CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Informe de Inteligencia de Amenazas - I

Febrero 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

Agencia para la Modernización Tecnológica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Año: 2026

Índice

1 Introducción

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

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

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

--

La creciente complejidad del **ecosistema de amenazas que impacta en los sistemas industriales y a las infraestructuras críticas** exige a las organizaciones disponer de capacidades de análisis que integren tendencias globales, europeas y nacionales, así como evidencias tácticas observables. En este contexto, este *Informe de Inteligencia de Amenazas del Observatorio de Ciberseguridad Industrial* se concibe como un documento orientado a traducir la evolución del escenario internacional en implicaciones reales y prácticas para organizaciones con entornos OT/ICS.

El propósito fundamental del informe es ofrecer **inteligencia accionable**, apoyada en fuentes nacionales e internacionales, en patrones emergentes vinculados a actores estatales, ciberdelincuencia organizada y hacktivismo, y potencialmente a futuro en telemetría propia obtenida a través de los **honeypots OT desplegados por AMTEGA**, que constituyen un aporte cercano en la observación directa de tendencias y comportamientos hostiles. Abarca amenazas que afectan o pueden afectar a entornos industriales y las infraestructuras 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 basado en información con carácter global debido a la inexistencia de fuentes específicas en Galicia, el riesgo es plenamente aplicable debido al carácter remoto y en gran medida transfronterizo de la mayoría de ataques a entornos ICS/OT.

El documento se dirige a responsables de ciberseguridad, equipos SOC/CSIRT, perfiles técnicos y operativos, administraciones públicas y responsables de riesgo que requieran una visión del panorama de amenazas y de sus implicaciones. Su relevancia se refuerza ante un entorno caracterizado por la proliferación **de ransomware industrial**, la aparición **de malware ICS específico**, la intensificación de actividades de **actores estatales**, **y la explotación sistemática de vulnerabilidades** en productos de fabricantes de equipo OT, en un escenario de máxima incertidumbre por la situación geopolítica mundial y **la proliferación de la IA**.

La estructura del informe se desarrolla de manera orgánica, iniciando con una introducción conceptual y continuando con un resumen ejecutivo que sintetiza indicadores clave, riesgos y recomendaciones estratégicas. El bloque central presenta el análisis de Threat Intelligence, que integra un marco teórico de ciberinteligencia y construcción de programas asociados, visión global de algunos de los principales fabricantes, europea y nacional, uso de IA por adversarios, incidentes y campañas recientes, vulnerabilidades ICS, actores de amenaza y TTPs basados en MITRE, seguido de conclusiones que resumen el contenido y proyectan la evolución previsible del panorama, cerrando finalmente con la recopilación bibliográfica de fuentes y un glosario de términos empleados.

En futuras ediciones, se trabajarán otros aspectos como por ejemplo construir información de inteligencia propia para un SOC interno, o un conjunto de recomendaciones operativas y estratégicas.

Este Informe de Inteligencia se articula como **pieza complementaria y evolutiva del Informe de Ciberalertas del Observatorio**, ampliando su alcance más allá del análisis táctico *de advisories y* vulnerabilidades para ofrecer una lectura estratégica y contextualizada del panorama de amenazas. Mientras el Informe de Ciberalertas se focaliza en la monitorización continua de fallos críticos, avisos de fabricantes y vulnerabilidades explotables —aportando un seguimiento inmediato y orientado a la acción técnica— este documento adopta una perspectiva más amplia, integrando tendencias, actores, motivaciones y patrones de actividad que permiten entender no sólo *qué* ocurre, sino *por qué ocurre* y *cómo podría evolucionar*.

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

El informe aspira a consolidarse como un recurso **riguroso, útil y orientado a la toma de decisiones**, que no sólo describe el estado del panorama de amenazas, sino que permite anticipar comportamientos, detectar puntos débiles y priorizar esfuerzos defensivos. De esta forma, se refuerza la capacidad de análisis del Observatorio, proporcionando una visión más completa e integrada que fortalece la **anticipación, la preparación y la resiliencia** del ecosistema industrial gallego.

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

2 Resumen ejecutivo

Esta sección pretende dotar **a los responsables de seguridad, gestores industriales y decisores estratégicos de una visión sintética y práctica del estado de las amenazas y las principales líneas de actuación defensiva a corto y medio plazo.**

El informe proporciona una radiografía actualizada del **panorama de amenazas sobre entornos industriales** a partir de múltiples fuentes globales, europeas y nacionales. En un contexto de creciente digitalización de procesos críticos, los ciberataques a infraestructuras OT escalaron en número, sofisticación y daño potencial.

A nivel global, se observa una clara intensificación del interés de **grupos patrocinados por Estados** (especialmente Rusia, China, Irán y Corea del Norte) sobre sectores industriales estratégicos. En paralelo, el **cibercrimen organizado y el hacktivismo ideológico** han sofisticado sus herramientas, destacando el uso de ransomware, campañas DDoS coordinadas y malware dirigido a dispositivos industriales. Europa ha registrado un **incremento de incidentes en sectores como la administración pública, el transporte y la energía**, con especial afectación a sistemas de supervisión y automatización.

Entre los indicadores clave destacan:

- La explotación de **servicios expuestos y uso de credenciales válidas** como vectores de acceso inicial más frecuentes. En 2024, ambos métodos representaron el 30% de los accesos comprometidos según X-Force.
- Una alta prevalencia de **vulnerabilidades no parcheables** en dispositivos OT, obligando a estrategias alternativas como segmentación o detección basada en comportamiento.
- La adopción generalizada de **técnicas de Inteligencia Artificial** por parte de los atacantes para mejorar sus campañas. Microsoft detectó más de 20 grupos de amenazas utilizando herramientas generativas para phishing, desinformación y scripting automatizado.
- Un entorno con **baja visibilidad y escasa compartición de inteligencia técnica** sobre amenazas OT, donde todavía predomina una 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

Estos factores generan **riesgos estratégicos** para la continuidad operativa, la seguridad física y el cumplimiento regulatorio. Por ejemplo, el impacto económico medio de un incidente en sistemas OT alcanza los **3,5 millones de dólares**, sin considerar el coste reputacional o las sanciones legales derivadas del RGPD o la NIS2.

Las organizaciones industriales **deben prepararse para afrontar escenarios de intrusión persistente, degradación progresiva de servicios y presión geopolítica** a través del ciberespacio.

A lo largo del informe se propone una serie de **recomendaciones**, entre las que destacan:

- **Formar equipos mixtos IT/OT**, promoviendo la convergencia de competencias.
- **No descuidar el factor humano** (políticas, procedimientos, formación y concienciación).
- **Segmentar y proteger** redes OT siguiendo modelos de defensa en profundidad.
- **Fortalecer la gestión de identidades**, eliminando credenciales por defecto y aplicando MFA donde sea viable.
- Controlar debidamente **la cadena de suministro**.

En futuras ediciones del informe, se pondrá el foco en aspectos adicionales de valor para el ecosistema gallego, como pueden ser:

- **Construir capacidades propias de inteligencia de amenazas**, apoyadas en plataformas como MISP u OpenCTI.
- **Adoptar marcos de ciberresiliencia de entidades internacionales reconocidas,** que aseguren respuesta y continuidad 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 Inteligencia de amenazas

3.1 Marco teórico

3.1.1 Introducción

La comprensión adecuada del **riesgo** en ciberseguridad industrial resulta esencial para interpretar el valor de la inteligencia. En términos generales, un riesgo surge cuando coinciden tres elementos: **un activo**, **una amenaza** y **una vulnerabilidad** susceptible de ser explotada. Sin amenaza, no existe agente que puede provocar daño; sin vulnerabilidad, la amenaza carece de un punto de entrada; y sin activo, no hay nada que proteger. En consecuencia, **conocer el comportamiento de las amenazas** —sus motivaciones, capacidades y técnicas— es **capital para anticipar riesgos antes de que se materialicen.**

En entornos OT/ICS esta relación es especialmente crítica: los impactos potenciales no se limitan a pérdidas económicas o robo de información, sino que pueden afectar a la disponibilidad operativa, provocar daños físicos en equipos y comprometer la seguridad de personas y procesos. Por ello, la inteligencia se convierte en una función estratégica que permite reducir incertidumbre, orientar decisiones y actuar de forma proactiva.

Veamos de manera somera una introducción [1][2][3] a esta disciplina de creciente importancia en el ámbito de la seguridad de la información.

La inteligencia en ciberseguridad consiste en **transformar información en conocimiento útil** para anticipar riesgos y comprender cómo, por qué y contra quienes podrían actuar los adversarios. En entornos **ICS/OT**, esta capacidad es especialmente crítica: las amenazas no sólo buscan comprometer datos, sino **alterar procesos físicos**, interrumpir la operación o provocar daños materiales y de seguridad. Por ello, la inteligencia permite identificar señales tempranas de actividad hostil, contextualizar vulnerabilidades en sistemas industriales y priorizar medidas que reduzcan la probabilidad de una 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

Encuesta State of Threat Intelligence. Fuente: Recorded Future (2025)

Esta disciplina puede aplicarse desde dos perspectivas complementarias:

- Por un lado, **la inteligencia ofensiva** ayuda a descubrir debilidades en arquitecturas OT —por ejemplo, configuraciones inseguras, servicios expuestos o fallos en dispositivos de control— habitualmente en el marco de ejercicios éticos como evaluaciones de seguridad o simulaciones de ataque.

- Por otro, **la inteligencia defensiva** se centra en entender cómo operan los adversarios, qué vectores prefieren en entornos industriales (acceso remoto, explotación de PLCs, abuso de protocolos ICS, etc.) y qué indicadores permiten identificarlos precozmente.

- A ello se suma la **contrainteligencia**, orientada a **detectar y neutralizar actividades hostiles** dirigidas contra operaciones críticas, incluyendo movimientos de espionaje industrial, intentos de sabotaje o comportamientos anómalos que puedan señalar la presencia de un *insider* o de un actor persistente.

El funcionamiento eficaz de estas capacidades se apoya en principios estructurados, entre los que destaca el **ciclo de inteligencia**, un proceso iterativo en el que las

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

necesidades operativas se transforman en conocimiento accionable mediante **planificación, recopilación de datos, análisis, difusión y retroalimentación**.

Ciclo de la inteligencia. Fuente: Elaboración propia (2026)

En entornos OT, este ciclo integra fuentes especializadas —como telemetría de redes industriales, eventos de dispositivos de control, informes de fabricantes o datos procedentes de honeypots ICS (sistemas trampa)— para producir inteligencia adaptada al dominio físico. A ello se suma la importancia de un enfoque **proactivo**, indispensable en sistemas donde los tiempos de respuesta son más largos y las interrupciones no son aceptables. Finalmente, el enfoque **centrado en amenazas** permite priorizar recursos en función de los adversarios más plausibles para el sector industrial afectado, ya sean grupos criminales orientados al ransomware, actores estatales con capacidad para manipular procesos, o campañas automatizadas que explotan vulnerabilidades OT a gran escalafón.

En conjunto, estos elementos permiten que la inteligencia y la contrainteligencia **fortalezcan de forma decisiva la protección de las operaciones industriales**, ayudando a reducir la incertidumbre, anticipar comportamientos hostiles y tomar decisiones informadas en un entorno donde la superficie de ataque crece y las consecuencias de un fallo pueden ser físicas y severas.

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

3.1.2 Métodos de captación de inteligencia de amenazas

En un programa maduro de **Ciberinteligencia**, especialmente en entornos **ICS/OT**, la calidad del análisis depende en gran medida de **cómo se obtienen los datos**. No todas las fuentes aportan el mismo tipo de valor: algunas ofrecen volumen y amplitud, otras profundidad y contexto, y otras, visibilidad técnica en tiempo real. Entre los cimientos clásicos de la obtención de información destacan tres disciplinas que se definen a continuación: **OSINT (Open Source Intelligence)**, **HUMINT (Human Intelligence)** y **SIGINT (Signals Intelligence)**.

Estas tres aproximaciones no compiten entre sí, sino que se **complementan**: OSINT aporta una visión amplia del entorno público y clandestino, HUMINT incorpora la dimensión humana y de intenciones, y SIGINT proporciona evidencias técnicas basadas en señales y tráfico de red. Integradas en el ciclo de inteligencia, permiten pasar de datos aislados a **conocimiento estructurado y** accionable sobre amenazas que pueden impactar tanto en infraestructuras IT como en sistemas de control industrial.

3.1.2.1 OSINT (Open Source Intelligence)

OSINT es, ante todo, una disciplina que permite observar el entorno a través de aquello que éste expone públicamente. En ciberseguridad defensiva, y especialmente en entornos industriales, su utilidad reside en la capacidad de **identificar señales tempranas de actividad maliciosa**, comprender la exposición real de la organización y anticipar riesgos sin recurrir a técnicas intrusivas. A partir de fuentes abiertas —páginas web, bases de datos de vulnerabilidades, repositorios de código, redes sociales, foros o espacios clandestinos accesibles— el analista puede construir una visión amplia del panorama de amenazas, detectar infraestructura sospechosa y comprender cómo puede verse afectada su propia superficie de ataque.

En el ámbito ICS/OT, OSINT permite descubrir si existen **dispositivos industriales expuestos**, si se ha publicado recientemente una vulnerabilidad crítica que afecte a PLCs o sistemas SCADA, o si grupos maliciosos comentan en la dark web herramientas o exploits específicos para protocolos industriales. Su valor radica en su capacidad **de contextualizar** información dispersa y convertirla en señales útiles para la defensa. Sin embargo, esa amplitud también conlleva desafíos: la información puede ser incompleta, sesgada o manipulada, y el volumen de datos puede exceder la capacidad del analista si no se aplican criterios rigurosos de selección y convalidación.

Algunas herramientas que se usan típicamente en OSINT son Maltego [4], Shodan [5] o Spiderfoot [6]. Además, el uso de APIs y scripts personalizados permite integrar herramientas OSINT con sistemas existentes, como los centros de operaciones de seguridad (SOC), aumentando su eficacia al generar alertas en tiempo real.

OSINT proporciona la **amplitud y perspectiva** necesarias para comprender el entorno de amenazas y anticiparse a ellas, siempre que se complemente con fuentes internas y con otros tipos de inteligencia.

3.1.2.2 HUMINT (Human Intelligence)

Si OSINT proporciona amplitud, **HUMINT** aporta profundidad. La inteligencia humana introduce una dimensión cualitativa que con cierta frecuencia, queda reflejada en registros automáticos: **intenciones, motivaciones, dinámicas sociales y comportamiento humano**. En ciberseguridad —y de forma especialmente importante en sectores industriales— HUMINT permite identificar amenazas difíciles de detectar mediante mecanismos puramente técnicos, como **insiders**, personal descontento o terceros con acceso privilegiado.

HUMINT se aplica también a la observación de comunidades clandestinas, donde actores maliciosos comparten información sobre vulnerabilidades, accesos robados o campañas dirigidas. Estas interacciones pueden revelar indicios sobre ataques en preparación, sectores industriales bajo interés o herramientas específicas para comprometer sistemas OT.

A diferencia de OSINT, HUMINT no se basa en lo que está disponible públicamente, sino en lo que puede extraerse mediante **interacción humana, observación encubierta o análisis social**. El uso de perfiles ficticios bien diseñados, la observación de foros cerrados o la recopilación de percepciones internas generan señales que complementan los indicadores técnicos. Sin embargo, HUMINT requiere un marco ético y legal estricto: la protección de datos, la justificación de actividades encubiertas y la documentación de cada paso son componentes imprescindibles.

Las metodologías de recopilación propias de HUMINT abarcan desde técnicas directas hasta aproximaciones más encubiertas. Una de las más habituales consiste en realizar **entrevistas y encuestas**, que permiten obtener información de primera mano de personas dentro o fuera de la organización, ya sea para detectar percepciones de riesgo, identificar comportamientos anómalos o comprender mejor el contexto operativo. A ello se suma la **observación de redes clandestinas**, como la dark web, foros de hacking o

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

mercados ilícitos, donde actores maliciosos comparten datos robados, comentan vulnerabilidades o preparan campañas dirigidas. En los casos en los que es necesario profundizar más, puede recurrirse a la **infiltración mediante perfiles ficticios o sock puppets**, creados específicamente para interactuar de forma anónima con comunidades sospechosas y convalidar hipótesis sin comprometer la identidad del analista.

Para apoyar este trabajo, existen herramientas que facilitan la documentación y el anonimato durante la investigación. **Hunchly** [7] resulta especialmente útil para registrar sistemáticamente la actividad realizada en línea, conservando evidencias y trazabilidad del proceso; mientras que extensiones como **Anonymox** [8] ayudan a preservar el anonimato, algo esencial cuando se opera en espacios donde una exposición prematura puede implicar riesgos operativos o legales.

Bien ejecutada, HUMINT responde a preguntas clave que no pueden resolverse mediante datos técnicos: **quién podría atacar, por qué lo haría y qué señales humanas anticipan su comportamiento**.

3.1.2.3 SIGINT (Signals Intelligence)

SIGINT completa la tríada aportando una visión técnica directa sobre la actividad que ocurre en redes y sistemas. Se basa en la **captura y análisis de señales electrónicas y comunicaciones**, proporcionando evidencias de lo que realmente está sucediendo en el entorno operativo. En ciberseguridad moderna, y especialmente en redes ICS/OT, SIGINT es fundamental para detectar intrusiones, identificar patrones anómalos y descubrir comportamientos que podrían anticipar un ataque.

Mediante el análisis del tráfico de red, los flujos de comunicación y las interacciones entre dispositivos, SIGINT permite detectar **conexiones no autorizadas hacia equipos de control**, variaciones anómalas en la frecuencia de comunicaciones entre PLCs, intentos de escaneo sobre segmentos industriales o comportamiento propio de malware que utilice canales cifrados o encubiertos.

SIGINT ofrece una lectura objetiva: allí donde OSINT muestra contexto y HUMINT revela intención, SIGINT aporta **evidencia técnica**. Su eficacia aumenta cuando se combina con los otros enfoques. Un dominio detectado en foros clandestinos puede ser monitorizado mediante SIGINT para confirmar si está comunicándose con la red industrial; una vulnerabilidad crítica identificada mediante OSINT puede correlacionarse con patrones inusuales de tráfico que indiquen intentos de explotación. Esta convergencia convierte

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

la información en inteligencia accionable, capaz de priorizar medidas defensivas en base a actividad real.

Dentro del ámbito de la ciberinteligencia, **SIGINT** puede dividirse en dos vertientes complementarias: **COMINT**, orientada al análisis del contenido y los metadatos de las comunicaciones —como correos electrónicos, mensajería o tráfico web—, y **ELINT**, centrada en las señales emitidas por dispositivos electrónicos, desde puntos de acceso Wi-Fi hasta sistemas IoT o equipamiento industrial. Esta distinción permite comprender tanto la **intención** como **las capacidades técnicas** de los actores maliciosos, aportando una visibilidad muy valiosa en contextos donde las comunicaciones constituyen el principal indicador de actividad hostil.

En su aplicación defensiva, SIGINT se basa en técnicas como el análisis continuo del **tráfico de red**, que permite identificar patrones anómalos, picos inesperados de actividad o conexiones hacia destinos sospechosos, así como en **la supervisión de comunicaciones cifradas**, ya que incluso sin acceder al contenido, cambios en su volumen, frecuencia o destino pueden delatar comportamientos maliciosos. Para ello, se recurre a un conjunto de herramientas especializadas capaces de capturar y correlacionar señales en tiempo real.

Categoría	Herramienta / Tecnología	Descripción funcional
Sistemas IDS/IPS	Snort [9]	Sistema de detección y prevención de intrusiones diseñado para identificar patrones de ataque conocidos y comportamientos maliciosos en tiempo real.
Sistemas IDS/IPS	Suricata [10]	Motor IDS/IPS de alto rendimiento que permite la detección de intrusiones, análisis de protocolos e identificación de amenazas avanzadas en redes de alta velocidad.
Análisis de tráfico de red	Wireshark [11]	Analizador de protocolos que ofrece una visión detallada del tráfico de red, permitiendo inspeccionar paquetes y analizar el comportamiento de las comunicaciones.

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

Análisis de tráfico de red	Zeek [12]	Plataforma de monitorización y análisis de tráfico orientado a la detección de comportamientos anómalos y a la obtención de inteligencia de red.
Análisis de flujos y datos retrospectivos	Arkime [13]	Plataforma de captura e indexación de tráfico que permite reconstruir sesiones y analizar actividades sospechosas de forma retrospectiva.
Análisis de flujos de red	NetFlow [14]	Tecnología de recogida y análisis de flujos de tráfico que facilita la visibilidad del uso de la red y la detección de patrones anómalos.
Análisis de flujos de red	sFlow [15]	Tecnología de muestra de paquetes y flujos que permite la monitorización escalable del tráfico y el análisis de tendencias de red.

Tecnologías de SIGINT. Fuente: Elaboración propia (2026)

Combinadas, estas capacidades proporcionan a los equipos defensivos una visión granular del comportamiento de la red y facilitan **la detección temprana de amenazas**, especialmente en entornos sensibles o altamente segmentados.

En conjunto, OSINT, HUMINT y SIGINT proporcionan una visión **complementaria y coherente** del panorama de amenazas. Su integración permite entender **qué ocurre, quién podría estar detrás y cómo se manifiesta técnicamente**, ofreciendo una base sólida para la defensa de infraestructuras industriales y sistemas de control.

3.1.3 Niveles de inteligencia

La **ciberinteligencia** constituye una capacidad esencial para cualquier organización que aspire a anticiparse a las amenazas, comprender la naturaleza de sus riesgos y adoptar decisiones fundamentadas para proteger sus activos, especialmente en entornos donde la continuidad operativa es crítica, como los **ICS/OT**.

Para aportar valor real, la inteligencia debe estructurarse en distintos niveles que responden a horizontes temporales y necesidades diferentes. De manera general, se distinguen tres dimensiones complementarias: la **ciberinteligencia estratégica**, **la operativa** y **la táctica**. Su combinación permite obtener una visión integral del panorama de amenazas y disponer de mecanismos eficaces tanto para prevenir como para responder ante incidentes.

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

- La **ciberinteligencia estratégica** ofrece una visión global y a largo plazo del ecosistema de amenazas. Está orientada a la alta dirección y a los responsables de definir políticas, ya que ayuda a comprender qué actores representan un riesgo significativo, cómo evolucionan sus capacidades y qué tendencias tecnológicas pueden modificar el entorno de amenaza en el futuro. Este nivel permite identificar, por ejemplo, el interés creciente **de APT apoyadas por Estados** en sectores como energía, transporte o manufactura avanzada, así como evaluar cambios en motivaciones, objetivos y patrones de actividad. En un informe estratégico, no se busca el detalle técnico, sino la **lectura contextual** que permite orientar inversión, priorizar capacidades defensivas y ajustar la estrategia general de ciberseguridad.

- La **ciberinteligencia operativa** actúa en un horizonte temporal intermedio y se centra en amenazas, campañas y vulnerabilidades concretas que pueden afectar a la organización en semanas o meses. Su propósito es apoyar a los equipos que protegen infraestructuras críticas, ofreciendo información suficientemente detallada como para anticipar riesgos y preparar defensas, pero sin llegar al nivel granular de la inteligencia táctica. En este ámbito se analizan, por ejemplo, campañas de phishing dirigidas a personal clave, explotación activa de una vulnerabilidad en un producto ampliamente desplegado en el sector o la actividad coordinada de un grupo criminal contra una región o industria específica. La inteligencia operativa permite comprender **qué está ocurriendo ahora mismo**, quién está detrás y con qué capacidades, proporcionando así un marco para priorizar medidas de mitigación.

- Por último, la **ciberinteligencia táctica** opera en el nivel más próximo a la ejecución y está dirigida a los equipos operativos: analistas de SOC, personal de respuesta a incidentes o responsables de detección. Su finalidad es ofrecer información **altamente procesable e inmediata**, como **indicadores de compromiso (IoCs)**, direcciones IP o dominios maliciosos, **hashes**, firmas de malware o descripciones detalladas de **tácticas, técnicas y procedimientos (TTPs)** utilizados por un adversario. Un producto de inteligencia táctica puede detallar, por ejemplo, el comportamiento de una variante de malware, cómo se propaga, qué artefactos deja en el sistema y qué evidencias pueden utilizarse para detectarlo o contenerlo. Este nivel es indispensable para mejorar reglas de

correlación, enriquecer alertas y responder más rápidamente a incidentes en curso.

En conjunto, los tres niveles aseguran que la inteligencia no sólo describa el panorama de amenazas, sino que permita **actuar** de manera informada en cada capa de la organización, desde la estrategia hasta la operación diaria.

3.1.4 Fuentes

La generación **de ciberinteligencia útil** requiere apoyarse en un conjunto diverso de fuentes que aporten profundidad, actualidad y fiabilidad. Estas fuentes no son homogéneas: cada una ofrece una perspectiva distinta del entorno de amenazas y resulta más adecuada para ciertos niveles de inteligencia —estratégico, operativo o táctico—. Para obtener análisis sólidos y accionables, es necesario combinar información procedente **de feeds comerciales**, **comunidades de intercambio**, **organismos gubernamentales**, **entornos clandestinos y telemetría interna**.

- Los **feeds comerciales** proporcionan inteligencia altamente estructurada, actualizada y generalmente enriquecida con análisis técnicos o contextuales realizados por equipos especializados. Soluciones como **Recorded Future** [16], que correlaciona datos originados en OSINT, SIGINT y múltiples repositorios globales, o los informes **de FireEye Threat Intelligence** [17], basados en investigaciones propias y en observaciones de incidentes reales, permiten a las organizaciones disponer de visibilidad avanzada sobre campañas emergentes, actividad de actores sofisticados y vulnerabilidades explotadas activamente. Este tipo de fuentes destaca por su capacidad para acelerar la toma de decisiones gracias a su profundidad analítica y a la calidad de sus modelos de riesgo.

- Paralelamente, **las fuentes comunitarias** fomentan la colaboración entre organizaciones y equipos de seguridad, proporcionando un espacio abierto donde compartir indicadores, tácticas observadas y experiencias comunes. Plataformas como **AlienVault OTX** [18], que permite intercambiar IoCs e análisis sobre amenazas, o **MISP** [19], diseñada para estructurar y compartir información de forma estandarizada, son especialmente valiosas para aumentar la velocidad de detección y fortalecer la respuesta ante incidentes, ya que ofrecen inteligencia basada en contribuciones reales de la comunidad.

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

- Las **fuentes gubernamentales y de infraestructuras críticas** constituyen otro cimiento fundamental, especialmente en sectores industriales. Organismos como **CISA** (Agencia de Ciberseguridad y Seguridad de Infraestructuras) [20] en Estados Unidos o **ENISA** (Agencia de la UE para la Ciberseguridad) [21] en Europa publican avisos, guías de mitigación, análisis sectoriales y estudios específicos sobre infraestructuras críticas. Estas publicaciones resultan imprescindibles para comprender amenazas que afectan a sectores concretos —energía, transporte, agua, manufactura— y para mantener alineados los programas de seguridad con las recomendaciones oficiales y la normativa vigente.

- En el extremo menos visible del espectro se encuentran las **fuentes clandestinas**, que permiten acceder a información procedente de entornos donde operan actores maliciosos. Foros en la dark web, mercados ilegales y canales privados cifrados son espacios donde se discuten vulnerabilidades recientemente descubiertas, se comercializan accesos comprometidos, se anuncian campañas en preparación o se intercambian herramientas ofensivas. Aunque su acceso y monitorización requieren precauciones éticas, legales y operativas, estas fuentes proporcionan señales críticas para anticipar actividades que aún no han emergido en canales públicos.

- Finalmente, **las fuentes internas** representan la perspectiva más directa y específica sobre el entorno tecnológico propio. Incluyen **logs de sistemas y redes**, telemetría procedente de soluciones SIEM (monitorización), **alertas de seguridad** generadas por el SOC, resultados de **pruebas de penetración y auditorías**, así como **IoCs detectados** dentro de la organización. Esta información refleja de manera inmediata la actividad real que impacta sobre la infraestructura, facilitando la detección temprana de anomalías y la validación de amenazas identificadas por fuentes externas. En entornos ICS/OT, la telemetría interna —incluyendo tráfico de red industrial, eventos de control o anomalías operativas— se convierte en una pieza esencial para contextualizar cualquier señal procedente del exterior.

En conjunto, la combinación de estas fuentes permite a la organización construir una visión equilibrada del panorama de amenazas: desde la actividad global hasta los detalles que afectan directamente a su infraestructura. La integración de fuentes

externas e internas es la base para producir inteligencia **fiable, accionable y adaptada al contexto operativo**.

3.1.5 Generación de inteligencia procesable

La generación de **inteligencia procesable** constituye el núcleo del trabajo de ciberinteligencia, ya que su valor real no reside únicamente en recopilar datos, sino como se ha indicado, en transformarlos en conocimiento **útil** capaz de mejorar de manera tangible la postura de seguridad de la organización.

Este proceso comienza con la transición *del dato al conocimiento*. La información bruta procedente de múltiples fuentes —internas, comunitarias, comerciales o clandestinas— debe analizarse, filtrarse y priorizarse para distinguir aquello que resulta verdaderamente relevante del ruido contextual. Esta priorización depende tanto de la **criticidad de los activos afectados**, como de la **probabilidad de explotación** y de la **capacidad demostrada por los adversarios**. Así, una vulnerabilidad que impacta directamente en un sistema de control industrial operativo tendrá una prioridad mucho mayor que otra que afecte a un componente periférico o poco utilizado, generando incluso **alertas inmediatas** cuando el riesgo es significativo.

De la información bruta al conocimiento accionable. Fuente: Elaboración propia (2026)

El proceso de análisis se enriquece mediante el uso de **matrices y frameworks** que permiten estructurar, contextualizar y normalizar la información disponible. Entre ellos, destaca especialmente **MITRE ATT&CK** [22] **y MITRE ATT&CK ICS** [23], convertido en un lenguaje común para describir las tácticas y técnicas utilizadas por los adversarios. Este marco facilita comprender cómo operan los atacantes, qué fases de la cadena de intrusión utilizan y en qué puntos concretos podría reforzarse la defensa.

Cuando un analista identifica, por ejemplo, que un actor conocido emplea técnicas específicas de **movimiento lateral**, puede mapearlas en el marco ATT&CK y reforzar controles en esas áreas antes de que la intrusión llegue a producirse. De esta forma, la inteligencia deja de ser un simple ejercicio descriptivo para convertirse en un

instrumento anticipatorio y operativo, capaz de guiar decisiones técnicas y estratégicas con impacto directo en la protección de la organización.

3.1.6 Contrainteligencia

La **contrainteligencia** desempeña un papel fundamental dentro de la seguridad de una organización, ya que su propósito es **identificar, neutralizar y prevenir actividades maliciosas** que puedan comprometer activos críticos, información sensible u operaciones esenciales. En el ámbito de la ciberseguridad, esta disciplina abarca tanto amenazas internas como externas y se orienta no sólo a responder a incidentes, sino a **anticipar las tácticas de los adversarios**, dificultar sus acciones y reducir su capacidad real de causar daño. En entornos industriales y de control, donde la manipulación o interrupción de procesos puede derivar en consecuencias operativas significativas, la contrainteligencia se convierte en un componente indispensable del modelo defensivo.

La **contrainteligencia defensiva** se apoya en dos principios fundamentales.

- El primero **es la detección de espionaje y actividades maliciosas dirigidas**, un aspecto clave en un escenario donde conviven cibercriminales, grupos con motivaciones económicas, competidores desleales o incluso actores apoyados por Estados. La identificación temprana de señales de espionaje industrial, intentos de infiltración o accesos anómalos resulta esencial para anticipar situaciones comprometedoras antes de que se materialicen.

- El segundo principio **es la protección de datos sensibles y operativos**, ya que la información crítica sigue siendo uno de los objetivos prioritarios de cualquier adversario. La contrainteligencia despliega controles específicos para salvaguardar estos datos, desde la clasificación y etiquetado según niveles de sensibilidad hasta la segmentación de redes o la aplicación de cifrado para minimizar el acceso no autorizado.

Para llevar a cabo estas funciones, la contrainteligencia emplea un conjunto amplio de técnicas y herramientas.

Una de las áreas más relevantes **es la supervisión de empleados y accesos internos**, orientada a detectar comportamientos potencialmente anómalos que puedan indicar un riesgo *de* insider threat (adversario procedente de dentro de la organización).

La disciplina también incluye **el análisis de anomalías en redes e infraestructuras**, mediante técnicas capaces de detectar comportamientos que se desvían de la norma, como intentos de movimiento lateral, transferencias de datos no autorizadas o tráfico inusual entre segmentos críticos.

Otra técnica clave es el uso **de honeypots y honeynets**, sistemas diseñados deliberadamente para atraer a los atacantes y estudiar su comportamiento. Estas infraestructuras cebo permiten comprender las **tácticas, técnicas y procedimientos (TTPs)** de los adversarios y anticipar posibles ataques contra la red real.

La contrainteligencia abarca también la **evaluación de amenazas internas y externas**, adoptando modelos que clasifican a los insiders según su acceso, intenciones y capacidades.

Por último, un elemento esencial es **la protección frente al spear phishing y la ingeniería social** (basados en engañar a las personas), ya que estos vectores suelen ser utilizados como puerta de entrada en la zona IT de las plantas productivas, para comprometer procesos críticos o acceder a información sensible. La combinación de análisis automatizado, filtrado avanzado y formación de empleados resulta crítica para reducir este riesgo.

3.1.7 Implementación de un programa de inteligencia

La creación de un **programa sólido de inteligencia y contrainteligencia** constituye un elemento esencial para que las organizaciones puedan anticiparse a las amenazas, proteger sus activos críticos y responder con eficacia a incidentes de ciberseguridad. Este tipo de programas combina procesos maduros, herramientas especializadas y recursos humanos calificados con el objetivo de **recopilar, analizar y aplicar inteligencia de forma sistemática**. Su implementación exige una planificación estratégica adecuada, una integración estrecha con operaciones clave —especialmente con el **Security Operations Center (SOC)**— y una evaluación continua mediante métricas que permitan medir su impacto real en la postura defensiva.

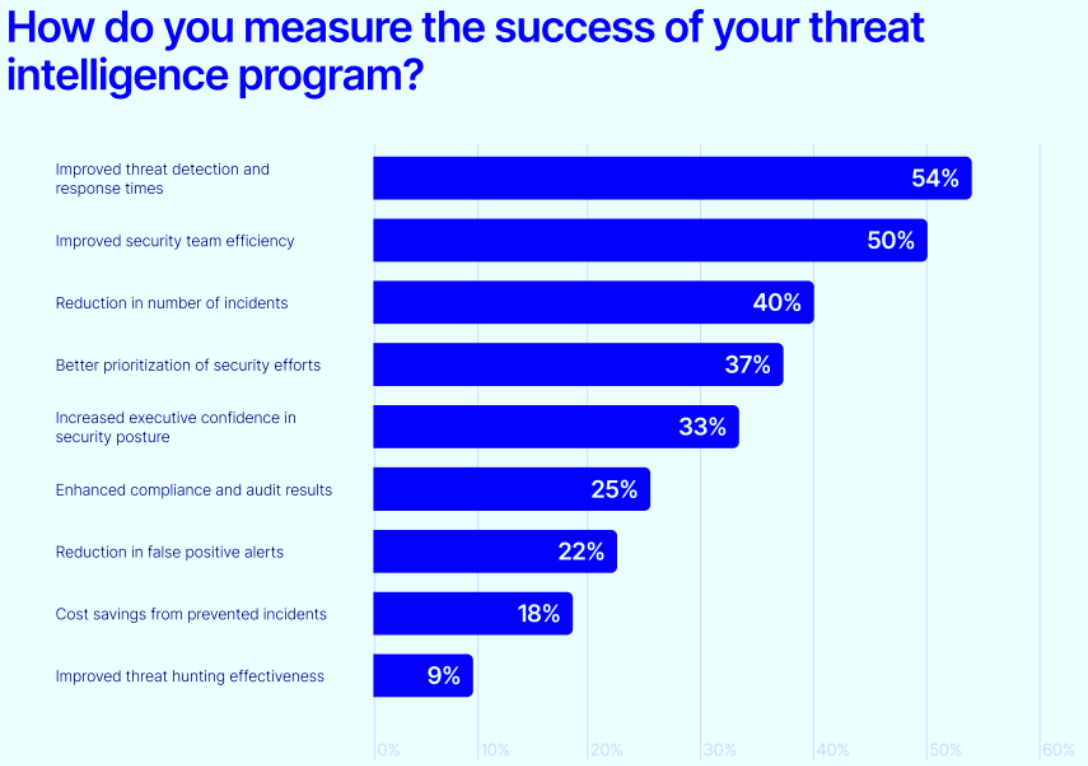
- El punto de partida es una **planificación clara del programa**, alineada con las necesidades específicas de la organización y con las particularidades de su infraestructura tecnológica, su sector y su nivel de exposición. En esta fase resulta fundamental definir **objetivos de inteligencia** concretos, orientados a responder a preguntas operativas y estratégicas: desde prevenir ataques dirigidos o identificar actores relevantes, hasta proteger activos especialmente

sensibles. Una vez establecidas estas metas, se diseña un **ciclo de inteligencia adaptado**, que articula la planificación, la recopilación de datos, el análisis, la difusión y la retroalimentación continua. Este enfoque personalizado permite integrar fuentes OSINT, telemetría interna e indicadores técnicos para generar productos de inteligencia accionables que puedan emplearse inmediatamente por los equipos defensivos.

- Para maximizar su eficacia, el programa debe integrarse de forma natural en el **SOC**, donde la inteligencia se convierte en un motor para la detección y la respuesta. La creación de **equipos especializados en Threat Intelligence** dentro del SOC permite disponer de analistas dedicados a monitorizar la evolución de actores y campañas, procesar grandes volúmenes de datos y generar informes operativos que guíen decisiones en tiempo real. Cuando, por ejemplo, un grupo APT adopta una nueva técnica de movimiento lateral, estos analistas pueden alertar inmediatamente al SOC para reforzar las capacidades de detección y ajustar las políticas de seguridad. Esta integración se ve reforzada por el uso **de Threat Intelligence Platforms (TIPs)**, herramientas diseñadas para centralizar y correlacionar información procedente de múltiples fuentes. Plataformas como **Anomali ThreatStream** [24] o **ThreatConnect** [25] facilitan la gestión de datos complejos, la automatización de flujos de análisis y la distribución rápida de inteligencia procesable a otros equipos, permitiendo actuar antes de que una amenaza llegue a materializarse.

- La última dimensión del programa está relacionada con **la evaluación de su desempeño**. Medir de forma objetiva la eficacia de la inteligencia y la contrainteligencia es esencial tanto para justificar inversión como para identificar áreas de mejora. Para ello se emplean **indicadores clave de desempeño (KPIs)**, que pueden incluir el número de amenazas detectadas antes de convertirse en incidentes, la reducción del tiempo de respuesta, la cantidad de IoCs relevantes incorporados a los sistemas de detección o la disminución de falsos positivos. No menos importante es evaluar el **impacto real de la inteligencia en la reducción de incidentes**, analizando cuántos ataques han sido prevenidos gracias a información anticipada o cómo la inteligencia contribuyó a mitigar de manera temprana intentos de explotación detectados en la red corporativa, como se ve en la siguiente figura. Esto ayudará a justificar el retorno de la inversión (ROI) en este tipo de programas, como se

describía en el entregable *Informe de Ciberalertas - I* de este mismo Observatorio [43].



Encuesta State of Threat Intelligence. Fuente: Recorded Future (2025)

3.1.8 Aspectos ético-legales de la inteligencia de amenazas

La implementación de **programas de inteligencia y contrainteligencia** no puede entenderse únicamente como un esfuerzo técnico orientado a proteger activos y anticipar amenazas. También requiere operar dentro de un **marco ético y legal sólido**, que garantice el respeto a la privacidad y a los derechos fundamentales de las personas. Las organizaciones que recopilan, analizan y utilizan información para sostener sus capacidades defensivas deben conocer en profundidad las normativas aplicables y ser conscientes de los límites éticos inherentes a estas actividades. La falta de cumplimiento o el uso inapropiado de datos no sólo puede derivar en sanciones regulatorias severas, sino también en un daño reputacional significativo que comprometa la confianza de clientes, socios y empleados.

El **cumplimiento normativo** constituye así un requisito esencial. Muchas actividades de inteligencia llevan el acceso a datos personales, y su tratamiento debe ser siempre transparente, responsable y conforme a las leyes vigentes. En el contexto europeo destaca **el Reglamento General de Protección de Datos (GDPR)** [26], que establece

directrices estrictas sobre la recopilación, almacenamiento y uso de información personal. Complementariamente, la **Directiva ePrivacy** [27] regula aspectos vinculados a las comunicaciones electrónicas, incluyendo la monitorización del tráfico de red, algo muy relevante para actividades como SIGINT. A estas normas se suman legislaciones locales —como la **CCPA** [28] en California o la Ley de Protección de Datos Personales en algunas jurisdicciones latinoamericanas— que amplían el marco legal de referencia. Para garantizar el cumplimiento, las organizaciones deben realizar **auditorías periódicas** que verifiquen que las prácticas de inteligencia respetan las obligaciones regulatorias en todas las regiones donde operan.

Más allá del marco legal, existe un componente imprescindible: **el tratamiento ético de los datos personales y confidenciales**. La minimización de datos —recopilar únicamente la información estrictamente necesaria—, el consentimiento informado cuando sea aplicable y la aplicación de medidas robustas de protección son elementos esenciales para reducir riesgos y garantizar un uso responsable de la información. En la práctica, esto implica adoptar principios **de anonimización y pseudonimización**, especialmente cuando se trabaja con datos obtenidos a través de OSINT o de telemetría interna. El objetivo no es sólo cumplir con la normativa, sino demostrar un compromiso ético con el manejo de datos sensibles.

La ciberinteligencia expone también **dilemas éticos** que requieren reflexión y políticas claras. Uno de los más relevantes es el equilibrio entre **seguridad y privacidad**. La monitorización de comunicaciones, la observación del comportamiento digital o el uso de herramientas avanzadas para prevenir fugas de información pueden entrar en conflicto con el derecho a la privacidad de empleados o usuarios. Resolver este dilema exige **transparencia**, **proporcionalidad** y **limitación del alcance** de las medidas adoptadas, asegurando que se utilicen únicamente para las fines legítimos de protección y que estén claramente documentadas en las políticas internas.

Otro dilema importante se plantea alrededor de los **límites de la interacción con actores maliciosos**. Actividades como la infiltración en foros clandestinos, la creación de perfiles ficticios o el análisis de herramientas adquiridas en mercados ilícitos son prácticas legítimas dentro de ciertos marcos, pero requieren valorar cuidadosamente qué comportamientos resultan aceptables y cuáles podrían traspasar líneas legales o morales. La observación pasiva puede ser apropiada en algunos casos, mientras que la participación activa podría suponer riesgos éticos considerables. Por ello, es imprescindible establecer **directrices claras** sobre qué acciones están permitidas, bajo

qué condiciones y con qué controles internos, asegurando que la actividad de inteligencia nunca derive en prácticas cuestionables.

3.2 Panorama actual

Lo restante de este bloque de **inteligencia de amenazas,** ofrece una visión estructurada y multidimensional del panorama actual, apoyándose en un conjunto amplio y heterogéneo de fuentes nacionales e internacionales. Antes de profundizar en las secciones específicas, vemos necesario contextualizar tres consideraciones fundamentales que condicionan la lectura e interpretación de los contenidos.

En primer lugar, la mayor parte de los informes de referencia —procedentes de organismos gubernamentales, CERTs nacionales, entidades supranacionales, empresas globales de ciberseguridad o centros de investigación— **no diferencian estrictamente entre ámbitos IT, OT o ICS** en sus análisis de amenazas. Este enfoque, lejos de ser una carencia, resulta especialmente útil en un escenario tecnológico en el que **la convergencia IT/OT** y la progresiva integración de sistemas propios de la **Industria 4.0 y 5.0** tienen difuminadas las fronteras tradicionales. La interpretación conjunta de estas fuentes permite comprender mejor la continuidad entre los vectores de amenaza que afectan a ambos dominios.

En segundo lugar, se buscó deliberadamente **una perspectiva amplia**, integrando fuentes con metodologías, ámbitos geográficos, tamaños muestrales o perfiles de cliente y taxonomías de incidentes muy diversas. Este enfoque enriquece el análisis, pero introduce factores de confusión y rumbos que implican necesariamente que **algunas estadísticas puedan diferir** o incluso resultar parcialmente contradictorias entre sí. Es un reflejo natural de la realidad: los ecosistemas de amenaza no impactan de igual forma en **Europa, en los Estados Unidos o en Asia**, ni todos los sectores industriales presentan la misma exposición, ni los diferentes fabricantes tienen presencia homogénea en todo el globo. Esta diversidad de datos se presenta de forma transparente, pues contribuye a una visión más completa del panorama.

Por último, las **recomendaciones operativas y estratégicas** incluirán tanto las directrices consolidadas de los grandes proveedores globales —derivadas de sus informes anuales de inteligencia— como materiales específicos para **entornos industriales**, sostenidos en bibliografía técnica, normativa y estudios centrados en OT/ICS. Debido al carácter coral de las fuentes empleadas, puede existir cierto solapamiento entre medidas sugeridas por distintas organizaciones, con algunos

matices. Se ha optado por **mantenerlas en su totalidad** para ofrecer al lector un abanico lo más amplio posible de aportes y prácticas relevantes, y facilitar así su aplicación en ambientes industriales variados.

Este conjunto de precisiones sirve de marco interpretativo para las secciones que siguen del bloque 3, orientado a proporcionar un análisis de utilidad directa para la protección del tejido empresarial e institucional en Galicia.

3.2.1 Análisis global

El análisis global de las amenazas en entornos industriales y tecnológicos durante 2024–2025 evidencia un escenario caracterizado por la **convergencia entre actores cada vez más sofisticados**, la **aceleración de tácticas criminales como el ransomware (bloqueo y secuestro de datos)** y un **deterioro progresivo (incremento) de la superficie de exposición industrial**, debido a la creciente interdependencia tecnológica. Los hallazgos procedentes de organismos internacionales y estudios sectoriales coinciden en describir un ecosistema donde la presión operativa sobre infraestructuras críticas continúa aumentando, tanto por motivos económicos como geopolíticos.

El informe **SANS *State of ICS/OT Security 2025*** [29] ofrece una panorámica amplia del estado real de la ciberseguridad industrial a partir de una **encuesta global con más de un millar de profesionales OT/ICS**, procedentes de sectores como **energía, manufactura, agua, transporte, químico y sanitario**, así como de múltiples regiones con fuerte representación **de Norteamérica y Europa**. Esta diversidad permite capturar una visión comparada sobre madurez, prioridades y carencias estructurales en la protección de infraestructuras industriales.

Las **principales aportaciones** recopiladas en la fase inicial del informe revelan tendencias consistentes:

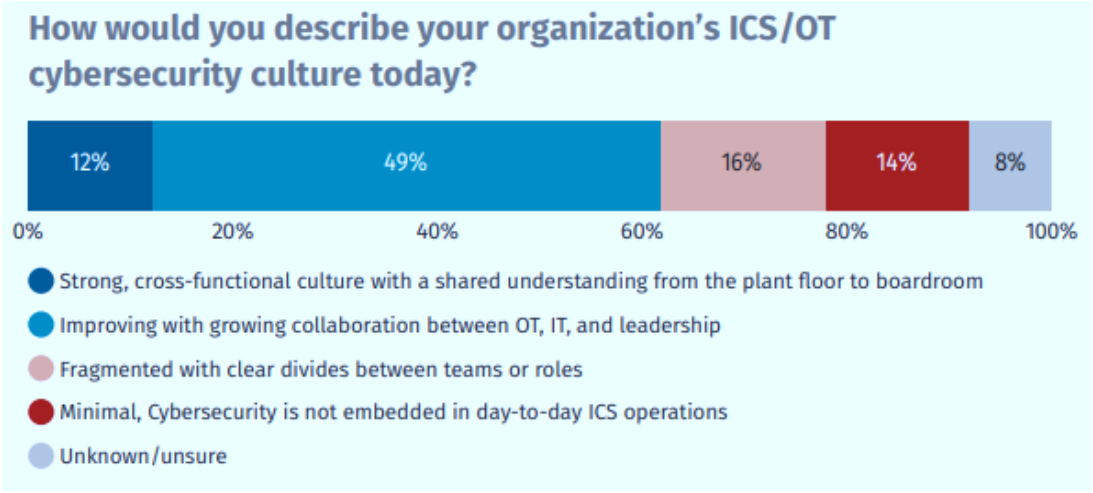
- **El 22**% de **las organizaciones** sufrió al menos un incidente de ciberseguridad en el último año, y el **40**% de ellas generó interrupciones operativas, subrayando el impacto directo en la continuidad del negocio. Aunque **casi la mitad** de los incidentes se detecta en menos de 24 h y **el 60**% se contiene en 48 h, los tiempos **de remediación** continúan siendo elevados, prolongándose días o incluso semanas, lo que evidencia una distancia relevante entre detección y recuperación.

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

- El **acceso remoto no autorizado** continúa siendo el principal vector de intrusión, seguido por la **ingeniería social** y la ausencia de controles específicos orientados a entornos OT.
- La inversión prevista refuerza estas prioridades: **visibilidad de activos**, **detección de amenazas ICS-aware** y acceso remoto seguro **encabezan tanto los despliegue de 2025, como las planificaciones a dos años vista (2027).**

Con todo, más allá de los aspectos técnicos, el informe vuelve a poner el foco en **el factor cultural**, probablemente el elemento menos resuelto en la defensa de los sistemas industriales. Sólo el **14% de las organizaciones** considera estar *plenamente preparada* para afrontar amenazas OT/ICS, lo que muestra una distancia significativa entre la percepción de riesgo y las capacidades reales. Además, SANS identifica una tendencia clara: aquellas organizaciones que sienten plenamente preparadas **integran a técnicos de planta y operadores en ejercicios y simulacros** con una probabilidad **un 66% mayor** que el resto, confirmando que la madurez no depende únicamente de tecnología, sino de la alineación entre equipos, procesos y responsabilidades.

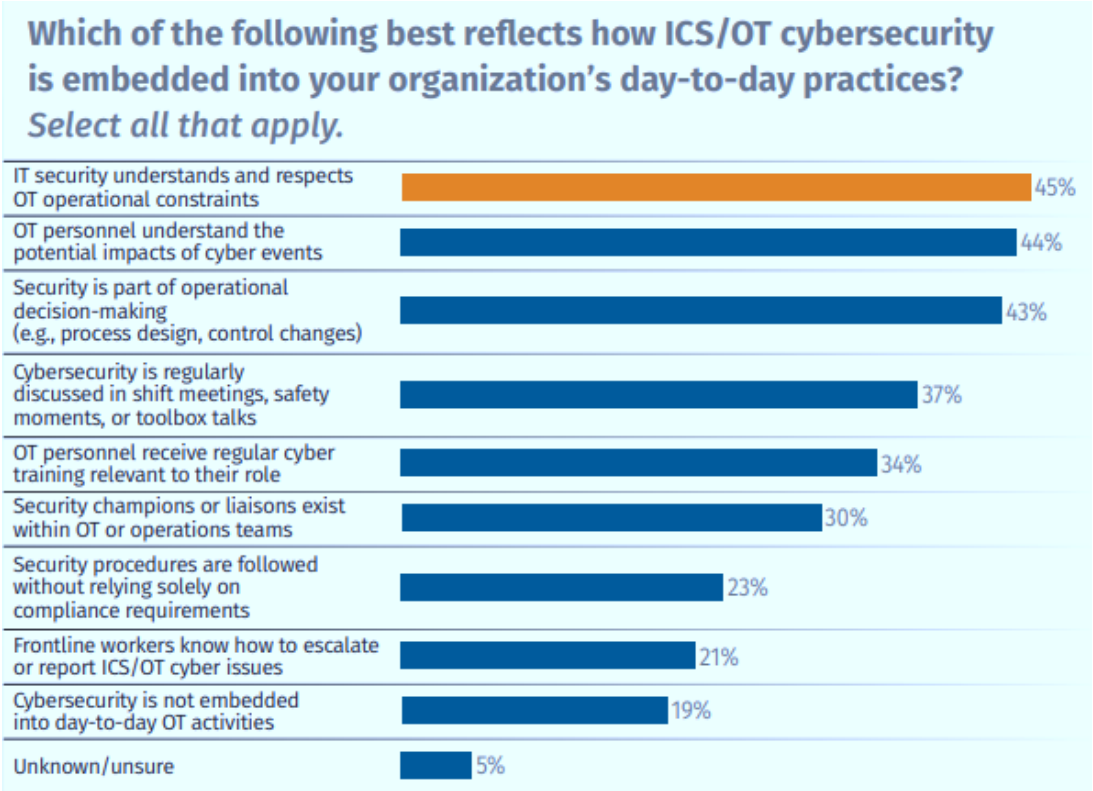
Este desfase cultural se refleja de forma visual en la siguiente figura, que muestra la persistente desconexión entre áreas **TI** y **OT** en la percepción del riesgo y la priorización de medidas.



Cultura IT, OT y liderazgo. Fuente: SANS (2025)

A su vez, el siguiente gráfico ilustra otro síntoma clave: **sólo un tercio** de las organizaciones **ha logrado integrar la ciberseguridad de manera efectiva dentro de las operaciones OT, lo** que evidencia que la convergencia técnica no siempre se acompaña de un alineamiento organizativo adecuado.

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

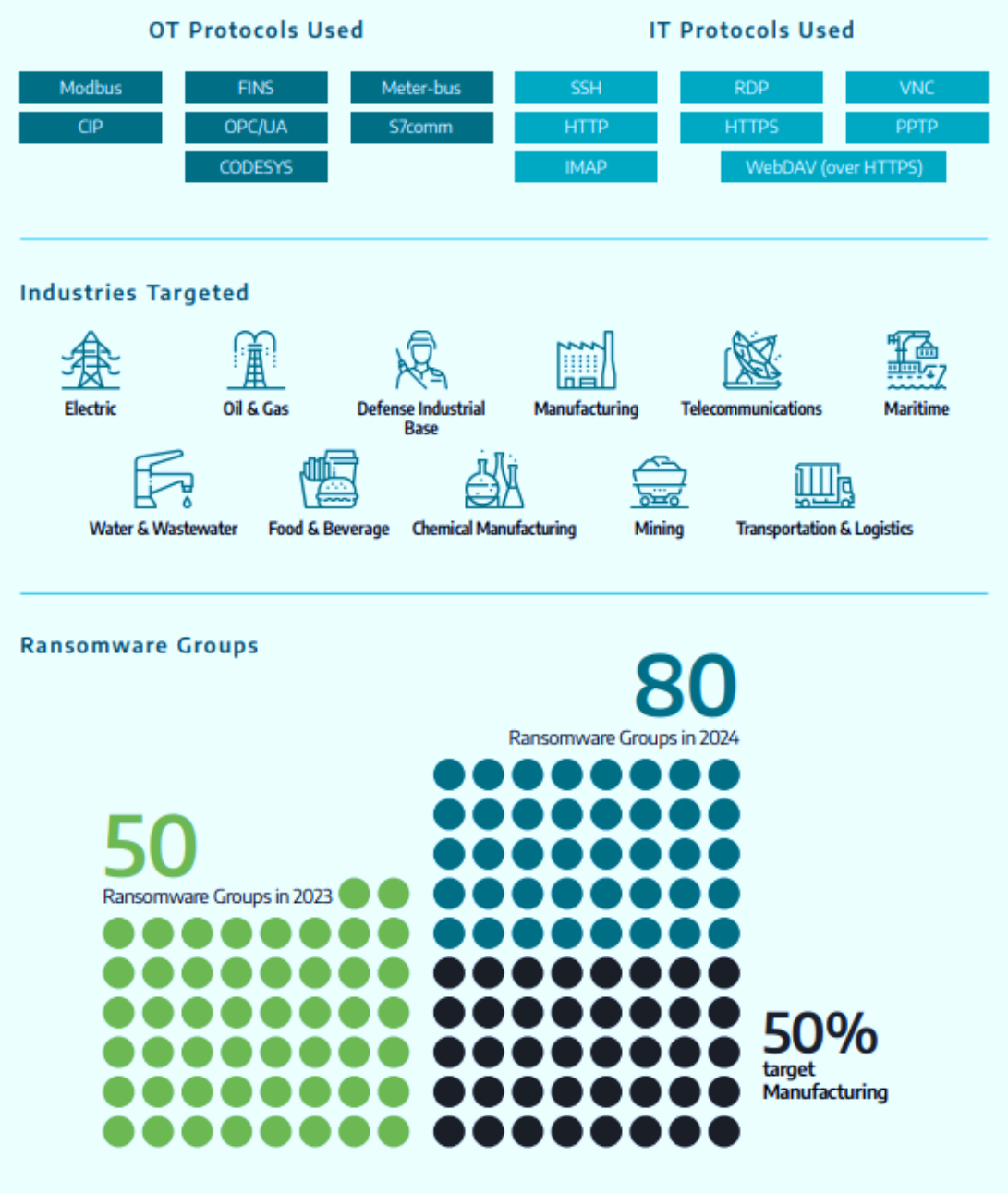


Ciberseguridad OT/ICS como parte de la actividad diaria. Fuente: SANS (2025)

El informe **Dragos *OT Cybersecurity Report – Year in Review 2025*** [30] constituye una de las fuentes más completas y especializadas sobre **amenazas y compromisos en entornos OT/ICS**, diferenciándose de los informes generalistas al centrarse exclusivamente en actividad adversaria con impacto real o potencial sobre procesos industriales, infraestructuras críticas y sistemas de control.

Desde el inicio del documento, Dragos recopila varios **hallazgos clave**, como el número total *de* threat groups monitorizados (hablaremos de actores y campañas en profundidad en informes venideros), la proporción de vulnerabilidades que afectan a la operación, el porcentaje de advisories con errores críticos o sin mitigación, y la distribución de vectores de acceso más frecuentes. Estos indicadores ofrecen un marco visual sólido para contextualizar el estado de las amenazas en OT/ICS. A continuación, otros elementos relevantes relativos a protocolos más vistos, sectores atacados, y 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



Estadísticos relevantes del informe Year Review. Dragos (2025)

En cuanto a las **tendencias generales**, Dragos identifica tres vectores estratégicos que explican la evolución de las amenazas en 2024–2025:

1. El aumento de **operaciones de guerra híbrida con orientación OT**, especialmente durante períodos de tensión geopolítica.
2. Un progreso defensivo **incremental, pero desigual**, con sectores muy maduros conviviendo con otros que mantienen brechas estructurales.

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

3. La consolidación de campañas adversarias menos orientadas a la sofisticación técnica y más a la **amplificación del impacto operativo**, aprovechando errores de configuración, accesos remotos inseguros y exposición innecesaria de activos.

Desde la perspectiva operacional, el informe dedica un análisis profundo a cómo el **malware específico para ICS** se ha convertido en una herramienta clave en campañas motivadas por conflictos. Para la **definición formal de ICS malware**. Dragos establece tres propiedades esenciales:

- que el software sea **ICS-capable**, es decir, pueda interactuar con protocolos, dispositivos o lógicas de control;
- que esté **diseñado con intención maliciosa**, no como herramienta de prueba o investigación;
- y que posea **la capacidad de generar efectos adversos en un entorno OT**, desde pérdida de visibilidad hasta pérdida de control o manipulación del proceso. Esta conceptualización permite diferenciar el malware verdaderamente orientado a industrias críticas de aquel que simplemente "alcanza" sistemas OT como daño colateral desde redes TI.

Se documentan varios casos recientes en los que malware orientado a OT —y no simplemente a entornos corporativos— se ha utilizado para degradar sensores, interrumpir operaciones o preparar escenarios para sabotaje, destacando que su empleo se está normalizando en contextos bélicos y operaciones híbridas. Este fenómeno confirma que la frontera entre intrusión estratégica y efectos físicos se está reduciendo.

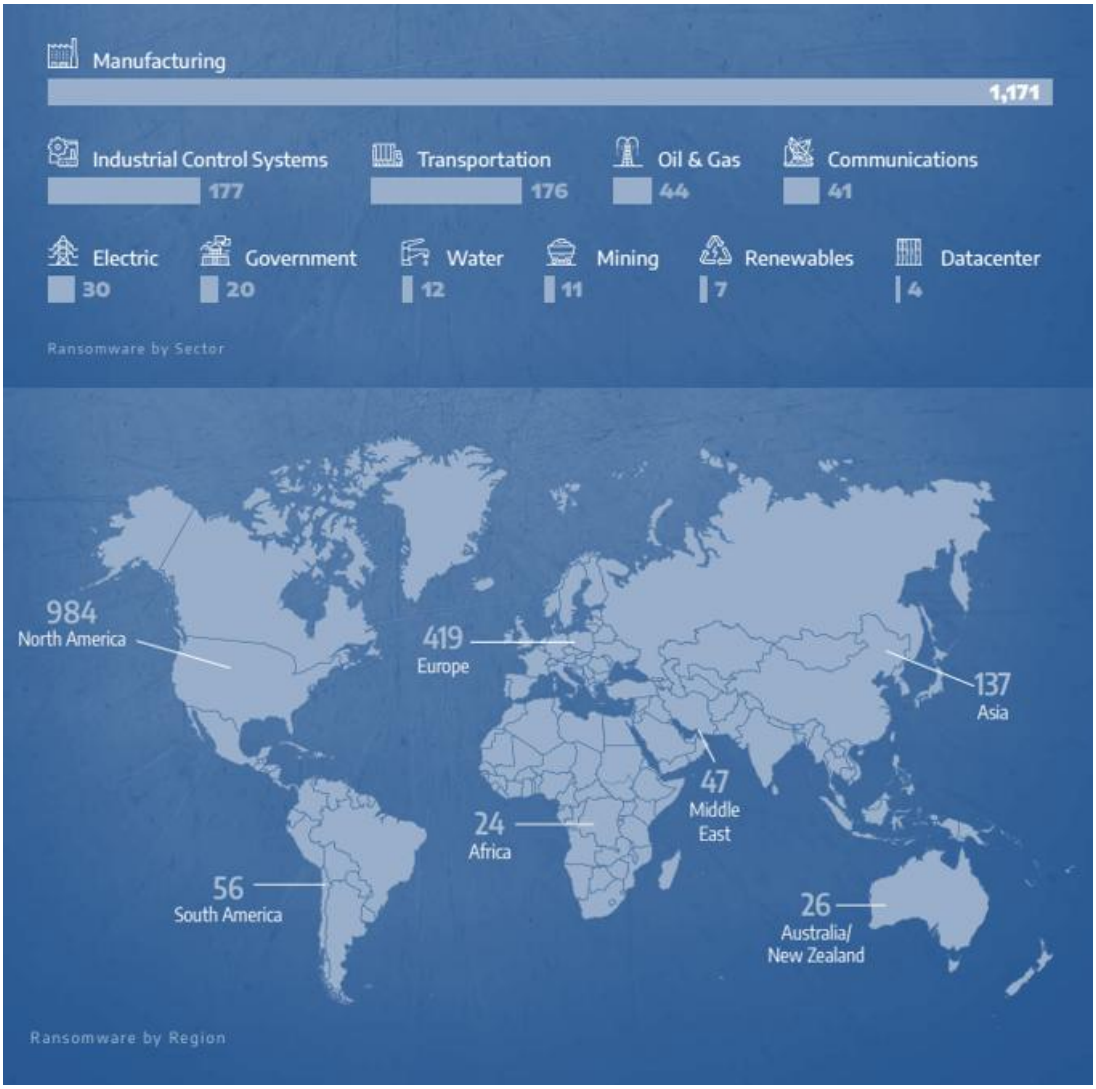
El informe también documenta **el resurgimiento del hacktivismo** con impacto potencial en OT. Dragos señala que numerosos grupos ideológicos aprovecharon 2023–2024 para reivindicar ataques contra infraestructuras críticas; aunque la mayoría carece de capacidades avanzadas, su volumen, su visibilidad pública y la proliferación de herramientas de acceso abierto incrementan la probabilidad de impactos no intencionados sobre sistemas industriales.

Finalmente, la sección dedicada a **ransomware** describe cómo esta amenaza continúa siendo el vector disruptivo predominante para organizaciones industriales, con un **incremento notable en las campañas dirigidas y en las técnicas de doble extorsión** (pago por desciframiento de datos y no divulgación). Dragos subraya que muchos incidentes OT tienen origen en compromisos iniciales TI, pero acaban afectando a la

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

producción debido a la interconectividad y a la dependencia de servicios corporativos críticos.

Esta sección del informe incluye varias gráficas de especial interés, que ilustran de forma directa el impacto de ransomware en industrias OT (no en balde era el cuarto escenario de las acciones de Continuidad de Negocio y Respuesta a Incidentes según el informe de SANS) [29]:



Ataques de ransomware por sector industrial y región. Dragos (2025)

El ***Microsoft Digital Defense Report 2025*** [31], basado en la inmensa visibilidad que proporciona su posición dominante en sistemas Windows, servicios en la nube y plataformas de productividad, presenta datos correspondientes a su año fiscal, que termina el 30 de junio de 2025, lo que permite observar tendencias muy recientes en actividad adversaria global. Aunque se trata de un informe generalista —no centrado en

OT— resulta relevante para comprender la evolución de los métodos de intrusión que también terminan impactando en las redes industriales.

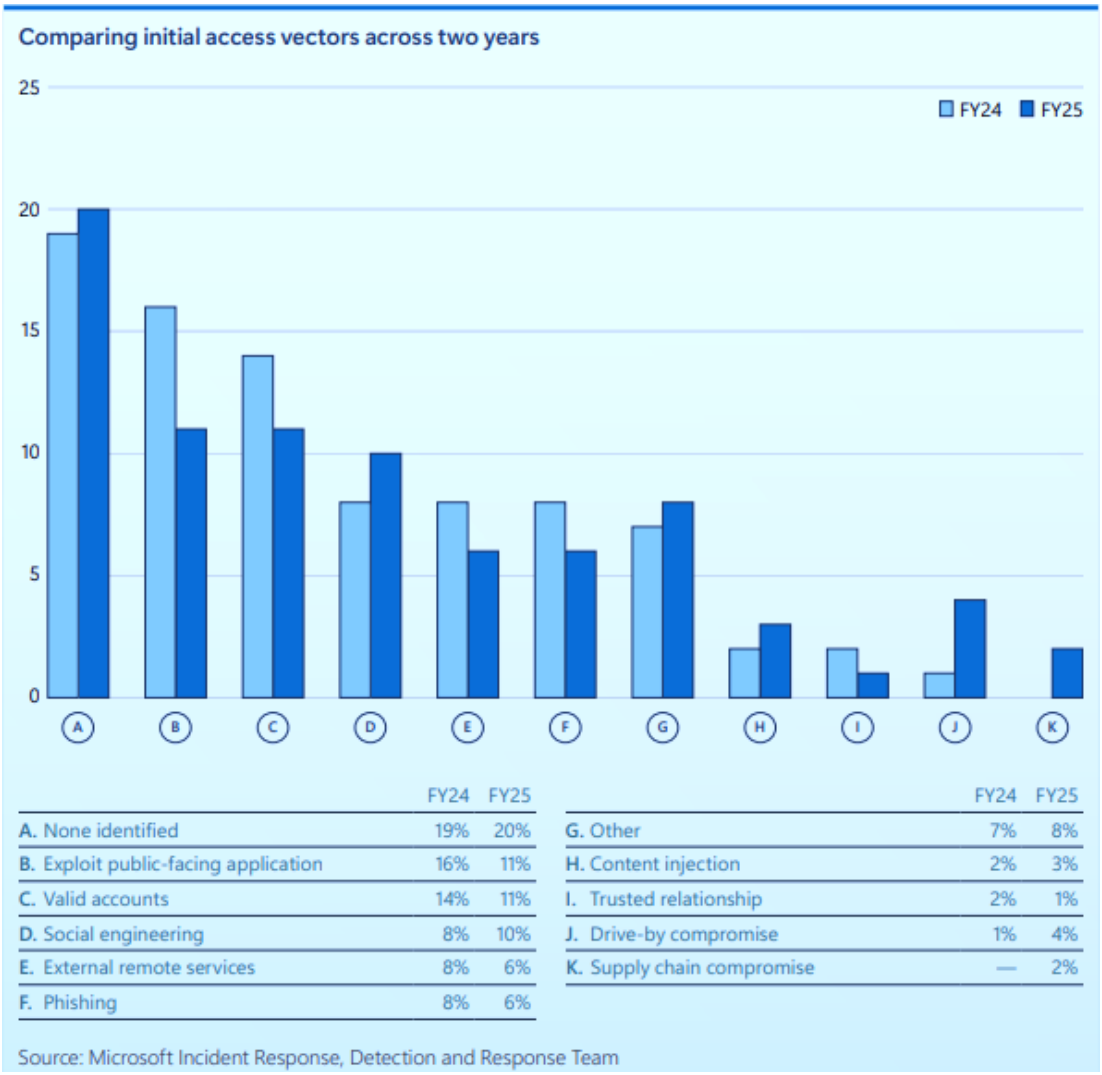
Sintetizan cuatro grandes **ideas fundamentales**:

1. La identidad digtal se consolida como **principal superficie de ataque**, siendo los accesos fraudulentos el vector dominante.
2. El uso **de IA por parte de actores maliciosos** está ampliando la escala y velocidad de campañas de phishing, intrusión y automatización del reconocimiento.
3. El crecimiento sostenido de los ataques a la infraestructura cloud (**cloud-targeting)**, con un aumento continuo de ataques a cargas de trabajo, configuraciones y servicios expuestos.
4. El refuerzo de las técnicas de **evasión y persistencia**, con adversarios capaces de operar durante largos períodos utilizando credenciales legítimas.

Las **gráficas de ciberataques y evolución de vectores** permiten visualizar este desplazamiento desde acciones puramente técnicas hacia tácticas basadas en credenciales, ingeniería social y abuso de funcionalidades legítimas.

Prevalencia de ciberamenazas por país. Fuente: 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. Fuente: Microsoft (2025)

La sección de **amenazas emergentes** subraya cinco dinámicas clave:

- **IA en operaciones ofensivas**

  La IA generativa permitirá campañas de ingeniería social más persuasivas y el desarrollo de malware y agentes autónomos capaces de moverse, escalar privilegios y evadir defensas sin intervención humana.

- **Compromisos en la cadena de suministro**

  Se intensificará el abuso de relaciones de confianza con MSP, VPN/VPS, RMM, CI/CD y terceros, mediante cuentas privilegiadas comprometidas o inserción de código malicioso.

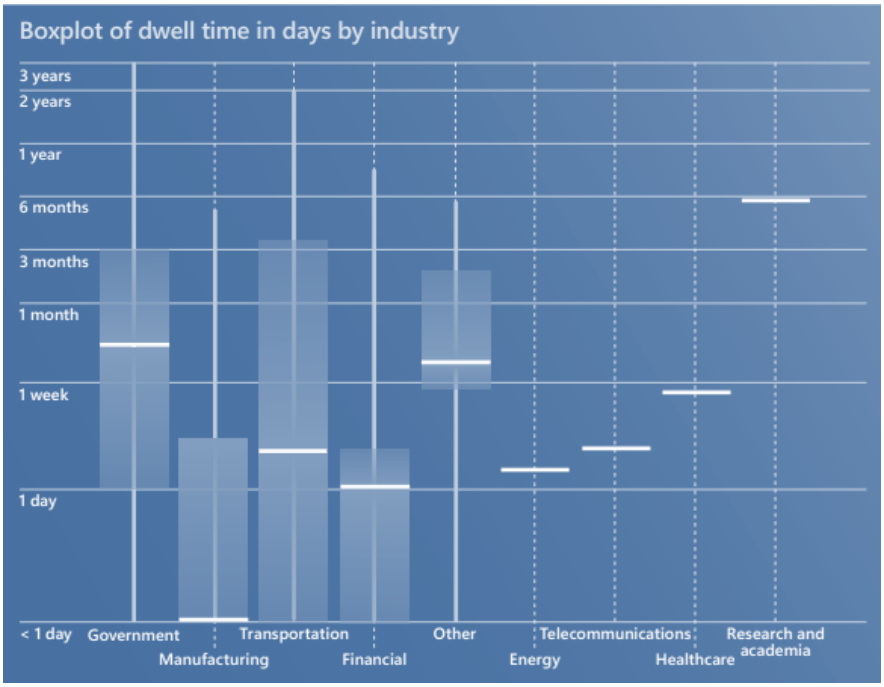
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

- **Infraestructuras descentralizadas y encubiertas**
  Los actores avanzados migrarán hacia redes P2P, blockchain y overlays del dark web para evadir atribución, distribuir malware y sostener operaciones incluso tras intentos de desmantelamiento.

- **Abuso creciente de identidades cloud**
  Aumentará la explotación de OAuth malicioso, autenticación heredada, device-code phishing y AiTM para evadir MFA y mantener acceso persistente, requiriendo mayor gobernanza y control continuo de tokens.

- **Expansión del mercado de intrusión comercial**
  Los *cyber mercenaries* ofrecerán capacidades ofensivas cada vez más disruptivas, facilitando sabotaje e interferencia con alta precisión y baja detección, dificultando la atribución y respuesta.

Un aspecto especialmente relevante para operaciones de seguridad es la gráfica de **tiempo de permanencia del adversario** (*dwell* en inglés).



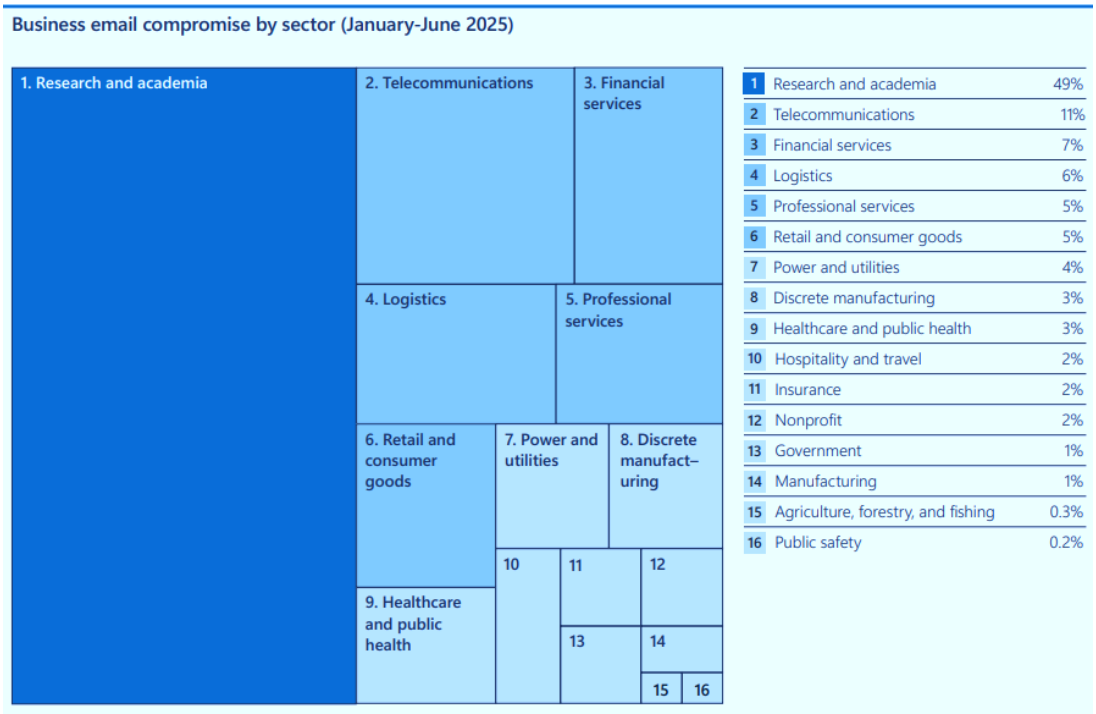
Tiempo de permanencia de los cibercriminales en el objetivo (mediana y rango min/máx). Fuente: MS (2025)

Microsoft muestra como muchos ataques consuman exfiltración o movimiento lateral en **menos de 24 horas**, y en un volumen significativo de casos **dentro de la primera hora**. Este dato refuerza la idea de que la defensa moderna exige **agilidad en detección**

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

y respuesta, reduciendo al mínimo la ventana de operación del adversario antes de que alcance sistemas críticos.

Por último, para ilustrar la importancia de la ingeniería social: en cuanto al **fraude BEC** (Business Email Compromise, o phising corporativo sofisticado), Microsoft destaca que representa una proporción creciente de incidentes graves, impulsado por el compromiso de credenciales y el uso de técnicas de ingeniería social cada vez más sofisticadas, incluyendo deepfakes de voz y manipulación de identidades digitales.



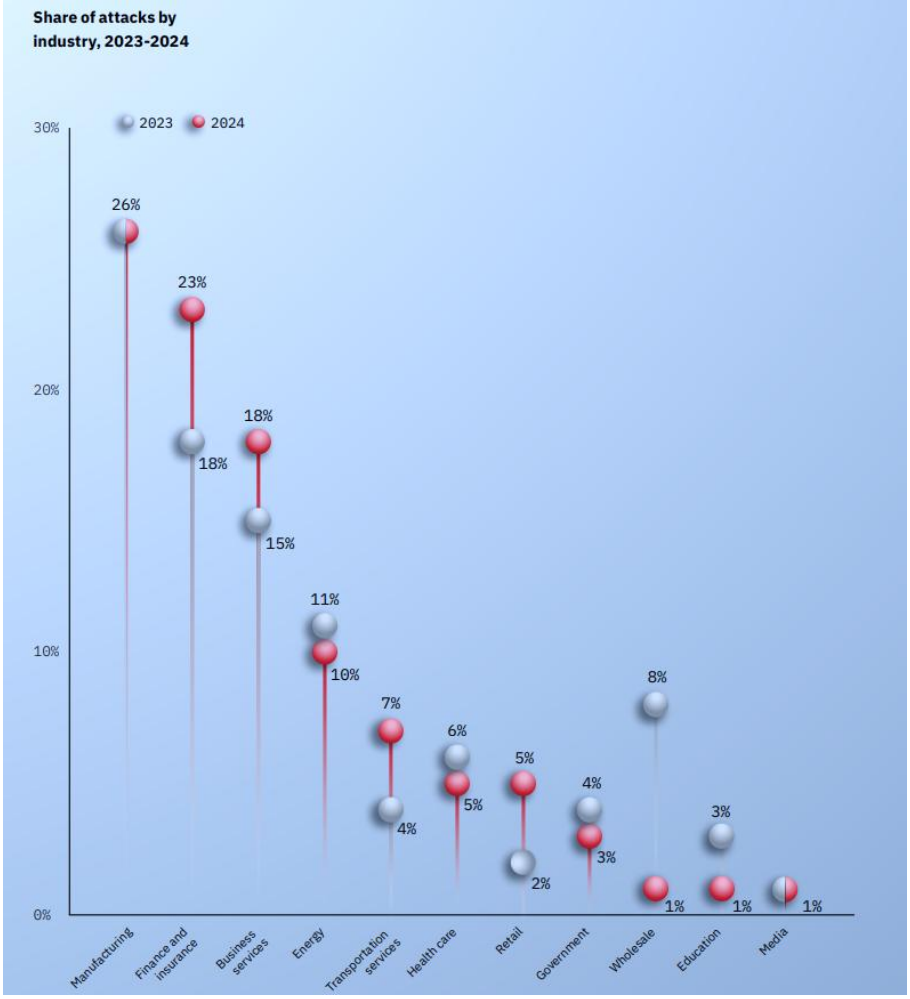
Ataques de ingeniería social BEC por sector en H1 2025. Fuente: Microsoft (2025)

El ***IBM X-Force Threat Intelligence Index 2025*** [32] describe un panorama dominado por adversarios cada vez más difíciles de detectar, capaces de operar con mayor sigilo y apoyados en vastos ecosistemas clandestinos que facilitan desde la venta de credenciales hasta la distribución de herramientas para intrusiones complejas. La introducción del informe advierte que los atacantes ya no necesitan "forzar la entrada": **simplemente inician sesión con credenciales robadas**, lo que les permite ocultar su actividad durante semanas y convertir cada brecha en una puerta de acceso a campañas más amplias y coordinadas. Este desplazamiento táctico sitúa a la **identidad y a la cadena de suministro digital** en el centro del riesgo.

En este contexto, uno de los mensajes más contundentes del informe es que **manufactura ha vuelto a ser el sector más atacado por cuarto año consecutivo**. La razón no es únicamente su peso en la economía: muchas organizaciones manufactureras

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

continúan operando con arquitecturas heredadas, sistemas OT expuestos y alta dependencia de activos críticos que no pueden detenerse. Eso explica que los impactos más frecuentes —según IBM— incluyan **extorsión (29%) y robo de datos (24%)**, así como el hecho de que manufactura registrara **el mayor número de casos de ransomware en 2024**, contraviniendo la tendencia global de descenso de este malware.



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

Otro cambio estructural observado en 2024 es el **aumento del 84% en infostealers (malware para robo de información) distribuidos a través de campañas de phishing**. Este fenómeno es especialmente relevante porque convierte al correo electrónico en un **vector invisible de compromiso**, capaz de proporcionar a los atacantes credenciales válidas que luego utilizan en intrusiones prolongadas basadas en identidad. Se señala que, a diferencia de un ataque de ransomware, cuya detección adopta ser inmediata, los infostealers permiten mantener un acceso silencioso y persistente, retrasando la reacción de los equipos defensivos.

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

A escala geográfica, Europa fue en 2024 **la tercera región más atacada**, concentrando el **24% de los incidentes** analizados por IBM. El vector inicial más habitual fue la **explotación de aplicaciones expuestas (36%)**, que dio paso a acciones como **acceso a servidores (15%)**, uso de **herramientas de adquisición de credenciales (12%)** y **ransomware o malware asociado (9%)**.

En cuanto a los impactos, predominó claramente el **credential harvesting** (o manipulación para que el usuario entregue sus credenciales) **(46%)**, seguido de **fugas de datos (31%)** y **robo de información (15%)**, reflejando una orientación clara hacia la monetización de datos sensibles. Sectorialmente, destacaron **servicios profesionales, de negocios y consumo (38%)**, por delante de **finanzas y seguros (18%)** y **manufactura (18%).**

A nivel de países, el **Reino Unido** fue el más afectado (**25%** de los incidentes europeos), seguido de **Alemania (18%)** y **Austria (14%)**.

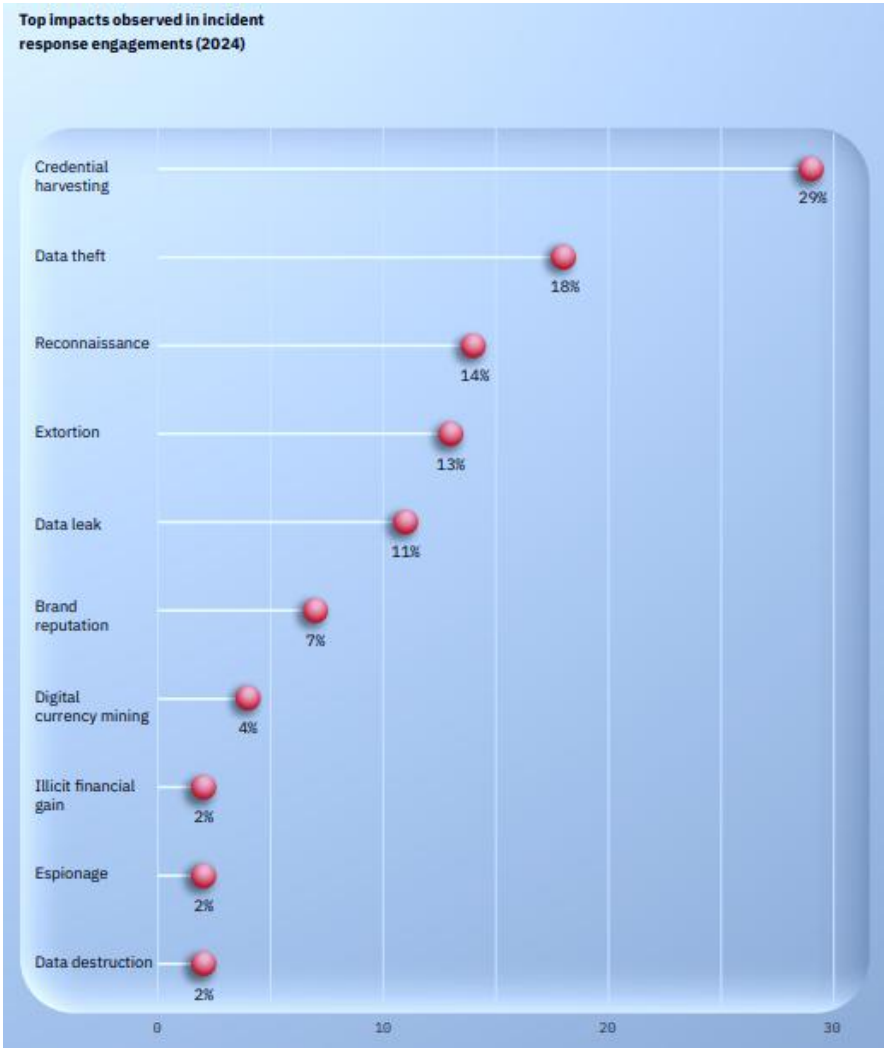
El informe también dedica atención al papel de la **inteligencia artificial**, observando que su adopción por parte de actores maliciosos es ya un hecho consolidado. IBM documenta casos en los que la IA se emplea para crear sitios web fraudulentos, generar código malicioso, elaborar correos de phishing altamente verosímiles e incluso producir **deepfakes** para reforzar campañas de ingeniería social. La IA no sólo acelera el proceso, sino que también reduce la barrera de entrada, permitiendo que actores menos sofisticados ejecuten operaciones más avanzadas. Más detalle en la siguiente sección.

Asimismo, el informe alerta de que **uno de cada cuatro ataques contra infraestructuras críticas comenzó explotando aplicaciones expuestas a Internet**. Tras el acceso inicial, los adversarios realizan escaneos activos, identifican nuevas debilidades y buscan escalar privilegios para moverse lateralmente. IBM hace hincapié en los riesgos derivados de los **tiempos de permanencia (dwell) prolongados vistos anteriormente en el informe de Microsoft** [31]**, que permiten** a los actores utilizar la estrategia de "vivir de la tierra" (*living-off-the-land*), es decir, operar con herramientas legítimas del sistema comprometido, dificultando su detección.

En relación con el ransomware, aunque IBM observa un descenso general en incidentes por tercer año consecutivo, este tipo de malware sigue representando el **28% de los casos de malware analizados**. El aparente declive no debe confundirse con una pérdida de relevancia: en la dark web, la actividad asociada a ransomware **aumentó un 25%**, impulsada por tácticas de múltiple extorsión y por la capacidad de operar en

entornos híbridos (Windows y Linux). Este comportamiento bifásico —reducción de incidentes detectados pero aumento de actividad subterránea— confirma que los grupos están a adaptando su modelo de negocio para minimizar exposición y maximizar beneficios.

En cuanto a **impactos globales**, el **robo de credenciales fue el impacto más común, presente en el 29% de los incidentes**, seguido del **robo de datos (18%)** y diversas **formas de extorsión (13%).**



Principales impactos observados en ciberincidentes en 2024. Fuente: IBM X-Force (2025)

Casi la mitad de los ataques conllevó el robo de credenciales o datos sensibles, lo que subraya la prioridad absoluta de proteger identidades y flujos de información.

El informe cierra con una revisión por sectores que confirma la **persistencia de manufactura como objetivo principal**. El **sector financiero y de seguros se sitúa en segundo lugar**, destacando la importancia de las campañas de phishing y la explotación

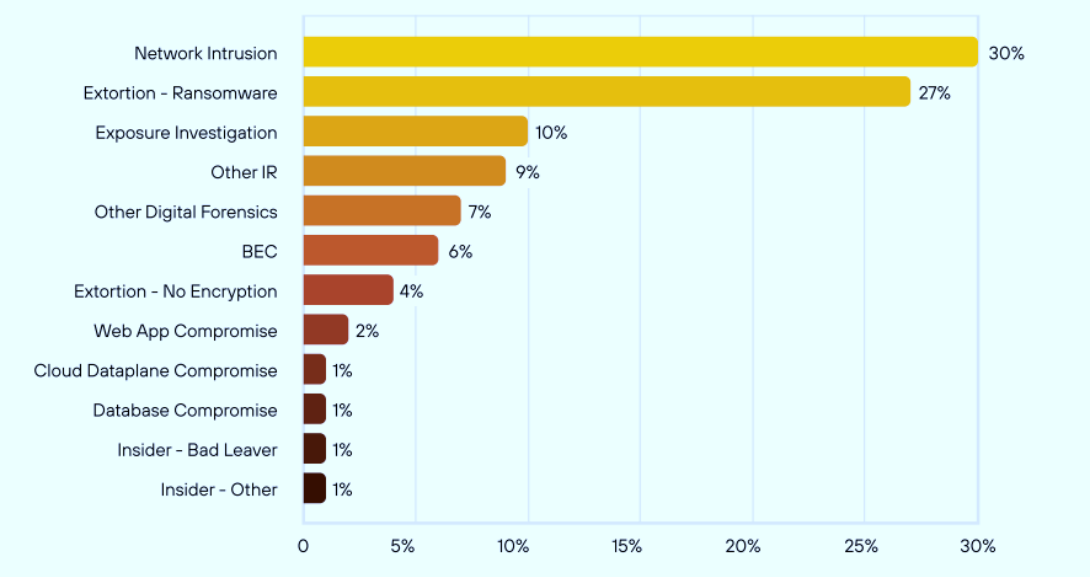
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

de credenciales. En tercer lugar, aparecen los **servicios profesionales, de negocios y consumo**, particularmente expuestos por su dependencia de aplicaciones accesibles desde Internet y por su alto volumen de datos sensibles. Sectores como energía, transporte, retail y salud también presentan patrones distintivos, pero todos comparten una misma constante: **el robo de credenciales y la exfiltración de datos como ejes centrales de las campañas maliciosas**.

El ***Global Incident Response Report 2025*** de Palo Alto Networks [33], elaborado por el equipo Unit 42 a partir de **más de 500 ciberincidentes reales a 38 países y múltiples verticales**, ofrece una buena panorámica de operaciones de gestión de incidentes.

Apunta a un incremento de ataques con objetivos no sólo económicos, sino también disruptivos: **sabotaje, degradación de servicios y parálisis operativo como método de presión**. Además, identifica **deficiencias sistemáticas en la gestión de identidades (IAM)** como un vector de riesgo crítico.

La amplitud del conjunto de casos permite apreciar cómo **la naturaleza de los ataques varía sensiblemente según región e industria**, algo que puede ilustrarse mediante las siguientes figuras. Ambas ayudan a contextualizar la diversidad de tácticas adversarias y la necesidad de adaptar las defensas a cada entorno:



Tipo de investigaciones por región (Europa). Fuente: Unit 42 Palo Alto (2025)

A partir de este corpus global, Unit 42 identifica **cinco tendencias emergentes** que, en conjunto, explican la aceleración y complejidad del panorama actual. Estas tendencias están asociadas tanto a la cibercriminalidad económica como a las operaciones de

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

Estados, amenazas internas e incluso hacktivismo, conformando un escenario en el que la motivación del atacante no cambia, pero sí lo hace su capacidad para causar impacto.

1. La tercera onda de extorsión

La primera tendencia destacada por Unit 42 **es la evolución de los ataques de extorsión**, que ya no se limitan al cifrado de archivos ni siquiera al modelo de doble extorsión con robo de datos. Según Palo Alto, estamos inmersos en una **tercera ola**, donde el objetivo principal es provocar **interrupciones operativas deliberadas** capaces de paralizar servicios esenciales y aumentar la presión económica sobre la víctima.

En 2024, **el 86% de los incidentes atendidos por Unit 42 generaron pérdidas operacionales, reputacionales o financieras**, desde tiempos de inactividad prolongados hasta daños en la relación con clientes y socios. Esta transición puede verse claramente en la gráfica sobre **tácticas de extorsión**, que ilustran cómo la combinación de cifrado, exfiltración, acoso y sabotaje se ha convertido en el 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. Fuente: Unit 42 Palo Alto (2025)

La explicación de esta evolución es doble: por una parte, la mejora de las defensas y las copias de seguridad reduce la efectividad de la mera encriptación; por otra, **la fatiga social ante filtraciones de datos disminuye** el impacto psicológico del chantaje. Ante ello, los atacantes encontraron en la interrupción del negocio el mecanismo más directo para exigir rescates más altos y acelerar pagos.

El informe insiste en que la respuesta más eficaz es reforzar la **resiliencia operativa**:

- Pruebas periódicas de continuidad de negocio y simulaciones de incidentes;
- Procesos de restauración verificables;
- Separación de dominios críticos;

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

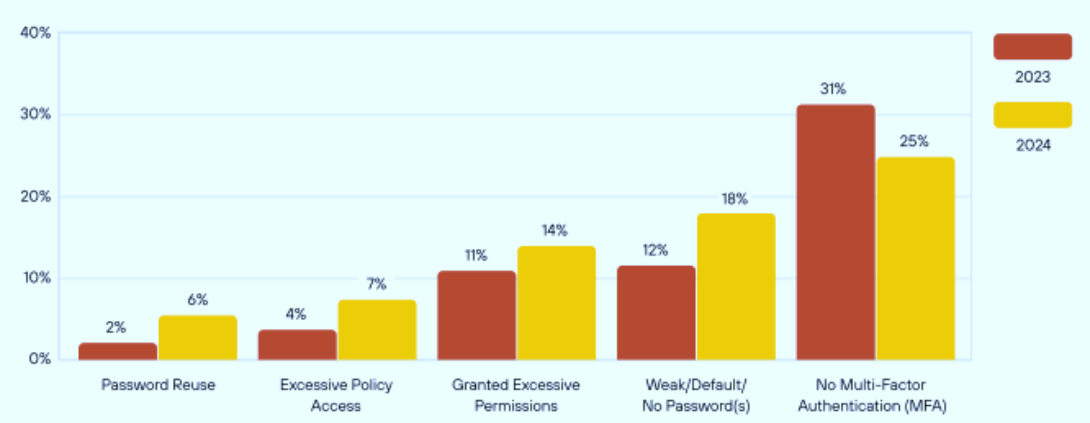
- Mecanismos de contención que permitan operar parcialmente incluso bajo ataque.

2. Cadena de suministro software y explotación en la nube

La segunda tendencia **es la amplificación del impacto asociado a la cadena de suministro software y a la explotación de entornos cloud**. Casi un tercio de los incidentes de 2024 estuvo relacionado con entornos SaaS o recursos cloud, y en uno de cada cinco casos los atacantes lograron causar daños operativos en dichas plataformas.

Unit 42 documenta casos en los que credenciales expuestas, configuraciones incorrectas o uso de contraseñas obsoletas han permitido a los adversarios **insertar infraestructura maliciosa dentro del propio entorno cloud de la víctima**, utilizándola como trampolín para ataques a terceros. En campañas sofisticadas se han llegado a escanear **más de 230 millones de objetivos únicos**, evidenciando el poder multiplicador de un punto débil en la nube.

Un elemento especialmente crítico es la gestión de identidades: el informe muestra un deterioro en varios parámetros clave —permisos excesivos, políticas laxas y fallos en rotación de claves—, como se muestra a continuación:



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

Para limitar este riesgo, desde Palo Alto recomiendan:

- Controles estrictos de **IAM** y privilegios mínimos;
- Uso de credenciales de corta duración y MFA consistente;
- Centralización de logs y auditorías en la nube;
- Monitorización de patrones de uso y detección de anomalías;

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

- Refuerzo de APIs y componentes de la cadena de suministro (incluyendo OSS).

La clave es asumir que la nube, por su elasticidad y conectividad, puede convertirse tanto en el **activo más productivo** como en **la superficie de ataque más peligrosa** si no existe gobernanza adecuada.

3. Velocidad: los ataques se aceleran y reducen drásticamente las capacidades de reacción

Una de las conclusiones más preocupantes del informe es la **aceleración extrema de los ataques**. La automatización, el uso *de* toolkits RaaS (Ransomware como servicio) y la integración de IA permiten a los adversarios identificar vulnerabilidades, moverse lateralmente y exfiltrar datos en tiempos que hace pocos años eran impensables.

En 2024, el **tiempo mediano de exfiltración fue de apenas dos días**, pero en el 25 % de los casos ocurrió en menos de cinco horas, y en el 19 %, **en menos** de una hora desde el compromiso inicial. Esta compresión temporal exige reformular las capacidades de detección: **una organización que necesite varias horas para confirmar un incidente ya está fuera de ventana**.

Acciones que pueden llevar a cabo:

- Medición estricta **de MTTDs** (tiempo medio entre caídas) y **MTTRs** (tiempo medio de reparación/respuesta);
- Analítica y correlación impulsadas por IA;
- **Playbooks automáticos** (manuales de respuesta a incidentes) que aíslen cuentas o endpoints sin intervención humana;
- Ejercicios continuos de *red teaming* y simulaciones aceleradas;
- Priorización de activos críticos para respuesta ultrarrápida.

La idea central es contundente: **la velocidad ofensiva ya supera a la defensa tradicional,** y sólo mediante automatización y visibilidad continua se puede equilibrar esta asimetría.

4. Amenaza interna: proliferación de operaciones norcoreanas altamente sofisticadas

La cuarta tendencia es el notable incremento de **amenazas internas**, protagonizadas de forma destacada por operaciones norcoreanas. Unit 42 documenta un crecimiento de un

300% en este tipo de casos, en los que operadores encubiertos logran acceder a puestos técnicos en organizaciones internacionales usando identidades sintéticas, portafolios creíbles y procesos de selección externalizados.

Una vez dentro, estos "IT workers" pueden:

- Exfiltrar información sensible de forma sistemática;
- Introducir herramientas no autorizadas;
- Manipular código fuente;
- Habilitar accesos persistentes;
- O incluso derivar hacia esquemas de extorsión.

Se advierte que su verdadero peligro reside en su legitimidad aparente: **no violan controles perimetrales, porque entran por la puerta principal**. Algunas contramedidas plausibles:

- Verificación reforzada de personal técnico y contratistas;
- Políticas de privilegios mínimos y revisión periódica de accesos;
- Monitorización basada en comportamiento, no sólo en indicadores técnicos;
- Correlación de señales dispersas (accesos inusuales, transferencias anómalas, actividad fuera de horario).

El mensaje es claro: la amenaza interna, especialmente cuando está apoyada por Estados, exige **modelos de confianza condicional y vigilancia continua**.

5. Aparición de ataques asistidos por IA

Por último, Unit 42 identifica la **emergencia de ataques asistidos por IA generativa**. Aunque aún están en una fase inicial, ya permiten campañas de phishing altamente verosímiles, creación automatizada de malware, ofuscación de código y optimización de exploits. Los laboratorios demostraron que una cadena de ataque que antes requería dos días, puede completarse en **25 minutos** cuando se integra IA en cada fase.

Posibles acciones a llevar a cabo:

- **Despliegue de sistemas defensivos basados en IA** para igualar velocidad;
- **Formación específica en detección de correos**, contenidos y deepfakes generados por IA;

- Incorporación de **tácticas de IA adversaria** en ejercicios de crisis;
- Automatización de **flujos de contención**.

La IA no sólo acelera los ataques: **aumenta su realismo y reduce el umbral de habilidad necesario para ejecutarlos**.

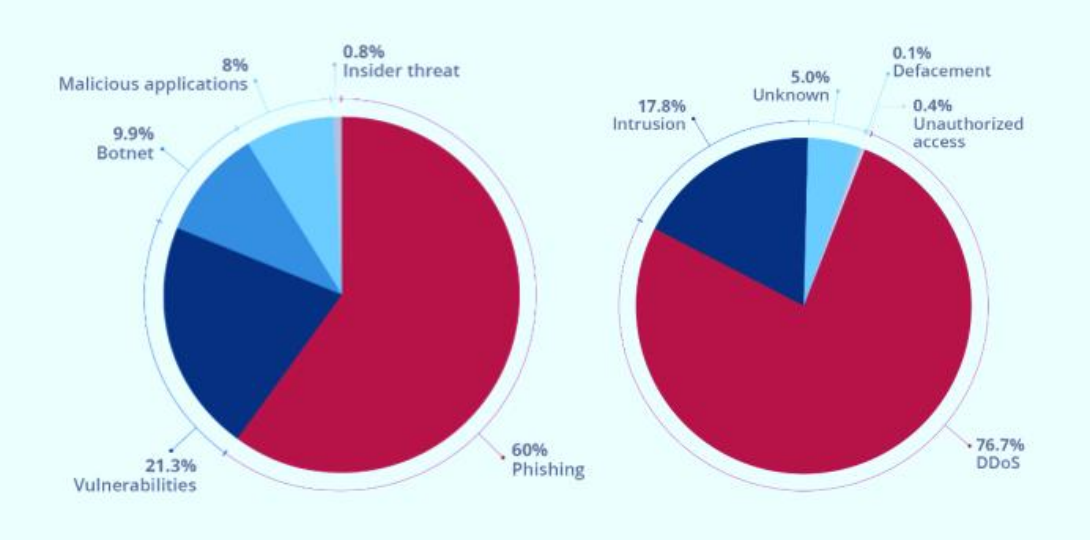
3.2.2 Europa

El **ENISA Threat Landscape 2025** [34] constituye uno de los análisis más amplios y sistemáticos del ecosistema de amenazas en Europa. Elaborado a partir de **casi 4.900 incidentes** reportados entre julio de 2024 y junio de 2025, describe un panorama marcado por la convergencia de cibercrimen, operaciones ideológicas y capacidad ofensiva de actores estatales. Aunque la mayoría de los incidentes registrados se corresponden con campañas de **motivación política —principalmente DDoS—**, las amenazas más lesivas en términos operativos y económicos siguen siendo **el ransomware**, el **robo y filtración de datos y la explotación de vulnerabilidades**. ENISA señala que Administraciones públicas, transporte, logística, servicios digitales y, de manera creciente, **infraestructuras industriales (ICS)**, figuran entre los objetivos prioritarios de los adversarios.

Panorama europeo

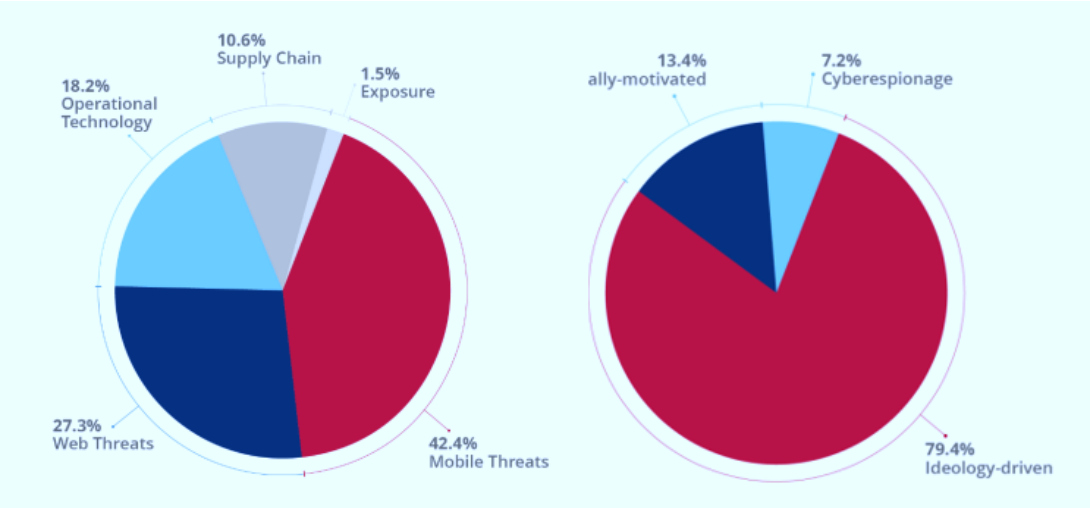
La sección introductoria del informe detalla la distribución y tipología de los incidentes observados, lo que permite caracterizar la actividad maliciosa en Europa con una visión comparativa. ENISA identifica un volumen sostenido de ataques de denegación de servicio —orquestados tanto por colectivos hacktivistas como por actores criminales que buscan generar interrupciones visibles— que representan alrededor del **80% de los incidentes registrados**. No obstante, cuando se analiza impacto, severidad y alcance, el protagonismo se desplaza hacia amenazas como **ransomware**, **fugas de datos**, **compromiso de cuentas**, e **intrusiones en redes internas** derivadas de credenciales comprometidas o fallos de configuración.

Las figuras siguientes, proporcionan una visión agregada de la frecuencia y tipología de incidentes, mostrando el predominio de ataques disruptivos frente a intrusiones más silenciosas, pero potencialmente más dañinas:



Vector de ataque principal y tipologías de ciberincidentes europeos. Fuente: ENISA (2025)

Asimismo, las siguientes ofrecen un desglose de **tipologías de objetivo y motivaciones**. El informe destaca que junto con AAPP, transporte y proveedores de servicios digitales, aparecen **entornos ICS** como vector de interés creciente para actores estatales y grupos con capacidad técnica. En cuanto a motivación, se observa un reparto claro entre **ideológica**, **económica** y **estratégica**, dependiendo del tipo de actor y de la región afectada:



Distribución de amenazas y objetivos de los cibercriminales en UE. Fuente: ENISE (2025)

Tendencias generales

El informe desarrolla varias tendencias transversales que explican la evolución del panorama de amenazas en Europa:

1. Persistencia del ransomware y maduración del modelo criminal

ENISA subraya que, a pesar de variaciones anuales en el número de víctimas, el ransomware continúa siendo la amenaza económica más significativa. Evoluciona como venimos diciendo, hacia modelos de **múltiple extorsión**, donde se combinan cifrado, robo de datos, chantaje directo y presión reputacional mediante sitios de filtraciones.

2. Explotación sistemática de vulnerabilidades recientes

Una parte importante de los incidentes más graves se inicia con la explotación de fallos publicados semanas o incluso días antes, especialmente en dispositivos perimetrales y servicios expuestos. La rapidez con la que los atacantes integran nuevas vulnerabilidades en sus campañas sigue siendo un factor crítico de riesgo.

3. Compromiso de identidades y abuso de credenciales

De la misma manera que otras agencias, ENISA observa un aumento continuado de incidentes basados en **credenciales robadas, accesos cloud mal configurados** y **phishing avanzado**, que constituyen uno de los vectores de entrada más efectivos. La monetización de accesos iniciales en mercados clandestinos amplifica este fenómeno, como veremos posteriormente en el informe de CrowdStrike de manera gráfica.

4. Ataques disruptivos e ideológicos

El informe documenta un incremento sostenido de campañas motivadas por conflictos geopolíticos, especialmente DDoS y defacement, impulsadas por colectivos alineados con bandos enfrentados. Aunque su impacto técnico acostumbra a ser limitado, su volumen explica su presencia dominante en las estadísticas.

5. Expansión del ecosistema de ciberdelincuencia

La profesionalización de infraestructuras como servicio (ransomware, botnets, infostealers, IABs) facilita que actores con poca capacidad técnica ejecuten ataques sofisticados a gran escala, reduciendo drásticamente la barrera de entrada.

6. Amenazas a la cadena de suministro

ENISA identifica un aumento de incidentes originados en proveedores tecnológicos, servicios cloud y software de terceros. La complejidad de las interdependencias digitales sigue generando riesgos sistémicos, especialmente para sectores regulados y operadores esenciales.

7. Empleo de inteligencia artificial por parte de los atacantes

El informe confirma un incremento notable de campañas que integran **IA generativa**, desde la elaboración de phishing altamente convincente hasta la automatización de fases de reconocimiento. ENISA menciona esta tendencia como relevante, pero advierte que su impacto operativo concreto se analizará en mayor profundidad en futuras ediciones; en este informe se trataba como un vector emergente, no aún dominante. Más, en la siguiente sección.

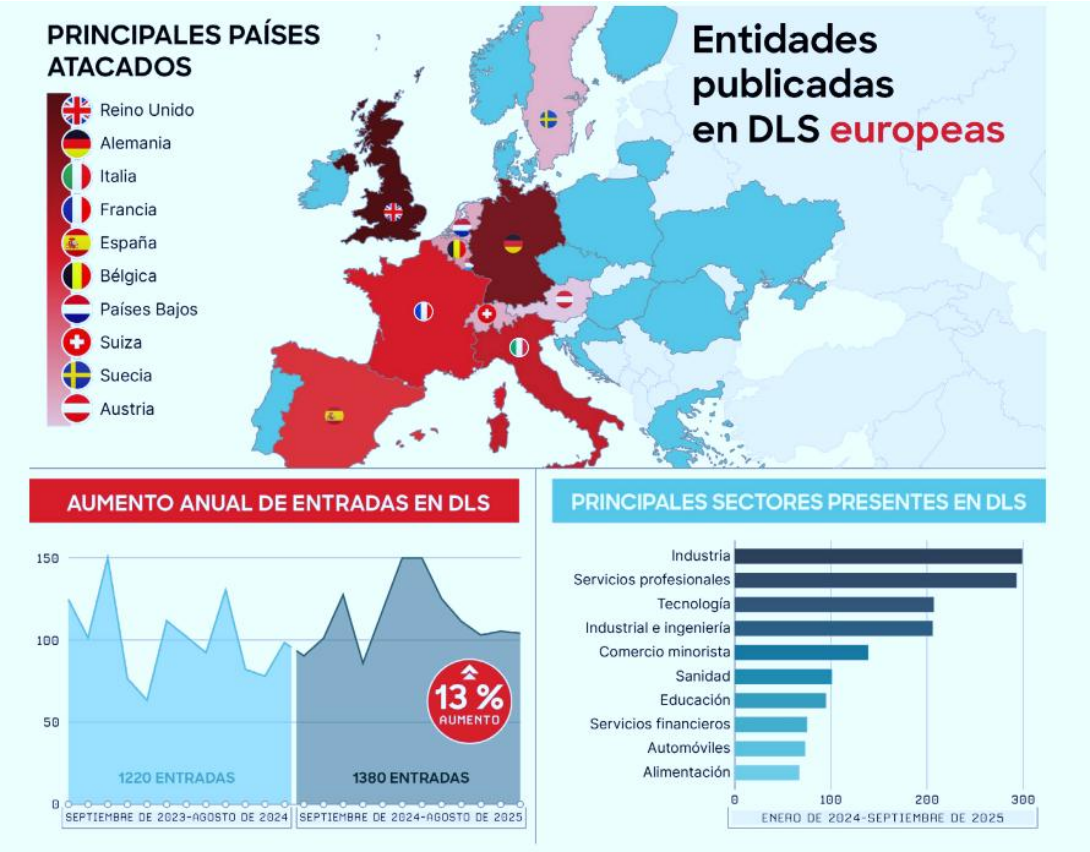
Por último, a nivel europeo, el **CrowdStrike European Threat Landscape Report 2025** [35] ofrece una visión detallada de la evolución de las amenazas en el continente, situando a Europa como uno de los principales escenarios de actividad tanto para actores criminales como para grupos con motivación política o estratégica.

En su resumen destaca una tendencia ya consolidada: el ransomware continúa siendo el vector de mayor impacto, y **el 92% de las víctimas europeas aparecen finalmente listadas en sitios de filtración**, lo que refleja la centralidad de la extorsión basada en robo y publicación de datos. El informe sitúa además la **velocidad operativa de los adversarios**, la disponibilidad de accesos comprometidos en mercados clandestinos y la expansión de actividades contra infraestructuras críticas como los factores que más han transformado el riesgo en el período analizado. A continuación, se desarrollan sus ideas más destacables.

Robo de datos e incidentes recientes

El informe documenta un patrón claro: los adversarios en Europa se focalizan cada vez más en **exfiltrar datos antes de cifrar o interrumpir operaciones**, consolidando un modelo híbrido de monetización que combina venta de información sensible, extorsión directa y presión reputacional. La mayoría de los incidentes analizados muestra que los atacantes buscan primero garantizar la posesión de datos críticos —credenciales, archivos corporativos, historiales financieros, información operativa— antes de desplegar otras tácticas.

El volumen de daños derivados de estas filtraciones se observa claramente en la siguiente figura, donde se aprecia el crecimiento continuo de incidentes centrados en la exfiltración. CrowdStrike subraya que esta tendencia no sólo afecta a grandes corporaciones, sino también a organizaciones medianas y pequeñas que carecen de una capacidad madura de respuesta y de medidas robustas de gestión de credenciales.



Filtraciones de datos por país europeo, sector y período de tiempo. Fuente: CrowdStrike (2025)

La economía del acceso inicial

Uno de los elementos más relevantes del informe es el análisis dedicado a los **intermediarios de acceso inicial** (IAB, por sus siglas en inglés). Se confirma que en 2024–2025 se consolidó un mercado sumamente activo donde se comercializan **credenciales válidas, accesos VPN comprometidos, sesiones cloud y puntos de entrada en sistemas corporativos**. Estos IABs actúan como proveedores para operadores de ransomware, grupos criminales y, en ocasiones, actores estatales, reduciendo drásticamente la barrera de entrada para ejecutar campañas complejas.

El informe incluye un gráfico específico sobre la actividad de estos intermediarios, que ilustra la magnitud de la 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. Fuente: CrowdStrike (2025)

Este fenómeno enlaza directamente con lo observado en el informe de ENISA, donde también se destacaba la importancia creciente de la economía clandestina de accesos para facilitar ataques posteriores, incluidos los dirigidos a infraestructuras industriales.

Ataques contra sistemas de control industrial

El informe adicional una sección específica a los sistemas **de control industrial**, destacando que en 2024–2025 se observó una **creciente atención de actores criminales, hacktivistas y grupos con motivaciones geopolíticas** hacia infraestructuras OT europeas. Según el análisis del proveedor, buena parte de esta actividad se ha concentrado en sectores como **energía, fabricación avanzada y ámbitos vinculados a la defensa**, donde la interdependencia entre procesos físicos y sistemas digitales incrementa tanto el atractivo como el potencial impacto de una intrusión.

Se señala que los ataques detectados se dirigieron principalmente a **obtener acceso no autorizado a redes industriales**, con el fin de **cosechar información sobre procesos, configuraciones técnicas y arquitecturas de planta**. En varios casos, los adversarios han tratado además de **interferir en operaciones**, aprovechando debilidades comunes como **la segmentación insuficiente**, el uso de activos **obsoletos** o **la exposición inadvertida de servicios industriales** a Internet. El informe destaca que estas intrusiones no siempre buscaban la interrupción inmediata: en numerosos incidentes,

la prioridad del atacante era **situarse dentro del entorno OT**, obtener conocimiento detallado y preparar posibles operaciones de mayor alcance.

Concluyen que **la superficie de ataque OT en Europa continúa ampliándose**, especialmente allí donde la convergencia entre redes IT y OT no está apoyada por controles de seguridad específicos. Esta dinámica explica la creciente presencia de actores avanzados y grupos criminales en este tipo de entornos (más detalle respecto a esta cuestión de actores y técnicas, tácticas y procedimientos, en una edición posterior).

3.2.3 España

El informe ***CCN-CERT IA-04/24 Ciberamenazas y Tendencias 2024*** [36] constituye el **análisis más actualizado a nivel nacional a fecha de elaboración de este informe, sobre la evolución de las amenazas estratégicas que afectan a España**. Su lectura permite comprender cómo actores estatales, cibercriminales y grupos hacktivistas están adaptando sus tácticas en un contexto marcado por la guerra en Ucrania, la inestabilidad en Oriente Medio y la consolidación del ecosistema del ransomware. Aunque el documento no está específicamente orientado a ICS, muchas de sus conclusiones tienen implicaciones directas para los entornos industriales, especialmente aquellos donde la visibilidad, la segmentación y la gestión de vulnerabilidades continúa siendo insuficiente.

Actores estatales

El informe identifica a **Rusia, China, Corea del Norte e Irán** como los principales impulsores de campañas de ciberespionaje dirigidas contra España y otros países occidentales. Sin descender al detalle de cada grupo operativo, el CCN-CERT describe patrones comunes: operaciones prolongadas, alta orientación a la obtención de inteligencia, explotación preferente de vulnerabilidades recientes y, en el caso de Rusia y China, campañas sincronizadas con objetivos geopolíticos o militares.

Los actores **rusos** centran gran parte de su actividad en organismos gubernamentales y aliados de Ucrania, con especial interés en comprometer redes institucionales y obtener información diplomática y estratégica. **China**, por su parte, mantiene una aproximación amplia, combinando espionaje económico e intrusiones orientadas a sectores tecnológicos y de I+D. **Corea del Norte** continúa caracterizándose por la motivación financiera —especialmente mediante compromisos de infraestructura crítica—, ataques a entidades financieras y robo de criptodivisas—, mientras que **Irán** combina

espionaje, operaciones de influencia y ataques oportunistas que buscan generar disrupción o presión política.

El CCN subraya que España figura de manera recurrente entre los objetivos de estas campañas debido a su alineamiento internacional y al valor de sus activos públicos y privados.

De nuevo a continuación, se desgranan las principales enseñanzas del informe.

Tendencias de ciberespionaje

El estudio describe un incremento significativo de las operaciones **de ciberespionaje**, tanto en número como en sofisticación. Una parte sustancial de estas campañas se dirige a **gobiernos, organismos internacionales, centros de investigación, diplomacia y sectores estratégicos**, utilizando técnicas que permiten mantener el acceso de forma prolongada: explotación de vulnerabilidades perimetrales, cadenas de ataque multietapa, movimiento lateral discreto y uso de malware modular.

Se destacan tres tendencias relevantes:

- **Reducción del umbral técnico** requerido para ejecutar campañas de espionaje, gracias a la disponibilidad de herramientas avanzadas y kits de explotación.
- **Mayor grado de automatización**, que reduce tiempos entre la explotación inicial y el establecimiento de persistencia.
- **Extensión de los objetivos**, donde sectores tradicionalmente menos expuestos —educación, logística, transporte o sanitario— se integra en el mapa de interés de actores estatales.

Ransomware

El CCN-CERT describe la persistencia del **ransomware como amenaza principal** para organizaciones públicas y privadas españolas. A pesar de los esfuerzos internacionales por desmantelar infraestructuras criminales, el modelo **ransomware-as-a-service (RaaS)** sigue en crecimiento: nuevos afiliados se incorporan con rapidez, el coste de entrada es bajo, y la disponibilidad de accesos iniciales mediante credenciales robadas o vulnerabilidades en dispositivos perimetrales facilita las intrusiones.

El informe analiza la evolución reciente del ransomware, marcada por:

- **Modelos de triple (incluso cuádruple extorsión)**, que combinan cifrado, robo de datos, publicación en leak sites y acoso directo a empleados o clientes.
- **Altísima orientación a monetización de datos**, especialmente en sectores donde su valor es mayor (finanzas, sanidad, administraciones públicas).
- **Uso intensivo de vulnerabilidades públicas**, con preferencia por dispositivos VPN, firewalls y soluciones de acceso remoto.

Aunque no se trate de un fenómeno puramente industrial, muchos operadores de ransomware han mostrado interés creciente en **interrumpir procesos productivos** como vía de presión, lo que podría impactar en infraestructuras industriales españolas si persisten debilidades estructurales en ICS.

Filtraciones de datos

El informe aborda el incremento de **filtraciones de datos**, tanto por cibercriminales como por actores estatales. En España, el CCN observa que las filtraciones afectan principalmente a **organismos gubernamentales y al sector educativo**, aunque se extienden también a empresas privadas. El mercado negro de datos sigue en expansión, incentivado por la monetización de información sensible y por la reutilización de credenciales en ataques posteriores.

La tendencia más preocupante **es la automatización en la exfiltración y publicación de datos**, que permite a los atacantes operar la gran escala y reducir el riesgo de detección. Estas filtraciones no sólo aumentan el impacto reputacional, sino que alimentan al ciclo de accesos iniciales utilizados en ataques contra ICS, especialmente cuando credenciales corporativas permiten pivotar hacia redes OT insuficientemente aisladas.

Malware

Se dedica un espacio a analizar la evolución del **malware** en 2023–2024, destacando el crecimiento del modelo **malware-as-service (MaaS)** y la oferta de módulos especializados para espionaje, robo de credenciales, persistencia o movimiento lateral. Este ecosistema industrializado facilitan que actores con poca capacidad técnica ejecuten intrusiones avanzadas.

El informe también resalta la actividad significativa **de botnets**, el auge **de troyanos bancarios**, y el uso **de malware modular** adaptable a múltiples fases del ataque. La

diversidad de herramientas permite escalar ataques rápidamente y comprometer infraestructuras amplias con mínima intervención humana.

Recordemos que en el informe de Dragos [30], se profundiza sobre malware especializado para entornos ICS.

Tendencias previstas

El CCN-CERT recoge adicionalmente siete tendencias clave a futuro, que, aunque generalistas, tienen implicaciones relevantes para la industria:

1. **Guerra multidominio**: la convergencia entre operaciones cinéticas, informativas y digitales continuará, lo que aumenta el riesgo de ataques contra infraestructuras críticas, especialmente en sectores como energía, transporte y agua.
2. **Actividad de actores estatales**: se prevé mayor presión sobre países alineados con la UE y la OTAN, lo que puede traducirse en campañas de espionaje y preposicionamiento dentro de redes corporativas con acceso potencial a ICS.
3. **Ransomware**: se mantendrá como la amenaza más rentable para los atacantes; en el contexto industrial, el riesgo principal es la **interrupción operacional** como mecanismo de chantaje.
4. **Cibercrimen**: continuará su expansión, con mayor oferta de accesos iniciales, herramientas de explotación y datos filtrados, facilitando compromisos en cadenas de suministro industriales.
5. **Amenazas a sistemas industriales (ICS)**: el CCN destaca que la falta **de segmentación**, **inventario de activos y telemetría específica** sigue siendo un problema crítico en España. Las tácticas observadas en Europa del Este podrían replicarse fácilmente en nuestro entorno si persisten tensiones geopolíticas.
6. **Vulnerabilidades**: se espera un incremento constante en su explotación, especialmente en dispositivos perimetrales y componentes OT expuestos, donde el ciclo de parcheo acostumbra a ser más lento.
7. **Compromiso de la cadena de suministro**: seguirá siendo un vector prioritario, especialmente en entornos ICS donde proveedores externos, mantenimiento remoto y software especializado amplían la superficie de riesgo.

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

El Centro Criptológico Nacional concluye que, para mitigar estas tendencias, será necesario reforzar las capacidades: llevándolo a nuestro terreno, hablaríamos de **detección avanzada**, formación específica en **seguridad OT**, mejora de la **segmentación y profesionalización del análisis de incidentes** en infraestructuras críticas.

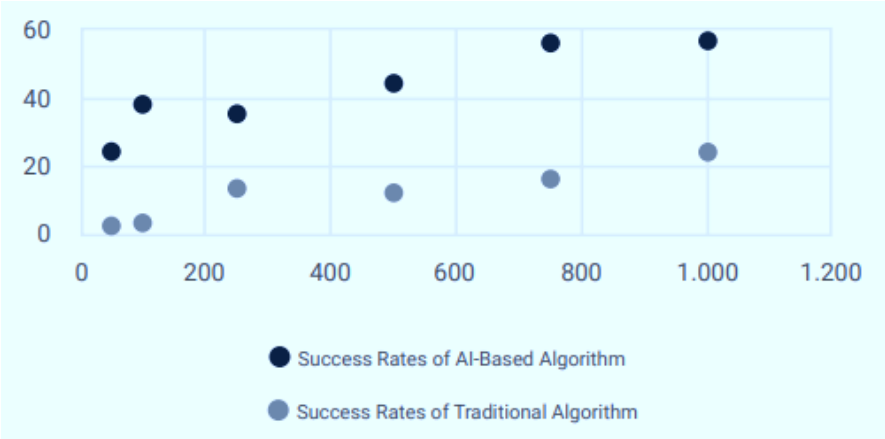
La revisión de la totalidad de las fuentes, sugiere un escenario donde convergen tres grandes amenazas: el **cibercrimen como servicio** (ransomware, BEC, filtración de datos), **el ciberespionaje patrocinado por estados**, y los **ciberataques ideológicos impulsados por conflictos geopolíticos**.

Los **sistemas industriales (ICS/OT)** se han consolidado como **objetivos de alto valor**. Las **vulnerabilidades conocidas**, el **abuso de credenciales y** los **fallos de segmentación** siguen siendo vectores comunes. Las diferencias regionales se manifiestan en el tipo de actores y técnicas empleadas, pero las tendencias son compartidas: **automatización del crimen**, **abuso de AI** (más sobre ello a continuación) y **explotación masiva de acceso remoto**. Este contexto requiere una **respuesta combinada a nivel técnico, organizativo y estratégico** que será detallada en un informe posterior del Observatorio.

3.3 Uso de IA por adversarios

Salvo que se indique lo contrario, los informes referidos a continuación son los mismos de la sección 3.2.

Los análisis recientes coinciden en que los **actores hostiles –tanto criminales como estatales– están adoptando la IA** para potenciar sus ataques. El CCN-CERT destaca, por ejemplo, un **aumento del 967% en campañas de spear phishing** para robo de credenciales gracias a IA, así como un crecimiento del 3.000% en fraudes basadas en deepfakes. En entornos ICS/OT –donde las redes industriales conviven con infraestructuras IT– estas técnicas suponen un riesgo directo: un phishing o deepfake más convincentes pueden engañar a operadores o ingenieros, y propagar malware hasta los sistemas de control. Además, usar IA agiliza ataques técnicos: según el CCN-CERT, **algoritmos de IA han mejorado en un 50% la tasa de éxito en el descifrado de contraseñas** por fuerza bruta, reduciendo el esfuerzo necesario para comprometer accesos de sistemas industriales o redes OT.



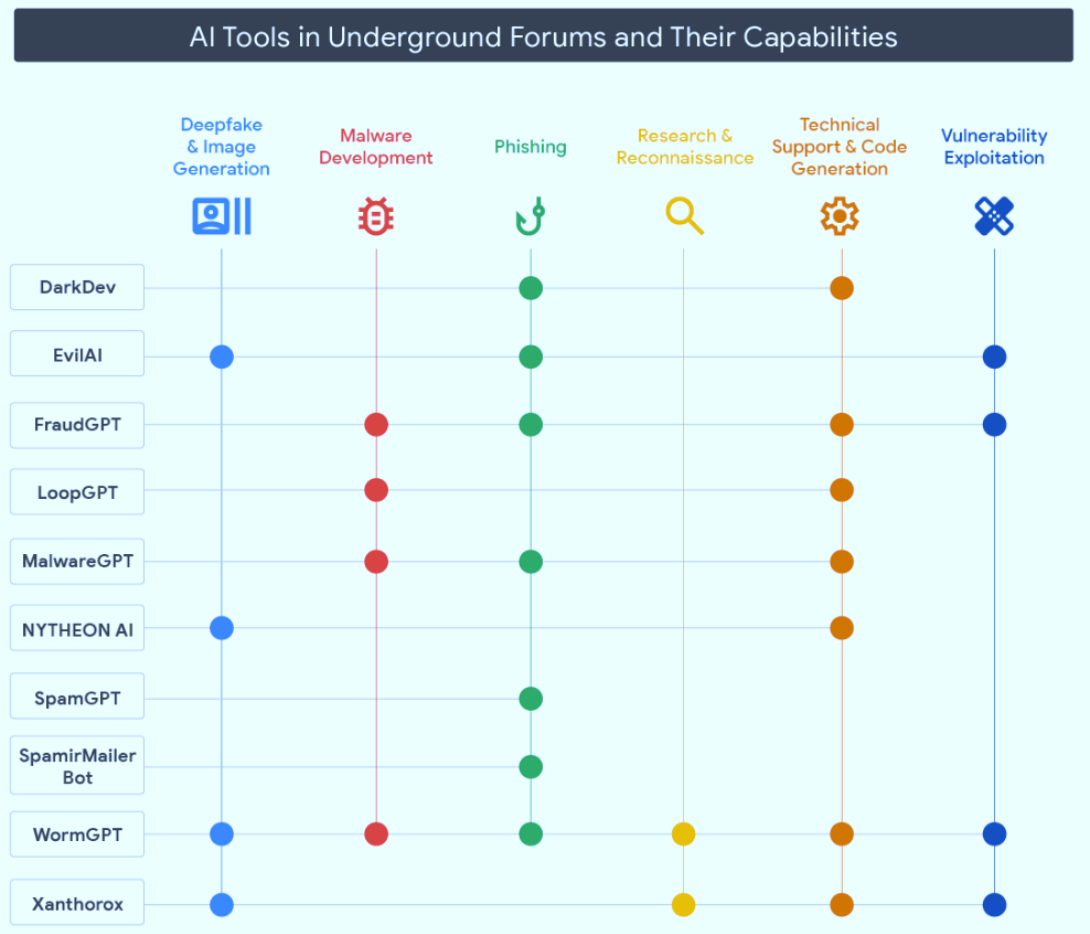
Mejora en descifrado de contraseñas por fuerza bruta apoyada en IA. Fuente: CCN-CERT (2024)

Surgieron también **LLM maliciosos y asistentes automatizados al servicio del cibercrimen.** En 2023 aparecieron herramientas como WormGPT, FraudGPT, DarkBART/DarkBERT, WolfGPT o XXXGPT, diseñadas expresamente para generar correos phishing o código malicioso. Estas *malicious GPTs* ofrecen a atacantes con pocos conocimientos la posibilidad de crear campañas sofisticadas, abaratando la barrera de entrada. El informe del CCN incluye una tabla que muestra como los actores más avanzados obtienen mejoras notables en reconocimiento y malware avanzado con IA, pero incluso los ciberdelincuentes oportunistas logran incrementos apreciables en phishing y movimientos laterales.

Más allá de las herramientas preempaquetadas, se detecta malware que invoca LLMs durante su ejecución. Investigaciones recientes documentan familias que utilizan IA en tiempo de ejecución para **generar dinámicamente comandos maliciosos, adaptar payloads o reescribir su propio código**, dificultando su detección por firmas tradicionales y EDR. También se observa un uso creciente de **ingeniería social inversa contra los propios modelos**, engañándolos para que entreguen información normalmente bloqueada por sus salvaguardas. Nuevas tecnologías, amplían la superficie de ataque.

Paralelamente, el **mercado clandestino de IA se ha consolidado**. El análisis *de Google Threat Intelligence* [37] muestra una oferta estable y madura de herramientas anunciadas en foros underground en inglés y ruso, orientadas a automatizar **phishing altamente personalizado, creación de identidades sintéticas, desarrollo y ofuscación de malware, análisis de vulnerabilidades y apoyo a campañas de desinformación**. Estas soluciones se sirven como servicios llave en mano, integrables en flujos criminales existentes, lo que reduce aún más la barrera de entrada y favorece

la escalabilidad de los ataques. En este punto resulta especialmente relevante introducir la **figura que recoge las capacidades de herramientas de IA maliciosas anunciadas en foros clandestinos**, donde se aprecia la amplitud funcional prometida por estos servicios.



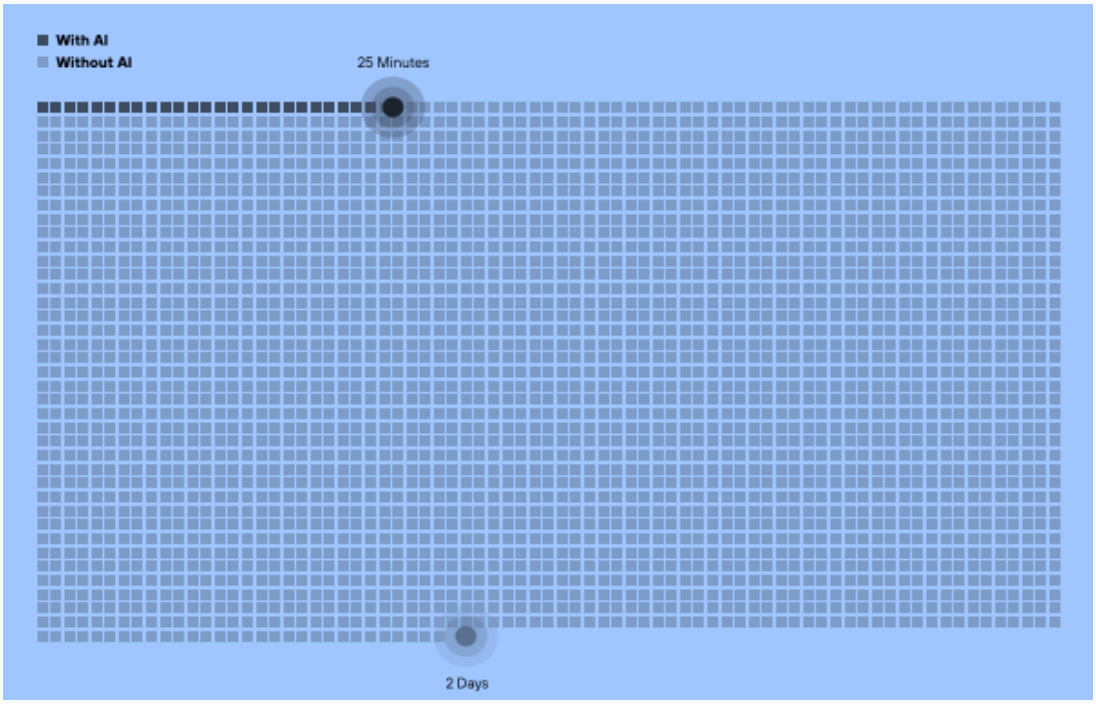
Soluciones basadas en IA en foros clandestinos en inglés y ruso. Fuente: Google Threat Intelligence (2025)

Los actores estatales también están incorporando IA en todas las fases de sus ciberoperaciones. ENISA señala que el uso de IA por parte de adversarios se ha generalizado como **factor habilitador transversal**, especialmente en las fases de reconocimiento, ingeniería social y evasión, incrementando la eficacia de técnicas ya conocidas sin necesidad de introducir TTPs radicalmente nuevas. Esta adopción permite campañas más persistentes, mejor adaptadas al contexto del objetivo y con menor coste operativo.

Se observó el uso de IA para **reconocimiento de objetivos, generación de cebos de phishing multilinguaje, automatización del movimiento lateral y aceleración de la exfiltración de datos**. En este sentido, el informe de Unit 42 de Palo Alto Networks resulta especialmente ilustrativo: en simulaciones controladas, la integración de IA

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

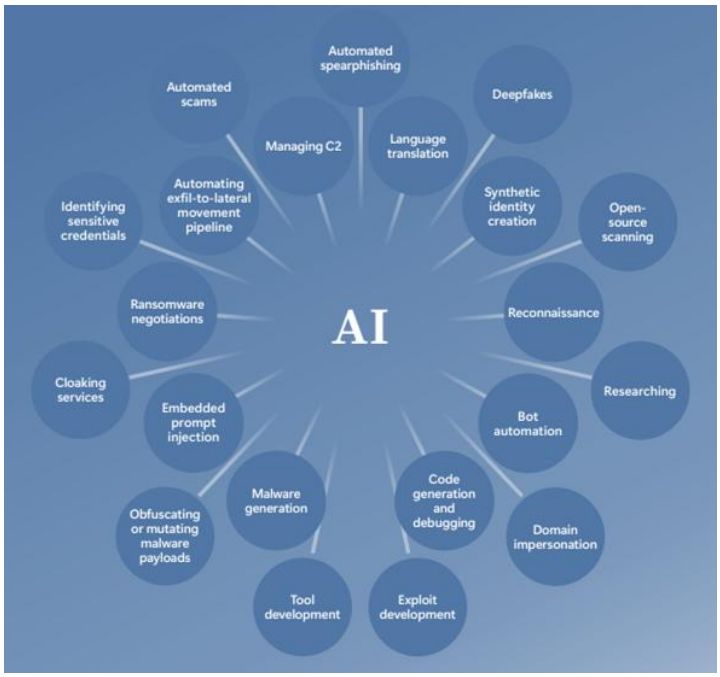
generativa en todas las fases del ataque ha reducido el tiempo de exfiltración de **días a minutos**, poniendo de manifiesto un cambio cualitativo en la velocidad de las operaciones ofensivas.



Diferencia de velocidad en un ataque simulado sin/con asistencia de IA. Fuente: Palo Alto Networks (2025)

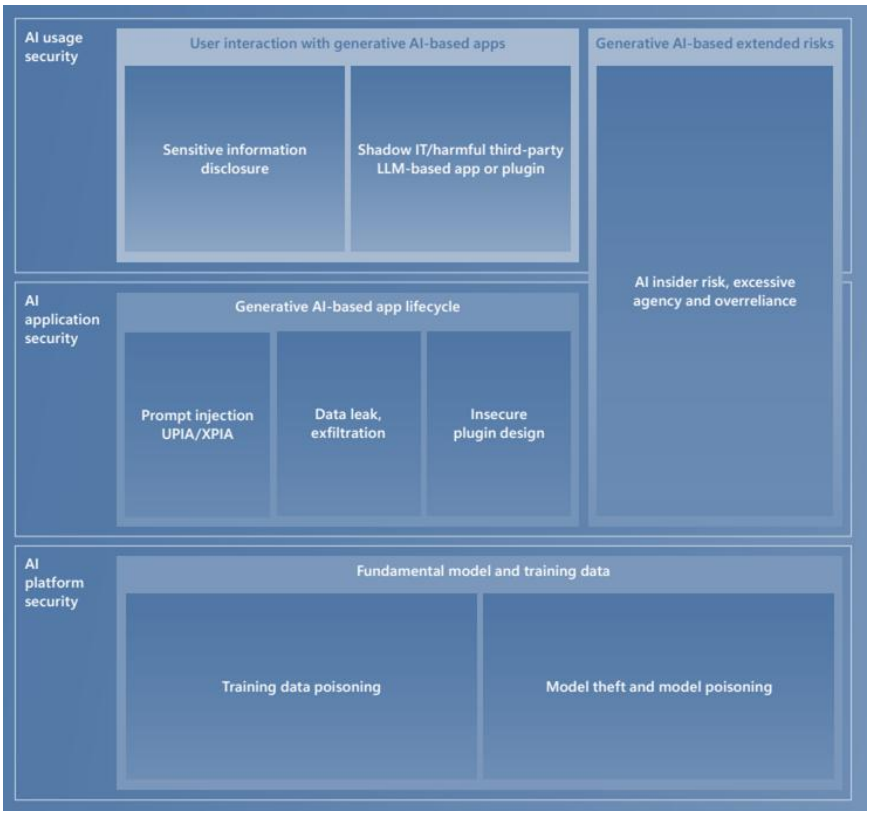
El ***Microsoft Digital Defense Report 2025*** profundiza en esta idea y describe la IA como un auténtico **multiplicador de ataques tradicionales**. Según Microsoft, los adversarios ya emplean IA generativa para automatizar y escalar tareas como el spear phishing dirigido, la traducción y localización de mensajes, la creación de deepfakes de voz e imagen, la generación de identidades sintéticas, el excaneo automatizado de vulnerabilidades y la producción de malware polimórfico.

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



Usos de la IA para aumentar capacidades de ataques tradicionales. Fuente: Microsoft (2025)

El informe advierte además de que la adopción de servicios basados en modelos de IA introduce **nuevas potenciales vulnerabilidades**: técnicas como **la inyección directa e indirecta de prompts**, la manipulación de herramientas conectadas a modelos, el envenenamiento de datos de adiestramiento o la exposición accidental de información sensible amplían el riesgo, especialmente en organizaciones que integran IA en procesos críticos.



Mapa de amenazas asociadas al uso de IAs generativas. Fuente: Microsoft (2025)

En entornos **ICS/OT, donde comienzan a introducirse soluciones basadas en IA para monitorización, mantenimiento predictivo o asistencia operativa, estas debilidades adquieren especial relevancia**. Un compromiso en sistemas IT apoyados en IA puede facilitar accesos indirectos a redes industriales si no existe una segmentación y gobernanza adecuadas.

En conjunto, los distintos informes coinciden en que la IA no ha creado amenazas completamente nuevas (salvo las asociadas a la explotación de tal tecnología), pero **sí amplificó de forma sustancial la escala, velocidad y credibilidad de las existentes**, actuando como catalizador de técnicas ya conocidas y reduciendo drásticamente los tiempos de ejecución de los ataques. La respuesta defensiva pasa por reforzar la concienciación, adaptar los procesos de detección y respuesta a tiempos mucho más cortos y desplegar, de forma controlada, capacidades defensivas basadas también en IA que permitan equilibrar esta nueva asimetría. El eterno juego del gato y el ratón.

3.4 Incidentes y campañas recientes

Este bloque se apoya en **fuentes complementarias y de distinta naturaleza**, que permiten combinar una visión **sectorial europea**, una **perspectiva histórica de largo**

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

plazo y datos **operacionales recientes** centrados específicamente en entornos industriales.

Las fuentes de que bebe son en primer lugar, los **informes sectoriales** del ya citado **Threat Landscape 2025 de ENISA,** que aporta una lectura estructurada del impacto de los ciberincidentes en los principales sectores críticos de la Unión Europea, alineados con el marco NIS2 y con especial atención a la evolución interanual de los ataques [34].

A esta visión se suma a **base de datos de incidentes de ICS Strive** [38][39], que recoge eventos historificados desde 2010, ofreciendo un repositorio de alto valor para el análisis retrospectivo. Esta fuente permite extraer lecciones aprendidas a partir de incidentes pasados, identificar sectores recurrentemente afectados y entender cómo evolucionaron las técnicas de ataque y sus consecuencias en entornos ICS a lo largo del tiempo.

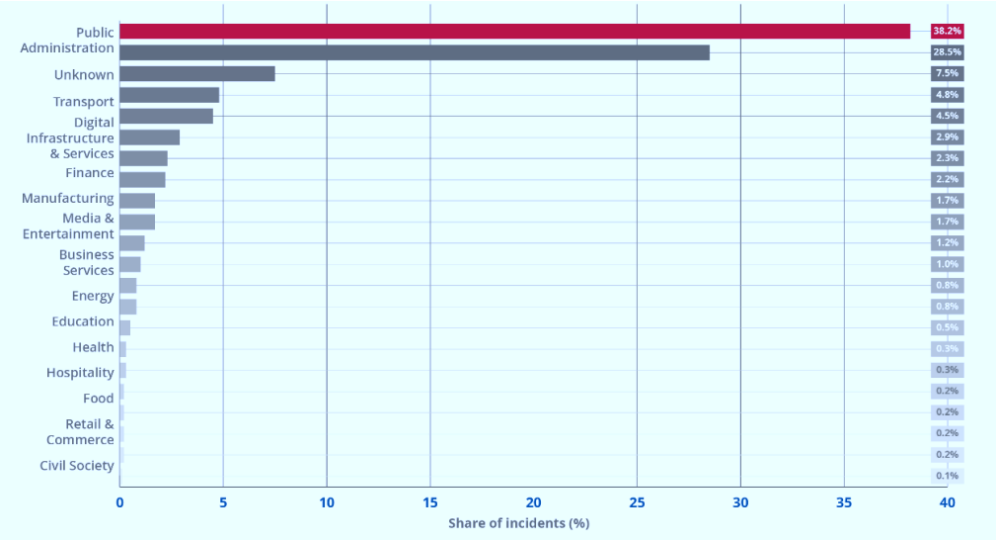
Finalmente, se incorporan los datos más recientes del **Threat landscape for Industrial Automation Systems. Europe, Q2 2025** y **A brief overview of the main incidents in industrial cybersecurity, Q2 2025 de Kaspersky** [40][41], que aportan una perspectiva **global y actualizada** sobre la afectación de **computadores y sistemas en entornos ICS**, permitiendo observar tendencias emergentes, cambios en los vectores de infección y la evolución del impacto del malware industrial en diferentes regiones y sectores.

La combinación de estas tres fuentes permite construir una visión **multidimensional** de los incidentes recientes: desde el análisis normativo y sectorial europeo, pasando por la experiencia acumulada de más de una década de incidentes industriales, hasta la observación más próxima de las amenazas que afectan hoy a los sistemas ICS.

3.4.1 Análisis sectorial europeo (ENISA)

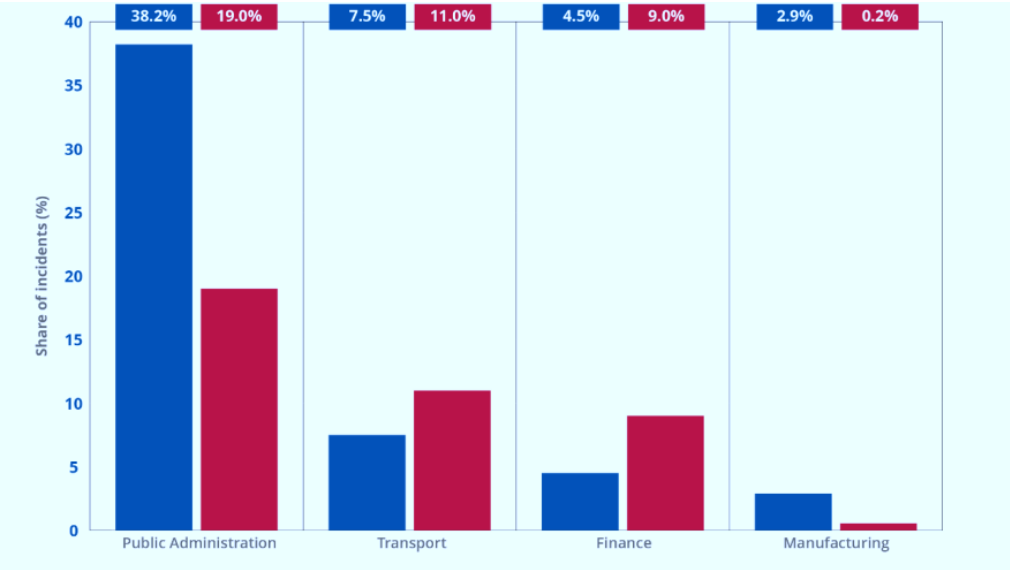
El análisis sectorial del ENISA [34] ofrece una visión detallada de cómo se distribuyen los incidentes de ciberseguridad entre los distintos sectores económicos y administrativos de la Unión Europea. Durante el período analizado, ENISA recopiló y analizó **4.875 eventos**, de los cuales un 28,5% no pudo asociarse a un sector concreto. Una vez excluidos estos casos, el análisis pone de manifiesto una **clara concentración**

de incidentes en un número reducido de sectores, muchos de ellos clasificados como esenciales o de alta criticidad en el marco de la **Directiva NIS2** [42]:



Incidentes registrados por sector. Fuente: ENISA (2025)

Los **cinco sectores más atacados** fueron **administración pública, transporte, infraestructuras y servicios digitales, finanzas y manufactura**, que en conjunto concentran más de la mitad de los incidentes registrados contra sectores identificados. Este reparto confirma la relevancia del enfoque sectorial de NIS2 y permite observar la evolución interanual de los ataques, especialmente al comparar los datos de **2024 frente a 2023**:



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

A continuación, se detallan las principales conclusiones por sector.

Administración pública

Se mantiene como **el objetivo más atacado**, concentrando aproximadamente el **38% de los incidentes**, con un incremento significativo respecto al período anterior. Este aumento está directamente vinculado al crecimiento de **ataques DDoS liderados por colectivos hacktivistas**, que representan más del **96% de los incidentes** contra este sector.

Geográficamente, los mayores impactos se han registrado en **Francia, Italia y Alemania**, seguidos por **España y Polonia**. Los incidentes afectaron principalmente a **entidades regionales y centrales**, incluyendo organismos gubernamentales, defensa, inteligencia, fuerzas de seguridad, partidos políticos, misiones diplomáticas y organizaciones europeas.

Además de los ataques DDoS, la administración pública ha continuado sufriendo **incidentes de ransomware** —especialmente a nivel municipal— y **fugas de datos**, que representaron una parte relevante de los casos documentados. Desde la perspectiva de amenazas avanzadas, este sector fue también **el principal objetivo de campañas de ciberespionaje vinculadas a actores estatales**, lo que subraya su importancia estratégica.

Transporte

El **sector transporte** se sitúa como el **segundo más atacado**, con un **7,5% del total de incidentes**, manteniendo una posición similar a la del período anterior. Una parte relevante de los incidentes de alto impacto notificados bajo la Directiva NIS correspondió a este sector.

Los ataques se han concentrado principalmente en **el transporte aéreo y en la logística**, siendo de nuevo **los ataques DDoS hacktivistas** el vector predominante, con más del **87% de los casos**. Estas campañas estuvieron estrechamente ligadas a acontecimientos geopolíticos y a decisiones políticas de Estados miembros en relación con el conflicto en Ucrania.

Junto a la actividad hacktivista, el sector transporte también sufrió **incidentes de cibercrimen**, en los que **el ransomware** ha tenido un papel destacado y, aunque numéricamente limitado, generó **impactos operativos significativos**, incluyendo interrupciones temporales de servicios críticos. Asimismo, se observó actividad de

actores estatales, principalmente vinculados a China y Rusia, con interés en infraestructuras clave de transporte y logística.

Infraestructuras y servicios digitales

Las **infraestructuras y servicios digitales** ocuparon **el tercer lugar**, con un **4,8% de los incidentes**. Este sector, que incluye telecomunicaciones, proveedores de servicios digitales y gestión de servicios TIC, destaca por **su alto valor estratégico**, tanto por la cantidad de datos que gestiona como por su capacidad de generar efectos en cascada sobre otros sectores.

Dentro del sector, **las telecomunicaciones** y los **proveedores de servicios digitales** han sido los subsectores más afectados. Los **ataques DDoS hacktivistas** representaron más de la mitad de los incidentes, mientras que **el cibercrimen** —especialmente fugas de datos y ransomware— tuvieron un peso relevante debido al potencial de extorsión y disrupción a gran escala.

Desde la óptica de amenazas avanzadas, este sector ha mostrado una **alta concentración de actividad de actores estatales**, principalmente de origen ruso, con campañas dirigidas a proveedores TIC y operadores de telecomunicaciones, lo que refuerza su papel como objetivo prioritario en operaciones de ciberespionaje.

Finanzas

El **sector financiero** representó alrededor del **4,7% de los incidentes**, con una clara dominancia de **ataques DDoS de carácter hacktivista**, que superaron el **80% de los casos**. Estos ataques se han dirigido principalmente contra **entidades bancarias**, buscando generar molestias a los usuarios y amplificar mensajes en contextos políticos o sociales sensibles.

Más allá del hacktivismo, el sector financiero continuó siendo un **objetivo prioritario para el cibercrimen**, especialmente en forma de **brechas de datos y ransomware**, dada la elevada concentración de información financiera y personal. Aunque la actividad de actores estatales ha sido minoritaria en términos cuantitativos, el informe señala que este tipo de amenazas sigue representando un **riesgo persistente**, en particular por su posible orientación a la obtención de información estratégica o financiera.

Manufactura

El **sector manufacturero**, aunque con una **proporción menor de incidentes (2,9%)**, experimentó un **ascenso relevante en el ranking sectorial**, pasando a ocupar una

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

posición más destacada entre los sectores NIS2. La mayoría de los casos afectaron a organizaciones no identificadas, pero los subsectores de **defensa y automoción** mostraron una exposición especialmente elevada.

Las campañas hacktivistas, nuevamente vinculadas a contextos geopolíticos, incluyeron **ataques DDoS** y, en algunos casos, **intentos de disrupción de sistemas de tecnología operacional**, lo que introduce un elemento de especial relevancia para entornos industriales.

Sin embargo, el **cibercrimen** fue la principal amenaza para este sector, tanto en volumen como en impacto, con **incidentes de ransomware** que provocaron **interrupciones prolongadas de la continuidad de negocio**. Además, se han identificado **campañas de ciberespionaje** de origen estatal dirigidas a organizaciones manufactureras, presumiblemente orientadas al **robo de propiedad intelectual**.

3.4.2 Resumen de incidentes históricos en ICS/OT

A continuación recopilamos **los incidentes más relevantes de la última anualidad completa en el informe** (2024) recogidos en el repositorio **de ICS Strive** [38][39]. A lo largo del mismo se han documentado numerosos incidentes con **consecuencias físicas, operativas y económicas tangibles**, muchos de ellos en **Europa** y algunos con impacto directo en **España**, lo que refuerza la relevancia del análisis para el contexto nacional.

Uno de los **patrones más claros en Europa es** la **afectación del sector transporte**, especialmente aeropuertos, logística y sistemas de movilidad. En enero, el **aeropuerto de Split (Croacia)** y, posteriormente, otros aeropuertos europeos sufrieron ataques de ransomware que afectaron a sistemas críticos como el Flight Information Display System (FIDS), manejo de equipajes y operaciones de tierra, obligando a operar manualmente durante días. A lo largo del año se han repetido incidentes similares en aeropuertos y operadores logísticos de **Italia, Alemania, Bélgica, Suecia y Reino Unido**, confirmando que los sistemas IT que soportan operaciones OT siguen siendo un vector prioritario.

Especial mención merece el **uso deliberado de interferencias GNSS (GPS jamming y spoofing)** en Europa del Este y el Báltico. En marzo de 2024, interferencias prolongadas afectaron a **más de 1.600 vuelos** sobre **Polonia, Suecia y Alemania**, y forzaron la suspensión durante semanas de la ruta Helsinqui–Tartu. Estos incidentes, atribuidos a actores estatales rusos, evidencian cómo **ataques de ciberseguridad y**

electromagnéticos híbridos pueden generar impactos directos sobre la seguridad operacional sin necesidad de comprometer sistemas IT tradicionales.

En el ámbito **industrial y manufacturero europeo**, 2024 estuvo marcado por una sucesión de **ataques de ransomware con parada de producción**, particularmente en **Alemania, Bélgica, Francia, Italia, Suecia, Finlandia y Austria**. Casos como **Varta, ThyssenKrupp Automotive Body Solutions, BerlinerLuft, LEMKEN, AKG Group, Peikko Group o Smeg** mostran un patrón repetido: detección de compromiso en sistemas IT (ERP, SAP, servicios de directorio), aislamiento preventivo de redes y **paradas completas de plantas durante semanas**, con impacto directo en entregas, empleo temporal y resultados financieros. En algunos casos, como **Schumag AG**, el incidente contribuyó a procesos de **reestructuración y bancarrota**, ilustrando el impacto sistémico del ciberataque más allá del plano técnico.

El **sector agroalimentario y de bebidas** también ha sufrido impactos significativos en Europa. En **Bélgica, Suecia, Alemania y España**, ataques de ransomware han provocado interrupciones de producción y distribución. Destaca especialmente el **caso del Matadero de Gijón (España)**, donde el grupo RansomHub afirmó acceder a sistemas **SCADA asociados al tratamiento de aguas residuales**, lo que obligó a detener la actividad y enviar a los trabajadores la casa en plena jornada. Aunque la producción se reanudó posteriormente en modo manual, el incidente representa uno de los ejemplos más claros de **impacto directo sobre OT/ICS en territorio español** durante 2024.

En el sector **energía y utilities**, aunque menos numerosos, los incidentes observados fueron especialmente sensibles. El caso **de Ignitis ON (Lituania)** evidenció como la dependencia de **servicios cloud y aplicaciones móviles** puede traducirse en impactos físicos: una intrusión en servicios SaaS dejó inutilizadas estaciones de recarga eléctrica en todo el país durante horas. En otros contextos europeos y limítrofes, ataques a sistemas de calefacción urbana, agua o electricidad han demostrado que la convergencia IT/OT sigue siendo un punto crítico.

Finalmente, el repositorio contempla múltiples ejemplos de **ataques a cadenas de suministro y proveedores tecnológicos**, como **Microlise (Reino Unido)** o **Blue Yonder**, cuyos incidentes se han propagado a clientes industriales, logísticos y de distribución alimentaria en varios países. Estos casos refuerzan la idea de que el **riesgo en entornos industriales no se limita a la propia organización**, sino que se extiende a ecosistemas completos de proveedores, integradores y servicios gestionados.

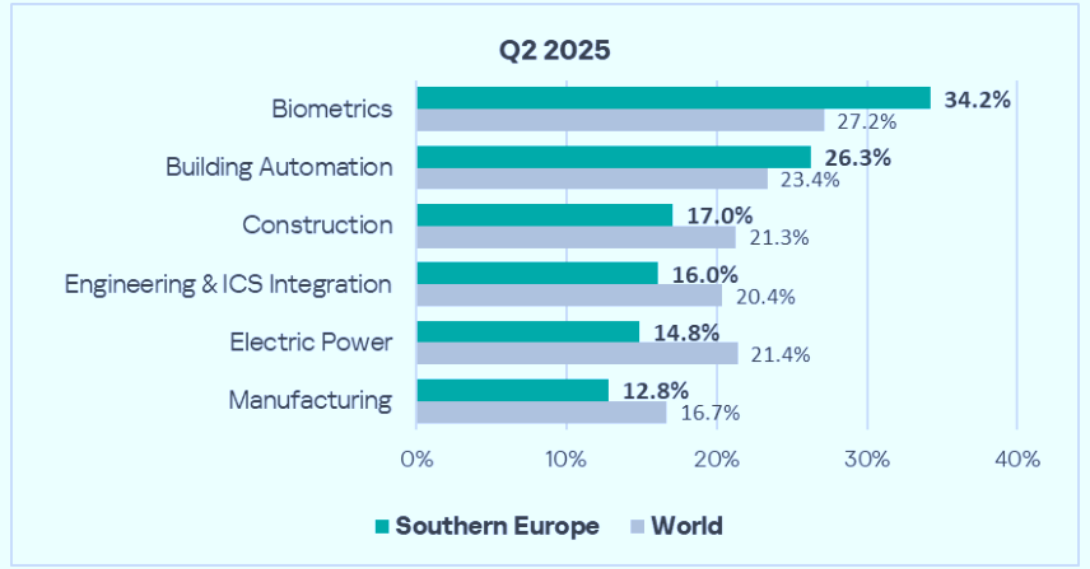
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

En conjunto, los incidentes documentados por ICS Strive en 2024 muestran que **Europa es un escenario activo de ciberincidentes con impacto OT**, dominados por ransomware, hacktivismo y, en determinados contextos, operaciones de carácter estatal. España, aunque con menor volumen, **no es ajena a estas dinámicas**, y los casos observados confirman que la materialización del riesgo en sistemas industriales es ya una realidad operativa y no un escenario hipotético.

3.4.3 Amenazas en computadores ICS

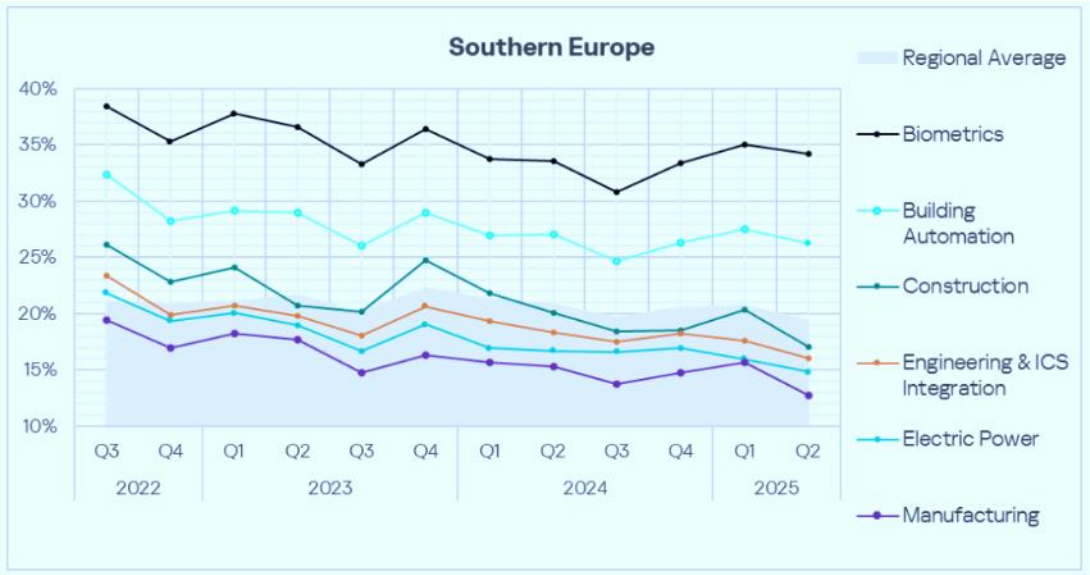
Para complementar el análisis de incidentes históricos y sectoriales, resulta especialmente relevante incorporar la perspectiva **de Kaspersky ICS-CERT**, que aporta una visión **telemetría-driven** centrada exclusivamente en **computadoras industriales** y no en incidentes corporativos generales. Esta aproximación permite observar **tendencias de afectación real en estaciones de ingeniería, HMIs, servidores SCADA y otros sistemas industriales**, independientemente de que el impacto final llegue o no a materializarse en una interrupción operativa.

El informe Threat Landscape for Industrial Automation Systems – Europe, Q2 2025 [40] ofrece una fotografía detallada de la situación durante el segundo trimestre de 2025, con especial interés para **Europa del Sur**, donde se observa una **exposición sostenida de los sistemas ICS a múltiples fuentes de amenaza**. En este contexto, el informe pone de relieve que las computadoras industriales continúan siendo comprometidas principalmente a través **de vectores heredados del entorno IT**, como malware genérico, infecciones procedentes de medios extraíbles, accesos remotos inseguros o movimiento lateral desde redes corporativas, lo que refuerza la importancia de la convergencia IT/OT en la gestión del riesgo, una vez más.



Se desglose de incidentes por sector en Europa del Sur. Fuente: Kaspersky (2025)

En el caso del **Sur de Europa**, el análisis evidencia que varios **sectores industriales mantienen niveles relevantes de sistemas ICS afectados**, con patrones consistentes a lo largo del tiempo. Este comportamiento permite introducir una **gráfica de tendencia de sectores afectados en computadoras ICS**, que ilustra como la exposición no es puntual ni episódica, sino estructural, y afecta de forma recurrente a determinadas verticales industriales.



Tendencia de incidentes por sector en Europa del Sur. Fuente: Kaspersky (2025)

Adicionalmente, el estudio facilita un análisis cruzado muy visual entre fuentes **de amenaza y categorías de malware por industria**, que resulta especialmente útil para comprender **qué tipos de actores y técnicas predominan en cada sector**.

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

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 fuentes de amenaza por industria en Europa del Sur. Fuente: Kaspersky (2025)

Estas visualizaciones refuerzan una conclusión clave: **no todos los sectores están expuestos a los mismos tipos de amenazas**, y la naturaleza del malware que impacta en computadoras ICS varía significativamente según el entorno industrial.

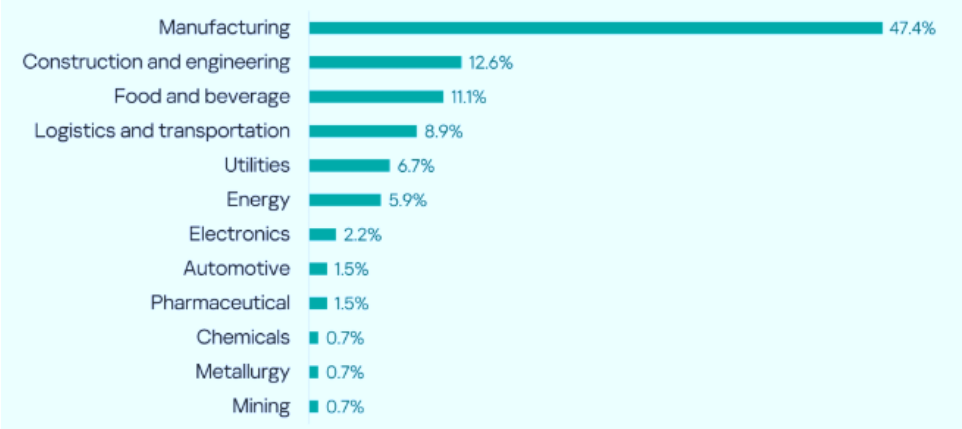
Threat category indicators for industries in Southern Europe, Q2 2025

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 amenaza por industria en Europa del Sur. Fuente: Kaspersky (2025)

De manera complementaria, el informe A brief overview of the main incidents in industrial cybersecurity – Q2 2025 [41] aporta una **síntesis de los principales incidentes conocidos en el ámbito industrial a nivel global,** nuevamente con foco en entornos OT/ICS. La diferencia del informe anterior, basado en telemetría, este documento se centra en **incidentes reportados y analizados**, ofreciendo una visión más próxima al impacto operativo y organizativo.

El informe presenta, en su parte superior, una **distribución de incidentes por sector**, acompañada de un **listado resumido de los casos más relevantes, lo** que permite contextualizar rápidamente que las mismas concentran mayor número de incidentes durante el período analizado (135 en total).



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

Muestra ejemplo de incidentes en ICS en Q2 2025. Fuente: Kaspersky (2025)

Asimismo, destacar que **el listado completo y detallada de incidentes del trimestre** se recoge al final del estudio, como referencia adicional.

3.5 Vulnerabilidades ICS

En esta sección, lo primero que cabe destacar es que existen otros entregables del Observatorio de Ciberseguridad Industrial de AMTEGA relacionados específicamente con esta materia: *Informes de Ciberalertas*. Se invita al lector a consultarlos [43].

El análisis de **vulnerabilidades** constituye un eje fundamental para comprender el **riesgo real** al que se enfrentan los entornos industriales. A diferencia de otros ámbitos, en ICS/OT las vulnerabilidades no sólo tienen una dimensión técnica, sino también

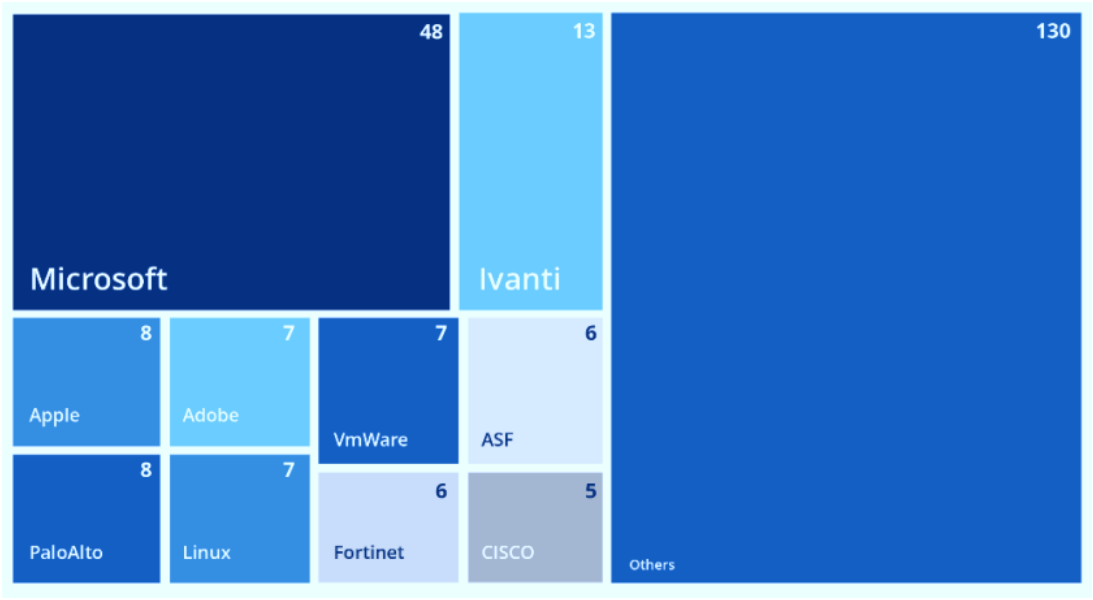
Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

operativa y de seguridad física, ya que su explotación puede traducirse en interrupciones prolongadas, degradación de procesos o impactos sobre personas y medio ambiente.

Contexto europeo

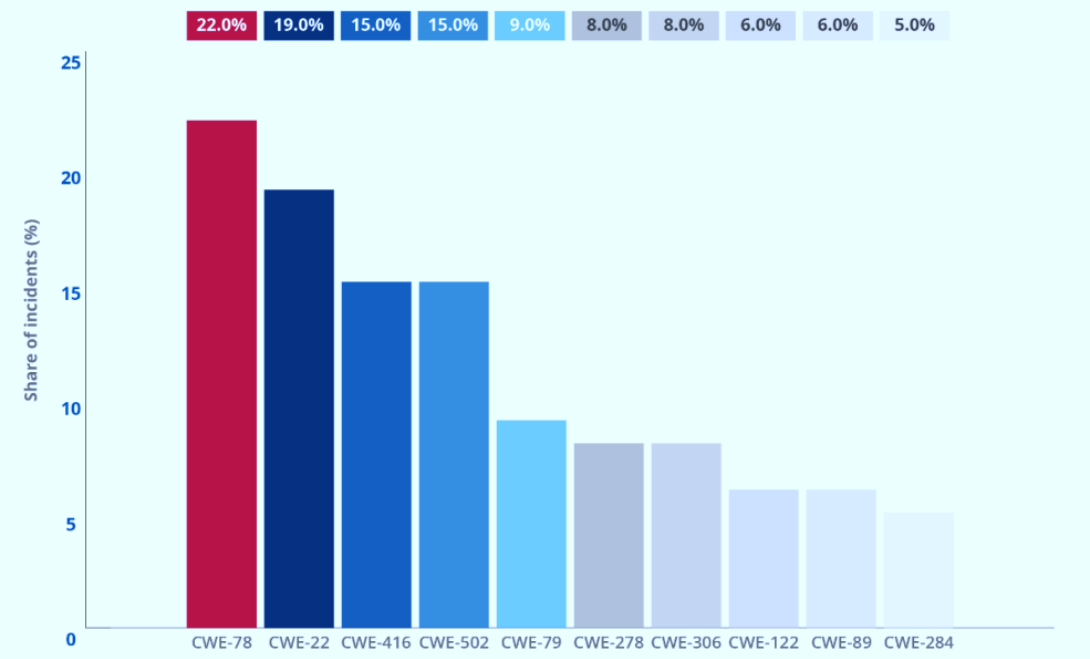
Desde una perspectiva europea, el **ENISA Threat Landscape 2025** [34] dedica una sección al análisis de vulnerabilidades observadas con mayor frecuencia en incidentes reales. El informe pone de relieve que una parte sustancial de los ataques se apoya en **vulnerabilidades incluidas en catálogos de explotación conocida**, lo que confirma que los atacantes priorizan fiabilidad y retorno frente a la complejidad técnica.

Entre las debilidades más recurrentes se encuentran fallos en productos de uso transversal —incluidos dispositivos de red, soluciones de acceso remoto y software ampliamente desplegado— que actúan como puertas de entrada hacia redes IT y, por extensión, hacia entornos OT mal segmentados. La siguiente figura recoge los fabricantes con más vulnerabilidades presentes en el catálogo KEV (vulnerabilidades más explotadas) [44]:



Fabricantes predominantes en el catálogo KEV. Fuente: ENISA (2025)

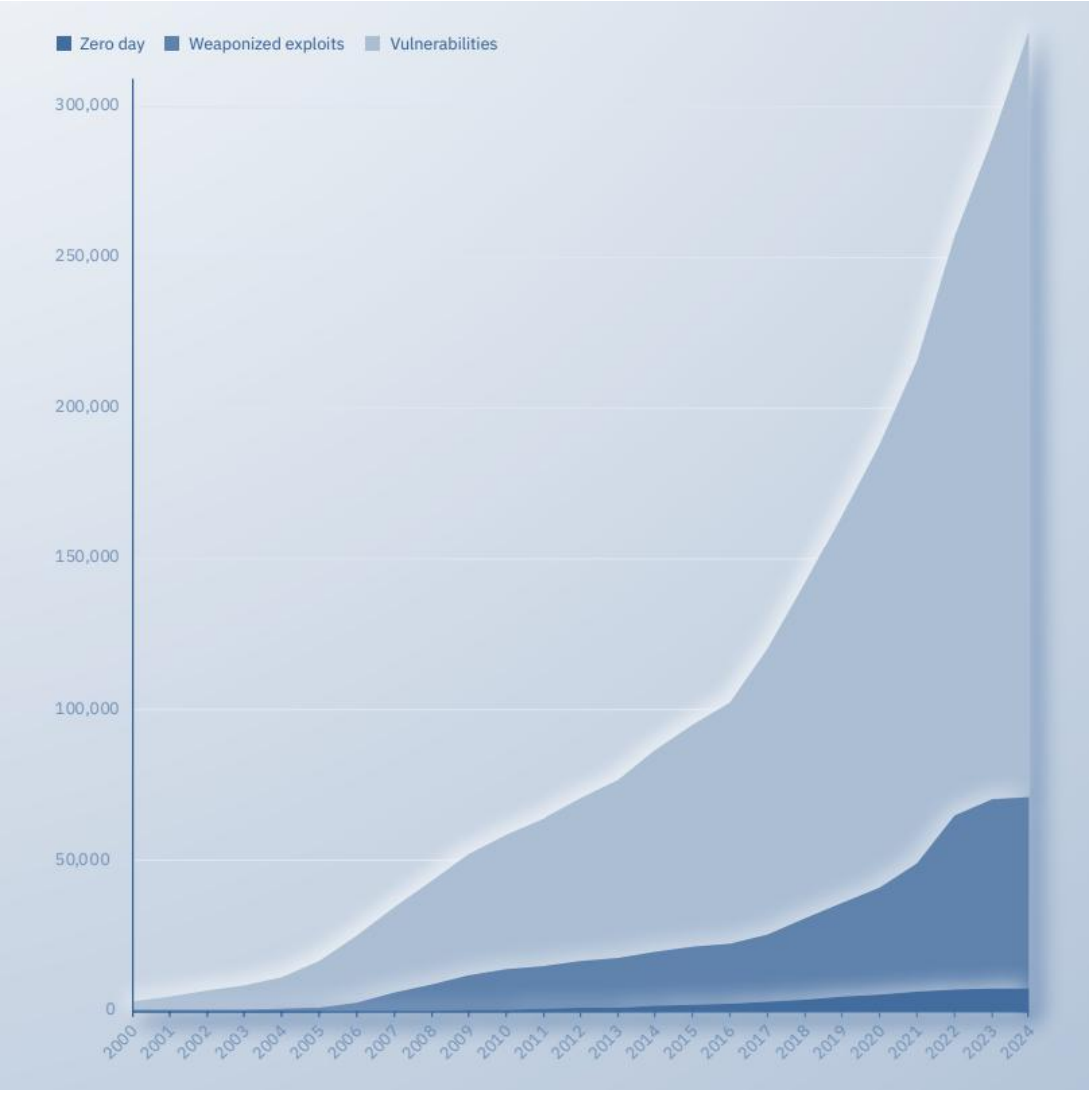
Y las debilidades más frecuentes que conducen a vulnerabilidades incorporadas al catálogo de las más explotadas (KEV):



TOP 10 debilidades en vulnerabilidades presentes en el catálogo KEV. Fuente: ENISA (2025)

Por otra parte y a nivel global, el reporte **IBM** X-Force **Threat Intelligence Index 2025** [32] refuerza estas conclusiones previas, al analizar la relación entre el crecimiento del número de vulnerabilidades, la disponibilidad de exploits y el aumento de zero-days explotados en entornos reales.

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



Crecimiento de vulnerabilidades, exploits y zero days. Fuente: IBM X-Force (2025)

Destacan que **el éxito de la explotación de vulnerabilidades** se debe, en gran medida, a la **rapidez** con que los actores de amenaza incorporan nuevos **exploits** a sus campañas.

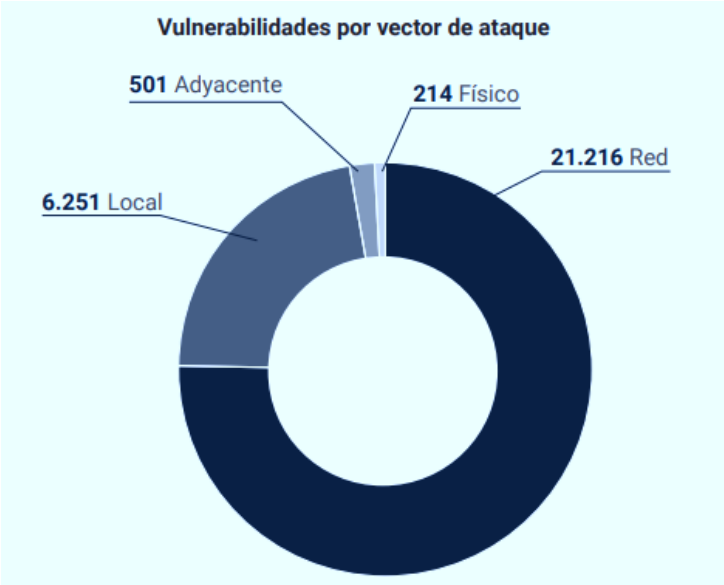
El crecimiento de vulnerabilidades, exploits y zero-days ilustra cómo el ecosistema ofensivo se ha industrializado, reduciendo drásticamente el tiempo necesario para pasar de la divulgación a la explotación. Estas conclusiones son plenamente aplicables a ICS/OT, donde la persistencia de sistemas legacy y la limitada visibilidad agravan el impacto potencial de estas dinámicas.

Panorama en España (CCN-CERT)

El informe del **CCN-CERT** [36] dedica un bloque específico al análisis de vulnerabilidades de manera general (IT/OT), en el que se observa un incremento

sostenido tanto en el número de vulnerabilidades publicadas como en su explotación efectiva. Subraya que una parte significativa de los **incidentes graves tiene** su origen en **vulnerabilidades conocidas**, para las que existen **parches disponibles** pero que permanecen sin corregir durante largos periodos de tiempo. Este fenómeno está estrechamente relacionado con problemas estructurales de gestión de parches, dependencias heredadas y limitaciones operativas, especialmente visibles en entornos industriales.

A continuación, se ilustra cómo el mayor volumen de debilidades se explota vía red:



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

Aunque la sección detalla numerosas vulnerabilidades de carácter eminentemente IT, el mensaje transversal es plenamente aplicable a ICS/OT: la **ventana de exposición** entre la divulgación de una vulnerabilidad y su **explotación efectiva** se está reduciendo de forma constante, mientras que los ciclos de actualización en entornos industriales siguen siendo largos y complejos.

Se incluyen a continuación las debilidades más frecuentes (CWE) [45] detectadas en relación con las vulnerabilidades del gráfico anterior.

Identificador	**Descripción**
CWE-79	Sanitización incorrecta de entradas durante la generación de páginas web (*Cross-Site Scripting, XSS*).
CWE-89	Sanitización incorrecta de elementos especiales empleados en comandos SQL (*SQL Injection*).

CWE-78	Sanitización incorrecta de elementos especiales empleados en comandos del sistema operativo (*OS Command Injection*).
CWE-77	Sanitización indebida de elementos especiales empleados en comandos (*Command Injection*).
CWE-787	Escritura fuera de los límites de la memoria (*Out-of-bounds Write*).
CWE-125	Lectura fuera de los límites de la memoria (*Out-of-bounds Read*).
CWE-120	Copia de buffer sin comprobación del tamaño de la entrada (*Classic Buffer Overflow*).
CWE-121	Desbordamiento de búsqueda en pila (*Stack-based Buffer Overflow*).
CWE-190	Desbordamento de número entero (*Integer Overflow or Wraparound*).
CWE-352	Falsificación de peticiones en sitios cruzados (*Cross-Site Request Forgery, CSRF*).
CWE-434	Carga sin restricciones de archivos de tipo peligroso.
CWE-22	Limitación incorrecta de un nombre de ruta a un directorio restringido (*Path Traversal*).
CWE-502	Deserialización de datos no fiables.
CWE-287	Autenticación incorrecta.
CWE-862	Falta de autorización.
CWE-798	Uso de credenciales codificadas (*Hard-coded Credentials*).
CWE-918	Falsificación de peticiones del lado del servidor (*Server-Side Request Forgery, SSRF*).
CWE-94	Control inadecuado de la generación de código (*Code Injection*).

Informe especializado

El **Dragos 2025 OT Cybersecurity Report – A Year in Review** [30] ofrece una visión específicamente centrada en OT, aportando un nivel de detalle especialmente relevante para entornos ICS.

Subraya que los **sistemas industriales no fueron concebidos con criterios de ciberseguridad**, lo que sigue generando un caldo de cultivo favorable para los adversarios. En este contexto, Dragos indica que la gestión del riesgo en ICS debe ir más allá del parcheo puntual, incorporando una comprensión profunda de cómo estas

debilidades pueden ser explotadas y mitigadas antes de que se deriven en impactos operativos.

Uno de los ejes más relevantes del informe es la **investigación sobre protocolos fieldbus**, en particular alrededor **de CANopen implementado en servoaccionamientos**. Identifican riesgos significativos asociados a protocolos industriales **encapsulados en capas sucesivas**, a los que denomina "*Turducken protocols*". Estos esquemas, en los que protocolos como Modbus-RTU pueden viajar encapsulados sobre CANopen y, a su vez, dentro de protocolos propietarios o incluso sobre Modbus/TCP, **reducen drásticamente la visibilidad y la capacidad de detección de ataques**. La complejidad aparente de estas pilas no supone una barrera real para atacantes avanzados, pero sí para muchas soluciones defensivas tradicionales.

Dragos considera que **gran parte del equipo fieldbus es inseguro por diseño**, y que muchas de las debilidades identificadas no siempre se traducen en CVEs. Con todo, esto no reduce su relevancia desde un punto de vista operativo: la manipulación no autorizada de parámetros, incluso por error, puede provocar desviaciones de proceso o interrupciones graves. El informe destaca que estas arquitecturas, con funcionalidades poco documentadas y comportamientos no estandarizados, **dificultan enormemente la creación de analíticas de red fiables**, reforzando la necesidad de desarrollar *disectores* capaces de desentrañar cada capa del protocolo.

Constatan que este tipo de exposiciones no es teórico, sino que afecta a **modelos concretos de PLC ampliamente desplegados**, incluidos sistemas de Rockwell Automation con módulos HART y controladores de Schneider Electric basados en CODESYS y CANopen. En estos casos, Dragos señala que existen **medidas de mitigación viables desde la propia lógica de control**, como la monitorización de parámetros sensibles y la ejecución de paradas seguras ante cambios fuera de banda, lo que refuerza la idea de que la defensa en OT debe apoyarse también en el propio proceso.

El informe dedica asimismo un bloque específico **al uso de equipamiento IoT en entornos industriales**, alertando de que estos dispositivos continúan siendo uno de los eslabones más débiles. Se documenta la explotación reciente de vulnerabilidades en IoT para la propagación de variantes de la **botnet Mirai**, capaz de comprometer miles de dispositivos mediante mecanismos automatizados. La raíz del problema reside en que gran parte de estos equipos ejecutan sistemas GNU/Linux poco bastionados, con servicios como TELNET o SSH expuestos por defecto y fallos triviales de autenticación o inyección de comandos.

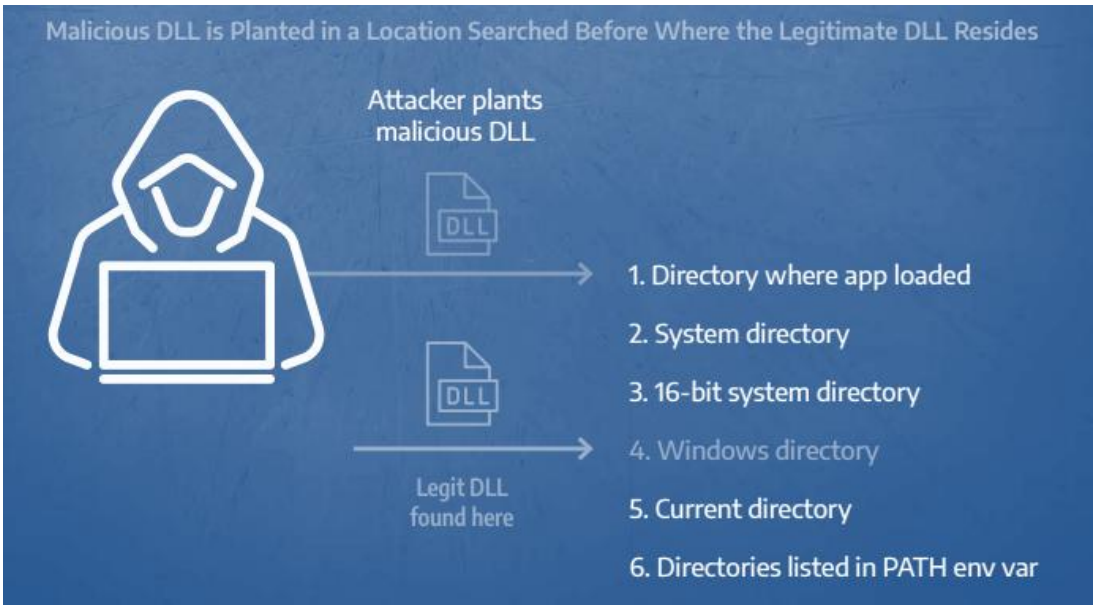
Aunque estos sistemas no siempre controlan directamente la producción, Dragos recalca que **infraestructuras auxiliares como HVAC, iluminación, control de accesos o seguridad física deben considerarse parte integral del proceso industrial**. La indisponibilidad de cualquiera de estos sistemas puede forzar la parada de la producción, especialmente en sectores regulados como el farmacéutico o el alimentario. En este sentido, el informe recomienda tratar el hardware IoT industrial como activos críticos, reforzando controles básicos como la eliminación de credenciales por defecto, la restricción de accesos de gestión y la planificación de procedimientos manuales de contingencia.

Otro aspecto destacado es **la exposición derivada del uso de herramientas de doble uso**. Analizan el caso del toolkit *IoT Exploit*, una plataforma pública que agrupa cientos de exploits contra dispositivos IoT y OT. Aunque no se observó su uso malicioso directo en la telemetría de Dragos, el informe advierte de que este tipo de herramientas, diseñadas inicialmente para investigación o *red teaming*, **tienden a incorporarse con rapidez a arsenales ofensivos automatizados**, reduciendo el umbral técnico necesario para explotar vulnerabilidades en entornos industriales.

El informe también pone el foco en los **riesgos asociados a componentes de terceros y a la cadena de suministro**, señalando que cerca de una quinta parte de los avisos analizados en 2024 estaban relacionados con vulnerabilidades en componentes externos integrados en productos OT. Aun cuando un fabricante mantiene su producto actualizado, la presencia de librerías o sistemas de terceros sin parchear puede introducir **vías indirectas de compromiso**, como ilustra el ejemplo del uso de PAN-VOS como componente integrado en dispositivos industriales. Subrayan la importancia de iniciativas como el **SBOM** para mejorar la visibilidad y acelerar la respuesta ante este tipo de exposiciones.

Finalmente, el informe dedica una atención especial a un problema persistente en software industrial: el **DLL hijacking**. Dragos identifica más de un centenar de vulnerabilidades de este tipo en aplicaciones OT, considerándolas "low-hanging fruit" o presa fácil, por su facilidad de explotación y versatilidad. Estas técnicas permiten desde acceso inicial hasta escalada de privilegios o persistencia, y han sido empleadas históricamente por actores estatales y grupos APT en campañas contra sectores industriales críticos. Dragos recomienda a los operadores industriales **buscar activamente este tipo de debilidades y** aplicar mitigaciones técnicas bien conocidas,

así como insta a los fabricantes OT a adoptar buenas prácticas de desarrollo seguro para reducir su recurrencia. A continuación, una explicación visual de la amenaza:



DLL hijacking. Fuente: Dragos (2025)

En conjunto, transmiten un mensaje claro: las vulnerabilidades en entornos ICS no son un problema marginal ni exclusivamente técnico, sino un **riesgo estructural ligado al diseño, la integración y la operación de los sistemas industriales**, que requiere enfoques de mitigación pragmáticos, continuos y alineados con la realidad operativa.

En este sentido, los recursos recopilados de forma sistemática en los **Informes de Ciberalertas del Observatorio** proporcionan una visión consolidada y redundada de avisos, CVE y Alertas específicas de fabricantes y organismos de referencia, facilitando la toma de decisiones informadas en un contexto operativo realista. Para referencia rápida, estos son recursos de especial interés [46][47][48][49].

4 Conclusiones

Este informe abordó de manera integral la evolución reciente del **panorama de amenazas de ciberseguridad sobre entornos OT/ICS**, extrayendo patrones, amenazas emergentes, vectores de ataque y vulnerabilidades clave a partir de fuentes nacionales, europeas e internacionales. A través del análisis de dichas fuentes, se identificaron las principales áreas de exposición para infraestructuras críticas y sectores industriales.

El informe comenzó estableciendo un **marco teórico sobre qué es la inteligencia de amenazas**, sus objetivos, ciclo de vida y niveles (**estratégico, operacional y táctico**). También se han descrito las **fuentes que nutren esta inteligencia** (fuentes abiertas, compartidas, privadas o técnicas) y cómo **articular un programa eficaz** en organizaciones con sistemas industriales.

A continuación, se contextualizó el **estado actual de la inteligencia de amenazas a nivel global, europeo y nacional**. Se han revisado las principales iniciativas de coordinación públicas, así como los informes de algunos de los principales fabricantes del sector.

El **empleo de Inteligencia Artificial por parte de los adversarios** representa un vector emergente. Se ha evidenciado su empleo tanto en la **automatización de ataques** (por ejemplo, generación de malware o evasión de EDR) como en la **fabricación de contenido de phishing personalizado**. La sofisticación de estas herramientas expone **nuevos retos para los operadores OT**, que deben considerar escenarios de compromiso en tiempos cada vez más reducidos.

En materia de **vulnerabilidades**, se ha observado una alta concentración en **debilidades clásicas como desbordamientos de buffer, ejecución de código remoto o fallos de autenticación**. Particularmente preocupantes son los entornos con **protocolos heredados o dispositivos imposibles de parchear**. Los de **Dragos y otros informes** subrayan la necesidad de compaginar **la gestión de vulnerabilidades con otras estrategias** como segmentación, detección por comportamiento y visibilidad granular.

Podemos concluir que las **perspectivas futuras** apuntan a un **incremento sostenido de las amenazas sobre infraestructuras OT**, impulsadas por:

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

- **Mayor conectividad** entre sistemas IT/OT e cloud.
- **Aparición de malware** específico para entornos industriales.
- **Adopción masiva de IA** tanto en defensa como en ataque.
- **Tensiones geopolíticas** que transforman el ciberespacio en un campo de confrontación indirecta.

En este contexto, disponer de **capacidades propias de vigilancia, detección y respuesta adaptadas a los entornos industriales** no es una opción, sino una necesidad urgente.

Como se ha indicado, **el análisis de actores de amenaza y técnicas, tácticas y procedimientos específicos, la construcción de fuentes de inteligencia propia y las pertinentes recomendaciones** de organismos y entidades internacionales para protegerse frente a estas amenazas, **serán objeto de informes posteriores.**

Este conjunto de informes sentará las bases para una **estrategia de defensa de ciberseguridad más robusta, informada por inteligencia, y centrada en la protección de procesos esenciales para la sociedad y la economía**.

Todo ello **ayuda a las organizaciones de Galicia a avanzar hacia una gestión más madura del riesgo en OT**, apoyándose en información accionable y en alineación con estándares y recomendaciones de las principales fuentes 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] Escuela Tecnológica Daferra (2023). *Materiales Bootcamp Ciberseguridad Técnica.* No 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). *Reglamento General 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 privacidad y comunicaciones 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 Ciberamenazas y 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 ciberseguridad en la Unión*. Recuperado de: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

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

[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 Seguridad en Sistemas de Control Industrial (SCI) — Alerta Temprana*. Recuperado de https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci

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

[48] CCN-CERT (2025). *Vulnerabilidades — Seguridad al 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 / Amenaza Persistente Avanzada)

Grupo de ataques altamente sofisticados, normalmente asociado a estados-nación, con objetivos estratégicos a largo plazo y capacidad de mantener presencia prolongada en las redes víctimas.

BYOVD (Bring Your Own Vulnerable Driver)

Técnica en la que el atacante introduce un controlador vulnerable en el sistema para escalar privilegios o evadir defensas de seguridad.

CISA (Cybersecurity and Infrastructure Security Agency)

Agencia de ciberseguridad de EE. UU., centrada en proteger infraestructuras críticas frente a amenazas de ciberseguridad.

CPS (Cyber-Physical Systems / Sistemas Ciberfísicos)

Sistemas que integran componentes computacionales con procesos físicos, como sensores y actuadores, típicos en entornos industriales.

CVE (Common Vulnerabilities and Exposures)

Identificador único asignado a una vulnerabilidad conocida, que facilita su referencia estandarizada y gestión en productos y sistemas.

CWE (Common Weakness Enumeration)

Clasificación de debilidades comunes en software que pueden derivar en vulnerabilidades explotables.

DLL (Dynamic Link Library)

Biblioteca de código compartido que puede ser cargada en tiempo de ejecución por diferentes programas en sistemas Windows.

EDR (Endpoint Detection and Response)

Solución de seguridad que monitoriza dispositivos finales (endpoints) para detectar, registrar y responder a amenazas.

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)

Agencia de la UE encargada de reforzar la ciberseguridad a nivel europeo mediante políticas, normativas y análisis técnicos.

GDPR (General Data Protection Regulation / Reglamento General de Protección de Datos)

Regulación europea por la que se establecen directrices para la protección de datos personales y privacidad en la UE.

HART (Highway Addressable Remote Transducer)

Protocolo de comunicación utilizado en instrumentación de procesos industriales para configurar y obtener datos de campo.

HIDS (Host-based Intrusion Detection System)

Sistema de detección de intrusiones que opera directamente sobre un dispositivo monitorizando su actividad.

HMI (Human-Machine Interface)

Interfaz gráfica o física que permite a los operadores humanos interactuar con los sistemas de control industrial.

ICS (Industrial Control Systems / Sistemas de Control Industrial)

Conjunto de tecnologías utilizadas para supervisar, controlar y automatizar procesos industriales.

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

Equipo especializado en dar respuesta a incidentes de ciberseguridad que afectan a sistemas de control industrial.

ICS-CSIRT (ICS Computer Security Incident Response Team)

Comunidad y centro de coordinación para el intercambio de información sobre amenazas y vulnerabilidades en entornos OT.

IDS (Intrusion Detection System)

Sistema diseñado para identificar accesos no autorizados o actividades maliciosas en redes y sistemas.

IIoT (Industrial Internet of Things)

Ecosistema de dispositivos interconectados en entornos industriales que permiten cosechar y transmitir datos operativos.

IoC (Indicator of Compromise / Indicador de Compromiso)

Prueba técnica que sugiere que un sistema puede ser comprometido, como una dirección IP maliciosa o un archivo sospechoso.

IoT (Internet of Things)

Red de dispositivos físicos conectados a internet que recopilan, transmiten y actúan sobre datos del entorno.

KEV (Known Exploited Vulnerabilities)

Listado mantenido por CISA de vulnerabilidades que se sabe están siendo activamente explotadas en el mundo real.

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

Modelo de inteligencia artificial adiestrado con grandes volúmenes de texto para generar contenido, resumir o responder en lenguaje natural.

MFA (Multi-Factor Authentication / Autenticación Multifactor)

Método de verificación de identidad que requiere al menos dos factores: algo que se sabe, que se tiene o que se es.

MISP (Malware Information Sharing Platform)

Plataforma de código abierto para el intercambio estructurado de indicadores de amenaza entre organizaciones.

MITRE ATT&CK

Base de conocimiento que recoge tácticas, técnicas y procedimientos (TTP) utilizados por actores maliciosos en diferentes etapas de un ataque.

MITRE D3FEND

Marco de conocimiento complementario al ATT&CK, centrado en documentar contramedidas defensivas ante amenazas de ciberseguridad.

NIS2 (Network and Information Security Directive 2)

Directiva europea que refuerza los requisitos de ciberseguridad para sectores críticos, ampliando su alcance y obligaciones.

OpenCTI (Open Cyber Threat Intelligence)

Plataforma de código abierto para almacenar, visualizar y compartir inteligencia de amenazas de forma estructurada y contextual.

OT (Operational Technology / Tecnologías de Operación)

Sistemas y dispositivos utilizados para controlar procesos físicos en entornos industriales. Priorizan disponibilidad, seguridad física y continuidad de operación.

PLC (Programmable Logic Controller)

Dispositivo electrónico programable que ejecuta tareas de control automático en procesos industriales.

RTU (Remote Terminal Unit)

Unidad remota que recopila datos de sensores y transmite órdenes a actuadores en sistemas distribuidos como SCADA.

SBOM (Software Bill of Materials)

Lista detallada de todos los componentes de software que forman parte de una aplicación o sistema, clave para la gestión de riesgos.

SCADA (Supervisory Control and Data Acquisition)

Sistema que permite la supervisión y el control remoto de procesos industriales mediante la recopilación de datos y envío de comandos.

SIEM (Security Information and Event Management)

Solución que centraliza eventos de seguridad para su análisis, correlación y generación de alertas en tiempo real.

SOC (Security Operations Center)

Centro especializado en la monitorización, análisis y respuesta ante incidentes de ciberseguridad de una organización.

TTP (Tactics, Techniques and Procedures)

Conjunto de patrones de comportamiento y métodos empleados por actores maliciosos para alcanzar sus objetivos.

USB (Universal Serial Bus)

Estándar industrial para la conexión de dispositivos periféricos a un computador u otros sistemas digitales.

VPN (Virtual Private Network)

Tecnología que permite crear una conexión segura y cifrada sobre una red pública para proteger la transmisión de datos.

WMI (Windows Management Instrumentation)

Conjunto de herramientas de Microsoft para la administración y monitoreo de sistemas operativos y dispositivos en red.

XSS (Cross-Site Scripting)

Vulnerabilidad que permite inyectar código malicioso en páginas web vistas por otros usuarios, comprometiendo su seguridad.

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial
Informe de ciberalertas – 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