CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial

Informe de Intelixencia de Ameazas - I

Febreiro 2026

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

Edita: Xunta de Galicia

Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Ano: 2026

Índice

1 Introdución

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

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

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

--

A crecente complexidade do **ecosistema de ameazas que impacta nos sistemas industriais e ás infraestruturas críticas** esixe ás organizacións dispor de capacidades de análises que integren tendencias globais, europeas e nacionais, así como evidencias tácticas observables. Neste contexto, este *Informe de Intelixencia de Ameazas do Observatorio de Ciberseguridade Industrial* concíbese como un documento orientado a traducir a evolución do escenario internacional en implicacións reais e prácticas para organizacións con entornos OT/ICS.

O propósito fundamental do informe é ofrecer **intelixencia accionable**, apoiada en fontes nacionais e internacionais, en patróns emerxentes vinculados a actores estatais, ciberdelincuencia organizada e hacktivismo, e potencialmente a futuro en telemetría propia obtida a través dos **honeypots OT despregados por AMTEGA**, que constitúen un achegue próximo na observación directa de tendencias e comportamentos hostís. Abrangue ameazas que afectan ou poden afectar a entornos industriais e a infraestruturas críticas.

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

A pesar de estar baseado en información con carácter máis ou menos global debido á inexistencia de fontes específicas en Galicia, o risco é plenamente aplicable debido ao carácter remoto e en gran medida transfronteirizo da maioría de ataques a entornos ICS/OT.

O documento diríxese a responsables de ciberseguridade, equipos SOC/CSIRT, perfís técnicos e operativos, administracións públicas e responsables de risco que requiran unha visión do panorama de ameazas e das súas implicacións. A súa relevancia refórzase ante un entorno caracterizada pola proliferación **de ransomware industrial**, a aparición **de malware ICS específico**, a intensificación de actividades de **actores estatais**, e a **explotación sistemática de vulnerabilidades** en produtos de fabricantes de equipamento OT, nun escenario de máxima incerteza pola situación xeopolítica mundial e **a proliferación da IA**.

A estrutura do informe desenvólvese de maneira orgánica, iniciando cunha introdución conceptual e continuando cun Resumo Executivo que sintetiza indicadores clave, riscos e recomendacións estratéxicas. O bloque central presenta a análise de Threat Intelligence, que integra un marco teórico de ciberintelixencia e construción de programas asociados, visión global dalgúns dos principais fabricantes, europea e nacional, uso de IA por adversarios, incidentes e campañas recentes, vulnerabilidades ICS, actores de ameaza e TTPs baseados en MITRE, seguido de conclusións que resumen o contido e proxectan a evolución previsible do panorama, pechando xa finalmente coa recompilación bibliográfica de fontes e un glosario de termos empregados.

En futuras edicións, traballaranse outros aspectos como por exemplo construír información de intelixencia propia para un SOC interno, ou un conxunto de recomendacións operativas e estratéxicas.

Este Informe de Intelixencia articúlase como **peza complementaria e evolutiva do Informe de Ciberalertas do Observatorio**, ampliando o seu alcance máis aló da análise táctica *de advisories* e vulnerabilidades para ofrecer unha lectura estratéxica e contextualizada do panorama de ameazas. Mentres o Informe de Ciberalertas se focaliza na monitorización continua de fallos críticos, avisos de fabricantes e vulnerabilidades explotables —achegando un seguimento inmediato e orientado á acción técnica— este documento adopta unha perspectiva máis ampla, integrando tendencias, actores, motivacións e patróns de actividade que permiten entender non só *que* ocorre, senón *por que ocorre* e *como podería evolucionar*.

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

O informe aspira a consolidarse como un recurso **rigoroso, útil e orientado á toma de decisións**, que non só describe o estado do panorama de ameazas, senón que permite anticipar comportamentos, detectar puntos débiles e priorizar esforzos defensivos. Deste xeito, refórzase a capacidade de análise do Observatorio, proporcionando unha visión máis completa e integrada que fortalece a **anticipación, a preparación e a resiliencia** do ecosistema industrial galego.

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

2 Resumo executivo

Esta sección pretende dotar **aos responsables de seguridade, xestores industriais e decisores estratéxicos dunha visión sintética e práctica do estado das ameazas e as principais liñas de actuación defensiva a curto e medio prazo.**

O informe proporciona unha radiografía actualizada do **panorama de ameazas sobre entornos industriais** a partir de múltiples fontes globais, europeas e nacionais. Nun contexto de crecente dixitalización de procesos críticos, os ciberataques a infraestruturas OT escalaron en número, sofisticación e dano potencial.

A nivel global, obsérvase unha clara intensificación do interese de **grupos patrocinados por Estados** (especialmente Rusia, China, Irán e Corea do Norte) sobre sectores industriais estratéxicos. En paralelo, o **cibercrime organizado** e o **hacktivismo ideolóxico** sofisticaron as súas ferramentas, destacando o uso de ransomware, campañas DDoS coordinadas e malware dirixido a dispositivos industriais. Europa rexistrou un **incremento de incidentes en sectores como a administración pública, o transporte e a enerxía**, con especial afectación a sistemas de supervisión e automatización.

Entre os indicadores clave destacan:

- A explotación de **servizos expostos e uso de credenciais válidas** como vectores de acceso inicial máis frecuentes. En 2024, ambos os métodos representaron o 30% dos accesos comprometidos segundo X-Force.
- Unha alta prevalencia de **vulnerabilidades non parcheables** en dispositivos OT, obrigando a estratexias alternativas como segmentación ou detección baseada en comportamento.
- A adopción xeneralizada de **técnicas de Intelixencia Artificial** por parte dos atacantes para mellorar as súas campañas. Microsoft detectou máis de 20 grupos de ameazas utilizando ferramentas xerativas para phishing, desinformación e scripting automatizado.
- Un entorno con **baixa visibilidade e escasa compartición de intelixencia técnica** sobre ameazas OT, onde aínda predomina unha cultura de compartimentos estancos.

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

Estes factores xeran **riscos estratéxicos** para a continuidade operativa, a seguridade física e o cumprimento regulatorio. Por exemplo, o impacto económico medio dun incidente en sistemas OT alcanza os **3,5 millóns de dólares**, sen considerar o custo reputacional ou as sancións legais derivadas do RGPD ou a NIS2.

As organizacións industriais **deben prepararse para afrontar escenarios de intrusión persistente, degradación progresiva de servizos e presión xeopolítica** a través do ciberespazo.

Ao longo do informe proponse unha serie de **recomendacións**, entre as que destacan:

- **Formar equipos mixtos IT/OT**, promovendo a converxencia de competencias.
- **Non descoidar o factor humano** (políticas, procedementos, formación e concienciación).
- **Segmentar e protexer** redes OT seguindo modelos de defensa en profundidade.
- **Fortalecer a xestión de identidades**, eliminando credenciais por defecto e aplicando MFA onde sexa viable.
- Controlar debidamente **a cadea de subministración**.

En futuras edicións do informe, porase o foco en aspectos adicionais de valor para o ecosistema galego, como poden ser:

- **Construír capacidades propias de intelixencia de ameazas**, apoiadas en plataformas como MISP ou OpenCTI.
- **Adoptar marcos de ciberresiliencia de entidades internacionales recoñecidas,** que aseguren resposta e continuidade operativa ante ataques disruptivos.

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

3 Intelixencia de ameazas

3.1 Marco teórico

3.1.1 Introdución

A comprensión axeitada do **risco** en ciberseguridade industrial resulta esencial para interpretar o valor da intelixencia. En termos xerais, un risco xorde cando coinciden tres elementos: **un activo**, **unha ameaza** e **unha vulnerabilidade** susceptible de ser explotada. Sen ameaza, non existe axente que tente provocar dano; sen vulnerabilidade, a ameaza carece dun punto de entrada; e sen activo, non hai nada que protexer. En consecuencia, **coñecer o comportamento das ameazas** —as súas motivacións, capacidades e técnicas— **é capital para anticipar riscos antes de que se materialicen.**

En entornos OT/ICS esta relación é especialmente crítica: os impactos potenciais non se limitan a perdas económicas ou roubo de información, senón que poden afectar á dispoñibilidade operativa, provocar danos físicos en equipos e comprometer a seguridade de persoas e procesos. Por iso, a intelixencia convértese nunha función estratéxica que permite reducir incerteza, orientar decisións e actuar de forma proactiva.

Vexamos de maneira somera unha pequena introdución [1][2][3] a esta disciplina de crecente importancia no ámbito da seguridade da información.

A intelixencia en ciberseguridade consiste en **transformar información en coñecemento útil** para anticipar riscos e comprender como, por que e contra que poderían actuar os adversarios. En entornos **ICS/OT**, esta capacidade é especialmente crítica: as ameazas non só buscan comprometer datos, senón **alterar procesos físicos**, interromper a operación ou provocar danos materiais e de seguridade. Por iso, a intelixencia permite identificar sinais temperáns de actividade hostil, contextualizar vulnerabilidades en sistemas industriais e priorizar medidas que reduzan a probabilidade dunha intrusión con impacto operativo.

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

Enquisa State of Threat Intelligence. Fonte: Recorded Future (2025)

Esta disciplina pode aplicarse desde dúas perspectivas complementarias:

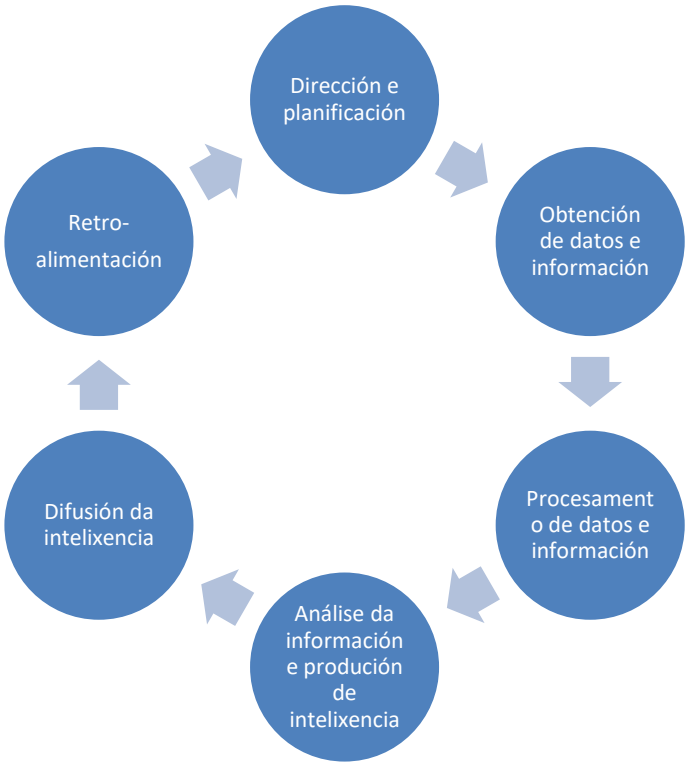
- Por unha banda, a **intelixencia ofensiva** axuda a descubrir debilidades en arquitecturas OT —por exemplo, configuracións inseguras, servizos expostos ou fallos en dispositivos de control— habitualmente no marco de exercicios éticos como avaliacións de seguridade ou simulacións de ataque.

- Por outro, a **intelixencia defensiva** céntrase en entender como operan os adversarios, que vectores prefiren en entornos industriais (acceso remoto, explotación de PLCs, abuso de protocolos ICS, etc.) e que indicadores permiten identificalos precozmente.

- A iso súmase a **contraintelixencia**, orientada a **detectar e neutralizar actividades hostís** dirixidas contra operacións críticas, incluíndo movementos de espionaxe industrial, intentos de sabotaxe ou comportamentos anómalos que poidan sinalar a presenza dun *insider* ou dun actor persistente.

O funcionamento eficaz destas capacidades apóiase en principios estruturados, entre os que destaca o **ciclo de intelixencia**, un proceso iterativo no que as necesidades operativas transfórmanse en coñecemento accionable mediante **planificación, recompilación de datos, análises, difusión e retroalimentación**.

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



Ciclo da intelixencia. Fonte: Elaboración propia (2026)

En entornos OT, este ciclo integra fontes especializadas —como telemetría de redes industriais, eventos de dispositivos de control, informes de fabricantes ou datos procedentes de honeypots ICS (sistemas trampa)— para producir intelixencia adaptada ao dominio físico. A iso súmase a importancia dun enfoque **proactivo**, indispensable en sistemas onde os tempos de resposta son máis longos e as interrupcións non son aceptables. Finalmente, o enfoque **centrado en ameazas** permite priorizar recursos en función dos adversarios máis plausibles para o sector industrial afectado, xa sexan grupos criminais orientados ao ransomware, actores estatais con capacidade para manipular procesos, ou campañas automatizadas que explotan vulnerabilidades OT a gran escala.

En conxunto, estes elementos permiten que a intelixencia e a contraintelixencia **fortalezan de forma decisiva a protección das operacións industriais**, axudando a reducir a incerteza, anticipar comportamentos hostís e tomar decisións informadas nun entorno onde a superficie de ataque crece e as consecuencias dun fallo poden ser físicas e severas.

3.1.2 Métodos de captación de intelixencia de ameazas

Nun programa maduro **de ciberintelixencia**, especialmente en entornos **ICS/OT**, a calidade da análise depende en gran medida de **como se obteñen os datos**. Non todas

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

as fontes achegan o mesmo tipo de valor: algunhas ofrecen volume e amplitude, outra profundidade e contexto, e outras, visibilidade técnica en tempo real. Entre os alicerces clásicos da obtención de información destacan tres disciplinas que se definen de seguido: **OSINT (Open Source Intelligence)**, **HUMINT (Human Intelligence)** e **SIGINT (Signals Intelligence)**.

Estas tres aproximacións non compiten entre si, senón que se **complementan**: OSINT achega unha visión ampla do entorno pública e clandestina, HUMINT incorpora a dimensión humana e de intencións, e SIGINT proporciona evidencias técnicas baseadas en sinais e tráfico de rede. Integradas no ciclo de intelixencia, permiten pasar de datos illados a **coñecemento estruturado** e accionable sobre ameazas que poden impactar tanto en infraestruturas IT como en sistemas de control industrial.

3.1.2.1 OSINT (Open Source Intelligence)

OSINT é, ante todo, unha disciplina que permite observar o entorno a través daquilo que este expón publicamente. En ciberseguridade defensiva, e especialmente en entornos industriais, a súa utilidade reside na capacidade de **identificar sinais temperáns de actividade maliciosa**, comprender a exposición real da organización e anticipar riscos sen recorrer a técnicas intrusivas. A partir de fontes abertas —páxinas web, bases de datos de vulnerabilidades, repositorios de código, redes sociais, foros ou espazos clandestinos accesibles— o analista pode construír unha visión ampla do panorama de ameazas, detectar infraestrutura sospeitosa e comprender como pode verse afectada a súa propia superficie de ataque.

No ámbito ICS/OT, OSINT permite descubrir se existen **dispositivos industriais expostos**, se se publicou recentemente unha vulnerabilidade crítica que afecte a PLCs ou sistemas SCADA, ou se grupos maliciosos comentan na dark web ferramentas ou exploits específicos para protocolos industriais. O seu valor radica na súa capacidade **de contextualizar** información dispersa e convertela en sinais útiles para a defensa. No entanto, esa amplitude tamén leva desafíos: a información pode ser incompleta, nesgada ou manipulada, e o volume de datos pode exceder a capacidade do analista se non se aplican criterios rigorosos de selección e validación.

Algunhas ferramentas que se usan tipicamente en OSINT son Maltego [4], Shodan [5] ou Spiderfoot [6]. Ademais, o uso de APIs e scripts personalizados permite integrar ferramentas OSINT con sistemas existentes, como os centros de operacións de seguridade (SOC), aumentando a súa eficacia ao xerar alertas en tempo real.

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

OSINT proporciona a **amplitude e perspectiva** necesarias para comprender o entorno de ameazas e anticiparse a elas, sempre que se complemente con fontes internas e con outros tipos de intelixencia.

3.1.2.2 HUMINT (Human Intelligence)

Se OSINT achega amplitude, **HUMINT** achega profundidade. A intelixencia humana introduce unha dimensión cualitativa que de cando en cando queda reflectida en rexistros automáticos: **intencións, motivacións, dinámicas sociais e comportamento humano**. En ciberseguridade —e de forma especialmente importante en sectores industriais— HUMINT permite identificar ameazas difíciles de detectar mediante mecanismos puramente técnicos, como **insiders**, persoal descontento ou terceiros con acceso privilexiado.

HUMINT aplícase tamén á observación de comunidades clandestinas, onde actores maliciosos comparten información sobre vulnerabilidades, accesos roubados ou campañas dirixidas. Estas interaccións poden revelar indicios sobre ataques en preparación, sectores industriais baixo interese ou ferramentas específicas para comprometer sistemas OT.

A diferenza de OSINT, HUMINT non se basea no que está dispoñible publicamente, senón no que pode extraerse mediante **interacción humana, observación encuberta ou análise social**. O uso de perfís ficticios ben deseñados, a observación de foros pechos ou a recompilación de percepcións internas xeran sinais que complementan os indicadores técnicos. No entanto, HUMINT require un marco ético e legal estrito: a protección de datos, a xustificación de actividades encubertas e a documentación de cada paso son compoñentes imprescindibles.

As metodoloxías de recompilación propias de HUMINT abarcan desde técnicas directas até aproximacións máis encubertas. Unha das máis habituais consiste en realizar **entrevistas e enquisas**, que permiten obter información de primeira man de persoas dentro ou fóra da organización, xa sexa para detectar percepcións de risco, identificar comportamentos anómalos ou comprender mellor o contexto operativo. A iso súmase a **observación de redes clandestinas**, como a dark web, foros de hacking ou mercados ilícitos, onde actores maliciosos comparten datos roubados, comentan vulnerabilidades ou preparan campañas dirixidas. Nos casos nos que é necesario profundar máis, pode recorrerse á **infiltración mediante perfís ficticios ou sock puppets**, creados

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

especificamente para interactuar de forma anónima con comunidades sospeitosas e validar hipóteses sen comprometer a identidade do analista.

Para apoiar este traballo, existen ferramentas que facilitan a documentación e o anonimato durante a investigación. **Hunchly** [7] resulta especialmente útil para rexistrar sistematicamente a actividade realizada en liña, conservando evidencias e trazabilidad do proceso; mentres que extensións como **Anonymox** [8] axudan a preservar o anonimato, algo esencial cando se opera en espazos onde unha exposición prematura pode implicar riscos operativos ou legais.

Ben executada, HUMINT responde a preguntas clave que non poden resolverse mediante datos técnicos: **quen podería atacar, por que o faría e que sinais humanos anticipan o seu comportamento**.

3.1.2.3 SIGINT (Signals Intelligence)

SIGINT completa a tríada achegando unha visión técnica directa sobre a actividade que ocorre en redes e sistemas. Baséase na **captura e análise de sinais electrónicos e comunicacións**, proporcionando evidencias do que realmente está a suceder no entorno operativo. En ciberseguridade moderna, e especialmente en redes ICS/OT, SIGINT é fundamental para detectar intrusións, identificar patróns anómalos e descubrir comportamentos que poderían anticipar un ataque.

Mediante a análise do tráfico de rede, os fluxos de comunicación e as interaccións entre dispositivos, SIGINT permite detectar **conexións non autorizadas cara a equipos de control**, variacións anómalas na frecuencia de comunicacións entre PLCs, intentos de escaneo sobre segmentos industriais ou comportamento propio de malware que utilice canles cifradas ou encubertas.

SIGINT ofrece unha lectura obxectiva: alí onde OSINT mostra contexto e HUMINT revela intención, SIGINT achega **evidencia técnica**. A súa eficacia aumenta cando se combina con estoutros enfoques. Un dominio detectado en foros clandestinos pode ser monitorizado mediante SIGINT para confirmar se está a se comunicar coa rede industrial; unha vulnerabilidade crítica identificada mediante OSINT pode correlacionarse con patróns inusuais de tráfico que indiquen intentos de explotación. Esta converxencia converte a información en intelixencia accionable, capaz de priorizar medidas defensivas con base en actividade real.

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

Dentro do ámbito da ciberintelixencia, **SIGINT** pode dividirse en dúas vertentes complementarias: **COMINT**, orientada á análise do contido e os metadatos das comunicacións —como correos electrónicos, mensaxería ou tráfico web—, e **ELINT**, centrada nos sinais emitidos por dispositivos electrónicos, desde puntos de acceso Wi-Fi até sistemas IoT ou equipamento industrial. Esta distinción permite comprender tanto a **intención** como as **capacidades técnicas** dos actores maliciosos, achegando unha visibilidade moi valiosa en contextos onde as comunicacións constitúen o principal indicador de actividade hostil.

Na súa aplicación defensiva, SIGINT baséase en técnicas como a análise continua do **tráfico de rede**, que permite identificar patróns anómalos, picos inesperados de actividade ou conexións cara a destinos sospeitosos, así como na **supervisión de comunicacións cifradas**, xa que mesmo sen acceder ao contido, cambios no seu volume, frecuencia ou destino poden delatar comportamentos maliciosos. Para iso, recórrese a un conxunto de ferramentas especializadas capaces de capturar e correlacionar sinais en tempo real.

Categoría	Ferramenta / Tecnoloxía	Descrición funcional
Sistemas IDS/IPS	Snort [9]	Sistema de detección e prevención de intrusións deseñado para identificar patróns de ataque coñecidos e comportamentos maliciosos en tempo real.
Sistemas IDS/IPS	Suricata [10]	Motor IDS/IPS de alto rendemento que permite a detección de intrusións, análise de protocolos e identificación de ameazas avanzadas en redes de alta velocidade.
Análise de tráfico de rede	Wireshark [11]	Analizador de protocolos que ofrece unha visión detallada do tráfico de rede, permitindo inspeccionar paquetes e analizar o comportamento das comunicacións.
Análise de tráfico de rede	Zeek [12]	Plataforma de monitorización e análise de tráfico orientada á detección de comportamentos anómalos e á obtención de intelixencia de rede.

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

Análise de fluxos e datos retrospectivos	Arkime [13]	Plataforma de captura e indexación de tráfico que permite reconstruír sesións e analizar actividades sospeitosas de forma retrospectiva.
Análise de fluxos de rede	NetFlow [14]	Tecnoloxía de recollida e análise de fluxos de tráfico que facilita a visibilidade do uso da rede e a detección de patróns anómalos.
Análise de fluxos de rede	sFlow [15]	Tecnoloxía de mostraxe de paquetes e fluxos que permite a monitorización escalable do tráfico e a análise de tendencias de rede.

Tecnoloxías de SIGINT. Fonte: Elaboración propia (2026)

Combinadas, estas capacidades proporcionan aos equipos defensivos unha visión granular do comportamento da rede e facilitan a **detección temperá de ameazas**, especialmente en entornos sensibles ou altamente segmentados.

En conxunto, OSINT, HUMINT e SIGINT proporcionan unha visión **complementaria e coherente** do panorama de ameazas. A súa integración permite entender **que ocorre, quen podería estar detrás e como se manifesta tecnicamente**, ofrecendo unha base sólida para a defensa de infraestruturas industriais e sistemas de control.

3.1.3 Niveis de intelixencia

A **ciberintelixencia** constitúe unha capacidade esencial para calquera organización que aspire a anticiparse ás ameazas, comprender a natureza dos seus riscos e adoptar decisións fundamentadas para protexer os seus activos, especialmente en entornos onde a continuidade operativa é crítica, como os **ICS/OT**.

Para achegar valor real, a intelixencia debe estruturarse en distintos niveis que responden a horizontes temporais e necesidades diferentes. De maneira xeral, distínguense tres dimensións complementarias: a **ciberintelixencia estratéxica**, a **operativa** e a **táctica**. A súa combinación permite obter unha visión integral do panorama de ameazas e dispor de mecanismos eficaces tanto para previr como para responder ante incidentes.

- A **ciberintelixencia estratéxica** ofrece unha visión global e a longo prazo do ecosistema de ameazas. Está orientada á alta dirección e aos responsables de definir políticas, xa que axuda a comprender que actores representan un risco significativo, como evolucionan as súas capacidades e que tendencias

tecnolóxicas poden modificar o entorno de ameaza no futuro. Este nivel permite identificar, por exemplo, o interese crecente **de APT apoiadas por Estados** en sectores como enerxía, transporte ou manufactura avanzada, así como avaliar cambios en motivacións, obxectivos e patróns de actividade. Nun informe estratéxico, non se busca o detalle técnico, senón a **lectura contextual** que permite orientar investimentos, priorizar capacidades defensivas e axustar a estratexia xeral de ciberseguridade.

- A **ciberintelixencia operativa** actúa nun horizonte temporal intermedio e céntrase en ameazas, campañas e vulnerabilidades concretas que poden afectar á organización en semanas ou meses. O seu propósito é apoiar os equipos que protexen infraestruturas críticas, ofrecendo información suficientemente detallada como para anticipar riscos e preparar defensas, pero sen chegar ao nivel granular da intelixencia táctica. Neste ámbito analízanse, por exemplo, campañas de phishing dirixidas a persoal clave, a explotación activa dunha vulnerabilidade nun produto amplamente despregado no sector ou a actividade coordinada dun grupo criminal contra unha rexión ou industria específica. A intelixencia operativa permite comprender **que está a ocorrer agora mesmo**, quen está detrás e con que capacidades, proporcionando así un marco para priorizar medidas de mitigación.

- Por último, a **ciberintelixencia táctica** opera no nivel máis próximo á execución e está dirixida aos equipos operativos: analistas de SOC, persoal de resposta a incidentes ou responsables de detección. A súa finalidade é ofrecer información **altamente procesable e inmediata**, como **indicadores de compromiso (IoCs)**, direccións IP ou dominios maliciosos, **hashes**, sinaturas de malware ou descricións detalladas de **tácticas, técnicas e procedementos (TTPs)** utilizados por un adversario. Un produto de intelixencia táctica pode detallar, por exemplo, o comportamento dunha variante de malware, como se propaga, que artefactos deixa no sistema e que evidencias poden utilizarse para detectalo ou contelo. Este nivel é indispensable para mellorar regras de correlación, enriquecer alertas e responder máis rapidamente a incidentes en curso.

En conxunto, os tres niveis aseguran que a intelixencia non só describa o panorama de ameazas, senón que permita **actuar** de maneira informada en cada capa da organización, desde a estratexia até a operación diaria.

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

3.1.4 Fontes

A xeración **de ciberintelixencia útil** require apoiarse nun conxunto diverso de fontes que acheguen profundidade, actualidade e fiabilidade. Estas fontes non son homoxéneas: cada unha ofrece unha perspectiva distinta do entorno de ameazas e resulta máis axeitada para certos niveis de intelixencia —estratéxico, operativo ou táctico—. Para obter análises sólidas e accionables, é necesario combinar información procedente **de feeds comerciais**, **comunidades de intercambio**, **organismos gobernamentais**, **entornos clandestinos** e **telemetría interna**.

- Os **feeds comerciais** proporcionan intelixencia altamente estruturada, actualizada e xeralmente enriquecida con análises técnicas ou contextuais realizados por equipos especializados. Solucións como **Recorded Future** [16], que correlaciona datos orixinados en OSINT, SIGINT e múltiples repositorios globais, ou os informes **de FireEye Threat Intelligence** [17], baseados en investigacións propias e en observacións de incidentes reais, permiten ás organizacións dispor de visibilidade avanzada sobre campañas emerxentes, actividade de actores sofisticados e vulnerabilidades explotadas activamente. Este tipo de fontes destaca pola súa capacidade para acelerar a toma de decisións grazas á súa profundidade analítica e á calidade dos seus modelos de risco.

- Paralelamente, as **fontes comunitarias** fomentan a colaboración entre organizacións e equipos de seguridade, proporcionando un espazo aberto onde compartir indicadores, tácticas observadas e experiencias comúns. Plataformas como **AlienVault OTX** [18], que permite intercambiar IoCs e análises sobre ameazas, ou **MISP** [19], deseñada para estruturar e compartir información de forma estandarizada, son especialmente valiosas para aumentar a velocidade de detección e fortalecer a resposta ante incidentes, xa que ofrecen intelixencia baseada en contribucións reais da comunidade.

- As **fontes gobernamentais e de infraestruturas críticas** constitúen outro alicerce fundamental, especialmente en sectores industriais. Organismos como **CISA** (Axencia de Ciberseguridade e Seguridade de Infraestruturas) [20] en Estados Unidos ou **ENISA** (Axencia da UE para a CIberseguridade) [21] en Europa publican avisos, guías de mitigación, análises sectoriais e estudos específicos sobre infraestruturas críticas. Estas publicacións resultan

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

imprescindibles para comprender ameazas que afectan a sectores concretos —enerxía, transporte, auga, manufactura— e para manter aliñados os programas de seguridade coas recomendacións oficiais e a normativa vixente.

- No extremo menos visible do espectro atópanse as **fontes clandestinas**, que permiten acceder a información procedente de entornos onde operan actores maliciosos. Foros da dark web, mercados ilegais e canles privadas cifrados son espazos onde se discuten vulnerabilidades recentemente descubertas, comercialízanse accesos comprometidos, anúncianse campañas en preparación ou se intercambian ferramentas ofensivas. Aínda que o seu acceso e monitorización requiren precaucións éticas, legais e operativas, estas fontes proporcionan sinais críticos para anticipar actividades que aínda non emerxeron en canles públicas.

- Finalmente, as **fontes internas** representan a perspectiva máis directa e específica sobre o entorno tecnolóxica propio. Inclúen **logs de sistemas e redes**, telemetría procedente de solucións SIEM (monitorización), **alertas de seguridade** xeradas polo SOC, resultados de **probas de penetración** e auditorías, así como IoCs detectados dentro da organización. Esta información reflicte de maneira inmediata a actividade real que impacta sobre a infraestrutura, facilitando a detección temperá de anomalías e a validación de ameazas identificadas por fontes externas. En entornos ICS/OT, a telemetría interna —incluíndo tráfico de rede industrial, eventos de control ou anomalías operativas— convértese nunha peza esencial para contextualizar calquera sinal procedente do exterior.

En conxunto, a combinación destas fontes permite á organización construír unha visión equilibrada do panorama de ameazas: desde a actividade global até os detalles que afectan directamente á súa infraestrutura. A integración de fontes externas e internas é a base para producir intelixencia **fiable, accionable e adaptada ao contexto operativo**.

3.1.5 Xeración de intelixencia procesable

A xeración de **intelixencia procesable** constitúe o núcleo do traballo de ciberintelixencia, xa que o seu valor real non reside unicamente en recompilar datos,

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

senón como se indicou, en transformalos en **coñecemento útil** capaz de mellorar de maneira tanxible a postura de seguridade da organización.

Este proceso comeza coa transición *do dato ao coñecemento*. A información bruta procedente de múltiples fontes —internas, comunitarias, comerciais ou clandestinas— debe analizarse, filtrarse e priorizarse para distinguir aquilo que resulta verdadeiramente relevante do ruído contextual. Esta priorización depende tanto da **criticidade dos activos afectados**, como da **probabilidade de explotación** e da **capacidade demostrada polos adversarios**. Así, unha vulnerabilidade que impacta directamente nun sistema de control industrial operativo terá unha prioridade moito maior que outra que afecte a un compoñente periférico ou pouco utilizado, xerando mesmo **alertas inmediatas** cando o risco é significativo.

Da información bruta ao coñecemento accionable. Fonte: Elaboración propia (2026)

O proceso de análise enriquécese mediante o uso de **matrices e frameworks** que permiten estruturar, contextualizar e normalizar a información dispoñible. Entre eles, destaca especialmente **MITRE ATT&CK** [22] **e MITRE ATT&CK ICS** [23], convertido nunha linguaxe común para describir as tácticas e técnicas utilizadas polos adversarios. Este marco facilita comprender como operan os atacantes, que fases da cadea de intrusión utilizan e en que puntos concretos podería reforzarse a defensa. Cando un analista identifica, por exemplo, que un actor coñecido emprega técnicas específicas de **movemento lateral**, pode mapearlas no marco ATT&CK e reforzar controis nesas áreas antes de que a intrusión chegue a producirse. Desta forma, a intelixencia deixa de ser un simple exercicio descritivo para converterse nun **instrumento anticipatorio e operativo**, capaz de guiar decisións técnicas e estratéxicas con impacto directo na protección da organización.

3.1.6 Contraintelixencia

A **contraintelixencia** desempeña un papel fundamental dentro da seguridade dunha organización, xa que o seu propósito é **identificar, neutralizar e previr actividades maliciosas** que poidan comprometer activos críticos, información sensible ou

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

operacións esenciais. No ámbito da ciberseguridade, esta disciplina abarca tanto ameazas internas como externas e oriéntase non só a responder a incidentes, senón a **anticipar as tácticas dos adversarios**, dificultar as súas accións e reducir a súa capacidade real de causar dano. En entornos industriais e de control, onde a manipulación ou interrupción de procesos pode derivar en consecuencias operativas significativas, a contraintelixencia convértese nun compoñente indispensable do modelo defensivo.

A **contraintelixencia defensiva** apóiase en dous principios fundamentais.

- O primeiro é a **detección de espionaxe e actividades maliciosas dirixidas**, un aspecto crave nun escenario onde conviven cibercriminais, grupos con motivacións económicas, competidores desleais ou mesmo actores apoiados por Estados. A identificación temperá de sinais de espionaxe industrial, intentos de infiltración ou accesos anómalos resulta esencial para anticipar situacións comprometedoras antes de que se materialicen.

- O segundo principio é a **protección de datos sensibles e operativos**, xa que a información crítica segue sendo un dos obxectivos prioritarios de calquera adversario. A contraintelixencia desprega controis específicos para salvagardar estes datos, desde a clasificación e etiquetaxe segundo niveis de sensibilidade até a segmentación de redes ou a aplicación de cifrado para minimizar o acceso non autorizado.

Para levar a cabo estas funcións, a contraintelixencia emprega un conxunto amplo de técnicas e ferramentas.

Unha das áreas máis relevantes é a **supervisión de empregados e accesos internos**, orientada a detectar comportamentos potencialmente anómalos que poidan indicar un risco *de* insider threat (adversario procedente de dentro da organización).

A disciplina tamén inclúe a **análise de anomalías en redes e infraestruturas**, mediante técnicas capaces de detectar comportamentos que se desvían da norma, como intentos de movemento lateral, transferencias de datos non autorizadas ou tráfico inusual entre segmentos críticos.

Outra técnica clave é o uso **de honeypots e honeynets**, sistemas deseñados deliberadamente para atraer aos atacantes e estudar o seu comportamento. Estas

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

infraestruturas cebo permiten comprender as **tácticas, técnicas e procedementos (TTPs)** dos adversarios e anticipar posibles ataques contra a rede real.

A contraintelixencia abarca tamén a **avaliación de ameazas internas e externas**, adoptando modelos que clasifican aos insiders segundo o seu acceso, intencións e capacidades.

Por último, un elemento esencial é a **protección fronte ao spear phishing e a enxeñaría social** (basados en enganar ás persoas), xa que estes vectores adoitan ser utilizados como porta de entrada na zona IT das plantas produtivas, para comprometer procesos críticos ou acceder a información sensible. A combinación de análise automatizado, filtrado avanzado e formación de empregados resulta crítica para reducir este risco.

3.1.7 Implementación dun programa de intelixencia

A creación dun **programa sólido de intelixencia e contraintelixencia** constitúe un elemento esencial para que as organizacións poidan anticiparse ás ameazas, protexer os seus activos críticos e responder con eficacia a incidentes de ciberseguridade. Este tipo de programas combina procesos maduros, ferramentas especializadas e recursos humanos calificados co obxectivo de **recompilar, analizar e aplicar intelixencia de forma sistemática**. O seu implementación esixe unha planificación estratéxica axeitada, unha integración estreita con operacións crave —especialmente co **Security Operations Center (SOC)**— e unha avaliación continua mediante métricas que permitan medir o seu impacto real na postura defensiva.

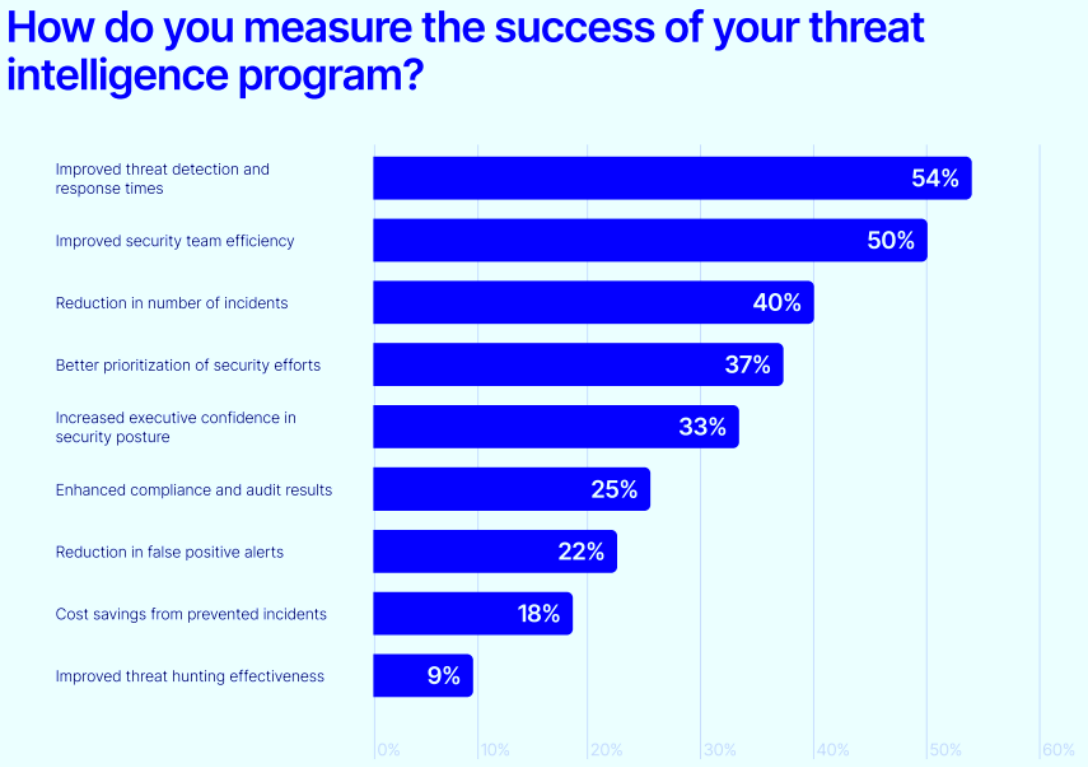
- O punto de partida é unha **planificación clara do programa**, aliñada coas necesidades específicas da organización e coas particularidades da súa infraestrutura tecnolóxica, o seu sector e o seu nivel de exposición. Nesta fase resulta fundamental definir **obxectivos de intelixencia** concretos, orientados a responder a preguntas operativas e estratéxicas: desde previr ataques dirixidos ou identificar actores relevantes, até protexer activos especialmente sensibles. Unha vez establecidas estas metas, deséñase un **ciclo de intelixencia adaptado**, que articula a planificación, a recompilación de datos, a análise, a difusión e a retroalimentación continua. Este enfoque personalizado permite integrar fontes OSINT, telemetría interna e indicadores técnicos para xerar produtos de intelixencia accionables que poidan empregarse inmediatamente polos equipos defensivos.

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

- Para maximizar a súa eficacia, o programa debe integrarse de forma natural no **SOC**, onde a intelixencia se converte nun motor para a detección e a resposta. A creación de **equipos especializados en Threat Intelligence** dentro do SOC permite dispor de analistas dedicados a monitorizar a evolución de actores e campañas, procesar grandes volumes de datos e xerar informes operativos que guíen decisións en tempo real. Cando, por exemplo, un grupo APT adopta unha nova técnica de movemento lateral, estes analistas poden alertar inmediatamente ao SOC para reforzar as capacidades de detección e axustar as políticas de seguridade. Esta integración vese reforzada polo uso **de Threat Intelligence Platforms (TIPs)**, ferramentas deseñadas para centralizar e correlacionar información procedente de múltiples fontes. Plataformas como **Anomali ThreatStream** [24] ou **ThreatConnect** [25] facilitan a xestión de datos complexos, a automatización de fluxos de análises e a distribución rápida de intelixencia procesable a outros equipos, permitindo actuar antes de que unha ameaza chegue a materializarse.

- A última dimensión do programa está relacionada coa **avaliación da súa desempeño**. Medir de forma obxectiva a eficacia da intelixencia e a contraintelixencia é esencial tanto para xustificar investimentos como para identificar áreas de mellora. Para iso utilízanse **indicadores clave de desempeño (KPIs)**, que poden incluír o número de ameazas detectadas antes de converterse en incidentes, a redución do tempo de resposta, a cantidade de IoCs relevantes incorporados aos sistemas de detección ou a diminución de falsos positivos. Non menos importante é avaliar o **impacto real da intelixencia na redución de incidentes**, analizando cantos ataques foron previdos grazas a información anticipada ou como a intelixencia contribuíu a mitigar de maneira temperá intentos de explotación detectados na rede corporativa, como se ve na figura. Isto axudará a xustificar o retorno do investimento (ROI) neste tipo de programas, como se veu no entregable *Informe de Ciberalertas - I* deste mesmo Observatorio [43].

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



Enquisa State of Threat Intelligence. Fonte: Recorded Future (2025)

3.1.8 Aspectos ético-legais da intelixencia de ameazas

A implementación de **programas de intelixencia e contraintelixencia** non pode entenderse unicamente como un esforzo técnico orientado a protexer activos e anticipar ameazas. Tamén require operar dentro dun **marco ético e legal sólido**, que garanta o respecto á privacidade e aos dereitos fundamentais das persoas. As organizacións que recompilan, analizan e utilizan información para sustentar as súas capacidades defensivas deben coñecer en profundidade as normativas aplicables e ser conscientes dos límites éticos inherentes a estas actividades. A falta de cumprimento ou o uso inapropiado de datos non só pode derivar en sancións regulatorias severas, senón tamén nun dano reputacional significativo que comprometa a confianza de clientes, socios e empregados.

O **cumprimento normativo** constitúe así un requisito esencial. Moitas actividades de intelixencia levan o acceso a datos persoais, e o seu tratamento debe ser sempre transparente, responsable e conforme ás leis vixentes. No contexto europeo destaca o **Regulamento Xeral de Protección de Datos (GDPR)** [26], que establece directrices estritas sobre a recompilación, almacenamento e uso de información persoal. Complementariamente, a **Directiva ePrivacy** [27] regula aspectos vinculados ás comunicacións electrónicas, incluíndo a monitorización do tráfico de rede, algo moi

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

relevante para actividades como SIGINT. A estas normas súmanse lexislacións locais —como a **CCPA** [28] en California ou a Lei de Protección de Datos Persoais nalgunhas xurisdicións latinoamericanas— que amplían o marco legal de referencia. Para garantir o cumprimento, as organizacións deben realizar **auditorías periódicas** que verifiquen que as prácticas de intelixencia respectan as obrigacións regulatorias en todas as rexións onde operan.

Máis aló do marco legal, existe un compoñente imprescindible: o **tratamento ético dos datos persoais e confidenciais**. A minimización de datos —recompilar unicamente a información estritamente necesaria—, o consentimento informado cando sexa aplicable e a aplicación de medidas robustas de protección son elementos esenciais para reducir riscos e garantir un uso responsable da información. Na práctica, isto implica adoptar principios **de anonimización e pseudonimización**, especialmente cando se traballa con datos obtidos a través de OSINT ou de telemetría interna. O obxectivo non é só cumprir coa normativa, senón demostrar un compromiso ético co manexo de datos sensibles.

A ciberintelixencia expón tamén **dilemas éticos** que requiren reflexión e políticas claras. Un dos máis relevantes é o equilibrio entre **seguridade e privacidade**. A monitorización de comunicacións, a observación do comportamento dixital ou o uso de ferramentas avanzadas para previr fugas de información poden entrar en conflito co dereito á privacidade de empregados ou usuarios. Resolver este dilema esixe **transparencia**, **proporcionalidade** e **limitación do alcance** das medidas adoptadas, asegurando que se utilicen unicamente para as fins lexítimas de protección e que estean claramente documentadas nas políticas internas.

Outro dilema importante preséntase ao redor dos **límites da interacción con actores maliciosos**. Actividades como a infiltración en foros clandestinos, a creación de perfís ficticios ou a análise de ferramentas adquiridas en mercados ilícitos son prácticas lexítimas dentro de certos marcos, pero requiren valorar coidadosamente que comportamentos resultan aceptables e cales poderían traspasar liñas legais ou morais. A observación pasiva pode ser apropiada nalgúns casos, mentres que a participación activa podería supor riscos éticos considerables. Por iso, é imprescindible establecer **directrices claras** sobre que accións están permitidas, baixo que condicións e con que controis internos, asegurando que a actividade de intelixencia nunca derive en prácticas cuestionables.

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

3.2 Panorama actual

O restante deste bloque de **intelixencia de ameazas,** ofrece unha visión estruturada e multidimensional do panorama actual, apoiándose nun conxunto amplo e heteroxéneo de fontes nacionais e internacionais. Antes de afondar nas seccións específicas, vemos necesario contextualizar tres consideracións fundamentais que condicionan a lectura e interpretación dos contidos.

En primeiro lugar, a maior parte dos informes de referencia —procedentes de organismos gobernamentais, CERTs nacionais, entidades supranacionais, empresas globais de ciberseguridade ou centros de investigación— **non diferenzan estritamente entre ámbitos IT, OT ou ICS** nas súas análises de ameazas. Este enfoque, lonxe de ser unha carencia, resulta especialmente útil nun escenario tecnolóxico no que a **converxencia IT/OT** e a progresiva integración de sistemas propia da **Industria 4.0 e 5.0** teñen difuminado as fronteiras tradicionais. A interpretación conxunta destas fontes permite comprender mellor a continuidade entre os vectores de ameaza que afectan a ambos os dominios.

En segundo lugar, buscouse deliberadamente **unha perspectiva ampla**, integrando fontes con metodoloxías, ámbitos xeográficos, tamaños mostrais ou perfís de cliente e taxonomías de incidentes moi diversas. Este enfoque enriquece a análise pero introduce factores de confusión e rumbos que implican necesariamente que **algunhas estatísticas poidan diferir** ou mesmo resultar parcialmente contraditorias entre si. É un reflexo natural da realidade: os ecosistemas de ameaza non impactan de igual forma en **Europa, nos Estados Unidos ou en Asia**, nin todos os sectores industriais presentan a mesma exposición, nin os diferentes fabricantes teñen presenza homoxénea en todo o globo. Esta diversidade de datos preséntase de forma transparente, pois contribúe a unha visión máis completa do panorama.

Por último, as **recomendacións operativas e estratéxicas** incluirán tanto as directrices consolidadas dos grandes provedores globais —derivadas dos seus informes anuais de intelixencia— como materiais específicos para **entornos industriais**, sustentados en bibliografía técnica, normativa e estudos centrados en OT/ICS. Debido ao carácter coral das fontes empregadas, pode existir certo solapamiento entre medidas suxeridas por distintas organizacións, con algúns matices. Optouse por **mantelas na súa totalidade** para ofrecer ao lector un abanico o máis amplo posible de achados e prácticas relevantes, e facilitar así a súa aplicación en ambientes industriais variados.

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

Este conxunto de precisións serve de marco interpretativo para as seccións que seguen do bloque 3, orientadas a proporcionar unha análise de utilidade directa para a protección do tecido empresarial e institucional en Galicia.

3.2.1 Análise global

A análise global da ameaza en entornos industriais e tecnolóxicas durante 2024–2025 evidencia un escenario caracterizado pola **converxencia entre actores cada vez máis sofisticados**, a **aceleración de tácticas criminais como o ransomware (bloqueo e secuestro de datos)** e unha **deterioración progresiva (incremento) da superficie de exposición industrial**, debido á crecente interdependencia tecnolóxica. Os achados procedentes de organismos internacionais e estudos sectoriais coinciden en describir un ecosistema onde a presión operativa sobre infraestruturas críticas continúa aumentando, tanto por motivos económicos como xeopolíticos.

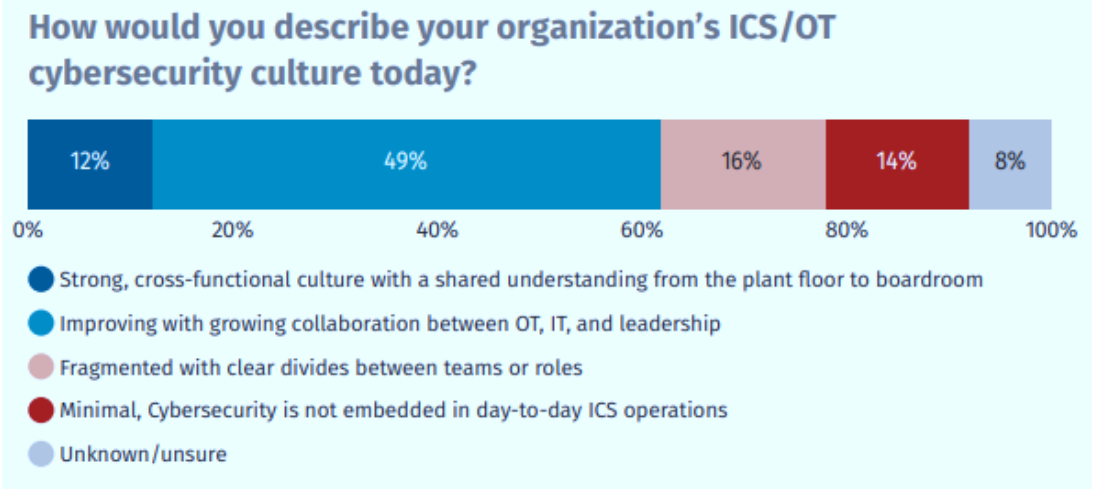
O informe **SANS *State of ICS/OT Security 2025*** [29] ofrece unha panorámica ampla do estado real da ciberseguridade industrial a partir dunha **enquisa global con máis dun milleiro de profesionais OT/ICS**, procedentes de sectores como **enerxía, manufactura, auga, transporte, químico e sanitario**, así como de múltiples rexións con forte representación **de Norteamérica e Europa**. Esta diversidade permite capturar unha visión comparada sobre madurez, prioridades e carencias estruturais na protección de infraestruturas industriais.

Os **principais achados** recompilados na fase inicial do informe revelan tendencias consistentes:

- **O 22** % **das organizacións** sufriu polo menos un incidente de ciberseguridade no último ano, e **o 40** % deles xerou interrupcións operativas, subliñando o impacto directo na continuidade do negocio. Aínda que **case a metade** dos incidentes detéctase en menos de 24 h e **o 60** % contense en 48 h, os tempos **de remediación** continúan sendo elevados, prolongándose a días ou mesmo semanas, o que evidencia unha eiva relevante entre detección e recuperación.
- O **acceso remoto non autorizado** continúa sendo o principal vector de intrusión, seguido pola **enxeñaría social** e a ausencia de controis específicos orientados a entornos OT.
- O investimento previsto reforza estas prioridades: **visibilidade de activos**, **detección de ameazas ICS-aware** e **acceso remoto seguro** encabezan tanto os despregamentos de 2025, como as planificacións a dous anos vista (2027).

Con todo, máis aló dos aspectos técnicos, o informe volve pór o foco no **factor cultural**, probablemente o elemento menos resolto na defensa dos sistemas industriais. Só **o 14 % das organizacións** considera estar *plenamente preparada* para afrontar ameazas OT/ICS, o que mostra unha distancia significativa entre a percepción de risco e as capacidades reais. Ademais, SANS identifica unha tendencia clara: aquelas organizacións que senten plenamente preparadas **integran a técnicos de planta e operadores en exercicios e simulacros** cunha probabilidade **un 66% maior** que o resto, confirmando que a madurez non depende unicamente de tecnoloxía, senón da aliñación entre equipos, procesos e responsabilidades.

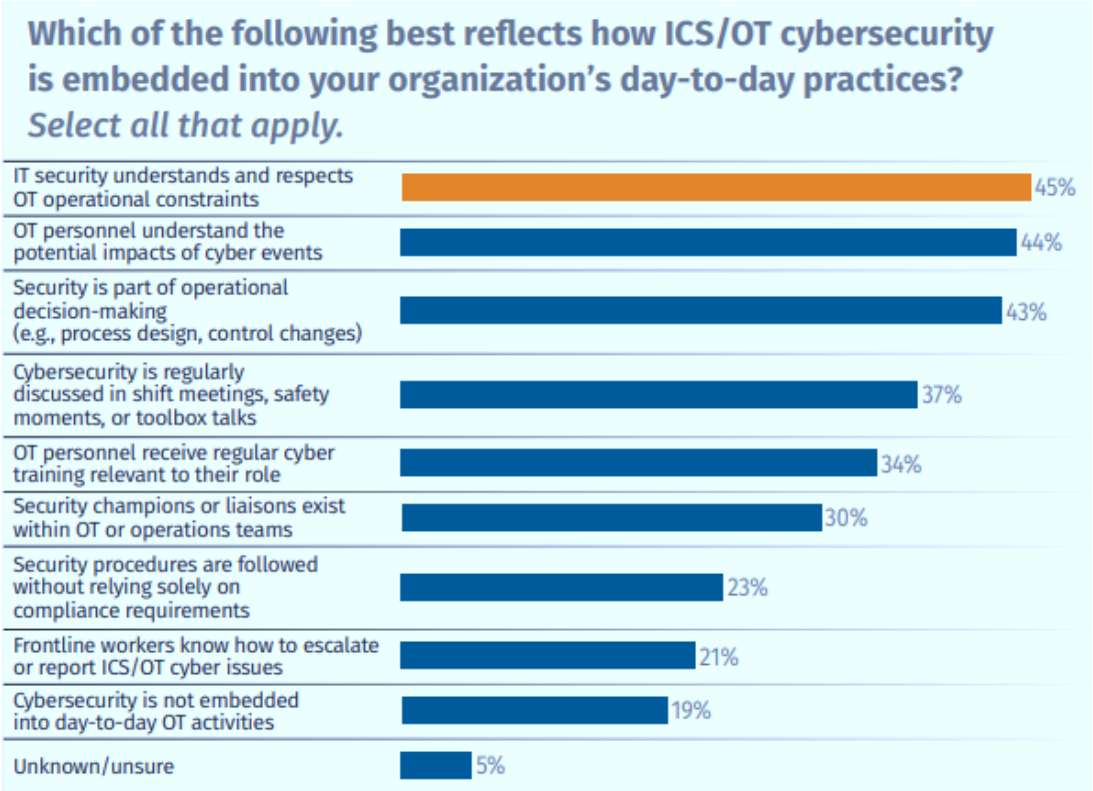
Este desfasamento cultural reflíctese de forma visual na seguinte figura, que mostra a persistente desconexión entre áreas **TI** e **OT** na percepción do risco e a priorización de medidas.



Cultura IT, OT e liderado. Fonte: SANS (2025)

Á súa vez, o seguinte gráfico ilustra outro síntoma crave: **só un terzo** das organizacións **logrou integrar a ciberseguridade de maneira efectiva dentro das operacións OT**, o que evidencia que a converxencia técnica non sempre se acompaña dunha converxencia organizativa axeitada.

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

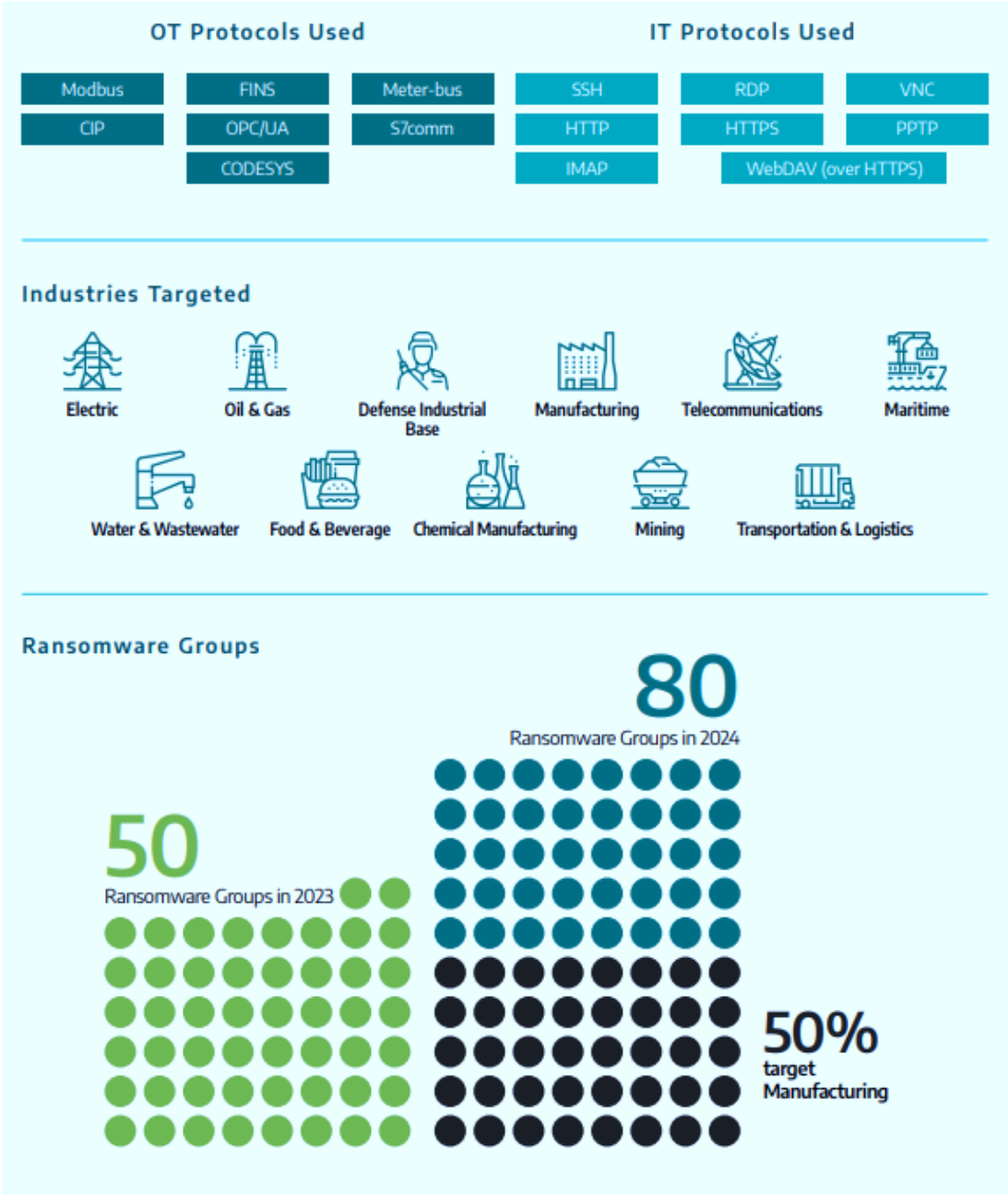


Ciberseguridade OT/ICS como parte da actividade diaria. Fonte: SANS (2025)

O informe **Dragos *OT Cybersecurity Report – Year in Review 2025*** [30] constitúe unha das fontes máis completas e especializadas sobre **ameazas e compromisos en entornos OT/ICS**, diferenciándose dos informes xeneralistas ao centrarse exclusivamente en actividade adversaria con impacto real ou potencial sobre procesos industriais, infraestruturas críticas e sistemas de control.

Desde o inicio do documento, Dragos recompila varios **achados crave**, como o número total *de* threat groups monitorizados (falaremos de actores e campañas en profundidade en informes vindeiros), a proporción de vulnerabilidades que afectan á operación, a porcentaxe de advisories con erros críticos ou sen mitigación, e a distribución de vectores de acceso máis frecuentes. Estes indicadores ofrecen un marco visual sólido para contextualizar o estado da ameaza OT/ICS. A continuación, outros relevantes relativos a protocolos máis vistos, sectores atacados, e grupos de ransomware detectados.

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



Estatísticos relevantes do informe Year Review. Dragos (2025)

En canto ás **tendencias xerais**, Dragos identifica tres vectores estratéxicos que explican a evolución das ameazas en 2024–2025:

1. O aumento de **operacións de guerra híbrida con orientación OT**, especialmente durante períodos de tensión xeopolítica.
2. Un progreso defensivo **incremental, mais desigual**, con sectores moi maduros convivindo con outros que manteñen brechas estruturais.

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

3. A consolidación de campañas adversarias menos orientadas á sofisticación técnica e máis á **amplificación do impacto operativo**, aproveitando erros de configuración, accesos remotos inseguros e exposición innecesaria de activos.

Desde a perspectiva operacional, o informe dedica unha análise profunda a como o **malware específico para ICS** converteuse nunha ferramenta crave en campañas motivadas por conflitos. Para a **definición formal de ICS malware**. Dragos establece tres propiedades esenciais:

- que o software sexa **ICS-capable**, é dicir, poida interactuar con protocolos, dispositivos ou lóxicas de control;
- que estea **deseñado con intención maliciosa**, non como ferramenta de proba ou investigación;
- e que posúa a **capacidade de xerar efectos adversos nun entorno OT**, desde perda de visión até perda de control ou manipulación do proceso. Esta conceptualización permite diferenciar o malware verdadeiramente orientado a industrias críticas daquel que simplemente "acada" sistemas OT como dano colateral desde redes TI.

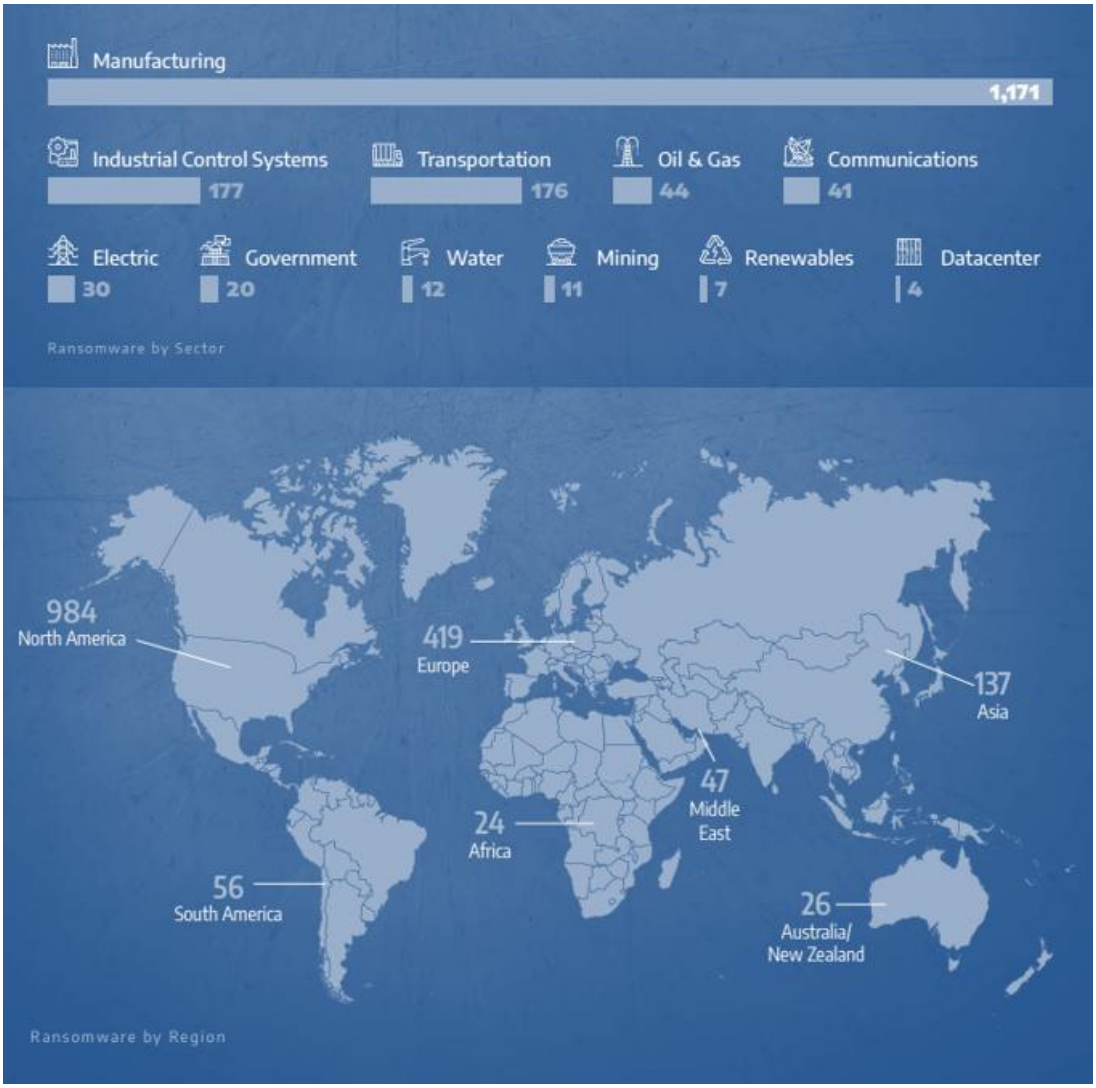
Documéntanse varios casos recentes nos que malware orientado a OT —e non simplemente a entornos corporativas— utilizouse para degradar sensores, interromper operacións ou preparar escenarios para sabotaxe, destacando que o seu emprego se está normalizando en contextos bélicos e operacións híbridas. Este fenómeno confirma que a fronteira entre intrusión estratéxica e efectos físicos está a reducirse.

O informe tamén documenta o **resurgimiento do hacktivismo** con impacto potencial en OT. Dragos sinala que numerosos grupos ideolóxicos aproveitaron 2023–2024 para reivindicar ataques contra infraestruturas críticas; aínda que a maioría carece de capacidades avanzadas, o seu volume, a súa visibilidade pública e a proliferación de ferramentas de acceso aberto incrementan a probabilidade de impactos non intencionados sobre sistemas industriais.

Finalmente, a sección dedicada a **ransomware** describe como esta ameaza continúa sendo o vector disruptivo predominante para organizacións industriais, cun **incremento notable nas campañas dirixidas e nas técnicas de dobre extorsión** (pago por desciframento e non divulgación). Dragos subliña que moitos incidentes OT teñen orixe en compromisos iniciais TI, pero acaban afectando á produción debido á interconectividade e á dependencia de servizos corporativos críticos.

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

Esta sección do informe inclúe varias gráficas de especial interese, que ilustran de forma directa o impacto de ransomware en industrias OT (non en balde era o cuarto escenario das actividades de Continuidade de Negocio e Resposta a Incidentes segundo o informe de SANS) [29]:



Ataques de ransomware por sector industrial e rexión. Dragos (2025)

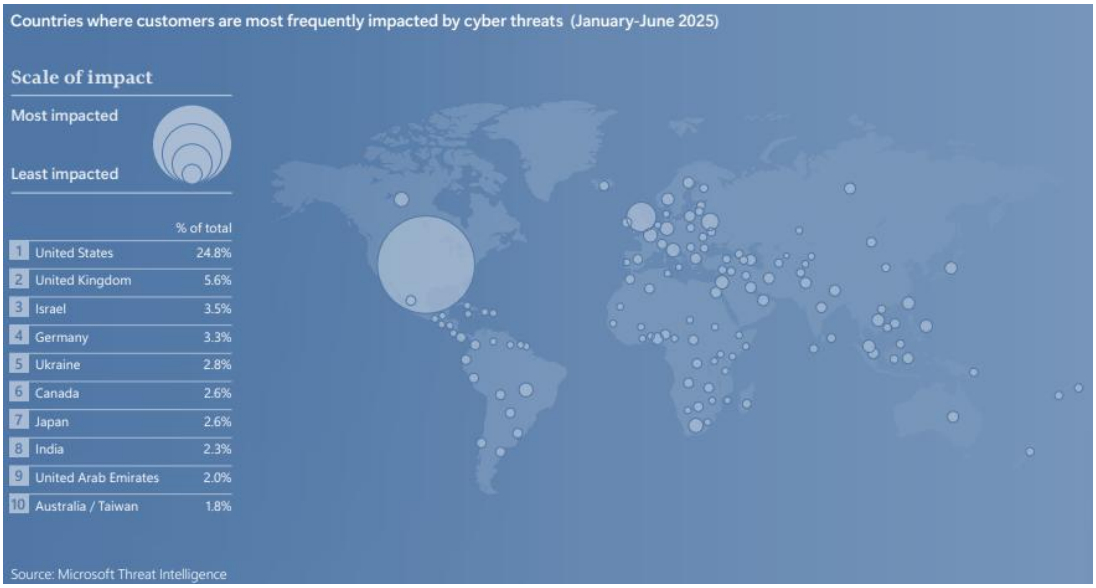
O *Microsoft Digital Defense Report 2025* [31], baseado na inmensa visibilidade que proporciona a súa posición dominante en sistemas Windows, servizos na nube e plataformas de produtividade, presenta datos correspondentes ao seu ano fiscal, que remata o 30 de xuño de 2025, o que permite observar tendencias moi recentes en actividade adversaria global. Aínda que se trata dun informe xeneralista —non centrado en OT— resulta relevante para comprender a evolución dos métodos de intrusión que tamén rematan impactando nas redes industriais.

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

Sintetizan catro grandes **ideas fundamentais**:

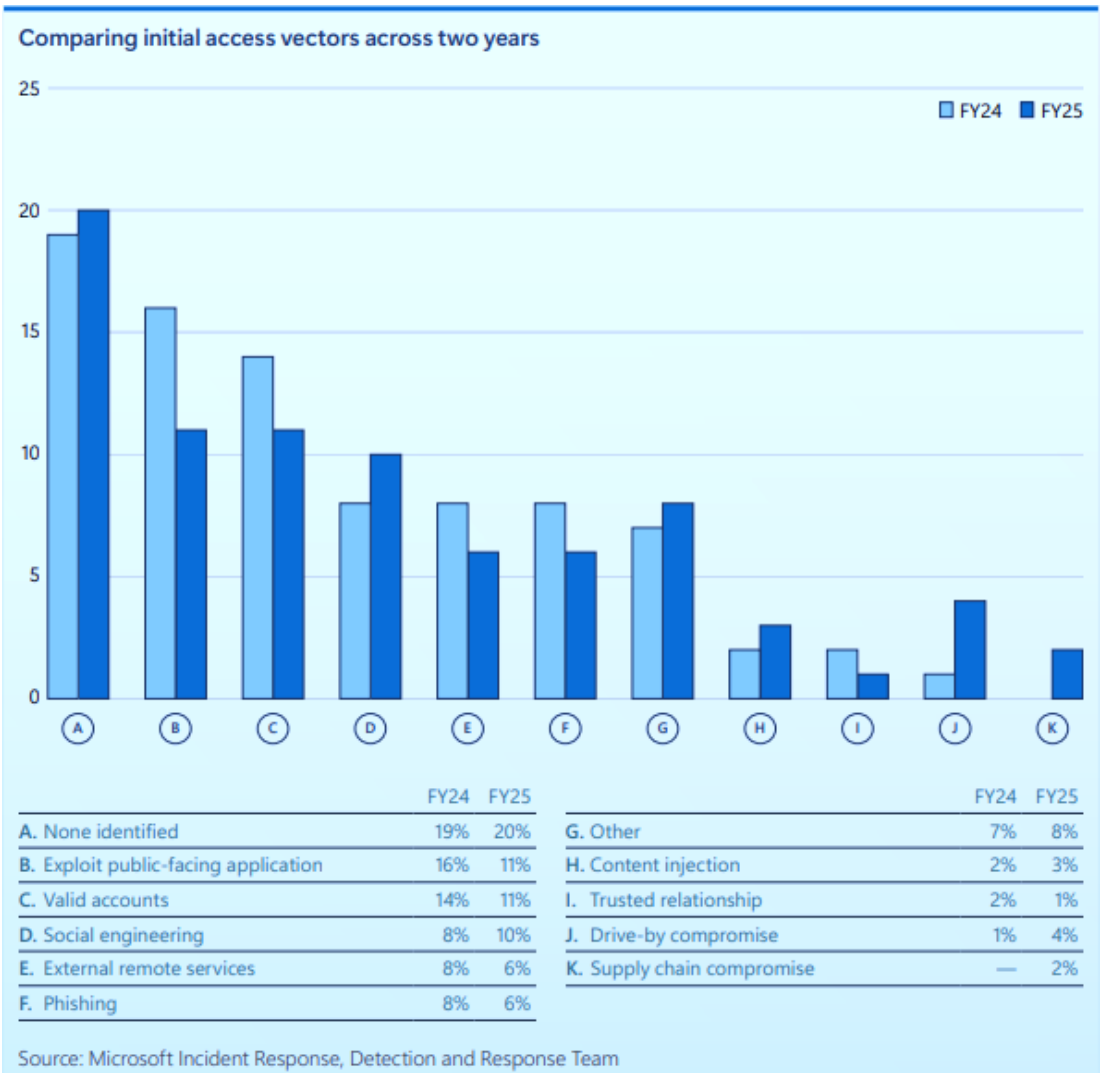
1. A identidade dixital consolídase como **principal superficie de ataque**, sendo os accesos fraudulentos o vector dominante.
2. O uso **de IA por parte de actores maliciosos** está a ampliar a escala e velocidade de campañas de phishing, intrusión e automatización do recoñecemento.
3. O crecemento sostido dos ataques a infraestructura cloud (**cloud-targeting)**, cun aumento continuo de ataques a cargas de traballo, configuracións e servizos expostos.
4. O reforzo das técnicas de **evasión e persistencia**, con adversarios capaces de operar durante longos períodos utilizando credenciais lexítimas.

As **gráficas de ciberataques e evolución de vectores** permiten visualizar este desprazamento desde vectores puramente técnicos cara a tácticas baseadas en credenciais, enxeñaría social e abuso de funcionalidades lexítimas.



Prevalencia de ciberameazas por país. Fonte: Microsoft (2025)

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



	FY24	FY25
A. None identified	19%	20%
B. Exploit public-facing application	16%	11%
C. Valid accounts	14%	11%
D. Social engineering	8%	10%
E. External remote services	8%	6%
F. Phishing	8%	6%

	FY24	FY25
G. Other	7%	8%
H. Content injection	2%	3%
I. Trusted relationship	2%	1%
J. Drive-by compromise	1%	4%
K. Supply chain compromise	—	2%

Source: Microsoft Incident Response, Detection and Response Team

Vectores de ataque 2025 vs 2024. Fonte: Microsoft (2025)

A sección de **ameazas emerxentes** subliña cinco dinámicas clave:

- **IA en operacións ofensivas**

  A IA xerativa permitirá campañas de enxeñaría social máis persuasivas e o desenvolvemento de malware e axentes autónomos capaces de moverse, escalar privilexios e evadir defensas sen intervención humana.

- **Compromisos na cadea de subministración**

  Intensificarase o abuso de relacións de confianza con MSP, VPN/VPS, RMM, CI/CD e terceiros, mediante contas privilexiadas comprometidas ou inserción de código malicioso.

- **Infraestruturas descentralizadas e encubertas**

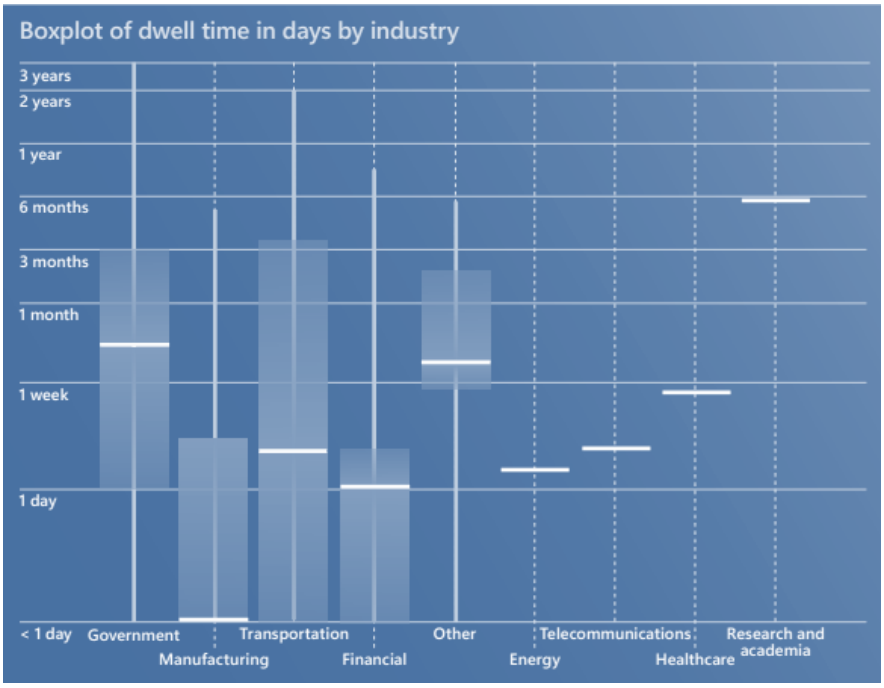
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

Os actores avanzados migrarán cara a redes P2P, blockchain e overlays do dark web para evadir atribución, distribuír malware e soster operacións mesmo tras intentos de desmantelamento.

- **Abuso crecente de identidades cloud**
  Aumentará a explotación de OAuth malicioso, autenticación herdada, device-code phishing e AiTM para evadir MFA e manter acceso persistente, requirindo maior gobernanza e control continuo de tokens.

- **Expansión do mercado de intrusión comercial**
  Os *cyber mercenaries* ofrecerán capacidades ofensivas cada vez máis disruptivas, facilitando sabotaxe e interferencia con alta precisión e baixa detección, dificultando a atribución e resposta.

Un aspecto especialmente relevante para operacións de seguridade é a gráfica de **tempo de permanencia do adversario** (dwell en inglés).

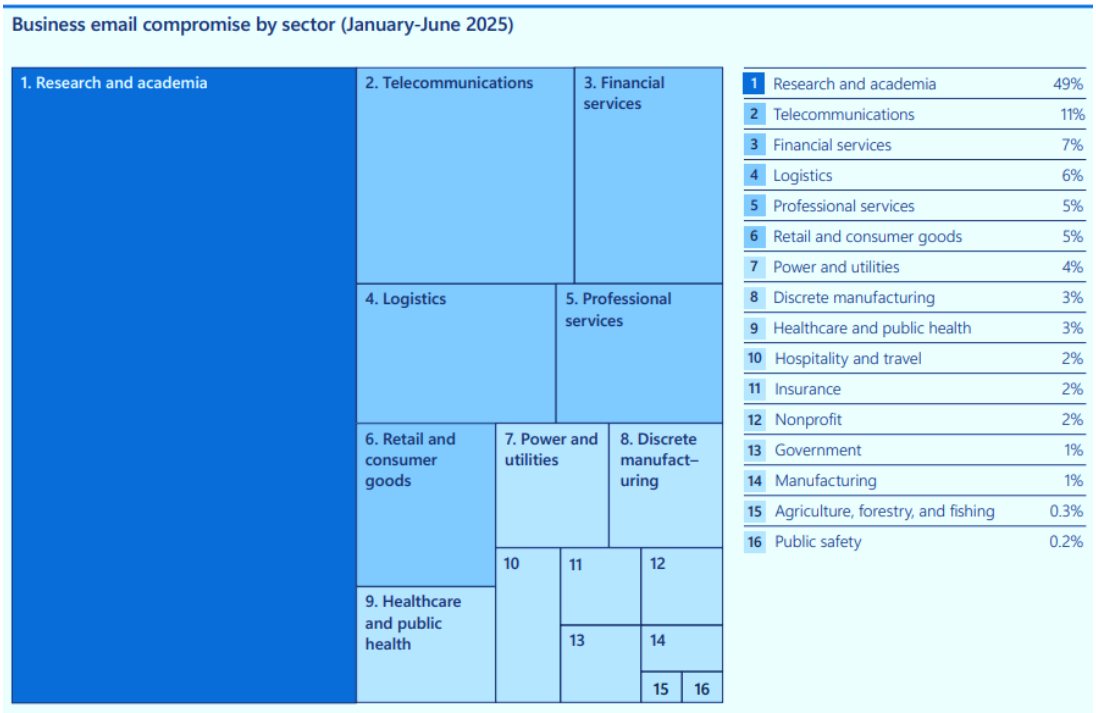


Tempo de permanencia dos cibercriminais no obxectivo (mediana e rango min/máx). Fonte: MS (2025)

Microsoft mostra como moitos ataques consuman exfiltración ou movemento lateral en **menos de 24 horas**, e nun volume significativo de casos **dentro da primeira hora**. Este dato reforza a idea de que a defensa moderna esixe **axilidade en detección e resposta**, reducindo ao mínimo a xanela de operación do adversario antes de que alcance sistemas críticos.

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

Por último para ilustrar a importancia da enxeñaría social: en canto á **fraude BEC** (Business Email Compromise, ou phising corporativo sofisticado), Microsoft destaca que representa unha proporción crecente de incidentes graves, impulsado polo compromiso de credenciais e o uso de técnicas de enxeñaría social cada vez máis sofisticadas, incluíndo deepfakes de voz e manipulación de identidades dixitais.



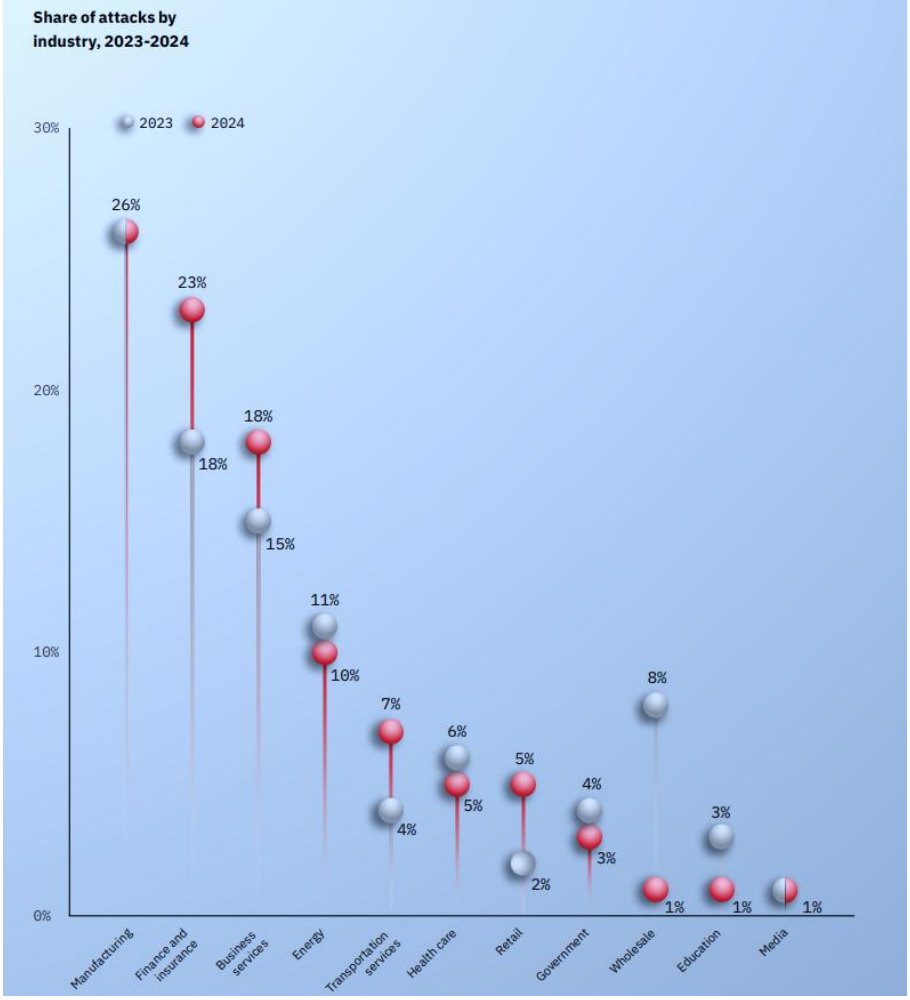
Ataques de enxeñaría social BEC por sector en H1 2025. Fonte: Microsoft (2025)

O ***IBM X-Force Threat Intelligence Index 2025*** [32] describe un panorama dominado por adversarios cada vez máis difíciles de detectar, capaces de operar con maior sixilo e apoiados en vastos ecosistemas clandestinos que facilitan desde a venda de credenciais até a distribución de ferramentas para intrusións complexas. A introdución do informe advirte que os atacantes xa non necesitan "forzar a entrada": **simplemente inician sesión con credenciais roubadas**, o que lles permite ocultar a súa actividade durante semanas e converter cada brecha nunha porta de acceso a campañas máis amplas e coordinadas. Este desprazamento táctico sitúa á **identidade e á cadea de subministración dixital** no centro do risco.

Neste contexto, unha das mensaxes máis contundentes do informe é que **manufactura volveu ser o sector máis atacado por cuarto ano consecutivo**. A razón non é unicamente o seu peso na economía: moitas organizacións manufactureiras continúan operando con arquitecturas herdadas, sistemas OT expostos e alta dependencia de activos críticos que non poden deterse. Iso explica que os impactos máis frecuentes —

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

segundo IBM— inclúan **extorsión (29 %) e roubo de datos (24 %)**, así como o feito de que manufactura rexistrase **o maior número de casos de ransomware en 2024**, contravindo a tendencia global de descenso deste malware.



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

Outro cambio estrutural observado en 2024 é o **aumento do 84 % en infostealers (malware para roubo de información) distribuídos a través de campañas de phishing**. Este fenómeno é especialmente relevante porque converte ao correo electrónico nun **vector invisible de compromiso**, capaz de proporcionar aos atacantes credenciais válidas que logo utilizan en intrusións prolongadas baseadas en identidade. Sinálase que, a diferenza dun ataque de ransomware, cuxa detección adoita ser inmediata, os infostealers permiten manter un acceso silencioso e persistente, atrasando a reacción dos equipos defensivos.

A escala xeográfica, Europa foi en 2024 a **terceira rexión máis atacada**, concentrando o **24 % dos incidentes** analizados por IBM. O vector inicial máis habitual foi a **explotación de aplicacións expostas (36 %)**, que deu paso a accións como **acceso s**

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

servidores (15 %), uso de **ferramentas de adquisición de credenciais (12 %)** e **ransomware ou malware asociado (9 %)**.

En canto aos impactos, predominou claramente o **credential harvesting** (ou manipulación para que o usuario entregue as súas credenciais) **(46 %)**, seguido de **fugas de datos (31 %)** e **roubo de información (15 %)**, reflectindo unha orientación clara cara á monetización de datos sensibles. Sectorialmente, destacaron **servizos profesionais, de negocios e consumo (38 %)**, por diante de **finanzas e seguros (18 %)** e **manufactura (18 %).**

A nivel de países, o **Reino Unido** foi o máis afectado (**25 %** dos incidentes europeos), seguido de **Alemaña (18 %)** e **Austria (14 %)**.

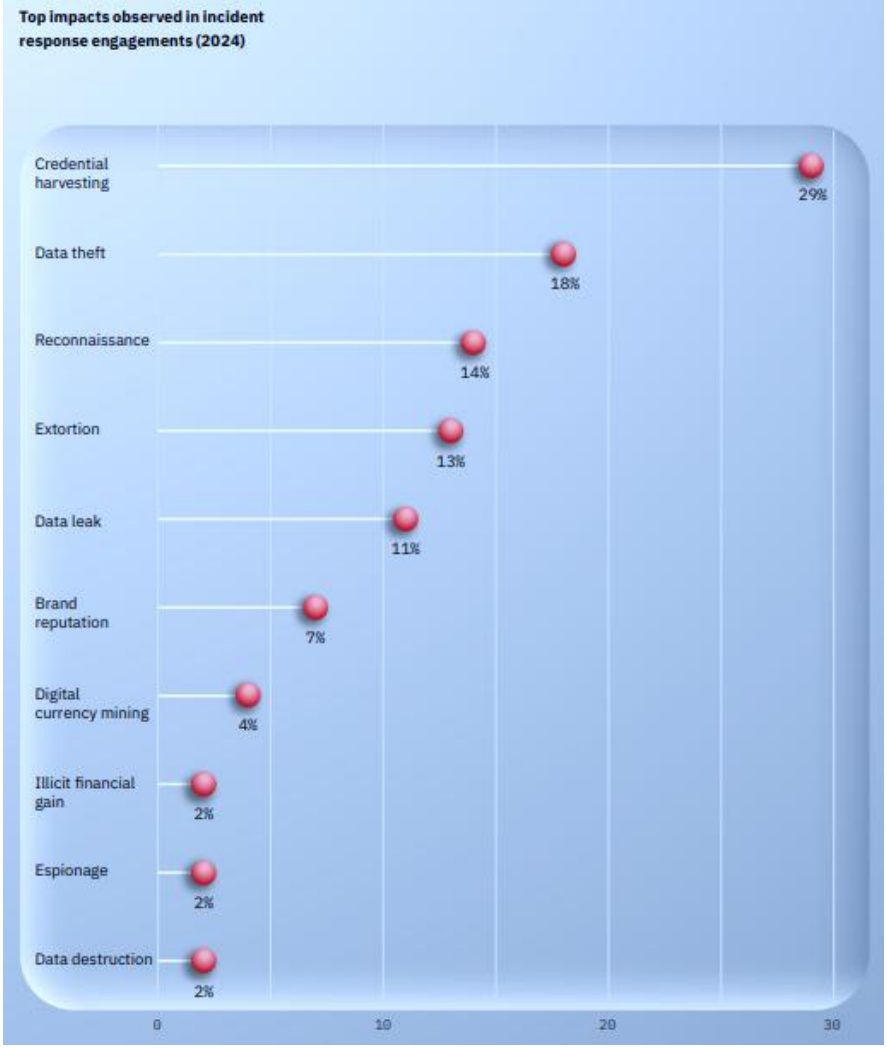
O informe tamén dedica atención ao papel da **intelixencia artificial**, observando que a súa adopción por parte de actores maliciosos é xa un feito consolidado. IBM documenta casos nos que a IA emprégase para crear sitios web fraudulentos, xerar código malicioso, elaborar correos de phishing altamente verosímiles e mesmo producir **deepfakes** para reforzar campañas de enxeñaría social. A IA non só acelera o proceso, senón que tamén reduce a barreira de entrada, permitindo que actores menos sofisticados executen operacións máis avanzadas. Máis detalle na seguinte sección.

Así mesmo, o informe alerta de que **un de cada catro ataques contra infraestruturas críticas comezou explotando aplicacións expostas a Internet**. Tras o acceso inicial, os adversarios realizan escaneos activos, identifican novas debilidades e buscan escalar privilexios para moverse lateralmente. IBM fai fincapé nos riscos derivados dos **tempos de permanencia (dwell) prolongados vistos anteriormente no informe de Microsoft** [31]**, que permiten** aos actores utilizar a estratexia de "vivir da terra" (living-off-the-land), é dicir, operar con ferramentas lexítimas do sistema, dificultando a súa detección.

En relación co ransomware, aínda que IBM observa un descenso xeral en incidentes por terceiro ano consecutivo, este tipo de malware segue representando **o 28 % dos casos de malware analizados**. O aparente declive non debe confundirse cunha perda de relevancia: na dark web, a actividade asociada a ransomware **aumentou un 25 %**, impulsada por tácticas de múltiple extorsión e pola capacidade de operar en entornos híbridos (Windows e Linux). Este comportamento bifásico —redución de incidentes detectados pero aumento de actividade subterránea— confirma que os grupos están a adaptar o seu modelo de negocio para minimizar exposición e maximizar beneficios.

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

En canto a **impactos globais**, **o roubo de credenciais foi o impacto máis común, presente no 29 % dos incidentes**, seguido do **roubo de datos (18 %)** e diversas **formas de extorsión (13 %).**



Principais impactos observados en ciberincidentes en 2024. Fonte: IBM X-Force (2025)

Case a metade dos ataques comportou o roubo de credenciais ou datos sensibles, o que subliña a prioridade absoluta de protexer identidades e fluxos de información.

O informe pecha como diciamos cunha revisión por sectores que confirma a **persistencia de manufactura como obxectivo principal**. O **sector financeiro e de seguros sitúase en segundo lugar**, destacando a importancia das campañas de phishing e a explotación de credenciais. En terceiro lugar aparecen os **servizos profesionais, de negocios e consumo**, particularmente expostos pola súa dependencia de aplicacións accesibles desde Internet e polo seu alto volume de datos sensibles. Sectores como enerxía, transporte, retail e saúde tamén presentan patróns distintivos,

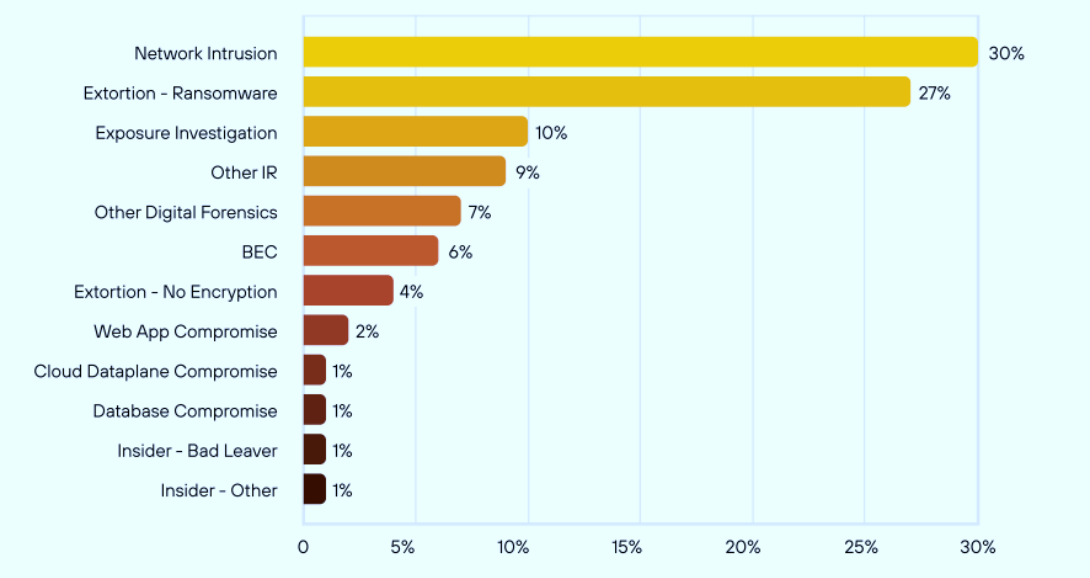
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

pero todos comparten unha mesma constante: **o roubo de credenciais e a exfiltración de datos como eixos centrais das campañas maliciosas**.

O ***Global Incident Response Report 2025*** de Palo Alto Networks [33], elaborado polo equipo Unit 42 a partir de **máis de 500 ciberincidentes reais en 38 países e múltiples verticais**, ofrece unha boa panorámica de operacións de xestión de incidentes.

Apunta a un incremento de ataques con obxectivos non só económicos, senón tamén disruptivos: **sabotaxe, degradación de servizos e parálise operativa como método de presión**. Ademais, identifica **deficiencias sistemáticas na xestión de identidades (IAM)** como un vector de risco crítico.

A amplitude do conxunto de casos permite apreciar como **a natureza dos ataques varía sensiblemente segundo rexión e industria**, algo que pode ilustrarse mediante as seguintes figuras. Ambas axudan a contextualizar a diversidade de tácticas adversarias e a necesidade de adaptar as defensas a cada entorno:



Tipo de investigacións por rexión (Europa). Fonte: Unit 42 Palo Alto (2025)

A partir deste corpus global, Unit 42 identifica **cinco tendencias emerxentes** que, en conxunto, explican a aceleración e complexidade do panorama actual. Estas tendencias están asociadas tanto á cibercriminalidade económica como ás operacións de Estados, ameazas internas e mesmo hacktivismo, conformando un escenario no que a motivación do atacante non cambia, pero si o fai a súa capacidade para causar impacto.

1. A terceira onda de extorsión

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

A primeira tendencia destacada por Unit 42 é a **evolución dos ataques de extorsión**, que xa non se limitan ao cifrado de arquivos nin sequera ao modelo de dobre extorsión con roubo de datos. Segundo Palo Alto, estamos inmersos nunha **terceira onda**, onde o obxectivo principal é provocar **interrupcións operativas deliberadas** capaces de paralizar servizos esenciais e aumentar a presión económica sobre a vítima.

En 2024, **o 86 % dos incidentes atendidos por Unit 42 xeraron perdas operacionais, reputacionais ou financeiras**, desde tempos de inactividade prolongados até danos na relación con clientes e socios. Esta transición pode verse claramente na gráfica sobre **tácticas de extorsión**, que ilustran como a combinación de cifrado, exfiltración, acoso e sabotaxe converteuse no modus operandi dominante.

Extortion Tactic	2021	2022	2023	2024
Encryption	96%	90%	89%	92%
Data Theft	53%	59%	53%	60%
Harassment	5%	9%	8%	13%

Prevalencia de tácticas de extorsión en ciberincidentes tipo ransomware. Fonte: Unit 42 Palo Alto (2025)

A explicación desta evolución é dobre: por unha banda, a mellora das defensas e as copias de seguridade reduce a efectividade da mera encriptación; por outro, **a fatiga social ante filtracións de datos** diminúe o impacto psicolóxico da chantaxe. Ante iso, os atacantes atoparon na interrupción do negocio o mecanismo máis directo para esixir rescates máis altos e acelerar pagos.

O informe insiste en que a resposta máis eficaz é reforzar a **resiliencia operativa**:

- Probas periódicas de continuidade de negocio e simulacións de incidentes;
- Procesos de restauración verificables;
- Separación de dominios críticos;
- Mecanismos de contención que permitan operar parcialmente mesmo baixo ataque.

2. Cadea de subministración software e explotación na nube

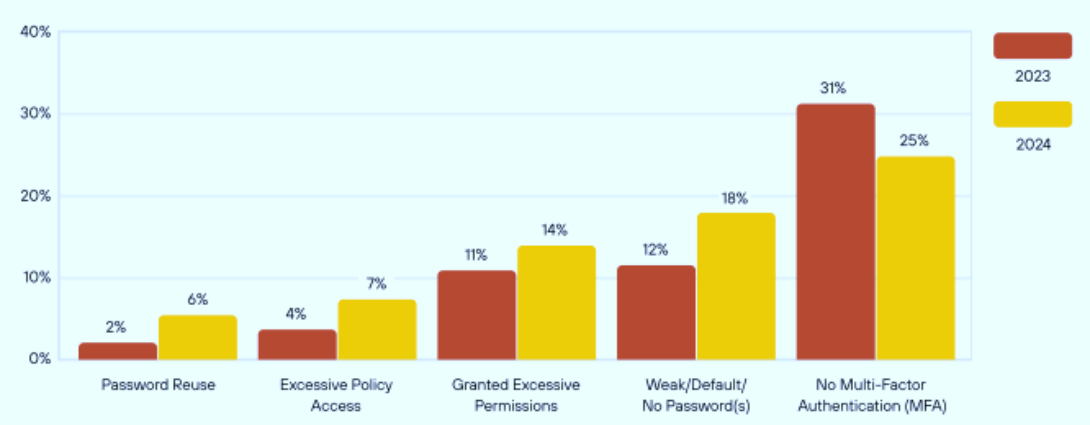
A segunda tendencia é a **amplificación do impacto asociado á cadea de subministración software e á explotación de entornos cloud**. Case un terzo dos

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

incidentes de 2024 estivo relacionado con entornos SaaS ou recursos cloud, e nun de cada cinco casos os atacantes lograron causar danos operativos nesas plataformas.

Unit 42 documenta casos nos que credenciais expostas, configuracións incorrectas ou uso de chaves de longa duración permitiron aos adversarios **inserir infraestrutura maliciosa dentro do propio entorno cloud da vítima**, utilizándoa como trampolín para ataques a terceiros. En campañas sofisticadas chegáronse a escanear **máis de 230 millóns de obxectivos únicos**, evidenciando o poder multiplicador dun punto débil na nube.

Un elemento especialmente crítico é a xestión de identidades: a informe mostra unha deterioración en varios parámetros clave —permisos excesivos, políticas laxas e fallos en rotación de claves—, como se mostra a continuación:



Tendencias en problemas relacionados con IAM en 2024 vs 2023. Fonte: Unit 42 Palo Alto (2025)

Para limitar este risco, desde Palo Alto recomendan:

- Controis estritos **de IAM** e privilexios mínimos;
- Uso de credenciais de curta duración e MFA consistente;
- Centralización de logs e auditorías na nube;
- Monitorización de patróns de uso e detección de anomalías;
- Reforzo de APIs e compoñentes da cadea de subministración (incluíndo OSS).

A clave é asumir que a nube, pola súa elasticidade e conectividade, pode converterse tanto no **activo máis produtivo** como na **superficie de ataque máis perigosa** se non existe gobernanza axeitada.

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

3. Velocidade: os ataques aceléranse e reducen drasticamente as xanelas de reacción

Unha das conclusións máis preocupantes do informe é a **aceleración extrema dos ataques**. A automatización, o uso *de* toolkits RaaS (Ransomware como servicio) e a integración de IA permiten aos adversarios identificar vulnerabilidades, moverse lateralmente e exfiltrar datos en tempos que hai poucos anos eran impensables.

En 2024, o **tempo mediano de exfiltración foi de apenas dous días**, pero no 25 % dos casos ocorreu en menos de cinco horas, e no 19 %, **en menos dunha hora** desde o compromiso inicial. Esta compresión temporal esixe reformular as capacidades de detección: **unha organización que necesite varias horas para confirmar un incidente xa está fóra de xanela**.

Accións que se poden levar a cabo:

- Medición estricta **de MTTDs** (tempo medio entre caídas) e **MTTRs** (tempo medio de reparación/resposta);
- Analítica e correlación impulsadas por IA;
- **Playbooks automáticos** (manuais de resposta a incidentes) que illen contas ou endpoints sen intervención humana;
- Exercicios continuos de *rede teaming* e simulacións aceleradas;
- Priorización de activos críticos para resposta ultrarrápida.

A idea central é contundente: **a velocidade ofensiva xa supera á defensa tradicional**, e só mediante automatización e visibilidade continua pódese equilibrar esta asimetría.

4. Ameaza interna: proliferación de operacións norcoreanas altamente sofisticadas

A cuarta tendencia é o notable incremento de **ameazas internas**, protagonizadas de forma destacada por operacións norcoreanas. Unit 42 documenta un crecemento dun **300 % neste tipo de casos**, nos que operadores encubertos logran acceder a postos técnicos en organizacións internacionais usando identidades sintéticas, portafolios cribles e procesos de selección externalizados.

Unha vez dentro, estes "IT workers" poden:

- Exfiltrar información sensible de forma sistemática;

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

- Introducir ferramentas non autorizadas;
- Manipular código fonte;
- Habilitar accesos persistentes;
- Ou mesmo derivar cara a esquemas de extorsión.

Advírtese que o seu verdadeiro perigo reside na súa lexitimidade aparente: **non violan controis perimetrais, porque entran pola porta principal**. Algunhas contramedidas plausibles:

- Verificación reforzada de persoal técnico e contratistas;
- Políticas de privilexios mínimos e revisión periódica de accesos;
- Monitorización baseada en comportamento, non só en indicadores técnicos;
- Correlación de sinais dispersos (accesos inusuais, transferencias anómalas, actividade fóra de horario).

A mensaxe é clara: a ameaza interna, especialmente cando está apoiada por Estados, esixe **modelos de confianza condicional e vixilancia continua**.

5. Aparición de ataques asistidos por IA

Por último, Unit 42 identifica a **emerxencia de ataques asistidos por IA xerativa**. Aínda que aínda están nunha fase inicial, xa permiten campañas de phishing altamente verosímiles, creación automatizada de malware, obfuscación de código e optimización de exploits. Os laboratorios demostraron que unha cadea de ataque que antes requiría dous días, pode completarse en **25 minutos** cando se integra IA en cada fase.

Posibles accións a levar a cabo:

- **Despregamento de sistemas defensivos baseados en IA** para igualar velocidade;
- **Formación específica en detección de correos**, contidos e deepfakes xerados por IA;
- Incorporación de tácticas de IA adversaria en exercicios de crises;
- Automatización de **fluxos de contención**.

A IA non só acelera os ataques: **aumenta o seu realismo e reduce o limiar de habilidade necesario para executalos**.

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

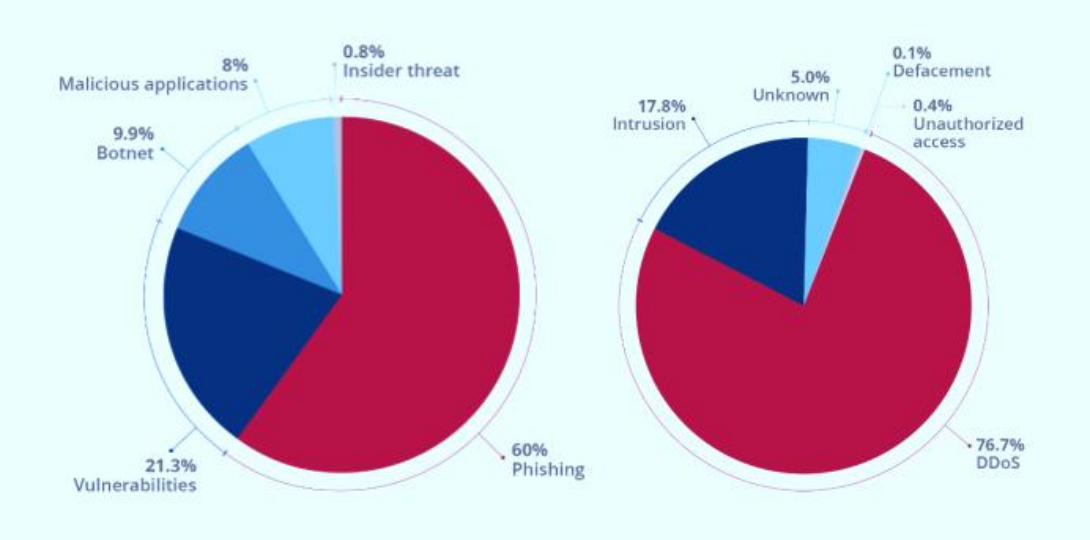
3.2.2 Europa

O **ENISA Threat Landscape 2025** [34] constitúe unha das análises máis amplas e sistemáticas do ecosistema de ameazas en Europa. Elaborado a partir de **case 4.900 incidentes** reportados entre xullo de 2024 e xuño de 2025, describe un panorama marcado pola converxencia de cibercrime, operacións ideolóxicas e capacidade ofensiva de actores estatais. Aínda que a maioría dos incidentes rexistrados correspóndense con campañas de **motivación ideolóxica —principalmente DDoS—**, as ameazas máis lesivas en termos operativos e económicos seguen sendo o **ransomware**, o **roubo e filtración de datos** e a **explotación de vulnerabilidades**. ENISA sinala que administracións públicas, transporte, loxística, servizos dixitais e, de maneira crecente, **infraestruturas industriais (ICS)**, figuran entre os obxectivos prioritarios dos adversarios.

Panorama europeo

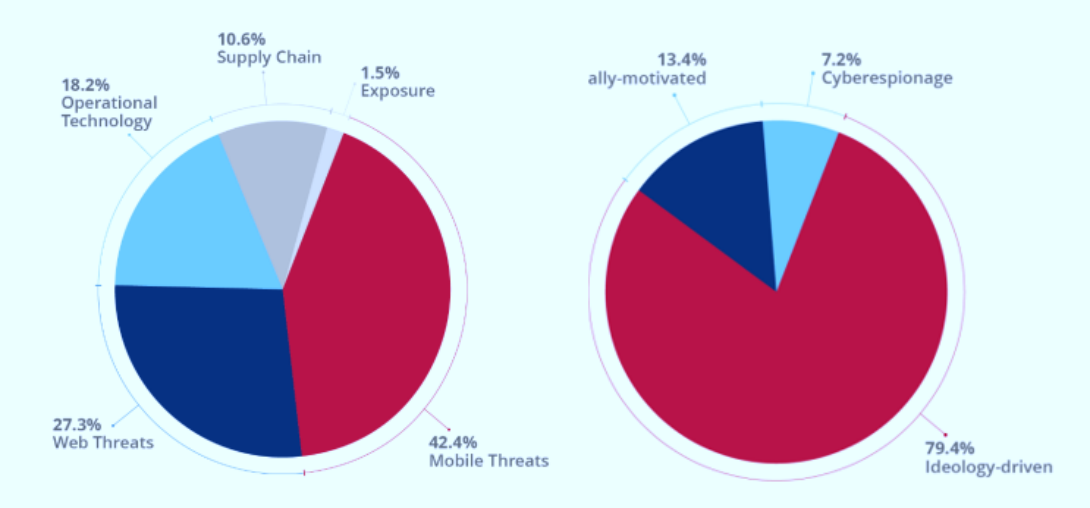
A sección introdutoria do informe detalla a distribución e tipoloxía dos incidentes observados, o que permite caracterizar a actividade maliciosa en Europa cunha visión comparativa. ENISA identifica un volume sostido de ataques de denegación de servizo —orquestrados tanto por colectivos hacktivistas como por actores criminais que buscan xerar interrupcións visibles— que representan ao redor do **80 % dos incidentes rexistrados**. Non obstante, cando se analiza impacto, severidade e alcance, o protagonismo desprázase cara a ameazas como **ransomware**, **fugas de datos**, **compromiso de contas**, e **intrusións en redes internas** derivadas de credenciais comprometidas ou fallos de configuración.

As figuras seguintes, proporcionan unha visión agregada da frecuencia e tipoloxía de incidentes, mostrando o predominio de ataques disruptivos fronte a intrusións máis silenciosas pero potencialmente máis daniñas:



Vector de ataque principal e tipoloxías de ciberincidentes europeos. Fonte: ENISA (2025)

Así mesmo, as seguintes ofrecen un desglose de **tipoloxías de obxectivo** e **motivacións**. O informe destaca que xunto con AAPP, transporte e provedores de servizos dixitais, aparecen **entornos ICS** como vector de interese crecente para actores estatais e grupos con capacidade técnica. En canto a motivación, obsérvase unha repartición clara entre **ideolóxica**, **económica** e **estratéxica**, dependendo do tipo de actor e da rexión afectada:



Distribución de ameazas e obxectivos dos cibercriminais en UE. Fonte: ENISE (2025)

Tendencias xerais

O informe desenvolve varias tendencias transversais que explican a evolución do panorama de ameazas en Europa:

1. Persistencia do ransomware e maduración do modelo criminal

ENISA subliña que, a pesar de variacións anuais no número de vítimas, o ransomware continúa sendo a ameaza económica máis significativa. Evoluciona como vimos dicindo, cara a modelos de **múltiple extorsión**, onde se combinan cifrado, roubo de datos, chantaxe directa e presión reputacional mediante sitios de filtracións.

2. Explotación sistemática de vulnerabilidades recentes

Unha parte importante dos incidentes máis graves iníciase coa explotación de fallos publicados semanas ou mesmo días antes, especialmente en dispositivos perimetrais e servizos expostos. A rapidez coa que os atacantes integran novas vulnerabilidades nas súas campañas segue sendo un factor crítico de risco.

3. Compromiso de identidades e abuso de credenciais

Do mesmo xeito que outras axencias, ENISA observa un aumento continuado de incidentes baseados en **credenciais roubadas, accesos cloud mal configurados** e **phishing avanzado**, que constitúen un dos vectores de entrada máis efectivos. A monetización de accesos iniciais en mercados clandestinos amplifica este fenómeno, como veremos posteriormente no informe de CrowdStrike de maneira gráfica.

4. Ataques disruptivos e ideolóxicos

O informe documenta un incremento sostido de campañas motivadas por conflitos xeopolíticos, especialmente DDoS e defacement, impulsadas por colectivos aliñados con bandos enfrontados. Aínda que o seu impacto técnico adoita ser limitado, o seu volume explica a súa presenza dominante nas estatísticas.

5. Expansión do ecosistema de ciberdelincuencia

A profesionalización de infraestruturas as a service (ransomware, botnets, infostealers, IABs) facilita que actores con pouca capacidade técnica executen ataques sofisticados a gran escala, reducindo drasticamente a barreira de entrada.

6. Ameazas á cadea de suministro

ENISA identifica un aumento de incidentes orixinados en provedores tecnolóxicos, servizos cloud e software de terceiros. A complexidade das interdependencias dixitais segue xerando riscos sistémicos, especialmente para sectores regulados e operadores esenciais.

7. Emprego de intelixencia artificial por parte dos atacantes

O informe confirma un incremento notable de campañas que integran **IA xerativa**, desde a elaboración de phishing altamente convincente até a automatización de fases de recoñecemento. ENISA menciona esta tendencia como relevante, pero advirte que o seu impacto operativo concreto analizarase en maior profundidade en futuras edicións; neste informe tratábase como un vector emerxente, non aínda dominante. Máis, na seguinte sección.

Por último, a nivel europeo, o **CrowdStrike European Threat Landscape Report 2025** [35] ofrece unha visión detallada da evolución das ameazas no continente, situando a Europa como un dos principais escenarios de actividade tanto para actores criminais como para grupos con motivación política ou estratéxica.

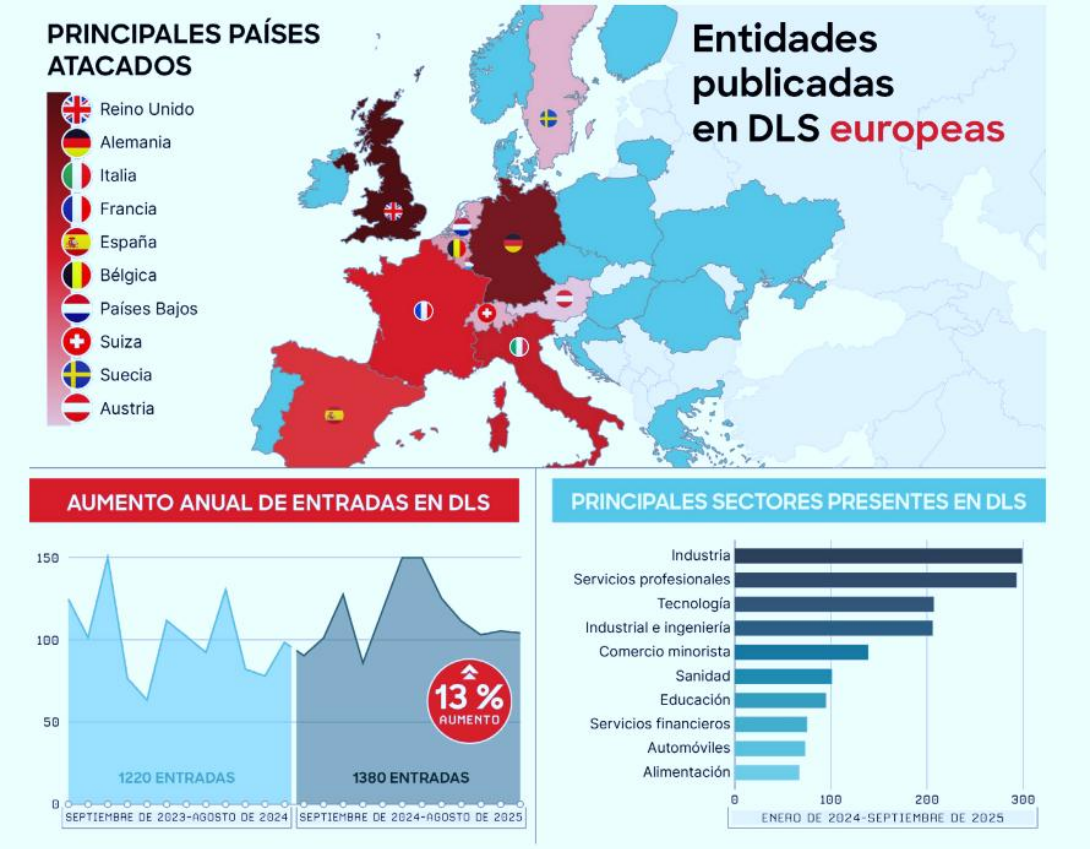
No seu resumo destaca unha tendencia xa consolidada: o ransomware continúa sendo o vector de maior impacto, e **o 92 % das vítimas europeas aparecen finalmente listadas en sitios de filtración**, o que reflicte a centralidade da extorsión baseada en roubo e publicación de datos. O informe sitúa ademais a **velocidade operativa dos adversarios**, a dispoñibilidade de accesos comprometidos en mercados clandestinos e a expansión de actividades contra infraestruturas críticas como os factores que máis transformaron o risco no período analizado. A continuación, desenvólvense as súas ideas mais salientables.

Roubo de datos e incidentes recentes

O informe documenta un patrón claro: os adversarios en Europa céntranse cada vez máis en **exfiltrar datos antes de cifrar ou interromper operacións**, consolidando un modelo híbrido de monetización que combina venda de información sensible, extorsión directa e presión reputacional. A maioría dos incidentes analizados mostra que os atacantes buscan primeiro garantir a posesión de datos críticos —credenciais, arquivos corporativos, historiais financeiros, información operativa— antes de despregar outras tácticas.

O volume de danos derivados destas filtracións obsérvase claramente na seguinte figura, onde se aprecia o crecemento continuo de incidentes centrados na exfiltración.

CrowdStrike subliña que esta tendencia non só afecta a grandes corporacións, senón tamén a organizacións medianas e pequenas que carecen dunha capacidade madura de resposta e de medidas robustas de xestión de credenciais.



Filtracións de datos por país europeo, sector e período de tempo. Fonte: CrowdStrike (2025)

A economía do acceso inicial

Un dos elementos máis relevantes do informe é a análise dedicada aos **intermediarios de acceso inicial** (IAB, polas súas siglas en inglés). Confírmase que en 2024–2025 consolidouse un mercado sumamente activo onde se comercializan **credenciais válidas, accesos VPN comprometidos, sesións cloud e puntos de entrada en sistemas corporativos**. Estes IABs actúan como provedores para operadores de ransomware, grupos criminais e, en ocasións, actores estatais, reducindo drasticamente a barreira de entrada para executar campañas complexas.

O informe inclúe un gráfico específico sobre a actividade destes intermediarios, que ilustra a magnitude da oferta de accesos comprometidos en Europa.

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

	REINO UNIDO	ESPAÑA	ALEMANIA	ITALIA	FRANCIA	PAÍSES BAJOS	BÉLGICA	SUECIA	SUIZA	PORTUGAL	AUSTRIA	POLONIA	DINAMARCA	NORUEGA	REPÚBLICA CHECA	OTROS	TOTAL FINAL
Educación	40	10	23	19	16	14	5	1	1	9	1	7	0	0	1	15	162
Comercio minorista	28	25	10	20	12	2	4	5	6	2	2	5	7	2	0	14	135
Servicios profesionales	34	10	24	6	13	9	2	6	5	3	5	2	4	3	2	6	133
Industria	20	9	16	14	3	6	3	3	5	0	4	1	0	2	0	6	92
Industrial e ingeniería	19	5	18	16	4	5	7	3	3	0	3	1	0	0	0	5	85
Tecnología	14	14	7	10	9	5	2	4	1	6	0	1	3	4	0	3	83
Administración pública	4	7	3	10	9	1	1	5	0	1	1	0	1	1	0	6	50
Servicios financieros	13	3	1	7	6	5	0	0	2	1	0	1	1	0	3	7	49
Telecomunicaciones	5	5	4	4	5	2	0	1	0	1	1	1	0	0	1	1	40
Sanidad	4	2	4	1	5	8	5	0	1	0	0	1	1	0	1	6	38
Automóviles	1	3	7	5	1	4	0	2	1	0	0	0	0	1	0	3	27
Energía	2	1	3	3	3	0	0	0	1	0	0	3	1	1	0	2	20
Medios de comunicación	4	1	1	0	10	0	0	0	1	0	0	0	0	0	1	2	20
Transporte	1	0	1	2	2	6	0	2	0	0	0	0	0	0	1	3	18
Logística	6	5	1	1	2	0	0	0	0	0	1	0	1	0	0	0	17
Otros	100	65	38	40	55	14	18	10	15	5	9	4	7	5	5	72	462
Total final	292	161	160	156	153	80	46	42	41	28	27	27	24	19	15	160	1431

Entidades promocionadas por intermediarios de acceso en Europa por sector. Fonte: CrowdStrike (2025)

Este fenómeno enlaza directamente co observado no informe de ENISA, onde tamén se destacaba a importancia crecente da economía clandestina de accesos para facilitar ataques posteriores, incluídos os dirixidos a infraestruturas industriais.

Ataques contra sistemas de control industrial

O informe adica unha sección específica aos **sistemas de control industrial**, destacando que en 2024–2025 observouse unha **crecente atención de actores criminais, hacktivistas e grupos con motivacións xeopolíticas** cara infraestruturas OT europeas. Segundo a análise do provedor, boa parte desta actividade concentrouse en sectores como **enerxía, fabricación avanzada e ámbitos vinculados á defensa**, onde a interdependencia entre procesos físicos e sistemas dixitais incrementa tanto o atractivo como o potencial impacto dunha intrusión.

Sinálase que os ataques detectados dirixíronse principalmente a **obter acceso non autorizado a redes industriais**, coa fin de **colleitar información sobre procesos, configuracións técnicas e arquitecturas de planta**. En varios casos, os adversarios trataron ademais de **interferir en operacións**, aproveitando debilidades comúns como a **segmentación insuficiente**, o uso de activos **obsoletos** ou a **exposición inadvertida de servizos industriais** a Internet. O informe salienta que estas intrusións non sempre buscaban a interrupción inmediata: en numerosos incidentes, a prioridade do atacante era **situarse dentro do entorno OT**, obter coñecemento detallado e preparar posibles operacións de maior alcance.

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

Conclúen que a **superficie de ataque OT en Europa continúa a se ampliar**, especialmente alí onde a converxencia entre redes IT e OT non está apoiada por controis de seguridade específicos. Esta dinámica explica a crecente presenza de actores avanzados e grupos criminais neste tipo de entornos (máis detalle respecto diso sobre esta cuestión de actores e técnicas, tácticas e procedementos, nunha sección posterior).

3.2.3 España

O informe ***CCN-CERT IA-04/24 Ciberamenazas y Tendencias 2024*** [36] constitúe a **análise máis actualizada a nivel nacional a data de elaboración deste informe, sobre a evolución das ameazas estratéxicas que afectan a España**. A súa lectura permite comprender como actores estatais, cibercriminais e grupos hacktivistas están a adaptar as súas tácticas nun contexto marcado pola guerra en Ucraína, a inestabilidade en Oriente Medio e a consolidación do ecosistema do ransomware. Aínda que o documento non está especificamente orientado a ICS, moitas das súas conclusións teñen implicacións directas para os entornos industriais, especialmente aqueles onde a visibilidade, a segmentación e a xestión de vulnerabilidades continúan a non ser de abondo.

Actores estatais

O informe identifica a **Rusia, China, Corea do Norte e Irán** como os principais impulsores de campañas de ciberespionaxe dirixidas contra España e outros países occidentais. Sen descender ao detalle de cada grupo operativo, o CCN-CERT describe patróns comúns: operacións prolongadas, alta orientación á obtención de intelixencia, explotación preferente de vulnerabilidades recentes e, no caso de Rusia e China, campañas sincronizadas con obxectivos xeopolíticos ou militares.

Os actores **rusos** centran gran parte da súa actividade en organismos gobernamentais e aliados de Ucraína, con especial interese en comprometer redes institucionais e obter información diplomática e estratéxica. **China**, pola súa banda, mantén unha aproximación ampla, combinando espionaxe económica e intrusións orientadas a sectores tecnolóxicos e de I+D. **Corea do Norte** continúa caracterizándose pola motivación financeira —especialmente mediante compromisos de infraestrutura crítica, ataques a entidades financeiras e roubo de criptodivisas—, mentres que **Irán** combina espionaxe, operacións de influencia e ataques oportunistas que buscan xerar disrupción ou presión política.

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

O CCN subliña que España figura de maneira recorrente entre os obxectivos destas campañas debido ao seu aliñamento internacional e ao valor dos seus activos públicos e privados.

De novo, a continuación debúllanse as principais ensinanzas do informe.

Tendencias de ciberespionaxe

O estudio describe un incremento significativo das operacións **de ciberespionaxe**, tanto en número como en sofisticación. Unha parte substancial destas campañas diríxese a **gobernos, organismos internacionais, centros de investigación, diplomacia e sectores estratéxicos**, utilizando técnicas que permiten manter o acceso de forma prolongada: explotación de vulnerabilidades perimetrais, cadeas de ataque multietapa, movemento lateral discreto e uso de malware modular.

Destácanse tres tendencias relevantes:

- **Redución do limiar técnico** requirido para executar campañas de espionaxe, grazas á dispoñibilidade de ferramentas avanzadas e kits de explotación.
- **Maior grao de automatización**, que reduce tempos entre a explotación inicial e o establecemento de persistencia.
- **Extensión dos obxectivos**, onde sectores tradicionalmente menos expostos — educación, loxística, transporte ou sanitario— intégranse agora no mapa de interese de actores estatais.

Ransomware

O CCN-CERT describe a persistencia do **ransomware como ameaza principal** para organizacións públicas e privadas españolas. A pesar dos esforzos internacionais por desmantelar infraestruturas criminais, o modelo **ransomware-as-a-service (RaaS)** segue a se fornecer: novos afiliados incorpóranse con rapidez, o custo de entrada é baixo, e a dispoñibilidade de accesos iniciais mediante credenciais roubadas ou vulnerabilidades en dispositivos perimetrais facilita as intrusións.

O informe analiza a evolución recente do ransomware, marcada por:

- **Modelos de triplo (mesmo cuádrupla extorsión)**, que combinan cifrado, roubo de datos, publicación en leak sites e acoso directo a empregados ou clientes.

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

- **Altísima orientación a monetización de datos**, especialmente en sectores onde o seu valor é maior (finanzas, sanidade, administracións públicas).
- **Uso intensivo de vulnerabilidades públicas**, con preferencia por dispositivos VPN, firewalls e solucións de acceso remoto.

Aínda que non se trate dun fenómeno puramente industrial, moitos operadores de ransomware mostraron interese crecente en **interromper procesos produtivos** como vía de presión, o que podería impactar en infraestruturas industriais españolas se persisten debilidades estruturais en ICS.

Filtracións de datos

O informe aborda o incremento de **filtracións de datos**, tanto por cibercriminais como por actores estatais. En España, o CCN observa que as filtracións afectan principalmente a **organismos gobernamentais e ao sector educativo**, aínda que se estenden tamén a empresas privadas. O mercado negro de datos segue a se espallar, incentivado pola monetización de información sensible e pola reutilización de credenciais en ataques posteriores.

A tendencia máis preocupante é a **automatización na exfiltración e publicación de datos**, que permite aos atacantes operar a gran escala e reducir o risco de detección. Estas filtracións non só aumentan o impacto reputacional, senón que alimentan o ciclo de accesos iniciais utilizados en ataques contra ICS, especialmente cando credenciais corporativas permiten pivotar cara a redes OT insuficientemente illadas.

Malware

Adícase un espazo a analizar a evolución do **malware** en 2023–2024, destacando o crecemento do modelo **malware-as-a-service (MaaS)** e a oferta de módulos especializados para espionaxe, roubo de credenciais, persistencia ou movemento lateral. Este ecosistema industrializado facilita que actores con pouca capacidade técnica executen intrusións avanzadas.

O informe tamén resalta a actividade significativa **de botnets**, o auxe **de troianos bancarios**, e o uso **de malware modular** adaptable a múltiples fases do ataque. A diversidade de ferramentas permite escalar ataques rapidamente e comprometer infraestruturas amplas con mínima intervención humana.

Lembremos que no informe de Dragos [30], profúndase sobre malware especializado para entornos ICS.

Tendencias previstas

O CCN-CERT recolle adicionalmente sete tendencias clave a futuro, que, aínda que xerais, teñen implicacións relevantes para a industria:

1. **Guerra multidominio**: a converxencia entre operacións cinéticas, informativas e dixitais continuará, o que aumenta o risco de ataques contra infraestruturas críticas, especialmente en sectores como enerxía, transporte e auga.
2. **Actividade de actores estatais**: prevese maior presión sobre países aliñados coa UE e a OTAN, o que pode traducirse en campañas de espionaxe e preposicionamento dentro de redes corporativas con acceso potencial a ICS.
3. **Ransomware**: manterase como a ameaza máis rendible para os atacantes; no contexto industrial, o risco principal é a **interrupción operacional** como mecanismo de chantaxe.
4. **Cibercrime**: continuará a se espallar, con maior oferta de accesos iniciais, ferramentas de explotación e datos filtrados, facilitando compromisos en cadeas de subministración industriais.
5. **Ameazas a sistemas industriais (ICS)**: o CCN destaca que a falta **de segmentación**, **inventario de activos** e **telemetría específica** segue sendo un problema crítico en España. As tácticas observadas en Europa do Leste poderían replicarse facilmente no noso entorno se persisten tensións xeopolíticas.
6. **Vulnerabilidades**: agárdase un incremento constante na súa explotación, especialmente en dispositivos perimetrais e compoñentes OT expostos, onde o ciclo de parcheo acostuma ser máis lento.
7. **Compromiso da cadea de subministración**: seguirá sendo un vector prioritario, especialmente en entornos ICS onde provedores externos, mantemento remoto e software especializado amplían a superficie de risco.

O Centro Criptolóxico Nacional conclúe que, para mitigar estas tendencias, será necesario reforzar as capacidades: levándoo ao noso terreo, falaríamos de **detección avanzada**, formación específica en **seguridade OT**, mellora da **segmentación** e **profesionalización da análise de incidentes** en infraestruturas críticas.

A revisión da totalidade das fontes, suxire un escenario onde converxen tres grandes ameazas: o **cibercrime como servizo** (ransomware, BEC, filtración de datos), o

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

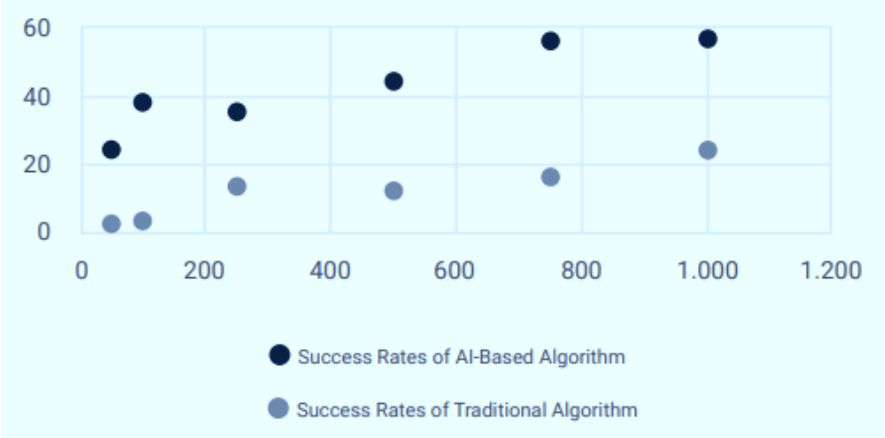
ciberespionaxe patrocinado por estados, e os **ciberataques ideolóxicos impulsados por conflitos xeopolíticos**.

Os **sistemas industriais (ICS/OT)** consolidáronse como **obxectivos de alto valor**. As **vulnerabilidades coñecidas**, o **abuso de credenciais** e os **fallos de segmentación** seguen sendo vectores comúns. As diferenzas rexionais maniféstanse no tipo de actores e técnicas empregadas, pero as tendencias son compartidas: **automatización do crime**, **abuso de AI** (mais sobre isto a continuación) e **explotación masiva de acceso remoto**. Este contexto require unha **resposta combinada a nivel técnico, organizativo e estratéxico** que será detallada nun apartado posterior do informe.

3.3 Uso de IA por adversarios

Salvo que se indique o contrario, os informes referidos a continuación son os mesmos da sección 3.2.

As análises recentes coinciden en que os **actores hostís –tanto criminais como estatais– están** a **adoptar a IA** para potenciar os seus ataques. O CCN-CERT destaca, por exemplo, un **aumento do 967 % en campañas de spear phishing** para roubo de credenciais grazas a IA, así como un crecemento do 3.000 % en fraudes baseadas en deepfakes. En entornos ICS/OT –onde as redes industriais conviven con infraestruturas IT– estas técnicas supoñen un risco directo: un phishing ou deepfake máis convincentes poden enganar a operadores ou enxeñeiros, e propagar malware até os sistemas de control. Ademais, usar IA axiliza ataques técnicos: segundo o CCN-CERT, **algoritmos de IA melloraron nun 50 % a taxa de éxito no desciframento de contrasinais** por forza bruta, reducindo o esforzo necesario para comprometer accesos de sistemas industriais ou redes OT.



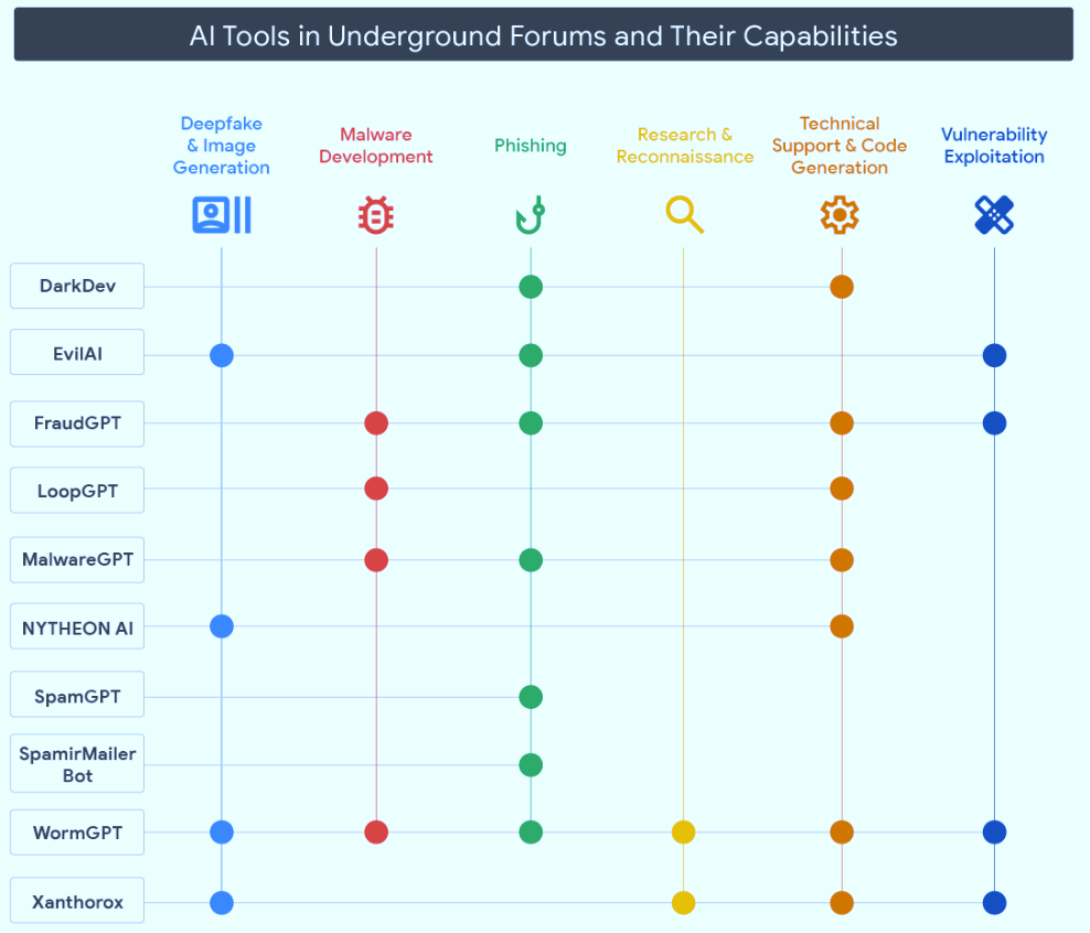
Mellora en desciframento de contrasinais por forza bruta apoiada en IA. Fonte: CCN-CERT (2024)

Xurdiron tamén **LLM maliciosos e asistentes automatizados ao servizo do cibercrime.** En 2023 apareceron ferramentas como WormGPT, FraudGPT, DarkBART/DarkBERT, WolfGPT ou XXXGPT, deseñadas expresamente para xerar correos phishing ou código malicioso. Estas *malicious GPTs* ofrecen a atacantes con poucos coñecementos a posibilidade de crear campañas sofisticadas, abaratando a barreira de entrada. O informe do CCN-CERT inclúe unha táboa que mostra como os actores máis avanzados obteñen melloras notables en recoñecemento e malware avanzado con IA, pero mesmo os ciberdelincuentes oportunistas logran incrementos apreciables en phishing e movementos laterais.

Máis aló das ferramentas preempaquetadas, detéctase malware que invoca LLMs durante a súa execución. Investigacións recentes documentan familias que utilizan IA en tempo de execución para **xerar dinámicamente comandos maliciosos, adaptar payloads ou reescribir o seu propio código**, dificultando a súa detección por firmas tradicionais e EDR. Tamén se observa un uso crecente de **enxeñaría social inversa contra os propios modelos**, enganándoos para que entreguen información normalmente bloqueada polas súas salvagardas. Novas tecnoloxías, amplían a superficie de ataque.

Paralelamente, o **mercado clandestino de IA consolidouse** . A análise *de Google Threat Intelligence* [37] mostra unha oferta estable e madura de ferramentas anunciadas en foros underground en inglés e ruso, orientadas a automatizar **phishing altamente personalizado, creación de identidades sintéticas, desenvolvemento e ofuscación de malware, análise de vulnerabilidades e apoio a campañas de desinformación**. Estas solucións preséntanse como servizos chave en man, integrables en fluxos criminais existentes, o que reduce aínda máis a barreira de entrada e favorece a escalabilidad dos ataques. Neste punto resulta especialmente relevante introducir a **figura que recolle as capacidades de ferramentas de IA maliciosas anunciadas en foros clandestinos**, onde se aprecia a amplitude funcional prometida por estes servizos.

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

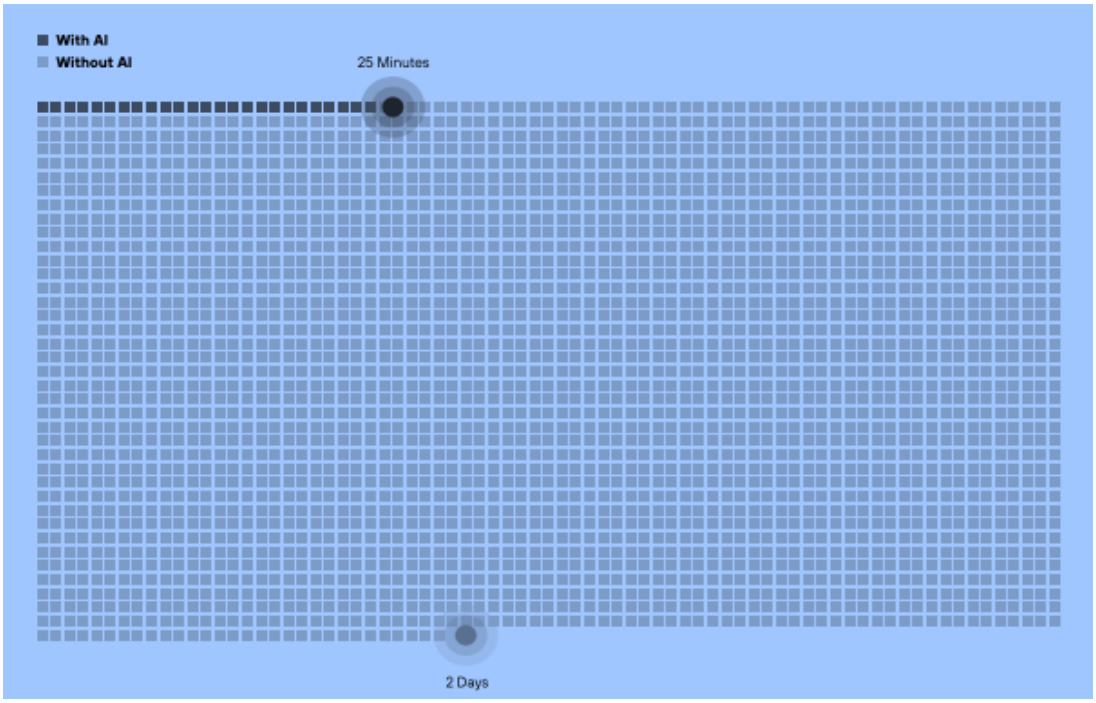


Solucións baseadas en IA en foros clandestinos en inglés e ruso. Fonte: Google Threat Intelligence (2025)

Os actores estatais tamén están a incorporar IA en todas as fases das súas ciberoperacións ENISA sinala que o uso de IA por parte de adversarios xeneralizouse como **factor habilitador transversal**, especialmente nas fases de recoñecemento, enxeñaría social e evasión, incrementando a eficacia de técnicas xa coñecidas sen necesidade de introducir TTPs radicalmente novas. Esta adopción permite campañas máis persistentes, mellor adaptadas ao contexto do obxectivo e con menor custo operativo.

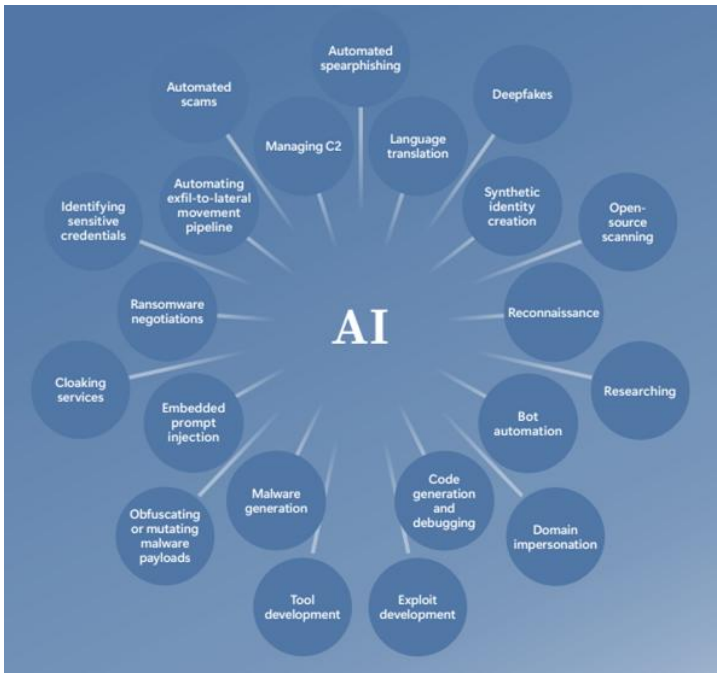
Observouse o uso de IA para **recoñecemento de obxectivos, xeración de cebos de phishing multilinguaxe, automatización do movemento lateral e aceleración da exfiltración de datos**. Neste sentido, o informe de Unit 42 de Palo Alto Networks resulta especialmente ilustrativo: en simulacións controladas, a integración de IA xerativa en todas as fases do ataque reduciu o tempo de exfiltración de **días a minutos**, pondo de manifesto un cambio cualitativo na velocidade das operacións ofensivas.

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



Diferenza de velocidade nun ataque simulado sen/con asistencia de IA. Fonte: Palo Alto Networks (2025)

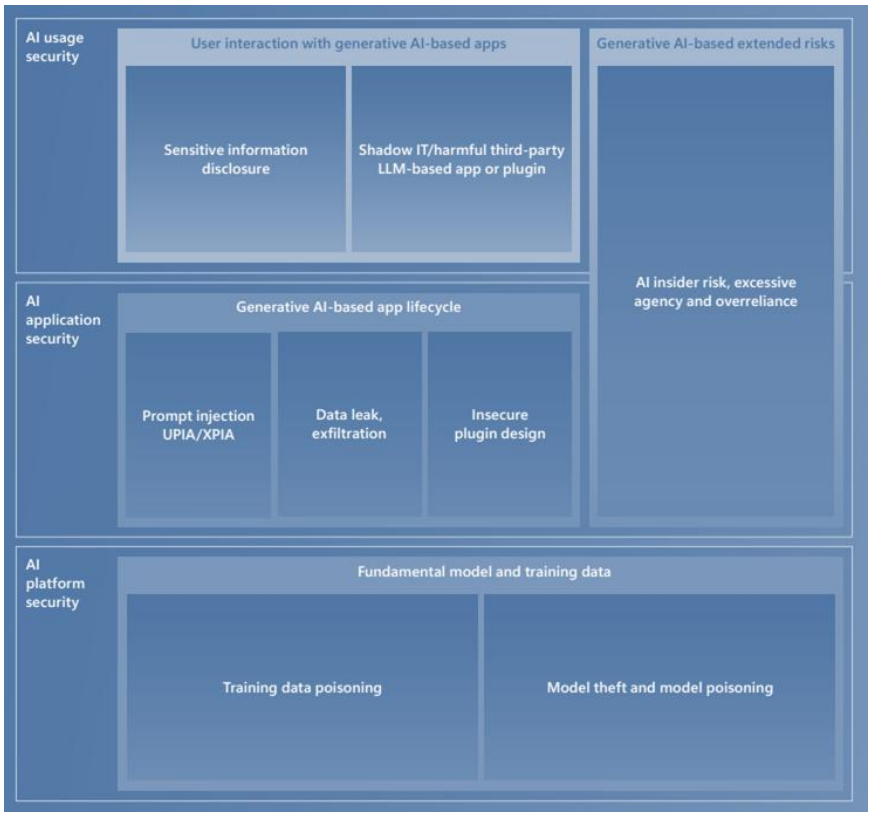
O ***Microsoft Digital Defense Report 2025*** profunda nesta idea e describe a IA como un auténtico **multiplicador de ataques tradicionais**. Segundo Microsoft, os adversarios xa empregan IA xerativa para automatizar e escalar tarefas como o spear phishing dirixido, a tradución e localización de mensaxes, a creación de deepfakes de voz e imaxe, a xeración de identidades sintéticas, o escaneo automatizado de vulnerabilidades e a produción de malware polimórfico.



Usos da IA para aumentar capacidades de ataques tradicionais. Fonte: Microsoft (2025)

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

O informe advirte ademais de que a adopción de servizos baseados en modelos de IA introduce **novas potenciais vulnerabilidades**: técnicas como a **inxección directa e indirecta de prompts**, a manipulación de ferramentas conectadas a modelos, o envelenamento de datos de adestramento ou a exposición accidental de información sensible amplían o risco, especialmente en organizacións que integran IA en procesos críticos.



Mapa de ameazas asociadas ao uso de IAs xerativas. Fonte: Microsoft (2025)

En entornos **ICS/OT, onde comezan a se introducir solucións baseadas en IA para monitorización, mantemento predictivo ou asistencia operativa, estas debilidades adquiren especial relevancia**. Un compromiso en sistemas IT apoiados en IA pode facilitar accesos indirectos a redes industriais se non existe unha segmentación e gobernanza axeitadas.

En conxunto, os distintos informes coinciden en que a IA non creou ameazas completamente novas (salvo as asociadas á explotación de tal tecnoloxía), pero si **amplificou de forma substancial a escala, velocidade e credibilidade das existentes**, actuando como catalizador de técnicas xa coñecidas e reducindo drasticamente os tempos de execución dos ataques. A resposta defensiva pasa por reforzar a concienciación, adaptar os procesos de detección e resposta a tempos moito

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

máis curtos e despregar, de forma controlada, capacidades defensivas baseadas tamén en IA que permitan equilibrar esta nova asimetría. O eterno xogo do gato e o rato.

3.4 Incidentes e campañas recentes

Este bloque apóiase en **fontes complementarias e de distinta natureza**, que permiten combinar unha visión **sectorial europea**, unha **perspectiva histórica de longo prazo** e datos **operacionais recentes** centrados especificamente en entornos industriais.

As fontes de que bebe son primeiro lugar, os **informes sectoriais** do xa citado **Threat Landscape 2025 de ENISA,** que achega unha lectura estruturada do impacto dos ciberincidentes nos principais sectores críticos da Unión Europea, aliñados co marco NIS2 e con especial atención á evolución interanual dos ataques [34].

A esta visión súmase a **base de datos de incidentes de ICS Strive** [38][39], que recolle eventos historificados desde 2010, ofrecendo un repositorio de alto valor para a análise retrospectiva. Esta fonte permite extraer leccións apresas a partir de incidentes pasados, identificar sectores recurrentemente afectados e entender como evolucionaron as técnicas de ataque e as súas consecuencias en entornos ICS ao longo do tempo.

Finalmente, incorpóranse os datos máis recentes do **Threat landscape for industrial automation systems. Europe, Q2 2025** e **A brief overview of the main incidents in industrial cybersecurity. Q2 2025 de Kaspersky** [40][41], que achegan unha perspectiva **global e actualizada** sobre a afectación de **computadores e sistemas en entornos ICS**, permitindo observar tendencias emerxentes, cambios nos vectores de infección e a evolución do impacto do malware industrial en diferentes rexións e sectores.

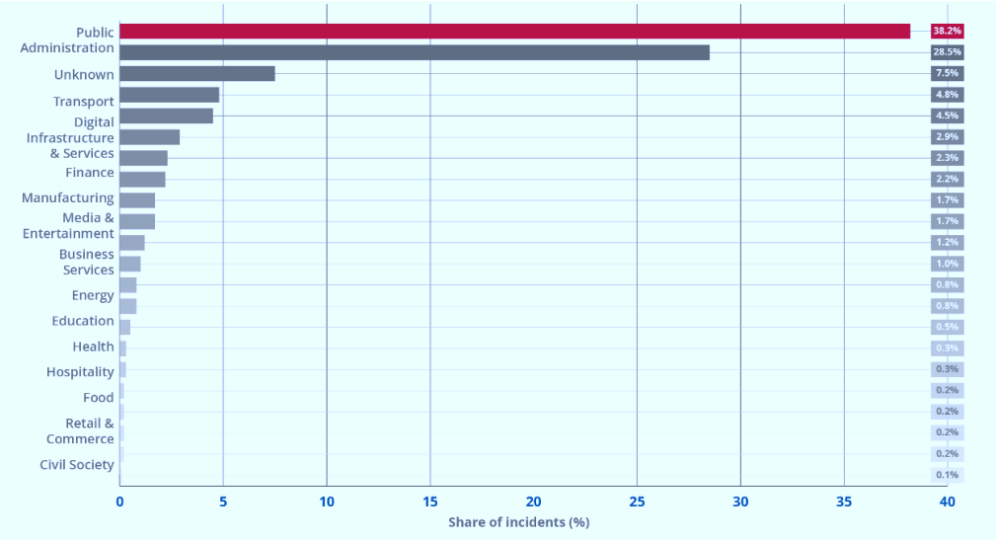
A combinación destas tres fontes permite construír unha visión **multidimensional** dos incidentes recentes: desde a análise normativa e sectorial europea, pasando pola experiencia acumulada de máis dunha década de incidentes industriais, até a observación máis próxima das ameazas que hoxe afectan os sistemas ICS.

3.4.1 Análise sectorial europea (ENISA)

A análise sectorial do ENISA [34] ofrece unha visión detallada de como se distribúen os incidentes de ciberseguridade entre os distintos sectores económicos e administrativos da Unión Europea. Durante o período analizado, ENISA recompilou e analizou **4.875 eventos**, dos cales un 28,5 % non puido asociarse a un sector concreto. Unha vez

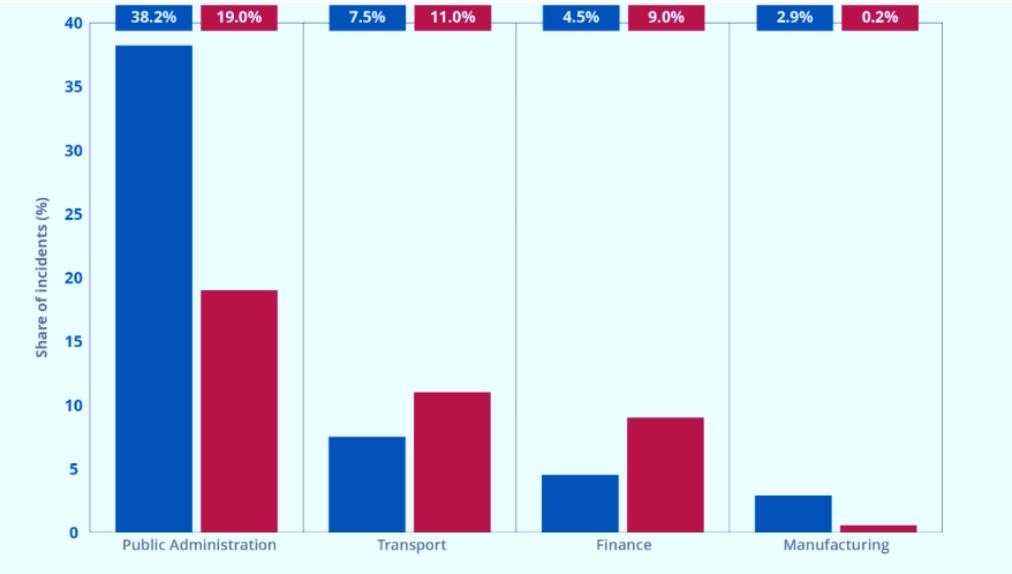
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · Axencia para a Modernización Tecnolóxica de Galicia · Xacobeo 2027

excluídos estes casos, a análise pon de manifesto unha **clara concentración de incidentes nun número reducido de sectores**, moitos deles clasificados como esenciais ou de alta criticidade no marco da **Directiva NIS2** [42]:



Incidentes rexistrados por sector. Fonte: ENISA (2025)

Os **cinco sectores máis atacados** foron **administración pública, transporte, infraestruturas e servizos dixitais, finanzas e manufactura**, que en conxunto concentran máis da metade dos incidentes rexistrados contra sectores identificados. Esta repartición confirma a relevancia do enfoque sectorial de NIS2 e permite observar a evolución interanual dos ataques, especialmente ao comparar os datos de **2024 fronte a 2023**:



Comparativa de incidentes informe 2025 vs 2024. Fonte: ENISA (2025)

A continuación, debúllanse as principais conclusións por sector.

Administración pública.

Mantense como o **sector máis atacado**, concentrando aproximadamente o **38 % dos incidentes**, cun incremento significativo respecto ao período anterior. Este aumento está directamente vinculado ao crecemento de **ataques DDoS liderados por colectivos hacktivistas**, que representan máis do **96 % dos incidentes** contra este sector.

Xeograficamente, os maiores impactos rexistráronse en **Francia, Italia e Alemaña**, seguidos por **España e Polonia**. Os incidentes afectaron principalmente a **entidades rexionais e centrais**, incluíndo organismos gobernamentais, defensa, intelixencia, forzas de seguridade, partidos políticos, misións diplomáticas e organizacións europeas.

Ademais dos ataques DDoS, a administración pública continuou sufrindo **incidentes de ransomware** —especialmente a nivel municipal— e **eivas de datos**, que representaron unha parte relevante dos casos documentados. Desde a perspectiva de ameazas avanzadas, este sector foi tamén o **principal obxectivo de campañas de ciberespionaxe vinculadas a actores estatais**, o que subliña a súa importancia estratéxica.

Transporte

O **sector transporte** situouse como o **segundo máis atacado**, cun **7,5 % do total de incidentes**, mantendo unha posición similar á do período anterior. Unha parte relevante dos incidentes de alto impacto notificados baixo a Directiva NIS correspondeu a este sector.

Os ataques concentráronse principalmente no **transporte aéreo** e na **loxística**, sendo de novo os **ataques DDoS hacktivistas** o vector predominante, con máis do **87 % dos casos**. Estas campañas estiveron estreitamente ligadas a acontecementos xeopolíticos e a decisións políticas de Estados membros en relación co conflito en Ucraína.

Xunto á actividade hacktivista, o sector transporte tamén sufriu **incidentes de cibercrime**, nos que o **ransomware** tivo un papel destacado e, aínda que numericamente limitado, xerou **impactos operativos significativos**, incluíndo interrupcións temporais de servizos críticos. Así mesmo, observouse actividade de **actores estatais**, principalmente vinculados a China e Rusia, con interese en infraestruturas crave de transporte e loxística.

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

Infraestruturas e servizos dixitais

As **infraestruturas e servizos dixitais** ocuparon o **terceiro lugar**, cun **4,8** % **dos incidentes**. Este sector, que inclúe telecomunicacións, provedores de servizos dixitais e xestión de servizos TIC, destaca polo seu **alto valor estratéxico**, tanto pola cantidade de datos que xestiona como pola súa capacidade de xerar efectos en fervenza sobre outros sectores.

Dentro do sector, as **telecomunicacións** e os **provedores de servizos dixitais** foron os subsectores máis afectados. Os **ataques DDoS hacktivistas** representaron máis da metade dos incidentes, mentres que o **cibercrime** —especialmente eivas de datos e ransomware— tivo un peso relevante debido ao potencial de extorsión e disrupción a gran escala.

Desde a óptica de ameazas avanzadas, este sector mostrou unha **alta concentración de actividade de actores estatais**, principalmente de orixe rusa, con campañas dirixidas a provedores TIC e operadores de telecomunicacións, o que reforza o seu papel como obxectivo prioritario en operacións de ciberespionaxe.

Finanzas

O **sector financeiro** representou ao redor do **4,7** % **dos incidentes**, cunha clara dominancia de **ataques DDoS de carácter hacktivista**, que superaron o **80** % **dos casos**. Estes ataques dirixíronse principalmente contra **entidades bancarias**, buscando xerar molestias aos usuarios e amplificar mensaxes en contextos políticos ou sociais sensibles.

Máis aló do hacktivismo, o sector financeiro continuou sendo un **obxectivo prioritario para o cibercrime**, especialmente en forma de **brechas de datos e ransomware**, dada a elevada concentración de información financeira e persoal. Aínda que a actividade de actores estatais foi minoritaria en termos cuantitativos, o informe sinala que este tipo de ameazas segue representando un **risco persistente**, en particular pola súa posible orientación á obtención de información estratéxica ou financeira.

Manufactura

O **sector manufactureiro**, aínda que cunha **proporción menor de incidentes (2,9** %**)**, experimentou un **ascenso relevante no ranking sectorial**, pasando a ocupar unha posición máis destacada entre os sectores NIS2. A maioría dos casos afectaron a

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

organizacións non identificadas, pero os subsectores de **defensa e automoción** mostraron unha exposición especialmente elevada.

As campañas hacktivistas, novamente vinculadas a contextos xeopolíticos, incluíron **ataques DDoS** e, nalgúns casos, **intentos de disrupción de sistemas de tecnoloxía operacional**, o que introduce un elemento de especial relevancia para entornos industriais.

No entanto, o **cibercrime** foi a principal ameaza para este sector, tanto en volume como en impacto, con **incidentes de ransomware** que provocaron **interrupcións prolongadas da continuidade de negocio**. Ademais, identificáronse **campañas de ciberespionaxe** de orixe estatal dirixidas a organizacións manufactureiras, presumiblemente orientadas ao **roubo de propiedade intelectual**.

3.4.2 Resumo de incidentes históricos en ICS/OT

Deseguido recompilamos **os incidentes máis relevantes da última anualidade completa no informe** (2024) recollidos no repositorio **de ICS Strive** [38][39]. Ao longo da mesma documentáronse numerosos incidentes con **consecuencias físicas, operativas e económicas tanxibles**, moitos deles en **Europa** e algúns con impacto directo en **España**, o que reforza a relevancia da análise para o contexto nacional.

Un dos **patróns máis claros en Europa** é a **afectación do sector transporte**, especialmente aeroportos, loxística e sistemas de mobilidade. En xaneiro, o **aeroporto de Split (Croacia)** e, posteriormente, outros aeroportos europeos sufriron ataques de ransomware que afectaron a sistemas críticos como o Flight Information Display System (FIDS), manexo de equipaxes e operacións de terra, obrigando a operar manualmente durante días. Ao longo do ano repetíronse incidentes similares en aeroportos e operadores loxísticos de **Italia, Alemaña, Bélxica, Suecia e Reino Unido**, confirmando que os sistemas IT que soportan operacións OT seguen sendo un vector prioritario.

Especial mención merece o **uso deliberado de interferencias GNSS (GPS jamming e spoofing)** en Europa do Leste e o Báltico. En marzo de 2024, interferencias prolongadas afectaron a **máis de 1.600 voos** sobre **Polonia, Suecia e Alemaña**, e forzaron a suspensión durante semanas da ruta Helsinqui–Tartu. Estes incidentes, atribuídos a actores estatais rusos, evidencian como **ataques de ciberseguridade e electromagnéticos híbridos** poden xerar impactos directos sobre a seguridade operacional sen necesidade de comprometer sistemas IT tradicionais.

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

No ámbito **industrial e manufactureiro europeo**, 2024 estivo marcado por unha sucesión de **ataques de ransomware con parada de produción**, particularmente en **Alemaña, Bélxica, Francia, Italia, Suecia, Finlandia e Austria**. Casos como **Varta, ThyssenKrupp Automotive Body Solutions, BerlinerLuft, LEMKEN, AKG Group, Peikko Group ou Smeg** mostran un patrón repetido: detección de compromiso en sistemas IT (ERP, SAP, servizos de directorio), illamento preventivo de redes e **paradas completas de plantas durante semanas**, con impacto directo en entregas, emprego temporal e resultados financeiros. Nalgúns casos, como **Schumag AG**, o incidente contribuíu a procesos de **reestruturación e bancarrota**, ilustrando o impacto sistémico do ciberataque máis aló do plano técnico.

O **sector agroalimentario e de bebidas** tamén sufriu impactos significativos en Europa. En **Bélxica, Suecia, Alemaña e España**, ataques de ransomware provocaron interrupcións de produción e distribución. Destaca especialmente o **caso do Matadoiro de Xixón (España)**, onde o grupo RansomHub afirmou acceder a sistemas **SCADA asociados ao tratamento de augas residuais**, o que obrigou a deter a actividade e enviar aos traballadores a casa en plena xornada. Aínda que a produción se renovou posteriormente en modo manual, o incidente representa un dos exemplos máis claros de **impacto directo sobre OT/ICS en territorio español** durante 2024.

No sector **enerxía e utilities**, aínda que menos numerosos, os incidentes observados foron especialmente sensibles. O caso **de Ignitis ON (Lituania)** evidenciou como a dependencia de **servizos cloud e aplicacións móbiles** pode traducirse en impactos físicos: unha intrusión en servizos SaaS deixou inutilizadas estacións de recarga eléctrica en todo o país durante horas. Noutros contextos europeos e limítrofes, ataques a sistemas de calefacción urbana, auga ou electricidade demostraron que a converxencia IT/OT segue sendo un punto crítico.

Finalmente, o repositorio recolle múltiples exemplos de **ataques a cadeas de subministración e provedores tecnolóxicos**, como **Microlise (Reino Unido)** ou **Blue Yonder**, cuxos incidentes se propagaron a clientes industriais, loxísticos e de distribución alimentaria en varios países. Estes casos reforzan a idea de que **o risco en entornos industriais non se limita á propia organización**, senón que se estende a ecosistemas completos de provedores, integradores e servizos xestionados.

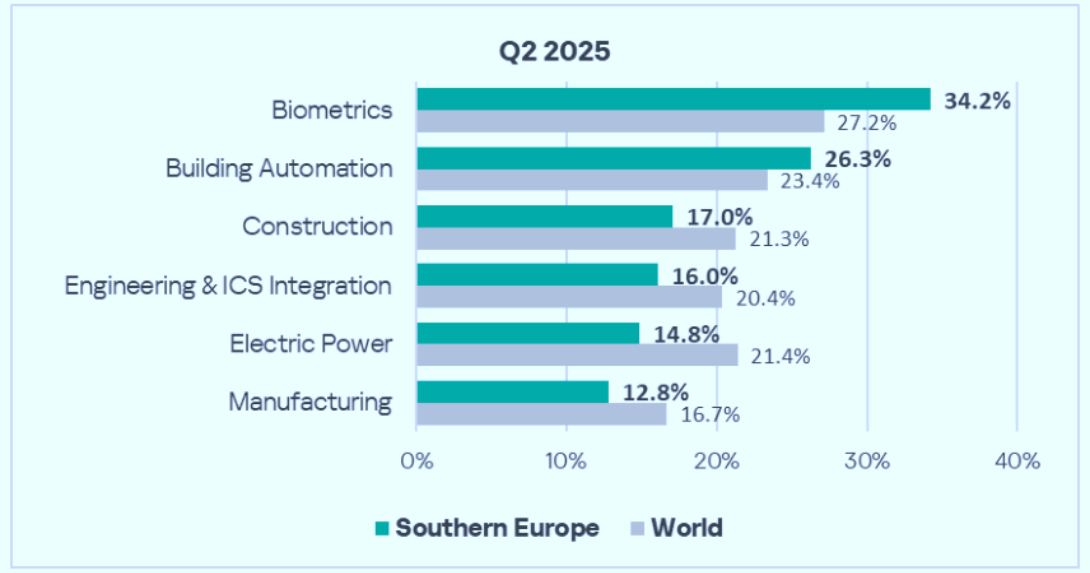
En conxunto, os incidentes documentados por ICS Strive en 2024 mostran que **Europa é un escenario activo de ciberincidentes con impacto OT**, dominados por ransomware, hacktivismo e, en determinados contextos, operacións de carácter estatal.

España, aínda que con menor volume, **non é allea a estas dinámicas**, e os casos observados confirman que a materialización do risco en sistemas industriais é xa unha realidade operativa e non un escenario hipotético

3.4.3 Ameazas en computadores ICS

Para complementar a análise de incidentes históricos e sectoriais, resulta especialmente relevante incorporar a perspectiva **de Kaspersky ICS-CERT**, que achega unha visión **telemetría-driven** centrada exclusivamente en **computadoras industriais** e non en incidentes corporativos xenerais. Esta aproximación permite observar **tendencias de afectación real en estacións de enxeñaría, HMIs, servidores SCADA e outros sistemas industriais**, independentemente de que o impacto final chegue ou non a materializarse nunha interrupción operativa.

O informe Threat Landscape for Industrial Automation Systems – Europe, Q2 2025 [40] ofrece unha fotografía detallada da situación durante o segundo trimestre de 2025, con especial interese para **Europa do Sur**, onde se observa unha **exposición sostida dos sistemas ICS a múltiples fontes de ameaza**. Neste contexto, o informe pon de relevo que as computadoras industriais continúan sendo comprometidas principalmente a través **de vectores herdados do entorno IT**, como malware xenérico, infeccións procedentes de medios extraíbles, accesos remotos inseguros ou movemento lateral desde redes corporativas, o que reforza a importancia da converxencia IT/OT na xestión do risco, unha vez máis.



Desglose de incidentes por sector en Europa do Sur. Fonte: Kaspersky (2025)

No caso do **Sur de Europa**, a análise evidencia que varios **sectores industriais manteñen niveis relevantes de sistemas ICS afectados**, con patróns consistentes ao longo do tempo. Este comportamento permite introducir unha **gráfica de tendencia de sectores afectados en computadoras ICS**, que ilustra como a exposición non é puntual nin episódica, senón estrutural, e afecta de xeito recorrente a determinados verticais industriais.

Tendencia de incidentes por sector en Europa do Sur. Fonte: Kaspersky (2025)

Adicionalmente, o estudio facilita unha análise cruzada moi visual entre **fontes de ameaza e categorías de malware por industria**, que resulta especialmente útil para comprender **que tipos de actores e técnicas predominan en cada sector**.

Threat source indicators for industries in Southern Europe, Q2 2025

Industry / Threat source	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in region
Internet	8.97%	8.81%	7.63%	8.11%	8.02%	5.08%	8.35%
Email clients	20.38%	13.80%	3.19%	4.51%	5.20%	3.29%	7.23%
Removable media	0.06%	0.10%	0.16%	0.09%	0.06%	0.14%	0.11%
Network folders	0.00%	0.03%	0.02%	0.02%	0.00%	0.00%	0.01%
Industry total in the region	34.23%	26.25%	14.84%	16.04%	17.04%	12.76%	

Mapa de calor de fontes de ameaza por industria en Europa do Sur. Fonte: Kaspersky (2025)

Estas visualizacións reforzan unha conclusión clave: **non todos os sectores están expostos aos mesmos tipos de ameazas**, e a natureza do malware que impacta en computadoras ICS varía significativamente segundo o entorno industrial.

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

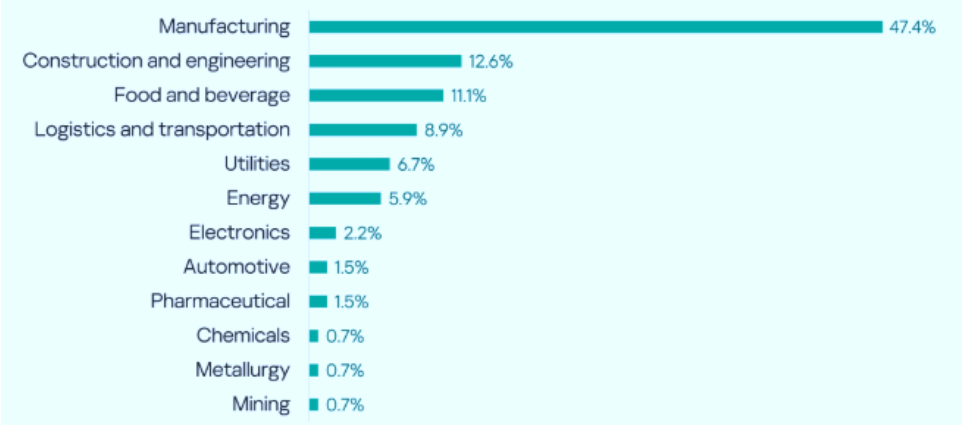
Threat category indicators for industries in Southern Europe, Q2 2025

Industry / Threat category	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in region
Denylisted internet resources	4.37%	4.25%	4.48%	4.41%	4.70%	2.89%	4.52%
Malicious scripts and phishing pages (JS and HTML)	16.91%	13.95%	5.31%	6.77%	6.53%	5.00%	8.78%
Spy Trojans, backdoors and keyloggers	18.15%	10.61%	2.39%	3.60%	3.21%	2.93%	5.88%
Worms	1.84%	1.14%	0.69%	0.54%	0.39%	0.68%	0.78%
Miners in the form of executable files for Windows	0.41%	0.27%	0.27%	0.25%	0.22%	0.25%	0.25%
Malicious documents (MSOffice + PDF)	12.25%	9.00%	1.81%	2.45%	2.99%	1.82%	4.39%
Viruses	0.43%	0.43%	0.31%	0.21%	0.44%	0.14%	0.31%
Ransomware	0.60%	0.33%	0.05%	0.08%	0.00%	0.18%	0.19%
Web miners running in browsers	0.31%	0.20%	0.22%	0.20%	0.06%	0.07%	0.19%
Malware for AutoCAD	0.04%	0.07%	0.02%	0.04%	0.39%	0.04%	0.06%
Industry total in the region	34.23%	26.25%	14.84%	16.04%	17.04%	12.76%	

Mapa de calor de indicadores de ameaza por industria en Europa do Sur. Fonte: Kaspersky (2025)

De xeito complementario, o informe A brief overview of the main incidents in industrial cybersecurity – Q2 2025 [41] achega unha **síntese dos principais incidentes coñecidos no ámbito industrial a nivel global**, novamente con foco en entornos OT/ICS. A diferenza do informe anterior, baseado en telemetría, este documento céntrase en **incidentes reportados e analizados**, ofrecendo unha visión máis próxima ao impacto operativo e organizativo.

O informe presenta, no seu parte superior, unha **distribución de incidentes por sector**, acompañada dunha **listaxe resumida dos casos máis relevantes**, o que permite contextualizar rapidamente que industrias concentran maior número de incidentes durante o período analizado (135 en total).



Distribución de incidentes por industria en Q2 2025. Fonte: Kaspersky (2025)

Mostra exemplo de incidentes en ICS en Q2 2025. Fonte: Kaspersky (2025)

Así mesmo, destacar que a **listaxe completa e detallada de incidentes do trimestre** recóllese ao final do estudio, para referencia posterior.

3.5 Vulnerabilidades ICS

Nesta sección, o primeiro que cabe destacar é que existen outros entregables do Observatorio de Ciberseguridade Industrial de AMTEGA relacionados especificamente con esta materia: *Informes de Ciberalertas*. Convídase o lector a consultalos [43].

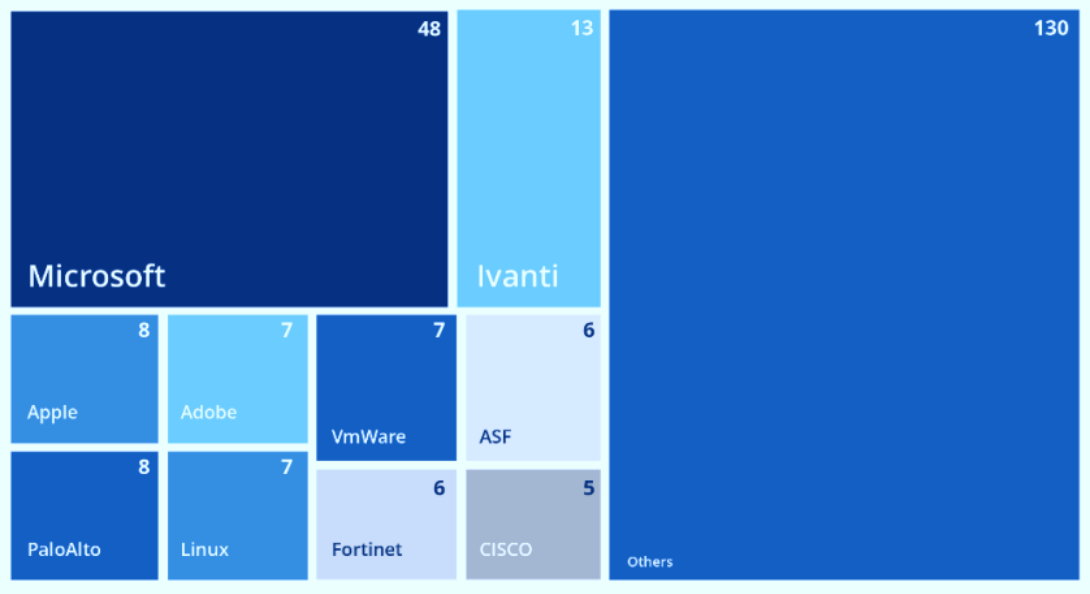
A análise de **vulnerabilidades** constitúe un eixo fundamental para comprender o **risco real** ao que se enfrontan os entornos industriais. A diferenza doutros ámbitos, en ICS/OT as vulnerabilidades non só teñen unha dimensión técnica, senón tamén operativa e de seguridade física, xa que a súa explotación pode traducirse en interrupcións prolongadas, degradación de procesos ou impactos sobre persoas e medio ambiente.

Contexto europeo

Desde unha perspectiva europea, o **ENISA Threat Landscape 2025** [34] dedica unha sección á análise de vulnerabilidades observadas con maior frecuencia en incidentes reais. O informe pon de relevo que unha parte substancial dos ataques apóiase en **vulnerabilidades incluídas en catálogos de explotación coñecida**, o que confirma que os atacantes priorizan fiabilidade e retorno fronte á complexidade técnica.

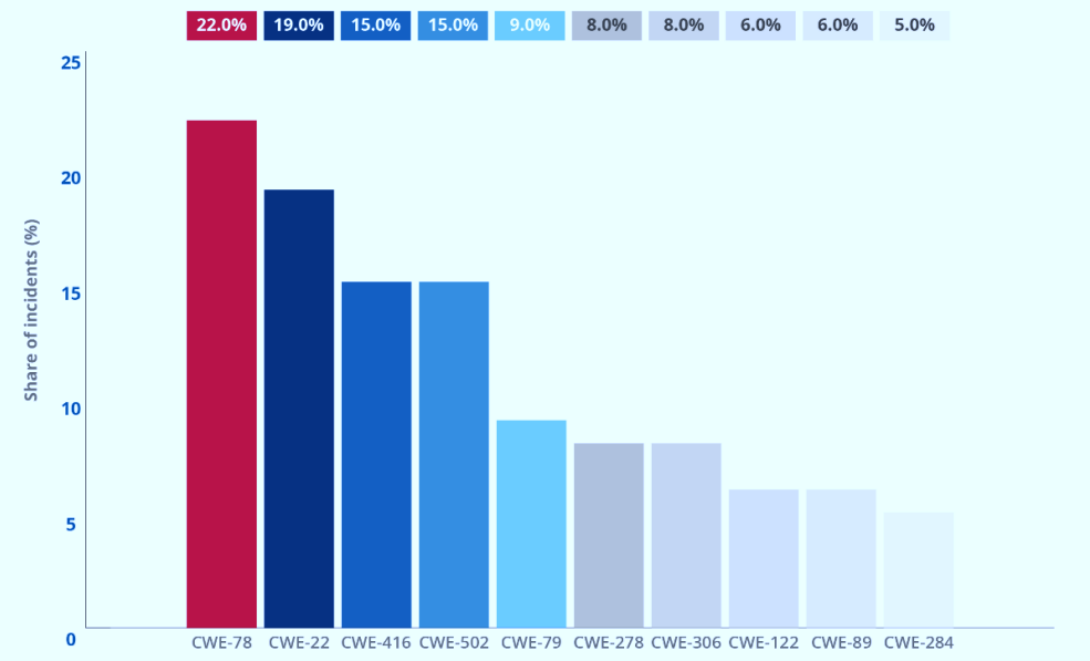
Entre as debilidades máis recorrentes atópanse fallos en produtos de uso transversal —incluídos dispositivos de rede, solucións de acceso remoto e software amplamente despregado— que actúan como portas de entrada cara a redes IT e, por extensión, cara a entornos OT mal segmentados. A seguinte figura recolle os fabricantes con máis vulnerabilidades máis presentes no catálogo KEV (vulnerabilidades mais explotadas) [44]:

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



Fabricantes predominantes no catálogo KEV. Fonte: ENISA (2025)

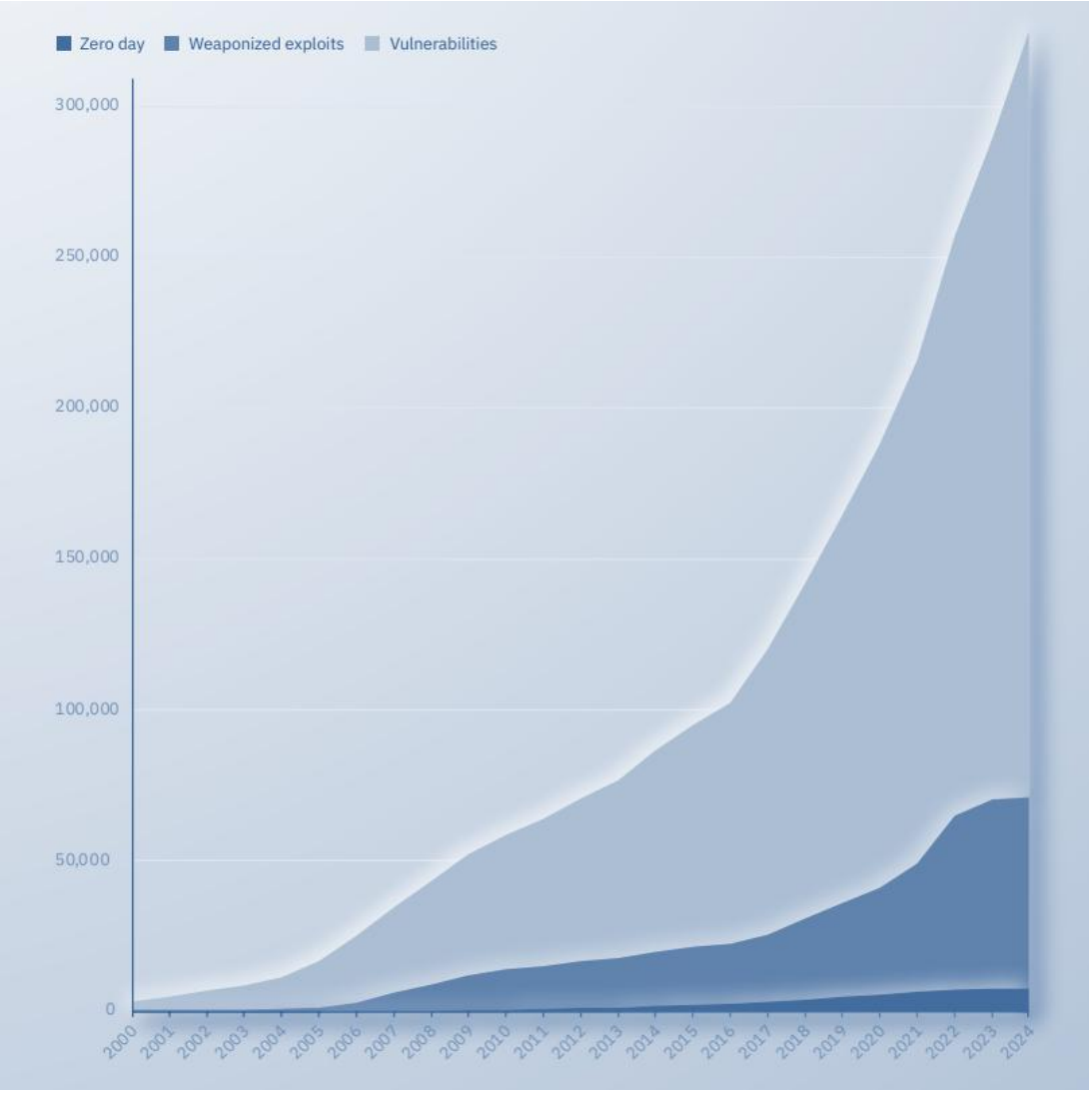
E as debilidades máis frecuentes que conducen a vulnerabilidades incorporadas ao catálogo das máis explotadas (KEV):



TOP 10 debilidades en vulnerabilidades presentes no catálogo KEV. Fonte: ENISA (2025)

Doutra banda e a nivel global, o reporte **IBM X-Force Threat Intelligence Index 2025** [32] reforza estas conclusións previas, ao analizar a relación entre o crecemento do número de vulnerabilidades, a dispoñibilidade de exploits e o aumento de zero-days explotados en entornos reais.

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



Medre de vulnerabilidades, exploits e zero days. Fonte: IBM X-Force (2025)

Destacan que o **éxito da explotación de vulnerabilidades** débese, en gran medida, á **rapidez** coa que os actores de ameaza incorporan **novos exploits** ás súas campañas.

O crecemento de vulnerabilidades, exploits e zero-days ilustra como o ecosistema ofensivo hase industrializado, reducindo drasticamente o tempo necesario para pasar da divulgación á explotación. Estas conclusión son plenamente aplicables a ICS/OT, onde a persistencia de sistemas legacy e a limitada visibilidade agravan o impacto potencial destas dinámicas.

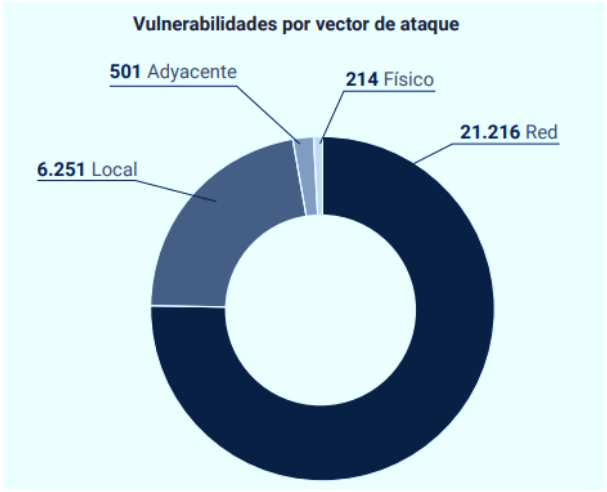
Panorama en España (CCN-CERT)

O informe do **CCN-CERT** [36] dedica un bloque específico á análise de vulnerabilidades de maneira xeral (IT/OT), no que se observa un incremento sostido tanto no número de vulnerabilidades publicadas como na súa explotación efectiva. Subliña que unha parte

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

significativa dos **incidentes graves** ten a súa orixe en **vulnerabilidades coñecidas**, para as que existen **parches dispoñibles** pero que permanecen sen corrixir durante longos períodos de tempo. Este fenómeno está estreitamente relacionado con problemas estruturais de xestión de parches, dependencias herdadas e limitacións operativas, especialmente visibles en entornos industriais.

A continuación, ilústrase como o maior volume de debilidades explótase vía rede:



Vulnerabilidades por vector de ataque. Fonte: CCN-CERT (2024)

Aínda que a sección detalla numerosas vulnerabilidades de carácter eminentemente IT, a mensaxe transversal é plenamente aplicable a ICS/OT: a **xanela de exposición** entre a divulgación dunha vulnerabilidade e a súa **explotación efectiva** está a reducirse de forma constante, mentres que os ciclos de actualización en entornos industriais seguen sendo longos e complexos.

Inclúense a continuación as debilidades máis frecuentes (CWE) [45] detectadas en conexión coas vulnerabilidades do gráfico anterior.

Identificador	Descripción
CWE-79	Sanitización incorrecta de entradas durante a xeración de páxinas web (*Cross-Site Scripting, XSS*).
CWE-89	Sanitización incorrecta de elementos especiais empregados en comandos SQL (*SQL Injection*).
CWE-78	Sanitización incorrecta de elementos especiais empregados en comandos do sistema operativo (*OS Command Injection*).
CWE-77	Sanitización indebida de elementos especiais empregados en comandos (*Command Injection*).

CWE-787	Escritura fóra dos límites da memoria (*Out-of-bounds Write*).
CWE-125	Lectura fóra dos límites da memoria (*Out-of-bounds Read*).
CWE-120	Copia de búfer sen comprobación do tamaño da entrada (*Classic Buffer Overflow*).
CWE-121	Desbordamento de búfer baseado en pila (*Stack-based Buffer Overflow*).
CWE-190	Desbordamento ou evoltura de enteiros (*Integer Overflow or Wraparound*).
CWE-352	Falsificación de peticións en sitios cruzados (*Cross-Site Request Forgery, CSRF*).
CWE-434	Carga sen restricións de arquivos de tipo perigoso.
CWE-22	Limitación incorrecta dun nome de ruta a un directorio restrinxido (*Path Traversal*).
CWE-502	Deserialización de datos non fiables.
CWE-287	Autenticación incorrecta.
CWE-862	Falta de autorización.
CWE-798	Uso de credenciais codificadas (*Hard-coded Credentials*).
CWE-918	Falsificación de peticións do lado do servidor (*Server-Side Request Forgery, SSRF*).
CWE-94	Control inadecuado da xeración de código (*Code Injection*).

Informe especializado

O **Dragos 2025 OT Cybersecurity Report – A Year in Review** [30] ofrece unha visión especificamente centrada en OT, achegando un nivel de detalle especialmente relevante para entornos ICS.

Subliña que os **sistemas industriais non foron concibidos con criterios de ciberseguridade**, o que segue xerando un caldo de cultivo favorable para os adversarios. Neste contexto, Dragos salienta que a xestión do risco en ICS debe ir máis aló do parcheo puntual, incorporando unha comprensión profunda de como estas debilidades poden ser explotadas e mitigadas antes de que deriven en impactos operativos.

Un dos eixos máis relevantes do informe é a **investigación sobre protocolos fieldbus**, en particular ao redor **de CANopen implementado en servoaccionamentos**. Dragos identifica riscos significativos asociados a protocolos industriais **encapsulados en capas sucesivas**, aos que denomina "*Turducken protocols*". Estes esquemas, nos que protocolos como Modbus-RTU poden viaxar encapsulados sobre CANopen e, á súa vez, dentro de protocolos propietarios ou mesmo sobre Modbus/TCP, **reducen drasticamente a visibilidade e a capacidade de detección de ataques**. A complexidade aparente destas pilas non supón unha barreira real para atacantes avanzados, pero si para moitas solucións defensivas tradicionais.

Dragos considera que **gran parte do equipamento fieldbus é inseguro por deseño**, e que moitas das debilidades identificadas non sempre se traducen en CVE formais. Con todo, isto non reduce a súa relevancia desde un punto de vista operativo: a manipulación non autorizada de parámetros, mesmo por erro, pode provocar desviacións de proceso ou interrupcións graves. O informe destaca que estas arquitecturas, con funcionalidades pouco documentadas e comportamentos non estandarizados, **dificultan enormemente a creación de analíticas de rede fiables**, reforzando a necesidade de desenvolver *disectores* capaces de desentrañar cada capa do protocolo.

Constatan que este tipo de exposicións non é teórico, senón que afecta a **modelos concretos de PLC amplamente despregados**, incluídos sistemas de Rockwell Automation con módulos HART e controladores de Schneider Electric baseados en CODESYS e CANopen. Nestes casos, Dragos sinala que existen **medidas de mitigación viables desde a propia lóxica de control**, como a monitorización de parámetros sensibles e a execución de paradas seguras ante cambios fóra de banda, o que reforza a idea de que a defensa en OT debe apoiarse tamén no propio proceso.

O informe dedica así mesmo un bloque específico ao **uso de equipamento IoT en entornos industriais**, alertando de que estes dispositivos continúan sendo un dos elos máis débiles. Documéntase a explotación recente de vulnerabilidades en IoT para a propagación de variantes da **botnet Mirai**, capaz de comprometer miles de dispositivos mediante mecanismos automatizados. A raíz do problema reside en que gran parte destes equipos executan sistemas GNU/Linux pouco bastionados, con servizos como TELNET ou SSH expostos por defecto e fallos triviais de autenticación ou inxección de comandos.

Aínda que estes sistemas non sempre controlan directamente a produción, Dragos recalca que **infraestruturas auxiliares como HVAC, iluminación, control de accesos**

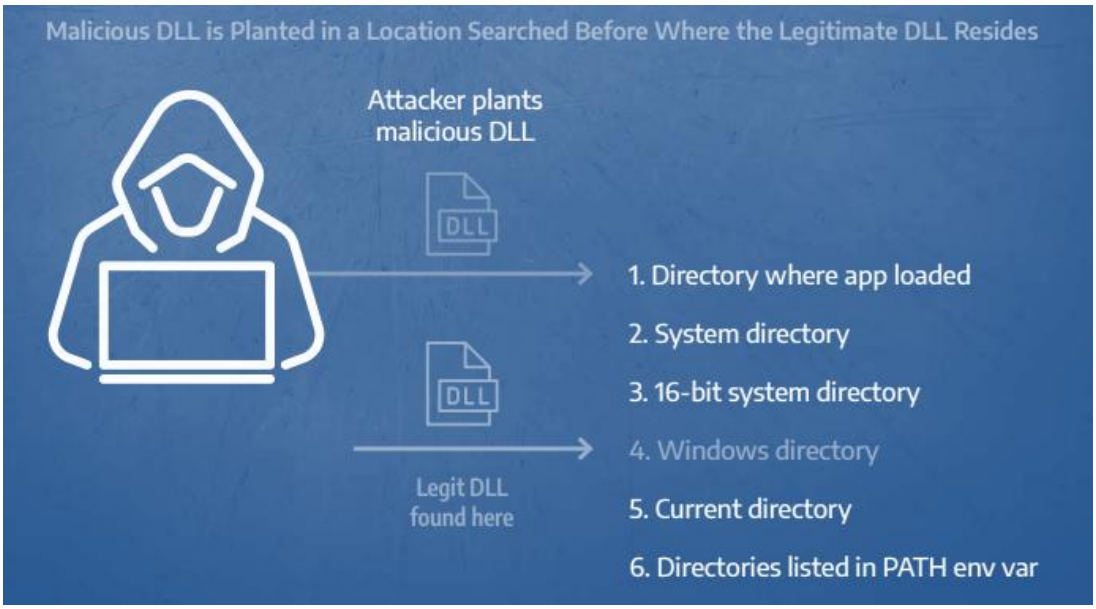
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · Xacobeo 2027

ou seguridade física deben considerarse parte integral do proceso industrial. A indisponibilidad de calquera destes sistemas pode forzar a parada da produción, especialmente en sectores regulados como o farmacéutico ou o alimentario. Neste sentido, o informe recomenda tratar o hardware IoT industrial como activos críticos, reforzando controis básicos como a eliminación de credenciais por defecto, a restrición de accesos de xestión e a planificación de procedementos manuais de continxencia.

Outro aspecto destacado é a **exposición derivada do uso de ferramentas de dobre uso**. Analizan o caso do toolkit *IoT Exploit*, unha plataforma pública que agrupa centos de exploits contra dispositivos IoT e OT. Aínda que non se observou o seu uso malicioso directo na telemetría de Dragos, o informe advirte de que este tipo de ferramentas, deseñadas inicialmente para investigación ou *rede teaming*, **tenden a incorporarse con rapidez a arsenais ofensivos automatizados**, reducindo o limiar técnico necesario para explotar vulnerabilidades en entornos industriais.

O informe tamén pon o foco nos **riscos asociados a compoñentes de terceiros e á cadea de subministración**, sinalando que preto dunha quinta parte dos avisos analizados en 2024 estaban relacionados con vulnerabilidades en compoñentes externos integrados en produtos OT. Mesmo cando un fabricante mantén o seu produto actualizado, a presenza de librarías ou sistemas de terceiros sen parchear pode introducir **vías indirectas de compromiso**, como ilustra o exemplo do uso de PAN-VOS como compoñente integrado en dispositivos industriais. Subliñan a importancia de iniciativas como o **SBOM** para mellorar a visibilidade e acelerar a resposta ante este tipo de exposicións.

Finalmente, o informe dedica unha atención especial a un problema persistente en software industrial: o **DLL hijacking**. Dragos identifica máis dun centenar de vulnerabilidades deste tipo en aplicacións OT, considerándoas “low-hanging fruit” ou presa fácil, pola súa facilidade de explotación e versatilidade. Estas técnicas permiten desde acceso inicial até escalada de privilexios ou persistencia, e foron empregadas historicamente por actores estatais e grupos APT en campañas contra sectores industriais críticos. Dragos recomenda aos operadores industriais **buscar activamente este tipo de debilidades** e aplicar mitigacións técnicas ben coñecidas, así como insta aos fabricantes OT a adoptar boas prácticas de desenvolvemento seguro para reducir o seu recurrencia. A continuación, unha explicación visual da ameaza:



DLL hijacking. Fonte: Dragos (2025)

En conxunto, Dragos transmite unha mensaxe clara: as vulnerabilidades en entornos ICS non son un problema marxinal nin exclusivamente técnico, senón un **risco estrutural ligado ao deseño, a integración e a operación dos sistemas industriais**, que require enfoques de mitigación pragmáticos, continuos e aliñados coa realidade operativa.

Neste sentido, os recursos recompilados de forma sistemática nos **Informes de Ciberalertas do Observatorio** proporcionan unha visión consolidada e redundada de avisos, CVE e alertas específicas de fabricantes e organismos de referencia, facilitando a toma de decisións informadas nun contexto operativo realista. Para referencia rápida, estes son recursos de especial interese [46][47][48][49].

4 Conclusións

Este informe abordou de maneira integral a evolución recente do **panorama de ameazas de ciberseguridade sobre entornos OT/ICS**, extraendo patróns, ameazas emerxentes, vectores de ataque e vulnerabilidades crave a partir de fontes nacionais, europeas e internacionais. A través da análise de **fontes nacionais e internacionais públicas e privadas**, identificáronse as principais áreas de exposición para infraestruturas críticas e sectores industriais.

O informe comezou establecendo un **marco teórico sobre que é a intelixencia de ameazas**, os seus obxectivos, ciclo de vida e niveis (**estratéxico, operacional e táctico**). Tamén se describiron as **fontes que nutren esta intelixencia** (fontes abertas, compartidas, privadas ou técnicas) e como **articular un programa eficaz** en organizacións con sistemas industriais.

A continuación, contextualizouse o **estado actual da intelixencia de ameazas a nivel global, europeo e nacional**. Revisáronse as principais iniciativas de coordinación públicas, así como os informes dalgúns dos principais fabricantes do sector.

O **emprego de Intelixencia Artificial por parte dos adversarios** representa outro vector emerxente. Evidenciouse o seu emprego tanto na **automatización de ataques** (por exemplo, xeración de malware ou evasión de EDR) como na **fabricación de contido de phishing personalizado**. A sofisticación destas ferramentas expón **novos retos para os operadores OT**, que deben considerar escenarios de compromiso en tempos cada vez máis reducidos.

En materia de **vulnerabilidades**, observouse unha alta concentración en **debilidades clásicas como desbordamentos de búfer, execución de código remoto ou fallos de autenticación**. Particularmente preocupantes son os entornos con **protocolos herdados ou dispositivos imposibles de parchear**. **Dragos e outros informes** subliñan a necesidade de compaxinar a **xestión de vulnerabilidades con outras estratexias** como segmentación, detección por comportamento e visibilidade granular.

Podemos concluír que as **perspectivas futuras** apuntan a un **incremento sostido das ameazas sobre infraestruturas OT**, impulsadas por:

- **Maior conectividade** entre sistemas IT/OT e cloud.
- **Aparición de malware** específico para entornos industriais.

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

- **Adopción masiva de IA** tanto en defensa como en ataque.
- **Tensións xeopolíticas** que transforman o ciberespazo nun campo de confrontación indirecta.

Neste contexto, dispor de **capacidades propias de vixilancia, detección e resposta adaptadas ós entornos industriais** non é unha opción, senón unha necesidade urxente.

Como se indicou, **a análise de actores de amenaza e técnicas, tácticas e procedementos específicos, a construción de fontes de intelixencia propia e mailas pertinentes recomendacións** de organismos e entidades internacionais para protexerse fronte a estas ameazas, **serán obxecto dun informe posterior.**

Este conxunto de informes sentará as bases para unha **estratexia de defensa de ciberseguridade máis robusta, informada por intelixencia, e centrada na protección de procesos esenciais para a sociedade e a economía**.

Todo iso **axuda ás organizacións de Galicia a avanzar cara a unha xestión máis madura do risco en OT**, apoiándose en información accionable e en aliñación con estándar e recomendacións das principais fontes a nivel global.

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

Bibliografía

[1] Dahj, J. N. M. (2022). *Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense.* Packt Publishing.

[2] Blair, R. (2023). *Aligning Security Operations with the MITRE ATT&CK Framework: Level up your security operations center for better security*. Packt Publishing.

[3] Escola Tecnolóxica Daferra (2023). *Materiais Bootcamp Ciberseguridade Técnica.* Non publicado.

[4] Maltego (2008). *Maltego OSINT and link analysis tool*. Recuperado de https://www.maltego.com

[5] Shodan (2009). *Shodan: The search engine for the Internet of Things*. Recuperado de https://www.shodan.io

[6] SpiderFoot (2020). *SpiderFoot – Open Source Intelligence Automation*. Recuperado de https://github.com/smicallef/spiderfoot

[7] Hunchly (2015). *Hunchly – Web Capture Tool for Online Investigations*. Recuperado de https://www.hunch.ly

[8] Anonymox (2024). *Anonymox – Online Privacy Extension*. Recuperado de https://www.anonymox.net

[9] Snort (1998). *Snort – Network Intrusion Detection & Prevention System*. Recuperado de https://www.snort.org

[10] Suricata (2007). *Suricata – Threat Detection Engine*. Recuperado de https://suricata.io

[11] Wireshark Foundation (1998). *Wireshark – Network Protocol Analyzer*. Recuperado de https://www.wireshark.org

[12] Zeek (1998). *Zeek Network Security Monitor*. Recuperado de https://zeek.org

[13] Arkime Project (2012). *Arkime – Full Packet Capture and Indexing System*. Recuperado de https://arkime.com

[14] Cisco (n.d.). *Cisco NetFlow – Network Traffic Monitoring*. Recuperado de https://www.cisco.com/go/netflow

[15] sFlow.org (2003). *sFlow – Real-time Network Visibility Technology*. Recuperado de https://sflow.org

[16] Recorded Future (2009). *Recorded Future Threat Intelligence Platform*. Recuperado de https://www.recordedfuture.com

[17] FireEye (2004). *FireEye Threat Intelligence*. Recuperado de https://www.trellix.com/es-es/

[18] AT&T Cybersecurity (2007). *Open Threat Exchange (OTX)*. Recuperado de https://otx.alienvault.com

[19] MISP Project (2011). *MISP – Malware Information Sharing Platform & Threat Sharing*. Recuperado de https://www.misp-project.org

[20] CISA (2018). *Cybersecurity and Infrastructure Security Agency – Alerts & Publications*. Recuperado de https://www.cisa.gov

[21] ENISA (2004). *European Union Agency for Cybersecurity – Publications*. Recuperado de https://www.enisa.europa.eu/publications

[22] MITRE Corporation (2015). *MITRE ATT&CK – Adversary Tactics and Techniques*. Recuperado de https://attack.mitre.org

[23] MITRE Corporation (2020). *MITRE ATT&CK for ICS – Techniques and Tactics for Industrial Control Systems*. Recuperado de https://attack.mitre.org/matrices/ics

[24] Anomali (2013). *Anomali ThreatStream – Threat Intelligence Platform*. Recuperado de https://www.anomali.com/products/threatstream

[25] ThreatConnect (2011). *ThreatConnect Threat Intelligence Platform*. Recuperado de https://threatconnect.com

[26] Unión Europea (2016). *Regulamento Xeral de Protección de Datos (GDPR)*. Recuperado de https://eur-lex.europa.eu/eli/reg/2016/679

[27] Unión Europea (2002, enmendada en 2009). *Directiva sobre privacidade e comunicacións electrónicas (ePrivacy)*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32002L0058

[28] Estado de California (2018). *California Consumer Privacy Act (CCPA)*. Recuperado de https://oag.ca.gov/privacy/ccpa

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

[30] Dragos (2025). *2025 OT Cybersecurity Year in Review*. Recuperado de https://www.dragos.com/ot-cybersecurity-year-in-review

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

[32] IBM X-Force (2025). *Threat Intelligence Index 2025*. Recuperado de https://www.ibm.com/es-es/reports/threat-intelligence

[33] Palo Alto Networks (2025). *Global Incident Response Report 2025*. Recuperado de https://www.paloaltonetworks.com/resources/research/2025-incident-response-report

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

[35] CrowdStrike (2025). *European Threat Landscape Report 2025*. Recuperado de https://www.crowdstrike.com/explore/crowdstrike-content-es/crowdstrike-2025-threat-landscape-es-ES?

[36] CCN-CERT (2024). *IA-04/24 Ciberameazas e Tendencias 2024*. Recuperado de https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html

[37] Google Threat Intelligence Group.(2025). *Threat actor usage of AI tools*. *Google Cloud Blog.* Disponible en: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools

[38] ICS Strive (2025). *2025 OT Cyber Threat Report*. Recuperado de: https://icsstrive.com/editorials/2025-ot-cyber-threat-report/

[39] ICS Strive (2025). *ICS Incident Database*. Recuperado de: https://icsstrive.com/incident/

[40] Kaspersky ICS CERT (2025). *Threat Landscape for Industrial Automation Systems in Europe – Q2 2025*. Recuperado de: https://ics-cert.kaspersky.com/publications/reports/2025/09/23/threat-landscape-for-industrial-automation-systems-europe-q2-2025/

[41] Kaspersky ICS CERT (2025). *A brief overview of the main incidents in industrial cybersecurity – Q2 2025*. Recuperado de: https://ics-cert.kaspersky.com/publications/reports/2025/10/09/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q2-2025/

[42] Unión Europea (2022). *Directiva (UE) 2022/2555 (NIS2) relativa a medidas para un alto nivel común de ciberseguridade na Unión*. Recuperado de: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

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

[44] CISA (2020). *Known Exploited Vulnerabilities Catalog (KEV)*. Recuperado de https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[45] MITRE (2006). *CWE — Common Weakness Enumeration*. Recuperado de https://cwe.mitre.org/

[46] INCIBE-CERT (2025). *Avisos de Seguridade en Sistemas de Control Industrial (SCI) — Alerta Temperá*. Recuperado de https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci

[47] CCN-CERT (2025). *Alertas CCN-CERT — Seguridade ó día*. Recuperado de https://www.ccn-cert.cni.es/es/seguridad-al-dia/alertas-ccn-cert.html

[48] CCN-CERT (2025). *Vulnerabilidades — Seguridad ó día*. Recuperado de https://www.ccn-cert.cni.es/es/seguridad-al-dia/vulnerabilidades.html

[49] CISA (2025). *ICS Advisories — Industrial Control Systems Security Alerts*. Recuperado de https://www.cisa.gov/news-events/ics-advisories

Glosario

APT (Advanced Persistent Threat / Ameaza Persistente Avanzada)

Grupo de ataque altamente sofisticado, normalmente asociado a estados-nación, con obxectivos estratéxicos a longo prazo e capacidade de manter presenza prolongada nas redes vítimas.

BYOVD (Bring Your Own Vulnerable Driver)

Técnica na que o atacante introduce un controlador vulnerable no sistema para escalar privilexios ou evadir defensas de seguridade.

CISA (Cybersecurity and Infrastructure Security Agency)

Axencia de ciberseguridade de EE. UU., centrada en protexer infraestruturas críticas fronte a ameazas de ciberseguridade.

CPS (Cyber-Physical Systems / Sistemas Ciberfísicos)

Sistemas que integran compoñentes computacionais con procesos físicos, como sensores e actuadores, típicos en entornos industriais.

CVE (Common Vulnerabilities and Exposures)

Identificador único asignado a unha vulnerabilidade coñecida, que facilita a súa referencia estandarizada e xestión en produtos e sistemas.

CWE (Common Weakness Enumeration)

Clasificación de debilidades comúns en software que poden derivar en vulnerabilidades explotables.

DLL (Dynamic Link Library)

Biblioteca de código compartido que pode ser cargada en tempo de execución por diferentes programas en sistemas Windows.

EDR (Endpoint Detection and Response)

Solución de seguridade que monitoriza dispositivos finais (endpoints) para detectar, rexistrar e responder a ameazas.

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

ENISA (European Union Agency for Cybersecurity)

Axencia da UE encargada de reforzar a ciberseguridade a nivel europeo mediante políticas, normativas e análises técnicas.

GDPR (Xeral Data Protection Regulation / Regulamento Xeral de Protección de Datos)

Regulación europea que establece directrices para a protección de datos persoais e privacidade na UE.

HART (Highway Addressable Remote Transducer)

Protocolo de comunicación utilizado en instrumentación de procesos industriais para configurar e obter datos de campo.

HIDS (Host-based Intrusion Detection System)

Sistema de detección de intrusións que opera directamente sobre un dispositivo monitorizando a súa actividade.

HMI (Human-Machine Interface)

Interfaz gráfica ou física que permite aos operadores humanos interactuar cos sistemas de control industrial.

ICS (Industrial Control Systems / Sistemas de Control Industrial)

Conxunto de tecnoloxías utilizadas para supervisar, controlar e automatizar procesos industriais.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)

Equipo especializado en dar resposta a incidentes de ciberseguridade que afectan a sistemas de control industrial.

ICS-CSIRT (ICS Computer Security Incident Response Team)

Comunidade e centro de coordinación para o intercambio de información sobre ameazas e vulnerabilidades en entornos OT.

IDS (Intrusion Detection System)

Sistema deseñado para identificar accesos non autorizados ou actividades maliciosas en redes e sistemas.

IIoT (Industrial Internet of Things)

Ecosistema de dispositivos interconectados en entornos industriais que permiten colleitar e transmitir datos operativos.

IoC (Indicator of Compromise / Indicador de Compromiso)

Proba técnica que suxire que un sistema pode ser comprometido, como unha dirección IP maliciosa ou un arquivo sospeitoso.

IoT (Internet of Things)

Rede de dispositivos físicos conectados a internet que recompilan, transmiten e actúan sobre datos do entorno.

KEV (Known Exploited Vulnerabilities)

Listaxe mantida de vulnerabilidades que se sabe están a ser activamente explotadas no mundo real.

LLM (Large Language Model / Modelo de Linguaxe de Gran Escala)

Modelo de intelixencia artificial adestrado con grandes volumes de texto para xerar, resumir ou responder en linguaxe natural.

MFA (Multi-Factor Authentication / Autenticación Multifactor)

Método de verificación de identidade que require polo menos dous factores: algo que se sabe, que se ten ou que se é.

MISP (Malware Information Sharing Platform)

Plataforma de código aberto para o intercambio estruturado de indicadores de ameaza entre organizacións.

MITRE ATT&CK

Base de coñecemento que recolle tácticas, técnicas e procedementos (TTP) utilizados por actores maliciosos en diferentes etapas dun ataque.

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

MITRE D3FEND

Marco de coñecemento complementario ao ATT&CK, centrado en documentar contramedidas defensivas ante ameazas de ciberseguridade.

NIS2 (Network and Information Security Directive 2)

Directiva europea que reforza os requisitos de ciberseguridade para sectores críticos, ampliando o seu alcance e obrigacións.

OpenCTI (Open Cyber Threat Intelligence)

Plataforma de código aberto para almacenar, visualizar e compartir intelixencia de ameazas de forma estruturada e contextual.

OT (Operational Technology / Tecnoloxías de Operación)

Sistemas e dispositivos utilizados para controlar procesos físicos en entornos industriais. Priorizan dispoñibilidade, seguridade física e continuidade de operación.

PLC (Programmable Logic Controller)

Dispositivo electrónico programable que executa tarefas de control automático en procesos industriais.

RTU (Remote Terminal Unit)

Unidade remota que recompila datos de sensores e transmite ordes a actuadores en sistemas distribuídos como SCADA.

SBOM (Software Bill of Materials)

Lista detallada de todos os compoñentes de software que forman parte dunha aplicación ou sistema, clave para a xestión de riscos.

SCADA (Supervisory Control and Data Acquisition)

Sistema que permite a supervisión e o control remoto de procesos industriais mediante a recompilación de datos e envío de comandos.

SIEM (Security Information and Event Management)

Solución que centraliza eventos de seguridade para a súa análise, correlación e xeración de alertas en tempo real.

SOC (Security Operations Center)

Centro especializado na monitorización, análise e resposta ante incidentes de ciberseguridade dunha organización.

TTP (Tactics, Techniques and Procedures)

Conxunto de patróns de comportamento e métodos empregados por actores maliciosos para alcanzar os seus obxectivos.

USB (Universal Serial Bus)

Estándar industrial para a conexión de dispositivos periféricos a un computador ou outros sistemas dixitais.

VPN (Virtual Private Network)

Tecnoloxía que permite crear unha conexión segura e cifrada sobre unha rede pública para protexer a transmisión de datos.

WMI (Windows Management Instrumentation)

Conxunto de ferramentas de Microsoft para a administración e monitoreo de sistemas operativos e dispositivos en rede.

XSS (Cross-Site Scripting)

Vulnerabilidade que permite inxectar código malicioso en páxinas web vistas por outros usuarios, comprometendo a súa seguridade.

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

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial
Informe de Intelixencia de Ameazas - I

AMTEGA – Xunta de Galicia 2026

Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Xacobeo 2027