: instalaciones químicas, farmacéuticas y de tratamiento de agua pueden verse afectadas por combinaciones de **amenaza física + intrusión digital**, o por abuso de información técnica y procedimientos.

4.2.2 Riesgos derivados de fallos operativos

- **Desafíos de fiabilidad**: la IA puede producir respuestas incorrectas, incompletas o inconsistentes, especialmente fuera de su dominio de

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

adiestramiento. En contexto OT/ICS, donde la seguridad funcional y continuidad son críticas, una recomendación errónea (por ejemplo, un diagnóstico de mantenimiento, una priorización de alarmas o una propuesta de cambio) puede inducir **decisiones operativas peligrosas**.

- **Pérdida de control**: se refiere a la dificultad de asegurar que sistemas de IA —en particular cuando se integran como agentes con capacidad de acción— permanezcan alineados con límites e intenciones humanas. En OT/ICS esto conecta con el riesgo de **automatización no validada**: agentes que ejecutan tareas (cambios, clasificación de incidencias, respuesta automatizada) pueden amplificar un error o introducir efectos no previstos si no existen autorizaciones, trazabilidad y convalidación humana.

4.2.3 Riesgos sistémicos

- **Impactos en el mercado laboral**: la adopción de IA puede reconfigurar perfiles y procesos, generando transiciones rápidas y tensión en competencias. Para OT/ICS, esto puede materializarse como **desequilibrios de capacidades**: aumento de demanda de perfiles híbridos (operación + seguridad + IA) y riesgo de que la falta de personas calificadas degrade la capacidad de supervisión, respuesta y gobernanza.

- **Riesgos para la autonomía humana**: incluye la dependencia excesiva de sistemas de IA para tomar decisiones, la erosión del criterio experto y la influencia sobre elecciones y conductas. En entornos industriales, donde la autoridad operativa y los procedimientos son determinantes, existe riesgo de **delegación implícita y** de pérdida de capacidad de decisión en crisis, especialmente si las recomendaciones de una IA se perciben como "objetivas" sin convalidación.

4.2.4 Cuadro resumen de amenazas

Cerramos la sección con un **cuadro resumen específico de amenazas emergentes basadas en el uso de IA en ciberseguridad industrial**, consolidando los *puntos claves* de Google Cloud/Mandiant, NCSC y el International AI Safety Report 2025, con un enfoque específico en entornos OT/ICS. Alguna de ellas, se solapa con la tabla análoga de la sección 3.1.6.

Riesgo	Descripción	Impacto potencial en OT/ICS
Ingeniería social asistida por IA	Uso de IA para crear mensajes, llamadas o contenidos hiperrealistas (texto, voz, vídeo) orientados a engañar personas con acceso privilegiado.	Acceso inicial no autorizado, compromiso de credenciales, habilitación de acceso remoto y progresión TI→OT.
Ransomware y extorsión amplificados por IA	Mejora de la selección de víctimas, personalización de campañas y explotación de dependencias digitales mediante IA.	Interrupción operativa, paradas de planta, impacto económico en cadena y afectación a proveedores y clientes.
Contenido generado por IA y actividad criminal	Generación masiva de contenido falso para fraude, suplantación y engaño sistemático.	Incremento de ataques oportunistas contra industria; erosión dos controles humanos en procesos críticos.
Influencia y manipulación	Campañas de desinformación más segmentadas, persistentes y difíciles de atribuir gracias a la IA.	Distorsión de la información en crisis, degradación de la coordinación y presión reputacional en servicios esenciales.
Ciberataques asistidos por IA	IA como acelerador de reconocimiento, explotación, malware y análisis de datos robados.	Aumento de la cadencia y precisión de las intrusiones, mayor probabilidad de impacto operativo en OT.
Investigación de vulnerabilidades asistida por IA	Uso de IA para descubrir y explotar fallos de código y configuración con mayor rapidez.	Reducción drástica del tiempo entre divulgación y explotación; alto riesgo para OT legado y con energías de parcheo limitadas.
Explotación acelerada de vulnerabilidades conocidas	Automatización de la identificación y explotación de fallos ya publicados.	Incremento de ataques contra sistemas no actualizados; amenaza directa a infraestructuras críticas.
Prompt injection y manipulación de sistemas de IA	Inyección de instrucciones maliciosas para forzar salidas incorrectas o exfiltración de información.	Exposición de documentación técnica y procedimientos; recomendaciones 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

Agentes de IA con privilegios excesivos	Agentes autónomos con capacidad de acción sin identidad clara ni control de permisos.	Automatización de cambios no validados; riesgos ciberfísicos en gestión de cambios y respuesta a incidentes.
IA de las sombras	Uso no gobernado de herramientas o agentes de IA fuera del control organizativo.	Canales invisibles de salida de datos; incumplimientos normativos y pérdida de control sobre información OT crítica.
Automatización ofensiva habilitada por IA	Automatización parcial de la cadena de ataque (reconocimiento, explotación, evasión).	Intrusiones más persistentes y difíciles de detectar; sobrecarga de los equipos de defensa OT.
Proliferación de herramientas de ataque con IA	Comercialización de capacidades de intrusión "as a service" basadas en IA.	Elevación del nivel medio de actores poco sofisticados; más ataques oportunistas contra industria.
Aumento da superficie de ataque por integración de IA	Conexión de sistemas de IA a datos corporativos y, progresivamente, a la operación OT.	Nuevos vectores de entrada (cadena de subministración, IA comprometida) con acceso indirecto a OT.
Fallos de fiabilidad de la IA	Respuestas incorrectas, incompletas o inconsistentes fuera del dominio de adiestramiento.	Decisiones operativas peligrosas, mala priorización de alarmas e impacto en seguridad funcional.
Pérdida de control sobre los sistemas de IA	Dificultad de garantizar límites, intenciones y comportamiento esperado de los sistemas de IA.	Automatización no validada; amplificación de errores con consecuencias operativas y físicas.
Riesgos biológicos y químicos asistidos por IA	Apoyo de la IA al diseño o manipulación de sustancias peligrosas.	Relevancia indirecta en sectores químico, farmacéutico y agua; amenaza combinada física + digital.
Impactos en el mercado laboral industrial	Reconfiguración rápida de perfiles y competencias por la adopción de IA.	Déficit de perfiles híbridos OT + seguridad + IA; pérdida de capacidad de supervisión y respuesta.

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

Riesgos para la autonomía humana	Dependencia excesiva de la IA y erosión del criterio experto.	Delegación implícita en situaciones críticas y pérdida de capacidad de decisión en crisis.
Brecha digital en la defensa asistida por IA	Desigualdad entre organizaciones que pueden adoptar defensa con IA y las que no.	Aumento estructural de la exposición en industria mediana e infraestructuras con menor madurez.
Mala seguridad por diseño en sistemas de IA	Priorizar velocidad de lanzamiento frente a la seguridad; malas prácticas de datos e identidad.	Compromiso de sistemas de IA conectados a OT; escalado de intrusiones y filtración de datos críticos.

Cuadro de riesgos basados en el uso de la IA del Informe. Fuente: elaboración propia (2026)

Podemos concluir que la IA no debe tratarse sólo como tecnología, sino como un **factor transversal de riesgo** que afecta a personas, procesos y tecnología. Por ello, las recomendaciones de securización deben combinar **gobernanza** (uso permitido, gestión de datos e identidades, control de proveedores), **controles técnicos** (tolerancias, registros, aislamiento, permisos mínimos) y **convalidación operativa**, tal y como se desarrollará en el apartado correspondiente de recomendaciones.

5 Gobierno de la ciberseguridad y resiliencia

Sirva como introducción de este apartado, el artículo publicado por **Industrial Cyber** que aborda una cuestión clave y recurrente en la ciberseguridad industrial: la existencia **de una debilidad estructural en la forma en que las organizaciones industriales gobiernan, gestionan y comunican los incidentes de seguridad en entornos OT/ICS,** en un contexto en el que las amenazas evolucionan más rápido que los modelos organizativos tradicionales [24].

En este sentido, el artículo sirve como punto de partida para reflexionar sobre la necesidad de evolucionar hacia modelos más integrados y resilientes, sobre los que, posteriormente, **se propondrán una serie de recomendaciones ejemplificativas extraídas de la literatura especializada**, orientadas a reforzar la capacidad real de gestión del riesgo en ciberseguridad industrial.

El escrito señala que **la notificación y gestión formal de incidentes de ciberseguridad en entornos OT/ICS continúa siendo una debilidad estructural**, especialmente en organizaciones industriales que operan con **modelos de gobernanza heredados**, diseñados para entornos TI más estáticos y previsibles. Mientras las amenazas evolucionan en velocidad, escala e impacto, **los mecanismos de reporte, escalado y aprendizaje organizativo no avanzan al mismo ritmo**.

Uno de los puntos centrales es que **muchos incidentes OT no se reportan o se reportan de forma incompleta**, bien por temor a impacto reputacional, por falta de obligaciones claras, o porque **no se reconocen como incidentes de ciberseguridad**, sino como fallos operativos o técnicos. Esto provoca una **infrarrepresentación del riesgo real**, dificulta el análisis agregado y limita la capacidad del sector para aprender de eventos previos, como ya adelantábamos en el informe de Dragos.

El artículo destaca también que **la convergencia TI/OT** incrementó la frecuencia de incidentes con impacto operativo, pero **la gobernanza sigue fragmentada**: TI adopta gestionar la seguridad de la información y OT la continuidad del proceso, sin mecanismos eficaces de coordinación cuando un incidente afecta a ambos dominios. Como consecuencia, **las decisiones de reporte, respuesta y comunicación se toman tarde o de forma desaliñada**.

Otro aspecto relevante es **la dependencia de tecnologías legadas y cadenas de suministro complejas**, que dificulta la atribución, la evaluación de impacto y la

comunicación externa. En muchos casos, la falta de visibilidad sobre activos OT y sobre la progresión de un ataque hace que **la organización no tenga certeza suficiente para activar procedimientos formales de notificación**.

Se pone asimismo el foco **en el desfase entre las nuevas obligaciones regulatorias emergentes** (especialmente en infraestructuras críticas) y la realidad operativa de las organizaciones industriales. La ausencia de procesos maduros de reporte y de métricas compartidas supone un riesgo adicional: **el incumplimiento no es sólo normativo, sino también estratégico**, al impedir una gestión del riesgo basada en evidencias.

Sostienen los autores que **mejorar la notificación de incidentes OT no es un ejercicio administrativo,** sino un **factor clave de resiliencia**. Sin datos fiables, oportunos y comparables, las organizaciones industriales seguirán reaccionando de forma aislada, mientras las amenazas —cada vez más automatizadas y asistidas por IA— **superan los modelos de gobernanza tradicionales**.

A partir de este análisis, se recoge una conclusión de fondo: **la gestión eficaz de los riesgos en entornos OT no puede basarse exclusivamente en controles técnicos aislados**, sino que requiere **construir una organización con una gobernanza clara, una estructura definida y funciones de seguridad adaptadas a la criticidad de la operación**. Profundizaremos ahora en estos dos campos, basándonos en elaboración propia y las fuentes de la literatura de gobierno y seguridad de la información propuestas [25][26][27][28].

5.1 Estructura organizativa

La **gobernanza** de un **Programa de Seguridad de la Información** constituye un **higiénico organizativo imprescindible** para gestionar de forma consistente los riesgos a los que están sometidas las organizaciones industriales gallegas, **sean estos tecnológicos, operativos, regulatorios o reputacionales**.

Resulta necesario disponer de una **estructura clara de gobernanza, con una** asignación explícita de responsabilidades**,** funciones de seguridad bien definidas **y mecanismos de coordinación y supervisión al máximo nivel**, que permitan identificar, evaluar, priorizar y tratar los riesgos de forma continuada y alineada con los objetivos de negocio. La aproximación propuesta —basada en la implicación de la alta dirección, en la independencia de las funciones de control, en la separación y coordinación entre IT/OT y Seguridad, y en la implantación de un conjunto coherente de capacidades a lo largo de todo el ciclo de vida del riesgo— **no lo elimina, pero**

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

reduce de manera estructural la incertidumbre y la exposición, convirtiéndose en un requisito previo para cualquier estrategia eficaz de resiliencia industrial.

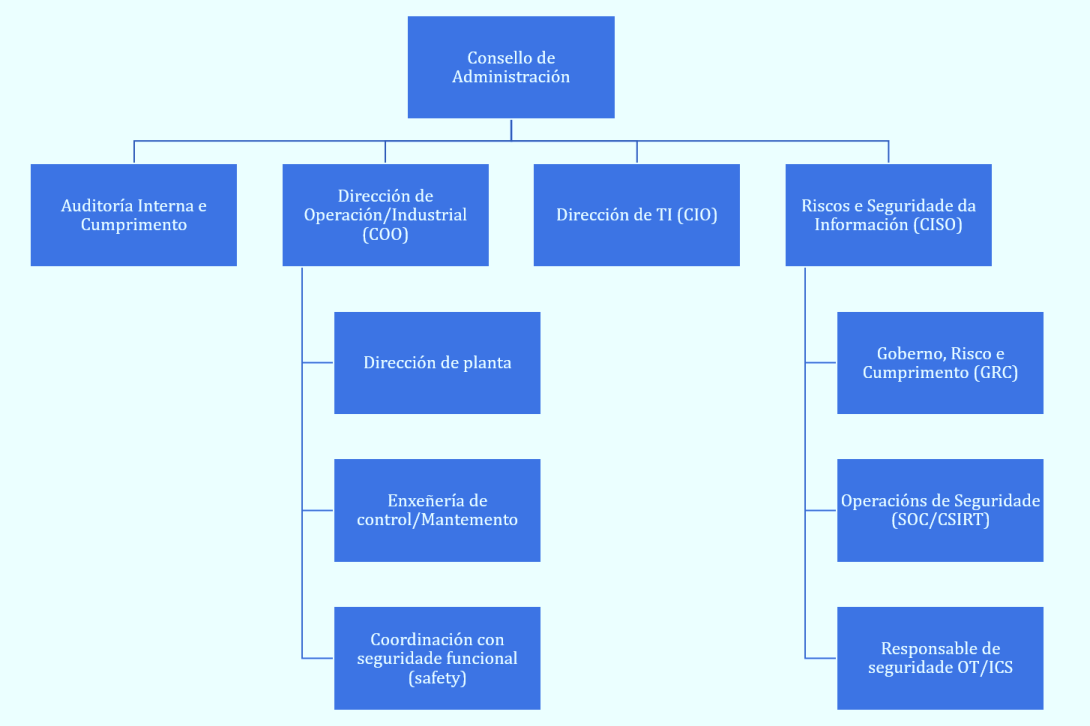
Teniendo en mente este marco, **se proponen una serie de recomendaciones ejemplificativas extraídas de la literatura especializada**, con el objetivo de ilustrar como adaptar estos principios a diferentes realidades organizativas del ámbito industrial gallego.

5.1.1 Estructura global

Es de dejar claro, en primer lugar, que **no existe una forma de organización canónica** que sea óptima en todos los escenarios y para cualquier entidad, ni tampoco esto implica que no existan otras alternativas que puedan funcionar adecuadamente. Con todo, sí se observa que existen **determinadas prácticas** que, en términos generales, adoptan ofrecer buenos resultados.

En todo caso, para una estructura jerárquica determinada, debe existir un **gobierno adecuado**, una **asunción clara de responsabilidades** y una **comunicación efectiva entre áreas**, de manera que se asegure que cada función se desempeña con éxito tanto a nivel interno de cada equipo como en el conjunto de la organización.

Veamos, a continuación, una posible propuesta de organización.



Organigrama propuesto para el gobierno de la seguridad IT/OT. Fuente: 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 Consejo de Administración / Comité ejecutivo

En la cúspide se sitúa **el Consejo de Administración (o Comité ejecutivo)**, responsable último del **Gobierno, supervisión y rendición de cuentas** sobre la operación y sobre el **Programa de Seguridad**. Su función no se limita a la aprobación presupuestaria: implica **definir la dirección estratégica**, establecer el **apetito de riesgo**, aprobar políticas y criterios de priorización, y asegurar que existen capacidades reales para **prevenir, detectar, responder y recuperarse** de incidentes.

En una organización con OT, esta supervisión debe cubrir explícitamente:

- **Protección de activos críticos**, incluyendo activos industriales e infraestructuras de soporte.
- **Continuidad del negocio y resiliencia operativa**, asumiendo que un incidente puede derivar en parada, operación degradada o impacto en servicios esenciales.
- **Cumplimiento y evidencia de control**, garantizando trazabilidad de las decisiones y cambios que afectan a la operación.

5.1.3 Auditoría interna y cumplimiento

El área de **Auditoría Interna y cumplimiento** debe depender exclusivamente del Consejo/Comité **y mantener independencia jerárquica absoluta**, con el mandato de evaluar y mejorar la eficacia del sistema de control interno. En entornos con componente OT/ICS, esto requiere capacidad para auditar no sólo TI, sino también operación: **gestión de accesos remotos industriales**, **gestión de cambios en sistemas de control**, **segmentación y arquitectura de red OT**, **inventarios de activos**, **registros y trazas**, o **gobernanza de proveedores industriales**.

5.1.4 Operaciones industriales (OT)

La **Dirección de Operaciones/Industrial (COO)**, junto con las **Direcciones de Planta**, constituye **el eje central de la gobernanza OT**, al asumir la responsabilidad directa sobre **la continuidad operativa**, **la seguridad del proceso industrial** y la ejecución diaria de las operaciones. Este ámbito se completa con la **Ingeniería de Control y Mantenimiento**, como función técnica clave responsable del **diseño, configuración, operación y mantenimiento** de los sistemas de automatización y control industrial a lo largo de todo su ciclo de vida.

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

De manera complementaria, la **Seguridad funcional (safety)** forma parte esencial de esta gobernanza, al ser la función encargada de garantizar la protección de personas, instalaciones y procesos frente a riesgos ciberfísicos. Su integración con las operaciones industriales es imprescindible para asegurar que las decisiones técnicas y organizativas no comprometan los niveles de seguridad exigidos por el proceso ni introduzcan riesgos adicionales durante cambios, incidencias o situaciones de operación degradada.

Para que la gestión del riesgo en entornos **OT/ICS** sea **realista, efectiva y ejecutable**, resulta imprescindible que en el ámbito de Operaciones estén claramente definidos los siguientes elementos:

- La **propiedad de activos y sistemas industriales** (asset owners / system owners), asignada a responsables de **Operaciones** o de **Ingeniería de control/Mantenimiento** según corresponda, para dominios como **SCADA, PLC, historiadores, redes industriales, estaciones de ingeniería, HMI, sistemas instrumentados de seguridad** y plataformas auxiliares, garantizando responsables identificables para la toma de decisiones y la aceptación del riesgo.
- Un **proceso formal de gestión de cambios**, liderazgo desde **Operaciones** e **Ingeniería de Control/Mantenimiento**, **y coordinado con la función de ciberseguridad y con la seguridad funcional (safety)**, que equilibre de forma explícita **seguridad, disponibilidad y seguridad del proceso**. Este proceso debe incluir evaluación previa de riesgo, pruebas técnicas, definición de ventanas de intervención, convalidación en producción y registro documental.
- Un **mecanismo claro de toma de decisiones ante compromisos o equilibrios entre seguridad, disponibilidad y seguridad funcional**, que permita escalar adecuadamente aquellas situaciones en las que el impacto potencial supere el ámbito de la planta, involucrando cuando sea necesario a la **Dirección de Operaciones/Industrial** y al **nivel ejecutivo**.

Esta estructura garantiza que la seguridad en OT no se gestione de forma ajena a la operación, sino **plenamente integrada en los procesos industriales**, con la participación activa de **Operaciones, Ingeniería de control/Mantenimiento y Seguridad funcional,** y con la coordinación necesaria con el resto de las funciones corporativas implicadas.

5.1.5 Informática corporativa

La **TI corporativa** (O función equivalente) mantiene las responsabilidades de diseño y operación de sistemas corporativos, infraestructura local y en nube, soporte y gestión de proveedores tecnológicos. En organizaciones industriales, TI es también una dependencia crítica de la operación: **identidad**, **correo**, **directorio**, **redes**, **acceso remoto** y plataformas corporativas condicionan la continuidad industrial y pueden actuar como vía de progresión hacia OT en movimientos laterales.

Por ello, la coordinación TI–OT debe estar institucionalizada mediante **procedimientos compartidos**, canales de escalado y trazabilidad de decisiones, evitando que dependa sólo de relaciones informales.

5.1.6 Ciberseguridad y gestión de riesgos tecnológicos

La función de **ciberseguridad y gestión de riesgos tecnológicos** debe mantener **independencia** y capacidad efectiva de priorización, con el reporte adecuado al nivel ejecutivo. La estructura recomendable combina:

- **Gobierno, riesgo y cumplimiento (GRC)**: gestión del riesgo tecnológico (incluyendo OT), riesgo de proveedores y cadena de suministro, cuerpo normativo interno, indicadores y reporte, y formación.
- **Operaciones de seguridad**: monitorización, respuesta a incidentes, gestión de vulnerabilidades y amenazas y coordinación con proveedores de servicio.
- En entornos OT/ICS es recomendable asimismo una función específica: el/la **Responsable de Seguridad OT/ICS**, que garantice que políticas, controles y operaciones de seguridad son aplicables a la realidad industrial y que existe coordinación diaria con la planta. Esta función debe tener **dependencia funcional del CISO** y coordinación operativa con **Operaciones/Plantas**, especialmente en ámbitos como gestión de cambios, acceso remoto, monitorización y respuesta, etc.

5.1.7 Coordinación TI–OT–Seguridad

La **coordinación entre TI, OT y ciberseguridad es crítica porque la protección y la continuidad dependen de infraestructuras compartidas y de respuestas coordinadas**. En particular, la respuesta a incidentes en OT requiere contener y recuperar sin comprometer la seguridad funcional ni la continuidad del proceso. Por este motivo, se recomienda institucionalizar un **mecanismo estable de coordinación**

(por ejemplo, un comité técnico TI–OT–Seguridad o una oficina de programa), con participación de Operaciones/Planta, para asegurar **visibilidad mutua**, **priorización consistente y ejecución segura** de cambios y medidas.

5.2 Funciones de seguridad

A continuación, se le cuenta una **propuesta de funciones de seguridad** orientada a organizaciones industriales, con el objetivo de cubrir de manera coherente todo el **ciclo de vida del riesgo**, desde su identificación hasta la recuperación tras un incidente. Esta propuesta parte de una visión integral de la seguridad, en la que **la seguridad de la información**, **la continuidad operativa y la protección de los procesos industriales** se abordan de forma conjunta, evitando una aproximación restringida exclusivamente al ámbito TI.

Como marco de referencia conceptual se emplea el **NIST Cybersecurity Framework (NIST CSF)**, un estándar internacional ampliamente adoptado que estructura las capacidades de ciberseguridad en torno a cinco funciones nucleares: **Identificar, Proteger, Detectar, Responder y Recuperar**. Estas funciones no describen soluciones técnicas concretas, sino **capacidades organizativas y operativas** que deben estar presentes en cualquier modelo de seguridad maduro [29][30].

Funciones NIST CSF 2.0. Fuente: NIST (2024)

Las funciones de seguridad que se describen a continuación se inspiran en estas cinco funciones del NIST CSF, que se toman como referencia común, pero se presentan con una **visión orientada al negocio y a la operación industrial**, de manera que resulten

comprensibles y aplicables al contexto real de las organizaciones con activos **OT/ICS**. Esta aproximación tiene en cuenta los riesgos, limitaciones y particularidades identificadas en las secciones previas del informe.

El **NIST CSF**, así como su aplicación específica a entornos industriales e infraestructuras críticas, se aborda con mayor detalle en **la Guía Normativa del Observatorio de Ciberseguridad Industrial de la AMTEGA** [31], que complementa este informe con un análisis más profunda de los requisitos, buenas prácticas y marcos de referencia aplicables.

Seguidamente se describe el conjunto de funciones **de seguridad propuestas**, indicando de forma implícita su correspondencia con las capacidades de **Identificación, Protección, Detección, Respuesta y Recuperación** del NIST CSF. Tal y como se expone, las cinco funciones nucleares del marco se encuentran cubiertas, con un enfoque adaptado a la realidad de las organizaciones industriales.

Funciones del Programa de Seguridad y relación con el NIST CSF. Fuente: elaboración propia (2026)

Se indica también en la figura la responsabilidad de cada función.

- Nombre de color blanco: área de Gestión del Riesgo (GRC).
- Color gris: área de Operaciones de Seguridad.

Pasemos ahora a describir cada función de forma individual.

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

5.2.1 Gestión del riesgo tecnológico y operativo

La **gestión del riesgo tecnológico y operativo** se encarga de identificar, analizar, evaluar y hacer seguimiento de los riesgos que afectan a la organización, tanto en el ámbito de las **tecnologías de la información (TI)** como en los **entornos operativos industriales (OT/ICS)**. Se trata de un componente transversal y estructura del modelo de gobernanza, desde el cual se realizan revisiones **como mínimo anuales**, así como análisis **ad hoc** cuando se producen cambios relevantes en el contexto tecnológico, operativo, regulatorio o de amenaza.

Estos análisis pueden conducirse empleando metodologías reconocidas, como **ISO/IEC 27005**, **ISO 31000** u otras aproximaciones equivalentes, adaptadas a la realidad industrial. Su objetivo es facilitar una visión estructurada del riesgo que permita el **seguimiento por parte de un Comité de revisión del riesgo tecnológico**, en lo que deben estar representadas las áreas de **Operaciones (OT)**, **TI**, **Gestión de Riesgos**, **Ciberseguridad**, **Negocio** y, cuando corresponda por el impacto potencial, el **nivel ejecutivo o Consejo**. Será este último quien adopte las decisiones de mayor impacto mediante **procesos formales de aprobación y aceptación del riesgo**.

De forma habitual, los riesgos son **identificados, evaluados, priorizados, tratados y monitorizados** a través de un registro centralizado, que puede gestionarse mediante plataformas especializadas de **gobernanza, riesgo y cumplimiento (eGRC)** o, en organizaciones con menor madurez, mediante herramientas más sencillas. En cualquier caso, el objetivo es garantizar un **seguimiento sistemático de los riesgos** y proporcionar información relevante a los distintos **stakeholders**, de manera que se mantenga un nivel de **incertidumbre suficientemente bajo** para cumplir los objetivos estratégicos, operativos y de continuidad de la organización.

Se mantendrá un **registro de riesgos permanentemente actualizado**, en el que cada riesgo contará con un **propietario claramente identificado** (Operaciones, TI o Negocio) responsable de ejecutar los planes de tratamiento acordados. La función de **Ciberseguridad o Gestión del Riesgo Tecnológico**, según la estructura organizativa, asumirá la coordinación global del proceso y la propiedad de aquellos riesgos **transversales**, no asociados a un servicio, activo o planta concreta, incluyendo los que afectan simultáneamente a múltiples dominios TI y OT.

Para la correcta implantación de esta función, existen una serie de aspectos clave que deben definirse de manera explícita:

- La **delimitación del alcance** del proceso de gestión del riesgo, incluyendo sistemas, procesos, activos industriales y cadenas de suministro relevantes.
- La definición del **apetito de riesgo** de la organización, aprobado al nivel ejecutivo, especialmente en lo relativo a continuidad operativa, seguridad del proceso e impacto en servicios esenciales.
- El acuerdo sobre la **metodología de identificación, evaluación y tratamiento de los riesgos**, adaptada a la realidad TI y OT.
- La **asignación clara de roles y responsabilidades**, incluyendo propietarios de riesgo y mecanismos de escalado.
- El **modelo de toma de decisiones**, diferenciando entre riesgos aceptables a nivel operativo y aquellos que requieren aprobación ejecutiva.

Adicionalmente, la función debe alinearse con los **principios de actuación establecidos en la norma ISO 31000 de Gestión del Riesgo**, que constituyen una guía sólida para una gestión eficaz y sostenible. Estos principios incluyen:

- **Gestión integrada**: la gestión del riesgo no es una actividad aislada, sino que debe estar integrada en los procesos de la organización, desde la planificación estratégica hasta la ejecución operativa, la gestión de proyectos y la definición de políticas y procedimientos.
- **Estructurada y exhaustiva**: el proceso debe seguir una aproximación sistemática que permita obtener resultados coherentes y comparables en el tiempo.
- **Adaptada al contexto**: el marco de referencia y los procesos deben ajustarse continuamente al contexto interno y externo de la organización, teniendo en cuenta su realidad industrial, su sector y sus objetivos.
- **Inclusiva**: deben participar de manera oportuna los distintos grupos de interés, garantizando decisiones informadas, un nivel adecuado de concienciación y una conexión real con el negocio y con la operación.
- **Dinámica**: la gestión del riesgo debe basarse en información histórica, situaciones actuales y expectativas futuras, incorporando la evolución de las amenazas y del contexto tecnológico.

- **Atención a los factores humanos y culturales**: los comportamientos, percepciones y sesgos de las personas influyen directamente en la gestión del riesgo, por lo que deben ser considerados de forma explícita.
- **Mejora continua**: el proceso debe optimizarse de manera constante, incorporando la experiencia adquirida, el feedback de los incidentes y la evolución de las buenas prácticas.

En conjunto, esta función permite establecer una **base sólida para la toma de decisiones informadas**, asegurando que los riesgos tecnológicos y operativos en entornos **OT/ICS** se gestionan de forma sistemática, proporcionada y alineada con la estrategia y con la continuidad de la organización.

5.2.2 Arquitectura de seguridad (TI y OT/ICS)

La función de **Arquitectura de seguridad** abarca todo lo relativo a la **gestión, operación y representación formal** (diseños, diagramas, tablas, modelos y especificaciones) de los componentes de seguridad de una organización. Su objetivo es describir de manera estructurada las **funciones, estructura y las interrelaciones** entre los distintos controles, servicios y productos de seguridad, garantizando una visión coherente y consistente tanto en entornos **TI** como **OT/ICS**.

En organizaciones industriales, esta función resulta especialmente crítica, ya que la arquitectura debe equilibrar **seguridad, disponibilidad y seguridad del proceso**, teniendo en cuenta limitaciones tecnológicas, dependencias de fabricantes, ciclos de vida largos y la necesidad de evitar impactos no deseados en la operación.

Arquitectura de redes

La arquitectura de redes se encarga de asegurar que toda **la documentación asociada a dispositivos, redes, comunicaciones y cableado** se encuentra permanentemente **actualizada, accesible al personal autorizado** y revisada de forma periódica por los responsables correspondientes. Siempre que sea posible, esta gestión debe apoyarse en **herramientas específicas** de documentación y gestión de red.

Los dispositivos de red —como **routers, switches, firewalls, balanceadores, pasarelas industriales y dispositivos de comunicación OT**— deben estar correctamente configurados, prestando especial atención a aspectos como:

- **Bastionado y configuración segura**.
- **Registro y almacenamiento seguro de eventos de seguridad**.

- **Generación de alertas y excepciones** ante comportamientos anómalos.
- **Integración con los mecanismos de control de acceso y gestión de identidades**.

Debe implementarse una **segmentación adecuada de la red**, especialmente relevante en entornos industriales, manteniendo un esquema que diferencie claramente:

- **Zona no segura**, que incluye Internet y servicios de terceros no controlados por la organización.
- **DMZ (zona desmilitarizada)**, que permite comunicaciones controladas entre la zona no segura y los sistemas internos.
- **Zona de confianza**, de acceso restringido, que permite principalmente conexiones salientes y conexiones entrantes muy controladas desde la DMZ.
- **Zona restringida u OT**, que no permite comunicación directa con la DMZ ni con la zona no segura, y sólo admite conexiones internas estrictamente necesarias y documentadas.

En el caso de **conexiones externas** (proveedores autorizados, mantenimiento remoto o personal desplazado), deben emplearse soluciones como **VPN con autenticación fuerte** (OTP, certificados, tokens, etc.) o entornos de acceso controlado (clientes ligeros, escritorios virtuales), manteniendo siempre un **inventario actualizado de conexiones remotas, usuarios y permisos asociados**.

Seguridad de la red Wi-Fi

Como buena práctica, las redes **Wi-Fi de invitados** deben estar completamente **segmentadas, sin** acceso a recursos corporativos ni industriales. En entornos industriales, además, se recomienda **ocultar routers y cableado**, así como ajustar la potencia de las antenas para evitar que la señal supere el perímetro de las instalaciones.

La red Wi-Fi corporativa debe emplear **protocolos y mecanismos de autenticación robustos**, y mantener una configuración bastionada, incluyendo la desactivación de funcionalidades innecesarias, la protección frente a cambios no autorizados y la revisión periódica de los parámetros de seguridad.

Gestión de cambios en arquitectura de seguridad

En el ámbito de la arquitectura de seguridad, **la gestión de cambios** se refiere específicamente a modificaciones que pueden afectar a la postura de seguridad de sistemas TI y OT, tales como:

- Actualizaciones y modificaciones de software, incluidos parches.
- Cambios en parámetros de configuración y tablas de control.
- Modificaciones en la estructura de la información (bases de datos, ficheros, registros).
- Cambios en procedimientos operativos y de usuario.
- Correcciones de emergencia.
- Cambios en infraestructuras, equipos y redes.

Estos cambios deben revisarse y aprobarse mediante un **procedimiento formal**, normalmente apoyado por un **Change Advisory Board (CAB)**, en el que participen **TI, Operaciones y Ciberseguridad**, y en el que, en entornos OT, debe considerarse también la **seguridad funcional (safety)**. Además, debe existir un procedimiento específico para **cambios de emergencia**, garantizando siempre la trazabilidad y la evaluación posterior del impacto.

Gestión de activos

La **gestión de activos hardware y software** es un requisito básico para la seguridad. Debe mantenerse un **inventario protegido y actualizado** que incluya tanto activos TI como OT, facilitando la posterior aplicación de controles de seguridad, la gestión de vulnerabilidades y la respuesta a incidentes.

En entornos industriales, este inventario debe recoger también información sobre **criticidad operativa**, localización, dependencia de proveedores, versiones de formular y relaciones con otros sistemas.

Copias de seguridad

Debe realizarse una **copia de seguridad de la información esencial**, incluyendo datos de negocio, sistemas y servicios críticos, con una periodicidad acorde a los **objetivos de recuperación** a nivel de tiempos y puntos de información previos **(RTO/RPO)** definidos por la organización.

La práctica habitual **es emplear estrategias de respaldo en capas**, que permitan restaurar rápidamente la información crítica y recuperar progresivamente el resto. Dado el riesgo creciente de **ransomware**, es imprescindible contar con una estrategia de protección de copias que incluya, por ejemplo, **segmentación de red**, almacenamiento aislado o destinos alternativos, así como **cifrado de las copias** para evitar accesos no autorizados.

Protección de endpoints (TI e OT)

Las **estaciones de trabajo y endpoints** deben adquirirse a proveedores homologados, probarse antes de su puesta en servicio, contar con acuerdos de mantenimiento y emplear **configuraciones técnicas estándar**. En entornos OT, esto incluye estaciones de ingeniería, HMI y Equipos de Operación.

Los endpoints deben estar protegidos frente a accesos no autorizados mediante:

- **Mecanismos de bloqueo automático por inactividad**.
- **Controles de acceso adecuados**.
- **Cortafuegos personales y cifrado de la información sensible**.

Los sistemas de protección frente a malware deben estar instalados, activos y configurados para analizar memoria, ficheros, medios extraíbles, correo electrónico y descargas, proporcionando alertas, cuarentena y eliminación segura, sin permitir la desactivación no autorizada ni afectar a la operación estándar.

En el caso de **servidores y sistemas críticos**, deberán configurarse según **líneas base documentadas**, como las guías de bastionado del **Center for Internet Security (CIS)** [32], teniendo en cuenta las limitaciones propias de OT. Como mínimo, debe considerarse:

- Desactivación o restricción de servicios innecesarios.
- Restricción del acceso a utilidades críticas y a la configuración.
- Aplicación controlada de parches y actualizaciones de seguridad.

Uso de Internet

El acceso a Internet debe estar **restringido por usuarios y funcionalidades**, apoyado por **políticas de uso aceptable** y acciones de concienciación. La organización debe conocer sus conexiones primarias y secundarias a Internet, quien está autorizado a

acceder y que **controles tecnológicos** existen para inspeccionar, filtrar y actuar sobre tráfico sospechoso (proxies, filtrado web, WAF, etc.).

En entornos OT, el acceso directo a Internet debe ser **excepcional**, estar justificado y documentado, y canalizarse siempre a través de mecanismos de control específicos.

Controles generales de seguridad

Los **controles generales de seguridad** incluyen políticas, procedimientos y mecanismos técnicos destinados a proteger la **confidencialidad, integridad y disponibilidad de** la información y de los procesos. Entre los marcos de referencia disponibles, los **Controles Críticos de Seguridad del CIS** constituyen una guía práctica y concisa, estructurada en 18 dominios que cubren desde la gestión de activos hasta la protección de datos y copias de seguridad [33]. Muchos otros marcos y estándares se contemplan en la Guía Normativa del Observatorio [31].

Un aspecto crítico es el **diseño de nuevos sistemas o la evolución de los existentes**. Los controles de seguridad deben considerarse desde las fases iniciales, evaluando su viabilidad e impacto. Cuando no sea posible implantarlos, deberá tomarse una **decisión basada en riesgo**, optando por omitir, posponer o compensar los controles mediante medidas alternativas, documentando siempre esta decisión.

En este proceso deben analizarse, entre otros aspectos:

- Los **flujos de información previstos**, incluyendo entradas, salidas, almacenamiento e interconexiones con otros sistemas.
- La totalidad de **controles de seguridad necesarios** para proteger la información y los procesos.
- Los controles específicos exigidos por los procesos **de negocio y operación industrial** soportados.
- La forma y el lugar donde aplicar los controles, mediante una **arquitectura de seguridad documentada**.
- La revisión de los diseños para asegurar el cumplimiento de los requisitos.
- La documentación explícita de aquellos controles que no cumplan plenamente los criterios establecidos.

En conjunto, la función de Arquitectura de Seguridad proporciona la **base técnica y organizativa** para una protección eficaz y sostenible de los sistemas **TI y OT/ICS**,

garantizando que la seguridad se integra desde el diseño y se mantiene de forma coherente a lo largo del tiempo.

5.2.3 Cumplimiento normativo y regulatorio

El **National Institute of Standards and Technology (NIST)** define una política de seguridad de la información como un *"conjunto de directivas, reglamentos, normas y prácticas que prescriben como una organización gestiona, protege y distribuye la información"*. Esta definición resulta plenamente aplicable a los entornos **OT/ICS**, con la particularidad de que la información y los sistemas que la procesan están directamente ligados a la operación de procesos físicos críticos.

Las políticas de seguridad constituyen **el nivel más alto de la jerarquía normativa interna** para la implantación de Programas de Gestión de la Seguridad. Se trata de documentos de alto nivel, de carácter general, que establecen que activos deben ser protegidos y bajo que principios, sin entrar en un excesivo detalle operativo. En el ámbito OT, estas políticas deben reflejar explícitamente prioridades como la **seguridad funcional, la disponibilidad y continuidad de la operación**, por encima de otras consideraciones habituales en entornos IT.

Estas políticas definen los **objetivos estratégicos de seguridad** y establecen el marco para los niveles inferiores, materializados mediante estándares, procedimientos, instrucciones técnicas, guías operativas y líneas base específicas para sistemas industriales. Su función es servir de referencia para diseñar e implantar los controles de seguridad de forma coherente y alineada con el riesgo.

Aun siendo documentos generales, las políticas deben **adaptarse al contexto operativo de la organización**, a su sector industrial, al nivel de criticidad de los procesos y a su marco regulatorio. Idealmente, deben ser **atemporales**, de forma que no dependan de tecnologías concretas, sino de principios estables que guíen la toma de decisiones a lo largo del tiempo. En entornos OT/ICS, esto es especialmente relevante debido a los largos ciclos de vida de los sistemas industriales.

En este marco, adoptan existir políticas y procedimientos específicos para ámbitos como:

- buenas prácticas de seguridad en entornos industriales,
- control de accesos físicos a instalaciones y zonas críticas,
- control de accesos lógicos a sistemas OT,

- gestión de usuarios y cuentas con privilegios,
- políticas de contratación y formación de personal con acceso a sistemas críticos,
- gestión de proveedores y de la cadena de suministro industrial,
- clasificación y tratamiento de la información técnica y operativa,
- gestión de incidentes de seguridad con impacto operacional o de seguridad física.

Los **requisitos legales y regulatorios** deben ser reconocidos y asumidos por la capa de dirección, así como por el resto de los actores implicados en la seguridad, incluyendo operaciones, mantenimiento, ingeniería e IT. En el ámbito OT, este reconocimiento resulta clave para garantizar que las decisiones técnicas y operativas no entren en conflicto con las obligaciones normativas.

Debe establecerse, además, un **proceso formal para garantizar el cumplimiento de los requisitos legales y reglamentarios aplicables a la seguridad**, incluyendo:

- Normativa específica de seguridad de la información y ciberseguridad (como ISO/IEC 27001, ENS, NIS2, IEC 62443, o NIST SP 800-82) [31],
- Legislación general con impacto en la seguridad (protección de datos, propiedad intelectual, responsabilidad corporativa),
- Regulación sectorial aplicable a las infraestructuras críticas o servicios esenciales (energía, agua, transporte, salud, financiero, etc.).

Aunque no pertenece estrictamente a la disciplina clásica de la Seguridad de la Información —y adopta recaer bajo la responsabilidad de IT o de operaciones— es imprescindible considerar el **impacto de los eventos disruptivos en la disponibilidad de los procesos industriales**. Por este motivo, resulta esencial una colaboración estrecha entre OT, IT y el resto de las áreas de la organización para la elaboración de un **Plan de Continuidad de Negocio (PCN)** y, cuando proceda, de planes de recuperación específicos para sistemas industriales.

Los PCN en entornos OT deben incluir, como mínimo:

- La lista priorizada de servicios y procesos industriales a recuperar,
- Tareas y procedimientos de respuesta y recuperación,
- Responsables claramente asignados,

- Dependencias críticas (energía, comunicaciones, proveedores externos).

Estos planes deben ser **probados periódicamente**, mediante ejercicios o simulaciones, con el objetivo de convalidar su viabilidad real e identificar mejoras. En determinados casos, puede ser necesario recurrir a **terceros especializados** para garantizar la recuperación de la operación dentro de los tiempos máximos aceptables (RTO, Recovery Time Objetive), especialmente cuando los procesos industriales tienen una tolerancia muy baja a la interrupción.

De nuevo, este ámbito requiere una **toma de decisiones basada en riesgo**, de manera que el alcance del plan, el nivel de detalle y la inversión asociada se ajusten a las expectativas realistas de impacto y a las consecuencias de un fallo operativo.

5.2.4 Formación y concienciación

Los controles automáticos de Seguridad de la Información **no eliminan la necesidad de formar a las personas**. Por una banda, la gestión eficaz de la seguridad requiere expertise especializado; por la otra, para un adversario adopta ser más sencillo **inducir a error a un usuario mediante ingeniería social** para que realice una acción en su beneficio que superar barreras técnicas avanzadas. Por este motivo, se declara tradicionalmente a las personas como "el eslabón más débil de la cadena de la ciberseguridad".

En entornos **OT/ICS**, esta realidad es aún más crítica, ya que una acción aparentemente menor (por ejemplo, la conexión de un dispositivo no autorizado o la ejecución de un fichero) puede tener **impacto directo en la seguridad física, en la disponibilidad del proceso o en la continuidad del servicio**. Resulta, por lo tanto, imprescindible implantar un **programa robusto de formación (calificación) y concienciación**, adaptado al contexto industrial.

Aspectos clave del programa:

- **Evaluación de necesidades**

  Existen herramientas automáticas que, mediante encuestas estructuradas, permiten obtener *feedback* sobre el nivel de conocimiento y percepción del riesgo. Esta información puede complementarse con entrevistas a perfiles clave (personal de operación, mantenimiento, ingeniería, mandos intermedios) y a empleados en general, con el objetivo de identificar carencias específicas en OT/ICS.

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

- **Programación de campañas**

  Una buena práctica en materia de concienciación consiste en combinar:

  - sesiones anuales obligatorias (cuando así lo exija la normativa aplicable),
  - con una **campaña trimestral continuada a lo largo de un período aproximado de tres años**.

  Estas campañas deben priorizar las áreas en las que se detecte un mayor nivel de riesgo según las evaluaciones realizadas, procurando, no obstante, cubrir progresivamente todos los colectivos. Pueden diseñarse campañas selectivas o personalizadas por objetivo (operadores, personal de mantenimiento, ingeniería, IT/OT), **evitando la sobrecarga** del personal con excesivas interacciones.

Se recomienda coordinar previamente con **Gestión de Personas y el Área Legal**, para garantizar que no existan solapamientos con otras iniciativas formativas corporativas que puedan generar fatiga o conflicto.

En los planes anuales, los elementos críticos serán:

- el diseño y creación de contenidos adaptados al contexto OT (carteles, píldoras *online*, comunicados, ciberejercicios, simulaciones),
- una comunicación eficaz y el compromiso de los interlocutores clave,
- y la **medición de la efectividad** de las campañas mediante indicadores objetivos (participación, resultados de pruebas, reducción de incidentes atribuibles a error humano).

5.2.5 Protección de datos y Privacidad

Esta función se encarga del **Gobierno y de la gestión del ciclo de vida de los datos sensibles**: que datos existen, donde se almacenan, como se transmiten, quien accede a ellos y que actuaciones deben realizarse en el caso de accesos indebidos, exfiltraciones o fugas no intencionadas. Todo esto debe hacerse en **estrecha colaboración con el área Legal y con el DPO (Delegado de Protección de Datos)**, cuando exista. Incluye datos de clientes, proveedores y empleados, así como información técnica y operativa relevante en entornos OT.

No se trata únicamente de buenas prácticas voluntarias: **las regulaciones vigentes lo exigen** (por ejemplo, RGPD y LOPD-GDD), incluso en organizaciones industriales en las que el foco principal no sea el tratamiento masivo de datos personales [31].

Aspectos clave para tener en cuenta:

- **Clasificación da información**

  La información debe clasificarse según su tipología y criticidad para las operaciones del negocio, valorando el impacto derivado de una pérdida de confidencialidad, integridad o disponibilidad. Esta clasificación debe aplicarse a:

  - documentación electrónica y en papel,
  - aplicaciones de negocio,
  - sistemas OT/ICS,
  - redes, puestos de trabajo y entornos en desarrollo, contemplando también como resolver posibles conflictos de clasificación.

  No es un proceso trivial. La aproximación recomendada es **comenzar por un ámbito reducido** (por ejemplo, un departamento o proceso crítico) e ir ampliando progresivamente en círculos concéntricos. Cada conjunto de datos debe tener siempre un **responsable (*owner*)**, encargado de asignar y revisar los niveles de seguridad.

  Un esquema típico de clasificación contempla cuatro niveles:

  - **C-1. Restringida** (máxima criticidad: planes estratégicos, M&A, información muy sensible).
  - **C-2. Confidencial** (acceso limitado a un ámbito interno reducido).
  - **C-3. Interna** (uso exclusivo de personal interno).
  - **C-4. Pública**.

  Una vez implantado el modelo, la información debe **etiquetarse, almacenarse, procesarse y compartirse** conforme a su nivel. Existen herramientas que permiten identificar automáticamente la clasificación y, por ejemplo, cifrar correos electrónicos con información de nivel elevado. Esto implica etiquetado, registro, formación, posibles adaptaciones contractuales y la aplicación de controles como **DLP (Fecha Loss Prevention)**.

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

Un enfoque basado en riesgo recomienda **concentrar mayores recursos** allí donde reside la información clasificada a más crítica, mediante medidas como segmentación de red, monitorización avanzada o controles reforzados en sistemas OT.

- **Requisitos de confidencialidad, integridad y disponibilidad**

  En entornos industriales, la prioridad de negocio adopta centrarse en la **disponibilidad**. Por ello resulta esencial implantar segmentación, redundancia y estrategias de copia de seguridad adaptadas a OT, sin descuidar los requisitos de confidencialidad e integridad.

- **Criptografía / cifrado**

  La criptografía permite garantizar confidencialidad, integridad y no repudio. Una gestión eficaz de las claves criptográficas debe cubrir:

  - generación segura,
  - distribución segura,
  - almacenamiento, recuperación y renovación de claves caducadas,
  - revocación en caso de compromiso o cambio de función do propietario,
  - recuperación de claves perdidas o dañadas,
  - copia de seguridad y archivo con mantenimiento del historial,
  - definición de datas de activación y desactivación,
  - restricción del acceso sólo a personal autorizado.

  Debe tener en cuenta la protección de los datos **en reposo, en tránsito y en uso**, incluyendo los endpoints y sistemas industriales.

- **Normas de tratamiento de la información en soporte electrónico**

  Además del cifrado, es necesario proteger la información sensible almacenada en soportes electrónicos (discos duros, medios extraíbles) mediante prácticas como:

  - borrado seguro de soportes reutilizables,
  - almacenamiento conforme a las recomendaciones del fabricante,
  - registro y autorización de las transferencias de datos,

  - control de los soportes que salen fuera del entorno habitual,
  - eliminación de la información antes de enviar equipos a mantenimiento o destrucción.

- **Soporte legal**

  Esta función debe apoyar **al DPO y al área Legal** en todo lo relativo a comunicaciones con clientes y/o Autoridades de Control, especialmente en caso de **brechas de seguridad**, garantizando una respuesta coordinada, conforme a la normativa y dentro de los plazos establecidos.

5.2.6 Gestión de Identidades y Accesos (IAM)

La **Gestión de Identidades y Accesos (IAM)** se refiere al gobierno y a la gestión de la provisión, modificación y retirada de los mecanismos de autenticación y control de acceso de **usuarios, entidades técnicas y procesos**, incluidos aquellos propios de entornos **OT/ICS**. Uno de los puntos tradicionalmente más febles se encuentra en la gestión del ciclo de vida del personal, especialmente en los **cambios de puesto, movilidad interna o salidas de la organización**, donde adoptan persistir accesos innecesarios.

Existen múltiples soluciones técnicas (autenticación multifactor, passkeys, cloud brokers, **SSO**, portales de self-service para reseteo de credenciales, etc.). Resulta eficiente emplear **Directorios centralizados** (como Directorio Activo) y aplicaciones compatibles con **LDAP**, siempre que sea viable también en entornos industriales. El foco principal debe situarse en los **administradores, superusuarios y perfiles con acceso a la información o sistemas más sensibles**, especialmente en operaciones industriales.

Aspectos clave de IAM:

- **Acceso basado en funciones (RBAC)**

  Los permisos deben asignarse siempre en base a **roles**, nunca mediante personalizaciones individuales. Deben observarse estrictamente los principios de **mínimo privilegio y segregación de funciones**, particularmente relevantes en OT para evitar que una única cuenta pueda operar, modificar y auditar un mismo proceso crítico.

- **Autenticación**

  Basada en credenciales (usuario y contraseña), idealmente reforzada con un

segundo factor de autenticación (tokens, certificados o biometría cuando proceda). Deben establecerse políticas de:

- longitud y complejidad mínimas,
- eliminación de contraseñas administrativas por defecto,
- convenciones de nombres de usuario que eviten duplicidades,
- refuerzo específico para accesos remotos a entornos OT. Los sistemas federados modernos incrementan la seguridad al automatizar la autenticación, exigiendo una **identificación inicial más robusta**.

- **Gestión de credenciales**

  Incluye el almacenamiento seguro de identidades, contraseñas, tokens y certificados. Siempre que sea posible, se recomienda la **centralización** para simplificar la gestión y el proceso de autenticación, evaluando el uso de **SSO** y Directorios Corporativos en aplicaciones industriales compatibles.

- **Supervisión y monitorización**

  La monitorización de los intentos de autenticación y de los accesos la información sensible es crítica. Puede realizarse mediante un **SIEM**, permitiendo detectar patrones anómalos (horarios inusuales, orígenes geográficos inesperadas, IP/MAC no habituales). Es tan importante definir correctamente **las reglas de alerta** como garantizar su gestión efectiva.

- **Mantenimiento de cuentas de usuario**

  Las herramientas de gestión deben permitir asociar un usuario a una o varias cuentas y revisar sus privilegios a lo largo del tiempo. Los riesgos habituales son **la acumulación de permisos** tras cambios de puesto y **la no desactivación de** las cuentas tras bajas voluntarias o forzosas. Deben existir procesos claros, preferiblemente automatizados, para revisiones periódicas.

5.2.7 Gestión de amenazas y vulnerabilidades

En ciberseguridad, una **amenaza** es un evento o agente externo con capacidad para causar daño o comprometer la seguridad de un sistema o red. Puede tener origen humano, técnica o ambiental (malware, ataques dirigidos, fallos de hardware/software, desastres naturales, etc.).

Una **vulnerabilidad**, por su parte, es una debilidad en un sistema que puede ser explotada por una amenaza. Puede deberse a errores de diseño, configuraciones incorrectas, ausencia de parches o mecanismos de control insuficientes.

En resumen: **la amenaza es el agente**, la **vulnerabilidad es la grieta**. La existencia de una vulnerabilidad no implica necesariamente un incidente, pero **toda amenaza precisa de una vulnerabilidad para materializarse**.

Esta función es responsabilidad del **equipo de Operaciones de Seguridad**, asumiendo que no existen entornos 100 % seguros. Las vulnerabilidades pueden identificarse mediante:

- escáneres automáticos,
- análisis de registros de seguridad (intentos de acceso fallidos, caídas de servicios, borrados anómalos),
- pruebas de intrusión controladas.

Las vulnerabilidades deben tratarse **por orden de prioridad según el riesgo**, dentro de un programa sistemático y documentado.

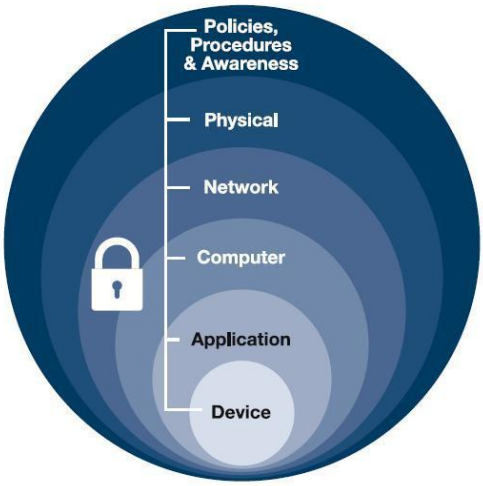
Los registros de eventos de seguridad deben analizarse de forma **continua y automatizada**, incluyendo:

- procesamiento y correlación de eventos relevantes,
- interpretación de comportamientos anómalos,
- respuesta coordinada ante eventos críticos, derivando a información al equipo de gestión de incidentes.

Aspectos clave:

- definición de **reglas de correlación** y playbooks asociados,
- establecimiento **de un proceso de gestión de parches**, adaptado a OT: aprobación formal por el owner del sistema, pruebas previas, entornos de test cuando sea posible, y evaluación del impacto operativo. Los cambios suelen realizarse en **ventanas de mantenimiento**, salvo parches críticos, que deben contar con un **procedimiento de emergencia** (idealmente <24 h).

Adicionalmente, es imprescindible disponer de **soluciones antimalware** en *Endpoints*, servidores y pasarelas. Más que apostar por mecanismos excesivamente sofisticados, se recomienda un enfoque de **defensa en profundidad**.



Esquema de defensa en profundidad. Fuente: OpenPracticeLabrary (2022)

La defensa en profundidad se basa en la combinación de múltiples capas de protección complementarias:

- políticas y procedimientos,
- formación y concienciación,
- controles físicos,
- protección perimetral y de red (cortafuegos, NDR, CPS PP, IDS/IPS, segmentación, *honeypots..*),
- controles al nivel de aplicación y dispositivo (DLP, cifrado, EDR, HIDS).

Este enfoque es eficaz, comprensible a nivel organizativo **y suficiente sin recurrir a soluciones extremadamente complejas o costosas**, que no están exentas de riesgos.

5.2.8 Respuesta a incidentes de seguridad

Un **incidente de ciberseguridad** es una violación —o amenaza inminente de violación— de las políticas de seguridad, de uso aceptable o de las prácticas estándar. Su gestión debe estar **perfectamente documentada y regulada**, permitiendo una respuesta coherente y una recuperación ágil.

El **Plan de Respuesta a Incidentes de Seguridad** es el documento central de las Operaciones de Seguridad. Incluye enfoques, métricas, contactos, secuencias de

actuación, escalados, métodos de notificación y listas de comprobación. El proceso simplificado, se estructura en cuatro fases:

1. **Iniciación / triaje**

   Se determinan que alertas o eventos activan el proceso y que acciones iniciales se ejecutan. Una alerta puede generar un evento, que a su vez se convierta en un incidente. Se evalúa la prioridad y la necesidad de apoyo de terceros.

2. **Contención**

   Se identifican los **IoC (indicadores de compromiso)** para determinar el alcance: *hosts* afectados, cuentas comprometidas, datos impactados. Se implantan medidas para limitar la propagación y reducir el impacto, evaluando nuevamente el apoyo externo si procede.

3. **Erradicación**

   El equipo de Seguridad, en coordinación con IT/OT, lidera las acciones técnicas: bloqueo de puertos, aislamiento de sistemas, scripts de limpieza, retirada de accesos indebidos, etc.

4. **Recuperación**

   El equipo de Seguridad suministra forense para restaurar los servicios. Se identifica la **causa raíz** y se formulan recomendaciones: cambios de arquitectura, mejoras de procesos, parcheado adicional o despliegue de nuevos controles para evitar recurrencias, a modo de mejora continua.

Los **roles y responsabilidades** deben estar claramente definidos para evitar confusiones en situaciones de crisis. Resulta imprescindible **practicar escenarios de incidente** mediante ejercicios periódicos, especialmente en entornos OT/ICS donde el tiempo de respuesta es crítico.

6 Marcos y cumplimiento normativos

Los marcos normativos, estándares y regulaciones en materia de ciberseguridad industrial constituyen un **elemento fundamental para la mitigación del riesgo** en entornos OT/ICS. Su principal valor reside en proporcionar un conjunto estructurado de **buenas prácticas reconocidas**, que ayudan a las organizaciones a abordar la seguridad desde una perspectiva integral: organizativa, procedimental y técnica.

A través de estos marcos se restablecen criterios claros sobre **cómo gobernar la seguridad**, como definir responsabilidades, como gestionar procesos críticos (accesos, cambios, incidentes, continuidad) y que **controles físicos y lógicos** deben implantarse para reducir la probabilidad y el impacto de incidentes. Su aplicación no garantiza la eliminación del riesgo, pero sí permite **reducirlo a niveles aceptables**, dotando además a la organización de un marco común para la toma de decisiones basada en riesgo.

Con el objetivo de profundar en este ámbito, el Observatorio ha desarrollado el entregable específico **Guía Normativa del Observatorio**, al que se invita expresamente al lector a acudir para un tratamiento exhaustivo y detallado [31]. Esta guía está concebida como un documento de referencia práctica y se estructura en tres grandes bloques de contenido, pero un elemento auxiliar:

- Normativa española aplicable a la industria y a las infraestructuras críticas.
- Marca regulatoria y reguladora de la Unión Europea.
- Estándares e marcos internacionales de referencia.
- Guía de implantación práctica orientada a contornos OT/ICS.

A continuación, se le viene una síntesis de alto nivel de los tres primeros apartados, con el objetivo de contextualizar su alcance y utilidad.

6.1 Normativa española

En la **Guía Normativa del Observatorio** la normativa nacional se presenta como un conjunto de referencias de obligado cumplimiento (o de aplicación práctica muy frecuente) que determinan "el suelo mínimo" regulatorio para muchas organizaciones, incluidas las que operan entornos OT/ICS [31]. En concreto, se incluyen:

- **Esquema Nacional de Seguridad (ENS):** es el marco normativo español que fija principios básicos, requisitos mínimos y medidas de seguridad para los **sistemas, datos y servicios en el ámbito del sector público y de sus proveedores**. Sirve para establecer una referencia común y auditable de controles (organizativos, operativos y técnicos) y para orientar la gestión del riesgo y la categorización de sistemas.
- **Ley 12/2018 y Real Decreto 43/2021 (transposición y desarrollo de la Directiva NIS 2016/1148)**: es el paquete normativo que trasladó a la normativa española las obligaciones de seguridad y notificación de incidentes para **operadores de servicios esenciales y proveedores de servicios digitales**. Sirve para obligar a implantar medidas de gestión de riesgos y establecer cauces y plazos de reporte y supervisión, hasta que la transposición de NIS2 en España la sustituya/modifique.
- **Ley de Protección de Infraestructuras Críticas (Ley PIC)**: es la norma nacional orientada a la protección de las infraestructuras críticas mediante la planificación, coordinación y obligaciones de seguridad asociadas (incluyendo figuras, planes y medidas de protección). Sirve para **asegurar la continuidad y la protección de servicios esenciales frente a amenazas**, incluidas las ciberamenazas con impacto operacional.
- **Estrategia Nacional de Ciberseguridad (2019) y Plan Nacional de Ciberseguridad**: son instrumentos estratégicos que definen **líneas de acción, prioridades y coordinación institucional en materia de ciberseguridad**. Sirven para orientar políticas públicas y reforzar capacidades (prevención, detección, respuesta y cooperación), actuando como marco director para planes e iniciativas sectoriales.
- **Ley Orgánica 3/2018 (LOPD-GDD) y obligaciones asociadas (incluyendo AIPD/EIPD)**: **es la norma española que desarrolla y complementa la protección de datos personales en el marco del RGPD**. Sirve para establecer deberes y garantías en el tratamiento de datos personales (derechos de los interesados, obligaciones para entidades, evaluaciones de impacto cuando proceda), algo relevante también en entornos industriales cuando existen datos personales en sistemas corporativos o en procesos digitalizados que convergen con OT.

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

Este bloque nacional **define obligaciones y expectativas auditables** que condicionan a gobernanza, la gestión del riesgo y la implantación de controles en organizaciones industriales, especialmente cuando prestan servicios esenciales, operan infraestructuras críticas o manejan datos personales.

6.2 Normativa de la Unión Europea

El bloque europeo recoge los instrumentos que elevan y armonizan el nivel de ciberseguridad y resiliencia en el conjunto de la UE, y que impactan directamente en los sectores industriales y en las infraestructuras críticas [31]. Se incluyen:

- **Directiva NIS2 (Directiva (UE) 2022/2555)**: es la norma europea que establece un **alto nivel común de ciberseguridad para una amplia lista de entidades esenciales e importantes, con obligaciones reforzadas de gobernanza, gestión de riesgos y notificación de incidentes**, así como un régimen de supervisión y sanciones. Sirve para profesionalizar y homogeneizar la gestión del riesgo ciber en sectores críticos, reforzando también la coordinación y la cooperación a nivel europeo. La guía incorpora, además, la referencia a la **CCN-STIC 892 (PCE-NIS2)** como apoyo práctico al cumplimiento y menciona el marco de transposición en España.
- **CRA (Cyber Resilience Act)**: es una regulación europea orientada a mejorar la **ciberresiliencia de los productos con elementos digitales a lo largo de su ciclo de vida.** Sirve para introducir requisitos de seguridad "por diseño y por defecto" y obligaciones para fabricantes y cadena de suministro, reduciendo riesgo sistémico por vulnerabilidades en componentes y productos empleados también en entornos industriales.
- **CER (Critical Entities Resilience):** es el **marco europeo centrado en la resiliencia de las entidades críticas frente a riesgos, incluyendo la dimensión ciber y la continuidad de servicio**. Sirve para reforzar la preparación y resiliencia operacional, complementando la visión de ciberseguridad con obligaciones y expectativas de continuidad y gestión de crisis en sectores esenciales.

El bloque europeo actúa como **impulsor de madurez y armonización**, elevando obligaciones de gestión del riesgo, gobernanza y resiliencia que las organizaciones industriales deben traducir a políticas, procedimientos y controles efectivos.

6.3 Normas internacionales e hitos

Los marcos y estándares internacionales funcionan como la capa que facilita pasar del "que debo cumplir" al "como lo implanto", proporcionando buenas prácticas estructuradas y, en el caso de OT/ICS, orientación muy aplicable a controles técnicos y operativos [31]. Se incluyen:

- **ESO/IEC 27001**: es el estándar internacional para implantar un **Sistema de Gestión de la Seguridad de la Información (SGSI/ISMS)**, con enfoque de mejora continua. Sirve para establecer gobernanza, procesos, análisis y tratamiento del riesgo, es un marco auditable/certificable para gestionar la seguridad de manera sistemática.
- **NIST CSF (Cybersecurity Framework)**: **es un marco de buenas prácticas estructurado en funciones (identificar, proteger, detectar, responder, recuperar) y perfiles de implantación**. Sirve para ordenar programas de ciberseguridad, evaluar situación actual vs. objetivo y definir hojas de ruta de mejora, con un lenguaje muy utilizado a nivel internacional.
- **CIS Controls:** es un **conjunto priorizado de controles/salvaguardias de ciberseguridad, organizado para facilitar una implantación progresiva** por nivel de madurez. Sirve para seleccionar medidas de alto impacto y bajo "ruido", apoyar análisis de brecha y estructurar planes de acción realistas, también como puente entre requisitos y evidencias.
- **ISA/IEC 62443**: **es la familia de normas más específica y completa** para ciberseguridad de **sistemas de automatización y control industrial (IACS/OT/ICS)**. Sirve para definir requisitos y controles por dominios (organización, procesos, sistemas y componentes), apoyar diseños "defendibles" y, cuando aplica, habilitar esquemas de evaluación y certificación en entornos industriales.
- **SANOS ICS Top 5 Controls:** es una **selección de controles críticos priorizados específicamente para ICS.** Sirve para **orientar de forma muy pragmática la implantación de medidas de alto retorno en entornos OT**, especialmente cuando hay limitaciones de recursos o necesidad de resultados rápidos.

Como complemento, la guía también introduce la conveniencia de emplear **modelos de madurez** (p.ex., C2M2, CSET) para evaluar capacidades y planificar mejoras más allá del

"check" de cumplimiento. Sirve para convertir el cumplimiento en una hoja de ruta realista de evolución y resiliencia.

De nuevo, aconsejamos al lector revisar la Guía Normativa con tranquilidad [31].

7 Controles y buenas prácticas

Como ya se ha mencionó en diversas ocasiones, la mitigación de los riesgos tecnológicos asociados a la ciberseguridad en entornos industriales **no depende de una única medida ni de una tecnología concreta**, sino de la aplicación coherente de un conjunto de **controles organizativos, procedimentales y técnicos**, priorizados en función del riesgo y adaptados a las particularidades de los sistemas OT/ICS.

Los informes previos del **Observatorio de Ciberseguridad Industrial** sentaron ya una base de recomendaciones prácticas, orientadas a la realidad operativa de las organizaciones industriales [4].

En este sentido, los informes y guías elaborados por organismos públicos, agencias nacionales de ciberseguridad, entidades de referencia internacional y fabricantes especializados, constituyen una fuente esencial de buenas prácticas contrastadas, que se recogerán a continuación de forma sintética en esta sección. Lógicamente dada su relevancia, hay solapamiento parcial entre las fuentes.

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

Resulta también relevante **la contribución de fabricantes especializados** como Fortinet, a través de su State of OT Cybersecurity Report 2025 ya citado, que ofrecía datos empíricos sobre tendencias de ataque, debilidades recurrentes y controles con mayor impacto real en entornos industriales [17].

Adicionalmente, el uso creciente de la **Inteligencia Artificial**, tanto por defensores como por adversarios, introduce nuevos riesgos que deben ser gestionados de forma específica. Para este ámbito, emplearemos como referencia una guía cocreada por la **CISA y el Australian Cyber Security Centre (ACSC)** [37], en colaboración con múltiples agencias gubernamentales y centros nacionales de ciberseguridad (entre ellos la National Security Agency americana [38], o Canadian Centre for Cyber Security [39], o National Cyber Security Centre británico ya presentado, o Bundesamt für Sicherheit in der Informationstechnik alemán, [40] o los NCSC de Países Baixos y Nueva Zelandia [41][42]). Esta guía establece principios para un **uso seguro, responsable y resiliente de la IA**, también aplicables a entornos industriales.

Finalmente, estas recomendaciones se completan con el análisis de riesgos emergentes recogido en el **International AI Safety Report**, ya tratado en este informe, que aporta una visión perspectiva sobre amenazas sistémicas, riesgos de abuso e impactos potenciales de la IA en infraestructuras críticas y sistemas ciberfísicos [23].

En conjunto, estas fuentes permiten construir un **catálogo coherente de medidas de seguridad aplicables**, fundamentado en evidencias, alineado con el estado de la amenaza real y orientado a la reducción efectiva del riesgo tecnológico en el ámbito industrial.

7.1 NCSC

Las siguientes recomendaciones sintetizan las principales líneas de buenas prácticas publicadas por el **National Cyber Security Centre (NCSC)** del Reino Unido en materia de seguridad OT. La sección se basa, por una banda, en el artículo divulgativo sobre la importancia de comprender el entorno OT como primer paso para mejorar la ciberseguridad, y por otra, en la colección completa de guías de Operational Technology, que constituye un cuerpo coherente de orientación práctica para organizaciones industriales [43][44].

7.1.1 Arquitectura OT

Según la guía del NCSC, la creación y mantenimiento de una visión definitiva de la arquitectura OT se basa en **cinco principios explícitos**, que deben aplicarse de forma sistemática:

- **Definir procesos para establecer y mantener el registro definitivo del entorno OT**, asegurando que existe una fuente autorizada y coherente de información.
- Establecer un **programa de gestión de la información OT**, que determine como se recopila, mantiene, protege y utiliza la información técnica y operativa.
- **Identificar y categorizar los activos OT** para soportar decisiones informadas basadas en riesgo, teniendo en cuenta criticidad e impacto.
- **Identificar y documentar la conectividad dentro del sistema OT**, incluyendo flujos de datos, interdependencias y puntos de interconexión.
- **Identificar y documentar los riesgos de terceros** que afectan al sistema OT, incluyendo proveedores, mantenimiento y accesos externos.

Estos principios tienen como objetivo garantizar que la organización **comprende realmente su entorno OT** antes de aplicar medidas técnicas de protección.

7.1.2 Conectividad OT segura

Defienden que la conectividad en entornos industriales debe diseñarse y gestionarse de acuerdo con ocho principios explícitos, que equilibran necesidad operativa y riesgo:

- **Balancear el riesgo y las oportunidades**: evaluar conscientemente que beneficios aporta cada conexión frente al risco adicional que introduce en el contorno OT.
- **Limitar la exposición de la conectividad**: reducir al mínimo necesario el número de conexiones y los puntos accesibles desde otros dominios.
- **Centralizar y estandarizar las conexiones de red**: emplear arquitecturas coherentes, evitando excepciones y conexiones ad hoc difíciles de controlar.
- **Emplear protocolos estandarizados y seguros**: priorizar protocolos conocidos, documentados y con capacidades de seguridad frente a soluciones propietarias opacas.
- **Endurecer el perímetro OT**: proteger los límites del sistema industrial mediante controles técnicos adecuados al riesgo.
- **Limitar el impacto de un posible compromiso**: diseñar la conectividad asumiendo que puede producirse un fallo o intrusión.
- **Garantizar que toda la conectividad está registrada y monitorizada**: disponer de visibilidad continua sobre las comunicaciones OT.
- **Establecer un plan de aislamiento**: definir con antelación como desconectar o aislar partes del sistema OT en caso de incidente.

El propósito de estos principios es **permitir la conectividad necesaria para la operación**, reduciendo a la vez la superficie de ataque y facilitando la detección, contención y recuperación frente a incidentes.

Hay que destacar que el NCSC aporta un ejemplo práctico que permite aplicar estos principios, en la misma fuente referida.

7.1.3 Uso de terminales de acceso privilegiado

Según la guía específica del NCSC sobre **PAW (Privileged Access Workstations) en entornos OT**, el uso de estaciones de trabajo privilegiadas debe basarse en ocho principios explícitos:

- **Establecer la estrategia de PAW de la organización**: definir claramente al alcance, objetivos y casos de uso de la PAW dentro del ecosistema OT.
- **Diseñar la solución PAW para que sea usable y segura**: equilibrar requisitos de seguridad con un uso práctico para los equipos técnicos.
- **Establecer una base de confianza**: garantizar la integridad de la PAW mediante arranque seguro, configuración controlada y cadena de confianza.
- **Escalar la solución**: diseñar la PAW para que pueda ampliarse a medida que crecen los requisitos operativos y organizativos.
- **Reducir la superficie de ataque**: minimizar software, servicios y capacidades disponibles en la PAW.
- **Actividades de alto riesgo de PAW de riesgo:** evitar que tareas peligrosas comprometan el contorno privilegiado.
- **Implantar monitorización protectora**: registrar y supervisar el uso de la PAW para detectar usos indebidos o anómalos.
- **Controlar los datos que entran y salen de la solución PAW**: evitar fugas de información o introducción de código malicioso.

Estos principios tienen como finalidad **proteger a las credenciales y acciones privilegiadas**, reduciendo el riesgo de compromiso de los sistemas OT.

7.1.4 SCADAs en la nube

La guía del NCSC sobre **SCADAs alojados en nube** aborda este modelo como una evolución emergente, con distintos grados de adopción y madurez en el ámbito OT. No se limita a recomendar o desaconsejar su adopción, sino que **propone un análisis reflexivo previo a la toma de decisiones.**

El despliegue de SCADA en cloud puede abarcar escenarios muy diversos, desde el procesamiento y enriquecimiento de datos operativos hasta arquitecturas más avanzadas en las que es posible el control remoto de activos físicos. En todos los casos,

el NCSC subraya que la decisión debe tomarse a partir de una **evaluación de riesgos rigurosa**, en la que la ciberseguridad sea un elemento central.

Migrar SCADA a la nube no supone un simple cambio de localización de la infraestructura, sino que **altera profundamente los límites tradicionales de seguridad**, **los modelos de conectividad y los mecanismos de control de acceso**. Sistemas históricamente aislados pasan a depender de conexiones a Internet y de modelos de responsabilidad compartida con los proveedores de cloud.

En este contexto, resulta imprescindible garantizar que la conectividad continúa siendo **limitada, controlada y monitorizada**, manteniendo niveles de protección equivalentes o superiores a los de los despliegues tradicionales. El NCSC recomienda, además, complementar esta orientación con su **guía general de seguridad en cloud** [45], dado que muchos principios aplicables a IT también son relevantes en entornos SCADA modernos.

El objetivo final de esta guía es ayudar a las organizaciones a **determinar la idoneidad real** de una solución SCADA en cloud en función de su contexto operativo, del nivel de riesgo asumible y de las capacidades de seguridad disponibles.

7.1.5 Comunidades de interese ICS

El **Industrial Control Systems Community of Interest (ICS CoI) es** una iniciativa promovida por el NCSC que sirve como ejemplo de **comunidad nacional de referencia** para mejorar la seguridad y la resiliencia de las infraestructuras críticas en el Reino Unido.

Se trata de un foro en el que participan profesionales del propio NCSC, operadores y propietarios de activos, fabricantes de sistemas ICS, investigadores en seguridad, Administraciones públicas, reguladores y ámbito académico. La comunidad está gobernada por un comité director que marca la orientación estratégica y promueve la colaboración entre los distintos actores.

El ICS CoI combina la elaboración de orientación técnica sobre problemas concretos con la **concienciación y capacitación** de perfiles que se incorporan al ámbito OT, contribuyendo a reducir la brecha de capacidades existente. Cuenta con más de 500 miembros activos y organiza sesiones periódicas de intercambio de conocimiento.

Aunque es un ejemplo específico del Reino Unido, este modelo es **perfectamente extrapolable** a otros ámbitos. A nivel europeo o nacional pueden identificarse iniciativas semejantes, como grupos de trabajo impulsados por **ENISA**, comunidades

técnicas en torno a **CERT/CSIRT nacionales** (por ejemplo, CCN-CERT en España) o foros sectoriales promovidos por asociaciones industriales y organismos de ciberseguridad.

La participación en comunidades de este tipo permite reforzar la **inteligencia colectiva**, compartir lecciones aprendidas y mejorar la preparación frente a incidentes OT.

7.2 CISA

La **Cybersecurity and Infrastructure Security Agency (CISA)** de los Estados Unidos publicó una guía específica centrada en las mitigaciones elementales para reducir las ciberamenazas en entornos de **Operational Technology (OT)**.

El enfoque de la CISA es eminentemente práctico y priorizado: no pretende cubrir todo el espectro posible de controles, sino identificar aquellas medidas fundamentales que, aplicadas de forma consistente, **reducen de manera significativa la superficie de ataque y el impacto de los incidentes** en sistemas industriales.

La hoja informativa identifica **cinco mitigaciones primarias** que las organizaciones con OT/ICS deberían priorizar para reducir la exposición frente a campañas que apuntan específicamente a sistemas OT conectados a Internet:

- **Eliminar conexiones OT al Internet público**: los dispositivos OT adoptan carecer de mecanismos de autenticación y autorización robustos y son fácilmente localizables a través de búsquedas de puertos en rangos IP públicos. La recomendación se celebra en identificar activos expuestos y eliminar exposiciones no intencionadas.
- **Cambiar inmediatamente contraseñas por defecto y emplear contraseñas fuertes y únicos**: la actividad observada por los organismos autores incluye el abuso de credenciales por defecto o fácilmente adivinables (incluyendo el uso de herramientas open source). La medida es especialmente crítica en dispositivos expuestos que pueden afectar procesos OT.
- **Asegurar el acceso remoto a las redes OT**: cuando el acceso remoto sea imprescindible, se recomienda pasar a conexiones sobre redes privadas (evitando exposición pública), emplear VPN y reforzar la autenticación con contraseña fuerte y **Factor de Autenticación Múltiple (MFA) resistente al *phishing***. También se enfatiza documentar/configurar el acceso remoto con **mínimo privilegio** y desactivar cuentas inactivas.

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

- **Segmentar las redes IT y OT**: introducir segmentación y, cuando aplique, una DMZ para el intercambio de datos de control con la red corporativa reduce el impacto potencial y disminuye el riesgo de interrupción de las operaciones OT.
- **Practicar y mantener la capacidad de operar manualmente los sistemas OT**: la posibilidad de volver a controles manuales para restaurar operaciones tras un incidente es vital. Se recomienda probar de forma rutinera planes de continuidad y recuperación, mecanismos *de* fallo seguro, capacidades de aislamiento, copias de seguridad de software y sistemas en reserva.

Adicionalmente, la guía recomienda **coordinarse regularmente con proveedores terceros**, integradores de sistemas y fabricantes, ya que configuraciones inseguras pueden introducirse durante operaciones habituales o derivarse de configuraciones por defecto, y su corrección reduce vulnerabilidades no intencionadas.

7.3 Fortinet

El informe **State of OT Cybersecurity 2025 de Fortinet** ofrece una visión basada en datos empíricos recogidos a partir de encuestas globales, telemetría y experiencia directa en entornos industriales [17].

A continuación, se presentan las principales buenas prácticas para entornos OT identificadas por este fabricante. Lógicamente por la naturaleza de la entidad, presentan cierto sesgo hacia la recomendación de solución específicas de ciberseguridad.

- **Implantar segmentación de red en entornos OT**: la segmentación es la base de un entorno OT endurecido. Mediante la creación de zonas y segmentos con políticas de control estrictas en todos los puntos de acceso, se reduce drásticamente la capacidad de un atacante para moverse lateralmente. Los estándares como ISA/IEC 62443 refuerzan este enfoque, promoviendo la separación entre redes IT y OT y entre diferentes dominios OT.
- **Mejorar la visibilidad y aplicar controles compensatorios sobre los activos OT:** una vez establecida la segmentación inicial, las organizaciones pueden ampliar la visibilidad del tráfico y del comportamiento de los activos OT. Ello permite identificar dispositivos vulnerables y aplicar controles compensatorios diseñados para entornos sensibles, como políticas basadas en protocolos industriales, análisis de comunicaciones sistema-a-sistema o monitorización específica de endpoints OT.

- **Incorporar inteligencia de amenazas y servicios de seguridad específicos para OT**: la seguridad OT requiere conocimiento actualizado de las amenazas reales que afectan a estos entornos. El fabricante destaca la necesidad de emplear inteligencia de amenazas y servicios de seguridad con contenido específico OT, capaces de detectar variantes de ataque y comportamientos maliciosos dirigidos a protocolos y dispositivos industriales.
- **Integrar OT en las operaciones de seguridad (SecOps) y en la planificación de respuesta a incidentes**: las organizaciones deben avanzar hacia modelos de **IT-OT SecOps**, en los que los entornos industriales se integren plenamente en los centros de operaciones de seguridad y en los planes de respuesta a incidentes. Esto requiere playbooks específicos OT y una colaboración estrecha entre equipos de seguridad, operaciones y producción, teniendo en cuenta el impacto físico y operativo de un incidente.
- **Adoptar un enfoque de plataforma para la arquitectura global de seguridad:** la proliferación de soluciones puntuales de distintos fabricantes incrementa la complejidad y la carga operativa. Se recomienda un enfoque de plataforma que permita consolidar capacidades para IT y OT, mejorar la integración entre herramientas y habilitar respuestas más rápidas y automatizadas frente a las amenazas, reduciendo a la vez la carga sobre equipos con recursos limitados.

En conjunto, estas recomendaciones refuerzan la idea de que la ciberseguridad OT efectiva requiere **visibilidad, integración y simplificación arquitectónica**, alineadas con una comprensión clara del riesgo y de las limitaciones operativas de los entornos industriales.

7.4 ISACA

Este apartado se basa en un artículo de opinión elaborado por un **experto certificado de ISACA**, publicado en sus canales oficiales, pero que **no constituye una posición normativa ni oficial de la asociación**.

El análisis aborda la ciberseguridad industrial desde una perspectiva de **gobernanza, gestión del riesgo** y control, complementaria a las guías más técnicas. En el artículo Common cybersecurity risks to ICS/OT systems, ISACA identifica un conjunto de riesgos recurrentes en entornos industriales y formula recomendaciones prácticas orientadas a

reducir su probabilidad e impacto, teniendo en cuenta las limitaciones operativas propias de OT [47].

- **Establecer y mantener un inventario completo de activos ICS/OT**: implantar procesos formales para identificar, clasificar y mantener actualizado el inventario de sistemas, dispositivos, software y comunicaciones OT, como base para la gestión del riesgo y la toma de decisiones informadas.
- **Definir y gobernar adecuadamente la conectividad IT/OT:** diseñar arquitecturas claras, aplicar segmentación de red y limitar las interconexiones al estrictamente necesario, asegurando que todas las conexiones estén documentadas, controladas y monitorizadas.
- **Aplicar una gestión rigurosa de identidades y accesos privilegiados:** implantar el principio de mínimo privilegio, eliminar cuentas compartidas, revisar periódicamente los accesos y emplear mecanismos de autenticación reforzada, incluyendo accesos de terceros a entornos OT.
- **Adoptar una gestión de vulnerabilidades y parches basada en riesgo:** priorizar la corrección de vulnerabilidades según el impacto operativo y de seguridad, complementando el parcheado con controles compensatorios cuando las limitaciones técnicas u operativas impidan la actualización inmediata.
- **Desarrollar capacidades específicas de respuesta a incidentes ICS/OT:** elaborar y probar planes de respuesta y recuperación adaptados a entornos industriales, garantizando la coordinación entre seguridad, operaciones y dirección, y priorizando la seguridad física y la continuidad del servicio.
- **Impulsar una cultura de ciberseguridad integrada en la operación industrial**: establecer programas de formación y concienciación dirigidos a operadores, ingenieros y personal de mantenimiento, reforzando la responsabilidad compartida en la protección de los sistemas ICS/OT.

De nuevo subrayar la coincidencia en gran medida con recomendaciones previas, como las del NCSC. En conjunto, ISACA recomienda tratar la ciberseguridad industrial como un **elemento de gobernanza y riesgo empresarial**, integrando personas, procesos y tecnología en un enfoque coherente y sostenible.

7.5 Uso de IA en OT

La integración de capacidades de Inteligencia Artificial (IA) en entornos OT/ICS puede aportar mejoras de eficiencia, mantenimiento predictivo, optimización operativa y apoyo a la toma de decisiones. Sin embargo, también introduce **nuevas superficies de ataque**, dependencias tecnológicas y riesgos específicos (por ejemplo, deriva del modelo, problemas de explicabilidad, nuevas vías de exfiltración de datos o impactos sobre la seguridad funcional).

En general, podemos ver a la luz de este informe de la Cloud Security Alliance [49] como las organizaciones aún no están preparadas a nivel procedimental para el empleo regulado de esta tecnología emergente:

Encuesta de políticas y guías para desarrollo y uso seguro de la IA. Fuente: CSA (2025)

7.5.1 Integración segura de IA en OT

Las siguientes recomendaciones sintetizan, de forma práctica y accionable, los **principios** recogidos en la guía **Principles for the Secure Integration of Artificial Intelligence in Operational Technology** creado de forma coral por varios organismos internacionales de ciberseguridad [48], y estructurados en los **cuatro bloques** del propio documento. El reporte es denso, por lo que se recomienda acudir a la fuente para un entendimiento exhaustivo.

7.5.1.1 Principio 1 — Comprender la IA

7.5.1.1.1 Comprender los riesgos únicos de la IA y el posible impacto en la TO

- **Tratar la IA como un componente ciberfísico**, evaluando impactos no sólo de confidencialidad, sino también de **disponibilidad y seguridad funcional** (paradas innecesarias, alarmística incorrecta, cambios de lógica de control, etc.).
- **Anticipar riesgos de calidad y centralización de datos**: los modelos dependen de datos de adiestramiento y operación (sensórica, telemetría, históricos). La dificultad de obtener datos normalizados en OT y la tentación de centralizarlos pueden **incrementar el riesgo** y dar más contexto al adversario.
- **Considerar la deriva del modelo (model drift)**: cambios de proceso, condiciones de operación o equipos pueden degradar la precisión con el tiempo; esto puede llevar a **falsos positivos/negativos** y decisiones operativas incorrectas.
- **Reconocer limitaciones de explicabilidad**: si no se entiende por qué el sistema recomienda una acción, aumenta el tiempo de recuperación y la complejidad de troubleshooting, y complica auditorías y cumplimiento.

7.5.1.1.2 Comprender el ciclo de vida de desarrollo seguro de un sistema de IA

- **Exigir prácticas de seguridad "secure-by-design" y "secure-by-default"** para la IA, incluyendo requisitos de seguridad desde el diseño, convalidación y mantenimiento.
- **Incorporar amenazas específicas de IA al modelado de amenazas**, como entradas adversariales y envenenamiento de datos.
- **Convalidar y refinar modelos de forma continua en entornos simuladas/non productivas** antes de despliegue y cambios relevantes, para reducir riesgo operacional.

7.5.1.1.3 Formar al personal sobre IA

- **Capacitar a operadores, ingeniería y seguridad** sobre cómo funciona la IA, sus límites y los riesgos más relevantes en OT.
- **Reducir la dependencia y el "automation bias"**: establecer criterios para que el personal cuestione recomendaciones y salga cuando escalar, detener o volver a la operación manual.

- **Preparar al personal para interpretar errores y alarmas**: la IA puede incrementar carga cognitiva si genera alertas incorrectas; la formación debe incluir procedimientos de verificación y reacción.

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

7.5.1.2.1 Consideremos el caso de negocio de OT para usar IA

- **Justificar el uso por objetivos OT reales** (seguridad, fiabilidad, continuidad, eficiencia), evitando despliegue "por moda".
- **Aplicar una decisión basada en riesgo**: evaluar si los beneficios superan los nuevos riesgos y costes (ciberseguridad, seguridad funcional, mantenimiento, dependencia del proveedor).

7.5.1.2.2 Gestionar los riesgos de seguridad de los datos OT para sistemas de IA

- **Proteger datos OT a lo largo de todo el ciclo** (en reposo, en tránsito y en uso), porque la IA amplifica el valor y el volumen de datos.
- **Aplicar control de acceso y cifrado**, y reforzar gobernanza de datos cuando la IA consume datos sensibles u operativos.
- **Minimizar exposición al mover datos fuera de OT**: favorecer patrones de transferencia controlados y auditables (por ejemplo, movimiento "push" de resúmenes/atributos) frente a accesos persistentes de entrada.

7.5.1.2.3 Comprender el rol de los proveedores OT en la integración de IA

- **Exigir evidencias de seguridad del proveedor** (auditorías, evaluaciones de riesgo, pruebas) y claridad contractual sobre responsabilidades.
- **Asegurar soporte y supervisión a lo largo del ciclo de vida** (procura, diseño, despliegue, operación y mantenimiento), incluyendo cuando el proveedor participe en la vigilancia o actualización del modelo.

7.5.1.2.4 Evaluar retos en la integración IA–OT

- **Planificar integración técnica y operativa** (protocolos, dependencias de versiones, requisitos de infraestructura, latencias, limitaciones en tiempo real).
- **Evitar que la IA se convierta en una "puente" permanente hacia OT**: mantener segmentación y separación por zonas, y diseñar conectividad de forma minimizada y controlada.

7.5.1.3 Principio 3 — Establecer marcos de gobernanza y aseguramiento de la IA

7.5.1.3.1 Establecer mecanismos de gobernanza para IA en OT

- **Crear políticas, procedimientos y estructuras de responsabilidad** para decisiones y riesgos asociados a la IA.
- **Implicar stakeholders clave**: dirección (incluyendo CISO), expertos OT/IT/IA, equipos de ciberseguridad y proveedores cuando corresponda.
- **Implantar gobernanza de datos estricta** (cifrado, control de acceso y analítica de comportamiento de usuario), y **definir roles y responsabilidades** para evitar confusión (e risco de responsabilidad) ante incidentes.
- **Realizar auditorías y pruebas de cumplimiento regulares**, y **convalidación/verificación continua** del rendimiento del sistema conforme a objetivos y requisitos.

7.5.1.3.2 Integrar la IA en los marcos existentes de seguridad y ciberseguridad

- **Incorporar evaluaciones de la IA a los procesos actuales de riesgo, mitigación y monitorización**, incluyendo gestión de vulnerabilidades y requisitos regulatorios aplicables a la infraestructura crítica.
- **Aplicar controles robustos** (cifrado, control de acceso, detección de intrusiones) y reforzar trazabilidad:
    - recoger logs do flujo de datos y accesos de los endpoints de IA
    - Controla y monitoriza las salidas de datos por activo e identidad
    - integrar con DLP para inspección de prompts y salidas cuando aplique
- **Añadir inteligencia y modelado de amenaza específico de IA**: incorporar TTPs (Técnicas, Tácticas y Procedimientos) relacionados con IA y emplear matrices/recursos orientados a IA cuando se analicen escenarios.

7.5.1.3.3 Realizar pruebas y evaluación exhaustivas de la IA

- **Comenzar pruebas en infraestructura de test**, permitiendo iteraciones rápidas (pruebas de baja fidelidad al inicio).
- **Evolucionar hacia pruebas más realistas en entornos no productivas** (incluyendo hardware-in-the-loop cuando aplique) antes de cualquier paso la producción.

- **Evitar exposición de datos de producción en entornos no productivas**, manteniendo prácticas tradicionales de protección de datos.

7.5.1.3.4 Navegar consideraciones regulatorias y de cumplimiento para IA en OT

- **Reconocer retos específicos**: ausencia de estándares orientados a OT, dificultad de auditoría/explicabilidad y encaje con certificaciones de seguridad.
- **Revisar estándares técnicos de IA aplicables y en evolución**, evaluando su pertinencia en el dominio OT.
- **Convalidar continuamente que el rendimiento cumple requisitos estrictos OT** (seguridad funcional y operación), **y definir umbrales de degradación** para volver a la operación sin IA cuando las salidas no cumplan los niveles de seguridad/precisión.

7.5.1.4 Principio 4 — Integrar supervisión y prácticas de seguridad funcional y fallo seguro

7.5.1.4.1 Establecer mecanismos de monitorización y supervisión de la IA en OT

- **Inventariar componentes de IA y dependencias asociadas** (lo que depende del modelo y de su output) como base para el control.
- **Registrar y monitorizar entradas y salidas**, y mantener un **estado conocido bueno** (o umbrales de comportamiento seguro) que permita detectar desviaciones y decidir cuándo restaurar desde copia/backup.
- **Introducir a la persona ("human-in-the-loop") en decisiones críticas**:
    - para sistemas pasivos, integrar recomendaciones en procesos de gestión del cambio
    - para sistemas activos que afectan al control, añadir puntos de intervención humana mediante umbrales de seguridad, señales alternativos o cambios de estado
- **Revisar de forma regular con stakeholders** (operación, gobernanza e provedores) resultados, incidencias y mejoras.
- **Actualizar modelos de amenaza y vigilar manipulación**: monitorizar anomalías, entradas adversarias e indicios de envenenamiento, y refinar modelos con nuevos datos OT para reducir falsos positivos/negativos.

- **Explorar mecanismos de explicabilidad y transparencia** (XAI) cuando sea viable, priorizando la capacidad de auditoría y seguridad en OT.
- **Preservar segmentación mediante diseños de conectividad seguros**: favorecer arquitecturas "push"/brokered, y cuando haya transferencia a redes de negocio emplear patrones unidireccionales y buffers auditados, evitando caminos persistentes hacia OT.

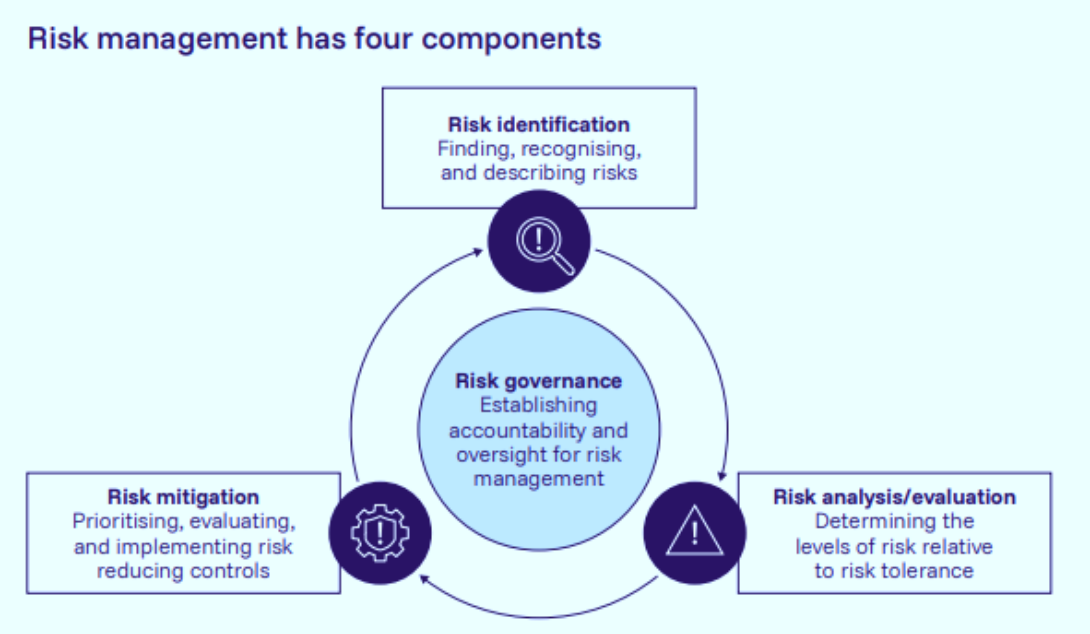
7.5.1.4.2 Integrar mecanismos “failsafe” y de recuperación segura

- **Establecer mecanismos de fallo seguro** para que la IA "hace adecuadamente" sin interrumpir operaciones críticas.
- **Incorporar nuevos estados de fallo de la IA** a los procesos existentes de seguridad funcional y respuesta a incidentes, definiendo como **bypassear, sustituir o retirar** el componente de IA.
- **Diseñar procedimientos de seguridad funcional que tengan en cuenta la IA**: adaptar estados y procedimientos por sector para contemplar la integración y el uso seguro.
- **Actualizar el plan de respuesta a incidentes** con pasos específicos para actividad maliciosa contra la IA y para fallos del sistema de IA, asumiendo que el riesgo no puede reducirse a cero.

7.5.2 Informe Internacional de Seguridad de la IA 2026

El **International AI Safety Report 2026** ya mencionado con anterioridad previamente es un informe internacional de síntesis que recopila y organiza el conocimiento existente sobre capacidades, riesgos y gestión del riesgo en IA de propósito general [23].

Como se puede apreciar, la metodología que proponen de gestión del riesgo en IA está alineada con la visión canónica habitual.



Metodología propuesta para la gestión de riesgos en el uso de la IA. Fuente: International AI Safety Report (2026)

La orientación del reporte es transversal (sociedad, economía, gobernanza y tecnología) y no está escrita específicamente para OT/ICS. Por este motivo, la contribución a nivel de recomendaciones que se incorpora en este informe es **parcial y selectiva**: se centra únicamente en los elementos de las secciones que pueden ser más afines a la **ciberseguridad industrial, a las infraestructuras críticas y a los sistemas ciberfísicos, haciendo** una interpretación del informe a nivel de gestión del riesgo, para llevarlo al terreno más operativo. Para un tratamiento completo y literal, se recomienda revisar la fuente original.

7.5.2.1 Desafíos técnicos e institucionales

- **Tomar decisiones con evidencia incompleta (dilema de la evidencia)**: en ámbitos críticos (energía, agua, industria), puede ser necesario establecer controles y gobernanza antes de disponer de pruebas definitivas sobre capacidades y riesgos futuros. Ello favorece enfoques de **precaución, escalado progresivo y revisión continua**.
- **Dificultad de evaluación y atribución**: los riesgos asociados a IA pueden ser difíciles de observar y medir en entornos reales, especialmente cuando la IA se integra en cadenas largas (proveedores → integradores → operadores). Ello refuerza la necesidad de **trazabilidad, registro y compartición estructurada de información**.

- **Brechas de coordinación e incentivos**: cuando existen múltiples actores, las responsabilidades pueden diluirse. Para OT/ICS, esto se traduce en reforzar **contratos, responsabilidades y mecanismos de aseguramiento** a lo largo de la cadena de suministro.

7.5.2.2 Prácticas de gestión del riesgo

- **Transparencia y documentación de riesgo**: adoptar prácticas de documentación (informes de transparencia, registros de evaluación y mitigación, etc.) para soportar decisiones y auditoría. En entornos industriales, esto es clave para demostrar **diligencia debida** en sistemas que pueden afectar seguridad y continuidad.
- **Notificación y gestión de incidentes**: integrar IA en los flujos existentes de gestión de incidentes, incluyendo criterios de reporte, análisis post-incidente y lecciones aprendidas.
- **Compromiso de la dirección e incentivos**: cultura, liderazgo e incentivos condicionan el éxito de la mitigación. Para OT, esto implica que la integración de IA debe tener **patrocinio ejecutivo**, responsabilidades claras y objetivos que prioricen seguridad y resiliencia sobre sólo eficiencia.
- **"Safety cases" y análisis de riesgo residual**: emplear enfoques estructurados (evaluación previa, mitigación, red teaming, análisis de riesgo residual) antes y durante el despliegue, particularmente en operaciones críticas.

7.5.2.3 Salvaguardias técnicas y monitorización

- **Defensa en profundidad como patrón de referencia**: las salvaguardias deben combinarse por capas (procesos, evaluación, controles técnicos, monitorización), evitando depender de una única medida.
- **Evaluación y *red teaming***: emplear pruebas adversariales y evaluaciones para descubrir fallos antes del despliegue y ante cambios relevantes. En OT, esto debe hacerse en entornos de prueba/simulación para no comprometer la operación.
- **Monitorización en producción y detección temprana**: asumir que las medidas pueden fallar y, por tanto, reforzar la monitorización, la detección de anomalías y los mecanismos de respuesta.
- **Limitaciones de la verificación formal en producción**: el informe indica que ciertas técnicas avanzadas (p.ej. verificación formal) aún tienen adopción

limitada en sistemas reales; en consecuencia, conviene priorizar combinaciones pragmáticas de **evaluación + monitorización + contención**.

7.5.2.4 Modelos de pesos abiertos (open-weight)

Los **modelos open-weight** son modelos de IA cuyos **pesos (parámetros aprendidos)** se publican y pueden descargarse para **ejecutarlos y modificarlos localmente**, sin depender del proveedor original. A este respecto, se señala lo siguiente:

- **Equilibrar beneficios y riesgos**: los modelos de pesos abiertos facilitan investigación e innovación, pero también pueden permitir la eliminación más donada de salvaguardias y dificultan la monitorización de su uso.
- **Riesgo de modificación maliciosa**: el informe señala que actores maliciosos pueden ajustar modelos para usos dañinos, retirar mecanismos de seguridad o deshacer ajustes de seguridad previos.
- **Riesgo heredado en la integración**: los desarrolladores y operadores que integran modelos open-weight heredan posibles debilidades (incluyendo vulnerabilidades a ataques adversariales) y pueden tener más difícil distribuir correcciones de forma universal.
- **Implicación para OT/ICS**: cuando se utilicen modelos open-weight en casos con impacto operacional, se recomienda reforzar:
    - evaluación previa y pruebas adversariales,
    - control de actualizaciones y versiones,
    - aislamiento y limitación de privilegios,
    - y una estrategia de reversión/retirada rápida.

7.5.2.5 Construir resiliencia social

- **Resiliencia como complemento a las salvaguardias**: el informe define resiliencia como la capacidad de resistir, absorber, recuperar y adaptarse a shocks y daños; subraya que algunas fallas emergen sólo en despliegues reales y pueden tener efectos en cadena.
- **Resiliencia aplicada a la infraestructura crítica**: para entornos industriales, esto se traduce en fortalecer capacidades de:
    - continuidad operativa y recuperación,

  - coordinación público-privada,
  - compartición de información en tiempo real,
  - y ejercicios/escenarios de crisis.

- **La IA también puede reforzar la defensa**: el informe menciona usos defensivos como detección de anomalías a gran escala, clasificación de malware y prevención de phishing. En entornos OT, estos usos deben implementarse con gobernanza, control de datos y supervisión, para no crear nuevas dependencias frágiles.
- **Gestión del equilibrio ofensiva-defensiva**: se reconoce que mejorar capacidades defensivas con IA puede tener efectos secundarios (aceleración de capacidades ofensivas). Para operadores industriales, esto refuerza la importancia de **evaluación continua**, segmentación y diseño para contención.

8 Conclusiones

El presente **Informe de riesgos tecnológicos** confirma una realidad ya observada en otros entregables del Observatorio: la progresiva digitalización industrial y la convergencia IT/OT incrementan de forma sostenida la superficie de exposición, mientras la amenaza evoluciona hacia modelos más rápidos, pero automatizados y con una orientación creciente **al impacto operativo**. La consecuencia práctica es clara: en entornos OT/ICS, la ciberseguridad debe formularse como **gestión del riesgo ciberfísico**, donde disponibilidad y seguridad funcional condicionan que controles son viables, cuando pueden implantarse y como se verifica su eficacia.

Desde una perspectiva estratégica, el informe muestra que el **riesgo no es exclusivamente tecnológico**. Factores sistémicos —como **la tensión geopolítica, la dependencia de cadenas de suministro y la concentración de proveedores**— amplifican la exposición y dificultan la recuperación cuando se produce un incidente. Este contexto refuerza **la necesidad de integrar la ciberseguridad industrial en la gobernanza corporativa e institucional**, asumiendo que el riesgo es **transfronterizo** y que la resiliencia requiere coordinación con terceros y con el ecosistema.

En el plano operativo, los patrones recurrentes que explican buena parte de los incidentes son conocidos y, por tanto, mitigables: falta de visibilidad e inventario, conexiones excesivas, accesos remotos insuficientemente controlados, gestión desigual de vulnerabilidades y una integración incompleta de OT en los procesos de detección y respuesta. Ello sugiere una prioridad inequívoca: antes de adoptar capacidades "avanzadas", **es de consolidar una base defensiva sólida basada en segmentación, control estricto de conectividad, autenticación y privilegios, monitorización y capacidad de contención.**

La incorporación de **Inteligencia Artificial introduce un cambio cualitativo**. Por una banda, puede reforzar capacidades defensivas y operativas; por otra, **habilita nuevas amenazas (automatización de reconocimiento y explotación, *phishing* más efectivo) y añade riesgos por fallos de funcionamiento y riesgos sistémicos**. En particular, el informe subraya dos puntos de atención: **la necesidad de gobernanza y supervisión** (para evitar decisiones opacas o degradación silenciosa del rendimiento) y el **riesgo organizativo asociado a la Shadow AI**, que puede provocar filtración de información sensible y dependencias tecnológicas no evaluadas.

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

Las recomendaciones sintetizadas a lo largo del documento convergen en un mensaje común: **la mitigación eficaz del riesgo en OT/ICS requiere un enfoque de defensa en profundidad y una aplicación disciplinada de controles, priorizados en función del riesgo y adaptados a las restricciones de la planta**. Esto incluye conocer y documentar el entorno (registro definitivo), reducir exposición (eliminar conexiones innecesarias y endurecer acceso remoto), limitar propagación (segmentación y aislamiento), mejorar detección (monitorización y correlación adaptadas a OT) y asegurar recuperación (operación manual, planes de aislamiento, continuidad y pruebas regulares).

En el caso específico de la IA en OT, el informe concluye que la adopción debe seguir una lógica de caso de negocio + riesgo, apoyada en principios de integración segura (formación, ciclo de vida seguro, protección de datos OT, gobernanza, pruebas rigurosas y mecanismos para fallar de forma seguro). De manera complementaria, la visión del International AI Safety Report refuerza la necesidad de **combinar salvaguardias técnicas con prácticas de gestión del riesgo** (transparencia, evaluación adversarial, monitorización en producción y resiliencia), prestando especial atención a los modelos open-weight cuando se integren en ámbitos con impacto operacional.

Finalmente, este informe cierra con una **conclusión de carácter programático: la mejora de la ciberseguridad industrial es un proceso continuo que requiere coherencia entre personas, procesos y tecnología.** El valor del Observatorio reside precisamente en facilitar dicha coherencia mediante inteligencia compartida, seguimiento de alertas y vulnerabilidades, orientación normativa y síntesis de buenas prácticas accionables, entre otras. En consecuencia, **se recomienda emplear este documento como base de priorización y complementarlo con los demás entregables (ciberalertas, inteligencia de amenazas, guía normativa o tendencias)** para **convertir el análisis en planificación y acción sostenible.**

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] Foro Económico Mundial (2025). *Informe de Riesgos Globales 2025.* Recuperado de https://www.weforum.org/publications/global-risks-report-2025/

[3] Nozomi Networks (2025). *OT Gestión de Riesgos de Ciberseguridad para 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] Inteligencia de amenazas en la nube de Google (2024). *Previsión de ciberseguridad para 2025*. Recuperado de https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025

[6] Google Cloud (2025). *Previsión de ciberseguridad 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). *El incendio en el contenedor de ClawDBot: 72 horas que expuso todo lo que fallaba en la seguridad de la IA*. 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). *El nuevo informe Dragos estima más de 300.000 millones de dólares en una posible exposición global al riesgo cibernético de OT*. 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). *Informe de riesgos financieros de valores OT 2025*. Recuperado de https://www.dragos.com/2025-ot-security-financial-risk-report

[13] Instituto SANS (2022). *Cinco controles críticos de ciberseguridad ICS*. 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). *Miles de millones en juego: el creciente impacto financiero del ciberriesgo tecnológico operativo*. 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). *Estado de la Tecnología Operativa y la Ciberseguridad*. Recuperado de https://www.fortinet.com/resources/reports/state-ot-cybersecurity

[18] Fortinet (2025). *Informe Fortinet: El riesgo de ciberseguridad en OT aumenta dentro de los rangos de liderazgo ejecutivo*. 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] Centro Nacional de Ciberseguridad (NCSC) (2025). *Impacto de la IA en la amenaza cibernética desde ahora hasta 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] Informe Internacional de Seguridad de la IA (2026). *Informe Internacional de Seguridad de la IA 2026*. Recuperado de https://internationalaisafetyreport.org/sites/default/files/2026-02/international-ai-safety-report-2026.pdf

[24] Ciber Industrial (2025). *La información sobre ciberseguridad en OT sigue siendo una debilidad estructural, ya que las amenazas superan a los modelos de gobernanza heredados*. Recuperado de https://industrialcyber.co/features/ot-cybersecurity-reporting-remains-a-structural-weakness-as-threats-outpace-legacy-governance-models/

[25] Brotby, K. (2009). *Gobernanza de la Seguridad de la Información: Un enfoque práctico de desarrollo e implementación*. Wiley.

[26] Calder, A. e Watkins, S. (2015). *Gobernanza de TI: Guía internacional sobre seguridad de datos y ISO27001/ISO27002*. Editoriales Kogan Page.

[27] Davies, J. (2016). *Realizar la Gobernanza de la Información: Una guía paso a paso para hacer que la Gobernanza de la Información funcione*. IBM Press.

[28] Gentile, M., Collette, R. E. D. August, T. (2005). *El manual CISO: Guía práctica para asegurar tu empresa*. 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). *Marco de Ciberseguridad del NIST, 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] Centro Nacional de Ciberseguridad (NCSC) (2016). *Orientación y mejores prácticas para la seguridad tecnológica industrial y operativa*. Recuperado de: https://www.ncsc.gov.uk

[35] Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) (2018). *Orientación sobre Sistemas de Control Industrial en Ciberseguridad*. 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] Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA); Centro Australiano de Ciberseguridad (ACSC) (2025). *Principios para la integración segura de la inteligencia artificial en la tecnología operativa.* 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] Centro Nacional de Ciberseguridad (NCSC) (2025). *Comprender tu entorno de terapia ocupacional: el primer paso para reforzar la ciberseguridad*. Recuperado de: https://www.ncsc.gov.uk/blog-post/understanding-ot-environment-1step-stronger-cyber-security

[44] Centro Nacional de Ciberseguridad (NCSC) (2024). *Tecnología Operativa – Recopilación de orientaciones*. Recuperado de: https://www.ncsc.gov.uk/collection/operational-technology

[45] Centro Nacional de Ciberseguridad (NCSC) (2023). *Seguridad en la nube – Recopilación de orientación*. Recuperado de: https://www.ncsc.gov.uk/collection/cloud

[46] Agencia de Ciberseguridad e Infraestructura (CISA) (2025). *Mitigaciones primarias para reducir las amenazas cibernéticas a la tecnología operativa*. Recuperado de: https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

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

[48] CISA (2025). *Principios para la integración segura de la inteligencia artificial en la tecnología operativa*. Recuperado de https://www.cisa.gov/resources-tools/resources/principles-secure-integration-artificial-intelligence-operational-technology

[49] Alianza de Seguridad en la Nube. (2024). *El estado de la seguridad y gobernanza de la IA*. Recuperado de: https://cloudsecurityalliance.org/artifacts/the-state-of-ai-security-and-governance

Glosario

ACSC (Australian Cyber Security Centre)

Centro nacional de ciberseguridad de Australia. Publica guías y avisos, y colabora con otras agencias internacionales en la definición de buenas prácticas, incluyendo recomendaciones para integrar IA y seguridad en entornos OT.

AIPD / EIPD (Evaluación de Impacto en la Protección de Datos)

Análisis sistemático para identificar y mitigar riesgos sobre la privacidad y los derechos de las personas al tratar datos personales, especialmente cuando se emplean tecnologías o tratamientos de alto riesgo.

AMTEGA (Agencia para la Modernización Tecnológica de Galicia)

Organismo de la Xunta de Galicia responsable de la modernización tecnológica y de la coordinación de iniciativas de ciberseguridad en el ámbito autonómico.

Antimalware

Conjunto de mecanismos y soluciones para detectar, bloquear y eliminar software malicioso en endpoints, servidores o pasarelas.

Auditoría interna

Función independiente que verifica la eficacia de los controles y procesos de seguridad y cumplimiento, evaluando evidencias y recomendando mejoras.

Bastionado (hardening)

Proceso de endurecimiento de un sistema mediante configuración segura, desactivación de servicios innecesarios y aplicación de buenas prácticas para reducir la superficie de ataque.

Biometría

Método de autenticación basado en características físicas o comportamientos (p.ej. impresión digital). Se usa como factor adicional cuando es compatible y está bien gobernado.

BSI (Bundesamt für Sicherheit in der Informationstechnik)

Agencia federal alemán de seguridad de la información. Publica guías y orientaciones técnicas, incluyendo contenidos sobre seguridad y riesgo en tecnologías emergentes.

CAB (Change Advisory Board)

Comité u órgano de gestión del cambio que revisa y aprueba cambios en sistemas, especialmente relevante en OT para equilibrar continuidad operativa, seguridad y seguridad funcional.

Cadena de suministro

Conjunto de proveedores, integradores y dependencias tecnológicas que pueden introducir riesgo (vulnerabilidades, accesos, software/firmware) en sistemas industriales.

C2M2 (Cybersecurity Capability Maturity Model)

Modelo de madurez para evaluar y mejorar capacidades de ciberseguridad, especialmente útil para planificar evolución por fases.

CER (Critical Entities Resilience)

Marco regulatorio europeo orientado a reforzar la resiliencia de entidades críticas frente a riesgos, incluyendo aquellos con componente tecnológico y ciberfísico.

CERT (Computer Emergency Response Team)

Equipo especializado en la gestión y coordinación de incidentes, análisis técnica y emisión de alertas y recomendaciones.

CCN-CERT

Centro de respuesta a incidentes del Centro Criptológico Nacional (España). Publica guías y avisos, y coordina la respuesta a incidentes en el ámbito público y sectores vinculados.

CCN-STIC

Serie de guías técnicas del CCN-CERT (España) para apoyar la implantación de controles, cumplimiento y buenas prácticas de seguridad.

CIO (Chief Information Officer)

Responsable ejecutivo de tecnología de la información. En entornos con convergencia TI–OT, es clave para alinear arquitectura, operación e inversión con requisitos de seguridad.

CISA (Cybersecurity and Infrastructure Security Agency)

Agencia federal de los EUA que publica guías y avisos para infraestructuras críticas, incluyendo mitigaciones primarias para reducir amenazas en entornos OT.

CIS (Center for Internet Security)

Organización que publica Benchmarks y Controles (Controles CIS), ampliamente empleados como referencia de buenas prácticas y líneas base de configuración.

CISO (Chief Information Security Officer)

Responsable ejecutivo de seguridad de la información y ciberseguridad. Coordina estrategia, riesgo, controles y respuesta a incidentes, incluyendo la integración TI–OT cuando aplica.

ClawDBot / Moltbot

Ejemplo de herramienta basada en IA difundida de forma viral, asociada al riesgo de Shadow Tech cuando se adoptan soluciones sin gobernanza ni salvaguardias.

Cloud

Modelo de provisión de servicios TIC bajo demanda (infraestructura, plataformas o aplicaciones). En OT puede introducir nuevas dependencias y riesgos de conectividad, datos y responsabilidad compartida.

COO (Chief Operating Officer)

Responsable ejecutivo de operaciones. En industria, es un stakeholder crítico porque los incidentes cibernéticos pueden impactar directamente la continuidad y el rendimiento operativo.

Conectividad OT

Conjunto de conexiones y flujos de comunicación dentro del sistema OT y entre OT y otros dominios (p.ex. IT, terceros). Su minimización y control son críticos para reducir exposición.

CRA (Cyber Resilience Act)

Reglamento europeo para mejorar la ciberresiliencia de productos con elementos digitales, exigiendo seguridad por diseño y por defecto y obligaciones a lo largo del ciclo de vida.

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

CSIRT (Computer Security Incident Response Team)

Equipo de respuesta a incidentes (sinónimo próximo a CERT), centrado en detección, análisis, contención y coordinación de la recuperación.

CSA (Cloud Security Alliance)

Organización internacional centrada en buenas prácticas de seguridad en la nube y gobernanza asociada, incluyendo análisis sobre seguridad y gobernanza de IA.

CSET (Cyber Security Evaluation Tool)

Herramienta de evaluación (CISA) para analizar postura de ciberseguridad y controles, utilizada como apoyo a diagnósticos y mejoras, incluyendo ámbitos industriales.

DDoS (Distributed Denial of Service)

Ataque distribuido de denegación de servicio que busca saturar servicios o redes para provocar indisponibilidad.

Defensa en profundidad

Estrategia que combina múltiples capas de controles (organizativos, físicos y técnicos) para prevenir, detectar y mitigar ataques, evitando depender de un único mecanismo.

Directorio Activo (Active Directory)

Servicio de Directorio de Microsoft para gestionar identidades, grupos y políticas. Se usa habitualmente como base para SSO, LDAP y gobernanza de accesos.

DMZ (Zona Desmilitarizada)

Zona intermedia de red para exponer servicios controlados y separar dominios (p.ej. IT y OT), reduciendo riesgo de acceso directo a sistemas críticos.

DLP (Data Loss Prevention)

Controles y herramientas para prevenir exfiltración o fuga de datos, mediante políticas, inspección de contenido y control de cauces de salida.

DoS (Denegación de Servicio)

Ataque de denegación de servicio que busca interrumpir la disponibilidad de un sistema o servicio, normalmente por saturación de recursos.

DPO (Data Protection Officer)

Delegado/a de Protección de Datos, responsable de asesorar y supervisar cumplimiento en materia de protección de datos y privacidad.

EDR (Endpoint Detection and Response)

Capacidad de detección y respuesta en Endpoints mediante telemetría, análisis y acciones de contención, útil también en entornos híbridos TI/OT cuando es compatible.

ENISA

Agencia de la Unión Europea para la Ciberseguridad. Publica orientación, informes y recomendaciones para mejorar capacidades y resiliencia a nivel europeo.

ENS (Esquema de Seguridad Nacional)

Marco español que establece principios y requisitos para proteger información y servicios en el sector público y entidades vinculadas, con impacto sobre gobernanza y controles.

Envenenamiento de datos

Ataque contra sistemas de IA que introduce o modifica datos para degradar el rendimiento el modelo o inducir salidas incorrectas, con riesgo operativo en OT.

Entradas opuestas

Técnicas que manipulan entradas a un modelo de IA para provocar errores de clasificación o comportamiento no deseado, incluso sin modificar el modelo.

ERP (Enterprise Resource Planning)

Sistemas corporativos de planificación y gestión (finanzas, compras, logística, producción) cuyo compromiso puede paralizar operación industrial al romper flujos de datos y procesos.

Escala de Likert

Escala de valoración por niveles (p.ej. 1–7) empleada en encuestas para estimar percepciones de severidad, probabilidad o impacto.

Failsafe

Diseño de fallo seguro: mecanismos para que un sistema pase a un estado seguro ante errores, anomalías o pérdida de confianza, priorizando continuidad y seguridad funcional.

Formación y concienciación

Programa de capacitación y sensibilización para reducir errores humanos, mejorar prácticas y reforzar cultura de seguridad, clave también en OT.

GCHQ (Government Communications Headquarters)

Organismo británico de inteligencia y seguridad, en el que se integra el NCSC como autoridad técnica en ciberseguridad.

GRC (Gobierno, riesgo y cumplimiento)

Disciplina que integra gobernanza, gestión del riesgo y cumplimiento normativo. En OT/ICS abarca riesgo tecnológico, proveedores, políticas, métricas y reporte.

HIDS (Host-based Intrusion Detection System)

Sistema de detección de intrusiones a nivel de host que supervisa eventos e integridad local para identificar actividad sospechosa.

HMI (Human-Machine Interface)

Interfaz hombre-máquina usada por operadores para supervisar y controlar procesos industriales. Su protección es crítica por la visibilidad y control que proporciona.

IAM (Identity and Access Management)

Gobierno y gestión del ciclo de vida de identidades, autenticación y autorización, incluyendo provisión, modificación y retirada de accesos.

IA (Inteligencia Artificial)

Conjunto de técnicas que permiten a sistemas realizar tareas cognitivas (análisis, predicción, generación). En OT puede aportar eficiencia, pero también introduce nuevos riesgos.

IA Generativa

Subcampo da IA capaz de generar texto, imágenes o código. Puede mejorar productividad, pero también facilitar fraude, *phishing* y filtración de información (incluyendo Shadow AI).

IACS (Industrial Automation and Control Systems)

Término equivalente/próximo a ICS, centrado en automatización y control industrial y en sus componentes e interdependencias.

ICS (Industrial Control Systems)

Conjunto de sistemas y dispositivos empleados para monitorizar y controlar procesos industriales, incluyendo PLC, SCADA e HMI.

ICS-CERT

Denominación empleada por ciertos equipos/capacidades especializadas en respuesta y análisis en entornos ICS; en el informe también aparece como referencia la telemetría e informes sectoriales.

IEC 62443 (ISA/IEC 62443)

Conjunto de estándares internacionales para seguridad de sistemas de automatización y control industrial, con enfoque por requisitos y niveles de seguridad.

INCIBE-CERT

Equipo de respuesta a incidentes y emisión de alertas del INCIBE (Instituto Nacional de Ciberseguridad de España), con contenidos específicos para ciberseguridad industrial.

Infostealer

Tipo de malware orientado al robo de información (credenciales, cookies, datos) que puede facilitar acceso inicial y movimiento lateral.

Integración IT/OT (convergencia TI–OT)

Proceso por el que sistemas de operación industrial se conectan o interaccionan con sistemas corporativos, aumentando eficiencia pero también superficie de ataque.

IoC (Indicadores de compromiso)

Evidencias técnicas de un posible compromiso (hashes, IPs, dominios, rutas, patrones de log) usadas para detección y respuesta a incidentes.

IP (Internet Protocol)

Protocolo base de comunicación en redes. Su gestión y segmentación es relevante para controlar conectividad y exposición de sistemas OT.

IDS (Intrusion Detection System)

Sistema de detección de intrusiones que monitoriza tráfico o eventos para identificar actividad maliciosa; puede existir en red (NIDS) o en host (HIDS).

ISACA

Asociación internacional de profesionales de auditoría, riesgo y seguridad. Publica orientación y análisis desde una óptica de gobernanza y control.

ISMS / SGSI (Sistema de Gestión de la Seguridad de la Información) Conjunto de políticas, procesos y controles para gestionar la seguridad de la información de forma sistemática y auditable, normalmente alineado con ISO/IEC 27001.

ISO/IEC 27001

Estándar internacional para sistemas de gestión de seguridad de la información (ISMS), que define requisitos para gobernanza, controles y mejora continua.

ELLO27002

Código de buenas prácticas asociado a ISO/IEC 27001 que detalla controles recomendados para la seguridad de la información.

IPS (Intrusion Prevention System)

Sistema de prevención de intrusiones que, además de detectar, puede bloquear o mitigar tráfico malicioso en tiempo real.

LDAP (Lightweight Directory Access Protocol)

Protocolo para acceso a servicios de directorio (identidades, grupos, permisos). Útil para centralizar autenticación y autorización en entornos con múltiples aplicaciones.

LOPD-GDD

Lei Orgánica española de Protección de Datos y garantía de los derechos digitales, complementaria al RGPD y relevante para tratamientos y gobernanza de datos.

MAC (Media Access Control)

Identificador de una interfaz de red. Puede emplearse en políticas de red y control de acceso, aunque no es un control de seguridad suficiente por sí solo.

Malware

Software malicioso diseñado para dañar, interromper o comprometer sistemas (p.ej. ransomware, infostealers).

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

MFA (Multi-Factor Authentication)

Autenticación multifactor que combina dos o más factores (contraseña + token/OTP, biometría, certificado), reduciendo riesgo por robo de credenciales.

Mínimo privilegio

Principio por el que las cuentas y procesos deben tener sólo los permisos imprescindibles para su función, limitando el impacto de un compromiso.

Modelado de amenazas

Proceso de identificar activos, superficies de ataque, amenazas y mitigaciones de un sistema, para diseñar controles de forma preventiva.

Deriva del modelo

Degradación progresiva del rendimiento de un sistema de IA debido a cambios en los datos, proceso o entorno, pudiendo causar decisiones incorrectas en OT.

Modelos de pesos abiertos (open-weight)

Modelos de IA cuyos pesos se publican y pueden ejecutarse/modificarse localmente, lo que facilita innovación, pero también puede permitir retirar salvaguardias e incrementar riesgo.

Monitorización

Recogida y análisis continuo de eventos y tráfico para detectar anomalías, compromisos y degradaciones, adaptada a las particularidades de OT/ICS.

NCSC (National Cyber Security Centre, UK)

Centro nacional británico de ciberseguridad (parte de GCHQ) que publica guías prácticas para OT, conectividad segura y arquitectura.

NCSC-NL (National Cyber Security Centre Netherlands)

Centro nacional de ciberseguridad de los Países Bajos. Publica guías y participa en iniciativas internacionales, incluyendo recomendaciones de seguridad en IA.

NCSC-NZ (National Cyber Security Centre New Zealand)

Centro nacional de ciberseguridad de Nueva Zelandia. Emite guías y participa en colaboraciones internacionales en materia de ciberseguridad e IA.

NDR (Network Detection and Response)

Capacidades para detectar y responder a actividades maliciosas en la red mediante análisis de tráfico y comportamiento.

NIS / NIS2

Directivas europeas sobre seguridad de redes y sistemas de información. NIS2 refuerza requisitos de gestión del riesgo, reporte de incidentes y cadena de suministro.

NIST

Instituto Nacional de Estándares y Tecnología (EUA). Publica estándares y guías de referencia en seguridad, incluyendo orientación para sistemas industriales.

NIST CSF (Cybersecurity Framework)

Marco de buenas prácticas de NIST estructurado en funciones (identificar, proteger, detectar, responder, recuperar) para gestión del riesgo de ciberseguridad.

NIST SP 800-82

Guía de NIST para seguridad de sistemas de control industrial, con recomendaciones específicas para arquitectura, riesgos y controles en OT/ICS.

NSA (National Security Agency)

Agencia estadounidense con papel destacado en seguridad y criptografía; participa en colaboraciones internacionales sobre recomendaciones y buenas prácticas de seguridad.

Operación manual

Capacidad de operar procesos industriales mediante procedimientos manuales cuando sistemas digitales fallan o se consideran no fiables, clave para continuidad y seguridad funcional.

OT (Operational Technology)

Sistemas y dispositivos que monitorizan y controlan procesos físicos. Prioriza disponibilidad y seguridad operacional frente a la confidencialidad.

OTP (One-Time Password)

Contraseña de un solo uso empleado como segundo factor en autenticación, normalmente generado por token, app o hardware.

Passkey

Mecanismo de autenticación moderno basado en criptografía de clave pública (generalmente FIDO2/WebAuthn) que reduce dependencia de contraseñas reutilizables.

PAW (Estación de trabajo de acceso privilegiado)

Estación de trabajo privilegiada y endurecida para tareas administrativas sensibles, destinada a proteger credenciales y acciones de alto impacto.

Parcheado virtual (virtual patching)

Medida compensatoria que bloquea explotaciones a nivel de red o aplicación (p.ej. IPS/WAF) cuando no es viable aplicar el parche en el activo vulnerable de inmediato.

PCE-NIS2 (CCN-STIC 892)

Guía del CCN-CERT que actúa como apoyo práctico al cumplimiento de NIS2 en España, ayudando a mapear obligaciones a medidas y evidencias.

BCP (Plan de Continuidad de Negocio)

Plan que define servicios prioritarios, tareas, responsables y procedimientos para mantener/restaurar operación tras incidentes disruptivos.

Phishing

Técnica de Ingeniería Social que busca engañar a las personas para obtener credenciales o ejecutar acciones maliciosas, relevante como vector inicial que puede afectar OT por convergencia.

PIC (Ley para la Protección de Infraestructuras Críticas)

Normativa española orientada a la protección y planificación de seguridad de infraestructuras críticas, reforzando coordinación y obligaciones para garantizar continuidad de servicios esenciales.

PLC (Programmable Logic Controller)

Controlador lógico programable empleado para automatizar procesos industriales. Su indisponibilidad o modificación puede tener impacto operativo y físico.

Playbook

Procedimiento operativo (frecuentemente en SecOps/SOC) que define pasos de respuesta a alertas o incidentes, facilitando actuación consistente y reproducible.

Privacidad

Conjunto de principios y medidas para garantizar un tratamiento adecuado de datos personales, minimizando riesgos legales y reputacionales.

Prompt injection (inyección de instrucciones)

Ataque que manipula un sistema de IA para ignorar limitaciones y ejecutar instrucciones del atacante, pudiendo causar exfiltración o recomendaciones peligrosas.

RBAC (Role-Based Access Control)

Modelo de control de acceso basado en roles, asignando permisos por función y facilitando mínimo privilegio y segregación de funciones.

Ransomware

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

Resiliencia (ciberresiliencia)

Capacidad de resistir, absorber, recuperar y adaptarse tras incidentes. En OT incluye contención, operación manual, continuidad y recuperación probada.

RGPD

Reglamento General de Protección de Datos de la UE, marco principal de privacidad y protección de datos personales.

ROI (Return on Investment)

Indicador que estima el retorno de una inversión. En ciberseguridad OT se usa para justificar medidas, aunque requiere modelos que capten impacto por indisponibilidad y riesgo ciberfísico.

RPO (Recovery Point Objective)

Objetivo de punto de recuperación: cantidad máxima de pérdida de datos aceptable medida en el tiempo, clave en el diseño de copias de seguridad.

RTO (Recovery Time Objective)

Objetivo de tiempo de recuperación: tiempo máximo aceptable para restaurar un servicio tras un incidente, determinando prioridades y recursos.

SaaS (Software as a Service)

Modelo cloud en el que aplicaciones se consumen como servicio. Puede acelerar Shadow Tech e introducir riesgos de datos y dependencia de terceros.

SANS

Organización de formación e investigación en seguridad que publica guías y recomendaciones, incluyendo contenidos específicos para sistemas industriales.

SCADA (Supervisory Control and Data Acquisition)

Sistema para supervisión y control a nivel de planta o infraestructura distribuida, agregando telemetría y permitiendo operación remota.

SecOps

Integración de seguridad en las operaciones diarias (detección, respuesta, automatización), buscando coordinación entre equipos y ciclos de mejora continua.

Segregación de funciones

Principio que separa responsabilidades críticas (p.ej. aprobación, ejecución, revisión) para reducir riesgo de abuso y errores.

Seguridad funcional

Disciplina orientada a garantizar que sistemas industriales operan de forma segura y previsible, reduciendo riesgo de daños físicos; debe considerarse junto a la ciberseguridad.

Segmentación de red

División de una red en segmentos/zonas con políticas de acceso y filtrado para limitar movimiento lateral y reducir impacto de un compromiso.

IA de las sombras

Uso de tecnología y/o herramientas de IA fuera de la gobernanza formal (sin aprobación ni controles), incrementando riesgo de filtración de datos y exposición indirecta de OT.

SIEM (Security Information and Event Management)

Plataforma para recoger, normalizar y correlacionar eventos de seguridad, generando alertas y facilitando investigación.

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

SOC (Security Operations Center)

Equipo/función que monitoriza seguridad, gestiona alertas y coordina respuesta a incidentes, idealmente integrando visibilidad TI y OT.

SSO (Single Sign-On)

Mecanismo que permite autenticación única para múltiples servicios, mejorando experiencia y control cuando se combina con MFA y gobernanza de identidades.

Token

Dispositivo o mecanismo lógico empleado para autenticación (p.ej. generación de OTP) o para representar credenciales/certificados.

UE (Unión Europea)

Marco institucional y regulatorio europeo que impulsa directivas y regulaciones relevantes (p.ej. NIS2, CER, CRA) y coordinación en ciberseguridad.

VPN (Virtual Private Network)

Tecnología para crear un túnel cifrado de acceso remoto. Útil para terceros y mantenimiento, pero debe reforzarse con MFA y control estricto de privilegios.

Vishing

Variante de phishing basada en llamadas de voz, la ministra amplificada por clonación/suplantación, usada para obtener credenciales o inducir acciones.

WAF (Web Application Firewall)

Cortafuegos de aplicación web que filtra y bloquea ataques contra aplicaciones; puede emplearse como medida compensatoria en ciertos escenarios.

FEM (World Economic Forum)

Foro Económico Mundial. Publica análisis de riesgo global (Global Risks Report) que ayudan a contextualizar riesgos sistémicos con impacto en infraestructuras críticas.

XAI (Explainable AI)

Conjunto de técnicas para mejorar la explicabilidad de la IA, facilitando auditoría, confianza e identificación de errores, especialmente relevante en decisiones críticas.

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial
Informe de Riesgos Tecnológicos

AMTEGA – Xunta de Galicia 2026

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