CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Informe de Inteligencia de Amenazas - II

Mayo 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

Este documento se distribuye bajo la **licencia Creative Commons Atribución–CompartirIgual 4.0 Internacional (CC BY-SA 4.0)**.

Disponible en: https://creativecommons.org/licenses/by-sa/4.0/deed.es

Índice

1 Introducción 4

2 Resumen ejecutivo 6

3 Inteligencia de amenazas 9

3.1 Actores de amenaza y TTPs 9

3.1.1 CCN-CERT 9

3.1.2 Microsoft Threat Intelligence 13

3.1.3 ENISA 14

3.1.4 Unit 42 Palo Alto Networks 19

3.1.5 IBM X-Force 22

3.1.6 Dragos 25

3.2 Inteligencia propia 41

4 Recomendaciones 46

4.1.1 Fabricantes de soluciones de ciberseguridad 47

4.1.2 ENISA 50

4.1.3 CISA 52

4.1.4 Resiliencia ciberfísica 60

5 Conclusiones 62

Bibliografía 65

Glosario 68

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

1 Introducción

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

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

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

--

La evolución hacia los modelos de **Industria 4.0 y 5.0**, caracterizados por la automatización avanzada, integración de sistemas ciberfísicos, analítica de datos en tiempo real y mayor interacción entre personas y tecnología, está transformando profundamente el ecosistema industrial. Esta transformación incrementa la complejidad técnica de las infraestructuras productivas e introduce nuevas dependencias digitales que deben ser gestionadas desde una perspectiva de riesgo. En este contexto, la inteligencia de amenazas orientada a OT/ICS se convierte en un instrumento esencial para la **priorización de riesgos**, el apoyo a la **toma de decisiones** y el fortalecimiento de la **resiliencia operativa** del tejido industrial gallego.

Este **Informe de inteligencia de amenazas OT – II** se concibe como una evolución natural del Informe inicial del Observatorio, con el que comparte enfoque y vocación práctica, pero **actualiza y amplía** el contenido para incorporar una caracterización más completa de actores, campañas y patrones operativos observados recientemente.

Mientras el Informe I establecía una base metodológica y una visión consolidada del panorama (marco teórico, alertas y recomendaciones), esta segunda versión refuerza de

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

manera explícita la dimensión de **atribución y perfilado de grupos**, con especial atención a la inteligencia especializada de Dragos y a su marco de lectura de la progresión adversaria en entornos industriales.

El propósito fundamental del documento es ofrecer **inteligencia accionable** para organizaciones con exposición a sistemas industriales —desde infraestructuras críticas y servicios esenciales hasta manufactura y cadenas de suministro—, traduciendo la actividad adversaria global en implicaciones operativas aplicables a Galicia. Para ello, el informe incluye:

(i) la recopilación de **actores de amenaza** con interés o capacidad sobre OT/ICS,

(ii) la identificación de las **Tácticas, Técnicas y Procedimientos (TTPs)** más recurrentes en la intrusión y en la persistencia del atacante,

(iii) y la **interpretación del riesgo según la posibilidad de progresión** desde intrusiones en IT hacia impactos sobre OT.

Un elemento diferencial de esta versión es la incorporación del marco **ICS Cyber Kill Chain** empleado por Dragos para distinguir niveles de madurez operativa del adversario. En particular, se presta atención a los grupos con capacidad confirmada para avanzar más allá del acceso inicial y del espionaje en IT, alcanzando fases de **interacción con el proceso industrial** (capacidad *Stage 2*), que constituyen el salto cualitativo hacia el impacto ciberfísico. Esta distinción resulta clave para orientar inversiones defensivas en sectores gallegos con alta dependencia de continuidad de operación, donde un incidente puede traducirse en **paradas de producción**, degradación de servicio, riesgos de seguridad y costes de recuperación elevados.

La estructura del informe mantiene una progresión didáctica: inicia con una introducción y un resumen ejecutivo orientado a decisores, continúa con un bloque central de **inteligencia de amenazas** que consolida fuentes de referencia y perfiles de actores (incluyendo el análisis de grupos y TTPs), y se completa con un apartado de **inteligencia propia** y recomendaciones de carácter técnico y organizativo.

El objetivo final es proporcionar una lectura coherente y operativa que permita **anticipar**, **detectar** y **mitigar** amenazas con impacto potencial sobre entornos industriales en el contexto 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

A continuación, sintetizamos los elementos más relevantes del **Informe de Inteligencia de Amenazas OT – II**, con el objetivo de facilitar la **toma de decisiones** por parte de responsables de ciberseguridad, operaciones industriales y Dirección. Se recuerda que la versión II da continuidad al enfoque del Informe I, manteniendo la visión integrada por fuentes, **y refuerza de manera específica el análisis de actores con relevancia OT/ICS**, especialmente aquellos con capacidad de progresar hacia impactos ciberfísicos.

En cuanto a **fuentes principales empleadas.** La elaboración de este estudio se basa en una combinación de fuentes de inteligencia y referencia ampliamente reconocidas en el campo OT/ICS, con el objetivo de equilibrar evidencias técnicas de campo, tendencias agregadas, y marcos metodológicos.

En particular, esta versión II apoya su bloque central de actores en la inteligencia especializada de **Dragos** (informe anual **OT Cybersecurity Year in Review 2025** y perfiles públicos de grupos de amenaza), y se completa con informes y guías de alcance más transversal que permiten contextualizar tendencias y priorización defensiva, incluyendo, entre otros, **ENISA** (panorama de amenazas), **Microsoft Digital Defense Report**, **IBM XForce**, informes de fabricantes y observabilidad OT (como **Crowdstrike**) y análisis de madurez y prácticas (por ejemplo de **CISA**), así como fuentes institucionales y sectoriales disponibles en el marco del Observatorio.

Mensajes clave para la toma de decisiones

1) La amenaza relevante no es solo "intrusión en IT", sino la progresión hacia OT. El criterio diferencial que debe guiar la priorización es la capacidad del adversario para avanzar en el ciclo de ataque hasta fases de **interacción con el proceso industrial** (capacidad Stage 2 en la ICS Cyber Kill Chain). En el corpus analizado, esto se materializa con claridad en actores como **ELECTRUM** (capacidad demostrada de ejecutar ataque ICS y desarrollo de wipers destructivos), **BAUXITE** (impactos Stage 2 por compromisos triviales de dispositivos expuestos) y **CHERNOVITE** (malware ICS avanzado asociado a PIPEDREAM).

2) La actividad adversaria está combinando sofisticación (malware ICS) con oportunismo (exposición y credenciales débiles). El mismo ecosistema incorpora

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

tanto capacidades avanzadas (como plataformas ICS específicas o wipers orientados a entornos embebidos) como operaciones de bajo coste basadas en **phishing**, **password spraying**, **servicios expuestos** y abuso de infraestructura de terceros. Esto implica que el riesgo no depende sólo del perfil del actor, sino también del **nivel de higiene y exposición** del operador.

3) El sector eléctrico y los servicios esenciales continúan en el foco, con impactos reales y observables. El caso del ataque a **Kyivstar** ejemplifica que la disrupción puede materializarse en degradación de servicios a gran escala, y que los adversarios pueden emplear capas de ocultación (por ejemplo, actores hacktivistas) para dificultar la atribución y la respuesta. En paralelo, el histórico de ELECTRUM (CRASHOVERRIDE/Industroyer) y la aparición de **AcidPour** refuerzan que la disrupción deliberada sigue siendo una amenaza prioritaria en ecosistemas eléctricos.

4) La información OT (GIS, topologías, instrucciones) es un activo estratégico que está siendo buscado de forma persistente. En campañas como las asociadas a **VOLTZITE**, la exfiltración de **datos GIS** y documentación OT (diagramas, instrucciones operativas) aparece como objetivo central. Para infraestructuras gallegas (energía, agua, transporte y puertos), esto obliga a tratar la documentación técnica como activo crítico, con controles equivalentes a los aplicados a credenciales y acceso remoto.

5) Europa no es un espectador: se observa targeting explícito y desplazamiento hacia objetivos europeos. La campaña de **KAMACITE** relacionada con la **Gas Infrastructure Europe (GIE)** en Alemania, combinando loaders/stealers y un backdoor a medida (**Edam**), ilustra un desplazamiento desde un foco casi exclusivo en Ucrania hacia **objetivos europeos en el ámbito de petróleo y gas**. Esto es relevante para Galicia por el peso de cadenas de suministro industriales y por la dependencia de servicios esenciales.

Se incluye una clasificación de actores de amenaza que puede emplearse como guía práctica para decidir **dónde invertir primero**: no sólo en tecnología, sino en políticas de acceso, operación y recuperación.

Decisiones defensivas recomendadas a corto y medio plazo

Las evidencias recopiladas apuntan a un conjunto de decisiones de alto impacto para organizaciones industriales:

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

a) Blindar el puente IT/OT como prioridad número 1. La **segmentación efectiva**, el control de flujos y la limitación del movimiento lateral son la medida más determinante para impedir que intrusiones en IT evolucionen hacia impactos OT.

b) Tratar accesos remotos y exposición como riesgo operativo. Deben priorizarse acciones como: restringir el acceso **SSH y servicios críticos tras VPN**, eliminar credenciales por defecto, auditar y rotar **credenciales SSH**, y revisar la exposición de dispositivos y servicios que puedan ser reutilizados como relés.

c) Proteger documentación OT y sistemas GIS como activos críticos. Establecer clasificación, control de acceso, registro de accesos y detección de exfiltración sobre diagramas de red, instrucciones operativas e información geoespacial.

d) Asegurar capacidad de recuperación frente a la disrupción y wipers. Para escenarios tipo ELECTRUM, es imprescindible disponer de **copias de seguridad fuera de línea, probadas**, incluyendo lógica de proyecto, configuraciones de IED e instaladores de aplicaciones ICS, así como controles que impidan o alerten sobre **ejecución de binarios** y cambios no autorizados.

e) Mejorar visibilidad y detección en OT con enfoque a comportamiento. Además de IoCs, es necesario observar patrones como comunicaciones anómalas hacia internet desde activos inesperados, uso inusual de protocolos y señales de movimiento lateral o acceso a repositorios de documentación técnica.

Implicación para gobernanza e inversión

La lectura agregada del informe refuerza una conclusión práctica: la mejora de ciberseguridad industrial en Galicia requiere combinar **medidas de prevención** (exposición, identidades, segmentación) con **medidas de resiliencia** (capacidad de detección y recuperación). Esto es especialmente relevante en sectores con dependencia de continuidad de operación —energía, agua, alimentación, manufactura y logística— donde el impacto de un incidente trasciende el ámbito tecnológico y puede derivar en costes operativos, reputacionales y de prestación de servicios esenciales.

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 Actores de amenaza y TTPs

La comprensión del riesgo en OT/ICS requiere ir más allá de la enumeración de vulnerabilidades o del registro de incidentes: requiere identificar **quién** opera (actores de amenaza), **cómo** opera (Tácticas, Técnicas y Procedimientos – **TTPs**) y **con qué intención y capacidad** puede progresar hacia el impacto sobre el proceso industrial. En esta sección se introduce una lectura estructurada del panorama de amenazas, combinando fuentes institucionales y de inteligencia (por ejemplo., organismos nacionales y equipos de *threat intelligence*) con marcos técnicos que permiten describir de forma consistente las acciones del adversario a lo largo del ciclo de ataque.

Se presentan por tanto, las principales aportaciones de las fuentes seleccionadas (CCN-CERT, inteligencia de fabricantes y proveedores, y análisis especializados), para culminar en una síntesis orientada a entornos industriales: **qué vectores predominan**, qué técnicas se repiten, y qué señales permiten anticipar una posible evolución desde intrusiones en IT hacia escenarios de **impacto ciberfísico** en OT/ICS.

3.1.1 CCN-CERT

Esta sección sintetiza la visión del **CCN-CERT** [1] en base al informe vinculado en bibliografía, sobre actores de amenaza, combinando **la perspectiva estratégica por Estado con la identificación de los principales grupos de ciberamenaza (APT, clústeres y colectivos)** que operan alineados o en apoyo de dichos Estados. Se mantiene así una doble lectura: por un lado, los **objetivos, motivaciones y patrones generales por país, y** por otro, los **grupos concretos** que materializan estas campañas, con especial atención a su impacto potencial en **entornos ICS/OT**. Comenzaremos con los actores estatales.

Federación Rusa

Desde una perspectiva estratégica, Rusia mantiene una **actividad sostenida y multifacética** en el ciberespacio, combinando **ciberespionaje, operaciones de influencia, sabotaje y apoyo a campañas de hacktivismo**. El CCN-CERT subraya que el foco ruso se dirige de forma recurrente a **infraestructuras críticas, administraciones públicas, defensa, energía, transporte e industria**, especialmente en el contexto del conflicto en Ucrania y las tensiones con la UE y la OTAN.

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

Esta estrategia se materializa a través de **grupos de ciberamenaza bien establecidos**, entre los que destacan:

- **APT28 (Fancy Bear)** y **APT29 (Cozy Bear)**, con campañas de espionaje dirigidas a gobiernos, organismos internacionales y sectores estratégicos.
- **Turla** y **Snake**, orientados a intrusiones persistentes y de alto sigilo.
- **Sandworm (Unidad 74455 del GRU)**, especialmente relevante para entornos **ICS/OT**, por su historial de ataques disruptivos contra redes eléctricas, sistemas industriales y servicios esenciales.

En el campo OT, el riesgo no se limita a ataques destructivos directos, sino también a **intrusiones previas, reconocimiento y preposicionamiento** en redes industriales, que pueden activarse en momentos de escalada geopolítica.

República Popular China

China centra su actividad **en el ciberespionaje a gran escala,** con un claro énfasis en la **obtención de propiedad intelectual, secretos industriales y ventaja tecnológica**. El informe del CCN-CERT señala que los sectores más afectados incluyen **industria avanzada, energía, telecomunicaciones, transporte y tecnologías estratégicas**, lo que sitúa a los entornos ICS/OT como objetivos de alto valor.

Esta estrategia se articula a través de múltiples grupos, entre los que destacan:

- **APT41**, conocido por combinar espionaje estatal con actividades de cibercrimen.
- **APT31** y **APT17**, activos contra administraciones públicas y empresas tecnológicas.
- **Mustang Panda**, con campañas persistentes contra gobiernos y sectores industriales.

En el contexto industrial, estas campañas suelen buscar **acceso prolongado y silencioso**, explotando vulnerabilidades en productos ampliamente desplegados, cadenas de suministro y proveedores tecnológicos, más que causar disrupciones inmediatas.

Corea del Norte

Este país combina **ciberespionaje, cibercrimen financiero y operaciones encubiertas** como herramienta de financiación del régimen y evasión de sanciones. El

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

CCN-CERT destaca su interés en **sector financiero, industria, energía y defensa**, con implicaciones indirectas para entornos OT.

Los principales grupos asociados incluyen:

- **Lazarus Group**, conocido por ataques de alto impacto, ransomware y sabotaje selectivo.
- **Kimsuky** y **Andariel**, orientados a espionaje y obtención de credenciales.

Aunque muchas campañas se originan en entornos IT, el acceso a **redes corporativas de organizaciones industriales** puede facilitar movimientos laterales hacia sistemas OT mal segmentados.

Irán

Irán mantiene una actividad creciente, caracterizada por **espionaje regional, sabotaje selectivo y operaciones de represalia**. El CCN-CERT identifica como objetivos prioritarios los sectores de **energía, agua, transporte e industria**, lo que confiere a OT un papel central.

Entre los grupos más representativos se encuentran:

- **APT33**, históricamente vinculado a ataques contra energía y aviación.
- **APT34 (OilRig)** y **APT35**, con campañas de espionaje prolongadas.
- **MuddyWater**, especialmente relevante por su actividad contra organismos gubernamentales y empresas industriales.

Estos actores han demostrado interés en **sistemas de control industrial y redes híbridas IT/OT**, combinando técnicas relativamente simples con una alta persistencia.

Otros actores estatales

El informe también contempla actividad atribuida a otros Estados, como **India** o **Israel**, generalmente con un alcance más limitado y focalizado en **espionaje estratégico y regional**. A continuación, un gráfico para ilustrar quiénes son mayoritariamente el objetivo de estos ataques:

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

Objetivo de campañas de espionaje. Fuente: CCN-CERT (2024)

Aunque su impacto directo en OT es menor, estas operaciones pueden afectar a **proveedores tecnológicos y cadenas de suministro industriales**.

Hacktivismo

El **hacktivismo** ocupa un papel destacado en el panorama actual, especialmente desde 2022. El CCN-CERT diferencia entre campañas de **bajo impacto técnico pero alta visibilidad** y otras con mayor capacidad de disrupción.

Desde una visión general, el hacktivismo se caracteriza por:

- **Motivación ideológica y geopolítica**.
- Empleo intensivo de **DDoS, defacement y filtraciones de información**.
- Coordinación a través de canales públicos (Telegram, foros).

En los últimos años han aparecido colectivos claramente alineados con intereses estatales, entre ellos:

- **Killnet** y **NoName057(16)**, activos contra países europeos y sectores críticos en apoyo a narrativas prorrusas.
- Alianzas temporales entre grupos, que incrementan la escala y frecuencia de los ataques.

Aunque estas campañas suelen dirigirse a **servicios digitales y portales web**, su relevancia para ICS/OT radica en varios factores: dependencia de **servicios IT para la operación industrial**, impacto reputacional y presión social, y riesgo de **efectos colaterales** cuando los ataques afectan a proveedores o infraestructuras compartidas.

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

En conjunto, la combinación de **estrategias estatales y grupos de amenaza concretos** refuerza la idea de que los entornos industriales deben considerarse objetivos legítimos dentro del ciberconflicto moderno, no sólo por su valor operativo, sino también por su importancia económica, social y geopolítica.

3.1.2 Microsoft Threat Intelligence

A continuación, la referencia más actualizada de Microsoft en su Digital Report 2025 [2], sobre las consideraciones anteriores de los estados nación que aportaba el CCN-CERT.

Rusia

Microsoft confirma que **Rusia mantiene un uso intensivo del ciberespacio como herramienta estratégica**, combinando espionaje, operaciones de influencia y actividades disruptivas. En línea con el CCN-CERT, se observa una **priorización de infraestructuras críticas, administraciones públicas, defensa y sectores energéticos y de transporte**, especialmente en el contexto del conflicto en Ucrania y sus efectos colaterales sobre Europa.

Desde la óptica de Microsoft, resulta relevante la **creciente convergencia entre operaciones de ciberseguridad y objetivos cinéticos**, así como el uso de **grupos con distintos niveles de sofisticación**, desde APT altamente capacitados hasta colectivos hacktivistas o criminales que actúan como fuerza de presión complementaria. Para entornos ICS/OT, esta combinación incrementa el riesgo de **ataques oportunistas y disruptivos** contra servicios esenciales, aun cuando el objetivo principal no sea industrial.

China

Microsoft describe a China como un actor **altamente persistente y orientado al ciberespionaje estratégico a largo plazo**. El foco principal sigue siendo **la obtención de información sensible, propiedad intelectual y conocimiento tecnológico**, con campañas prolongadas y de baja visibilidad.

El valor añadido del informe de Microsoft reside en subrayar la **amplitud sectorial de los objetivos**, incluyendo telecomunicaciones, administraciones públicas, proveedores de servicios digitales y sectores industriales avanzados. En el campo ICS/OT, este enfoque refuerza la idea de que **el acceso a redes IT puede ser un paso intermedio** hacia entornos industriales, especialmente en organizaciones con fuerte dependencia tecnológica o cadenas de suministro complejas.

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

Corea del Norte

Actor singular, donde **la motivación económica y la evasión de sanciones** tienen un peso comparable al espionaje. Se mantiene el uso de campañas dirigidas contra sectores financieros, tecnológicos y empresas con capacidad de generar ingresos directos o indirectos.

El informe de Microsoft aporta contexto adicional sobre la **profesionalización de estas operaciones** y su escalabilidad, lo que incrementa el riesgo de efectos colaterales en entornos industriales, especialmente cuando organizaciones OT dependen de servicios IT, proveedores externos o infraestructuras digitales compartidas.

Irán

Se caracteriza a Irán como un actor **más orientado a operaciones disruptivas, de influencia y de presión política**, con un nivel técnico generalmente inferior al de Rusia o China, pero compensado por un uso intensivo de técnicas conocidas y ataques oportunistas.

Para ICS/OT, esta convergencia de análisis refuerza la percepción de riesgo frente a **ataques de baja sofisticación técnica pero alto impacto operativo**, especialmente en sectores energéticos, transporte y servicios públicos, donde la disponibilidad es un factor crítico.

3.1.3 ENISA

3.1.3.1 Panorama general

En el informe Threat Landscape 2025 de ENISA, se recogen las **Tácticas, Técnicas y Procedimientos (TTPs) más comúnmente observados**, de manera informal (i.e. sin asignar código de la matriz de MITRE) [3].

Durante el período analizado, **los grupos de cibercrimen evolucionaron de forma continua sus TTPs,** con un énfasis claro en la **madurez de los ecosistemas ransomware y en el endurecimiento de las tácticas de presión sobre las víctimas**. Se mantiene la reutilización de builders filtrados, como en el caso de SafePay —derivado de LockBit 3—, y se prevé que la publicación del código fuente de VanHelsing RaaS reduzca aún más las barreras de entrada al cibercrimen, facilitando la aparición de nuevos operadores.

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

En paralelo, los **mecanismos de distribución de malware**, especialmente infostealers, se diversificaron. A los vectores clásicos (software pirata, phishing o repositorios públicos de código) se suman **métodos de bajo coste y alto alcance**, como falsos CAPTCHA, servicios de alojamiento en la nube o enlaces embebidos en plataformas de vídeo, lo que incrementa notablemente la superficie de exposición, también para organizaciones con entornos OT conectados indirectamente a IT.

Un cambio especialmente relevante **es el uso sistemático de herramientas diseñadas para desactivar soluciones EDR**, con el objetivo de realizar intrusiones más sigilosas y centradas en la exfiltración rápida de datos. Herramientas como AvNeutralizer (AuKill), EDRKillShifter o técnicas basadas en drivers firmados —como ABYSSWORKER— fueron adoptadas progresivamente por múltiples esquemas RaaS activos en la UE. Esta tendencia refuerza el riesgo para entornos industriales basados en Windows, habituales en capas de supervisión y operación.

En cuanto a la **extorsión**, nuevas familias como Fog y Qilin intensificaron tácticas agresivas, incorporando contadores regresivos, perfiles públicos de víctimas, muestras descargables y, en el caso de Qilin, incluso funcionalidades que simulan escaladas en procedimientos legales ("call lawyer"). En el contexto europeo, estas tácticas resultan especialmente eficaces debido a las **obligaciones regulatorias y de notificación (GDPR, NIS2)**, que incrementan la presión para pagar rescates.

Más allá del ransomware, se observa una **diversificación del cibercrimen hacia fraudes complejos**, como los esquemas de pig-butchering (estafas trabajadas en el tiempo), que crecieron cerca de un 40% interanual y generan entre 9,1 y 11,4 millones de euros a escala global. Estas campañas combinan **ingeniería social prolongada, criptomonedas, IA generativa y deepfakes,** y ya afectan de forma significativa a ciudadanos y organizaciones de la UE. Las operaciones policiales recientes muestran la escala industrial de estas redes, con millones de dispositivos y credenciales comprometidas.

Finalmente, emerge una dimensión especialmente preocupante: la **traslación del impacto digital al plano físico**, con ataques directos —incluidos secuestros— contra titulares de criptoactivos y sus familias, vinculados a filtraciones de datos de plataformas centralizadas. Casos documentados en varios Estados miembros evidencian cómo el cibercrimen está cruzando la frontera entre lo digital y el físico, un

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

riesgo que resulta particularmente crítico para sectores industriales y operadores de infraestructuras esenciales.

En una sección posterior se refieren a los TTPs asociados a hacktivismo. Durante el período analizado, **el hacktivismo ha mostrado una clara evolución desde campañas principalmente disruptivas hacia modelos híbridos**, incorporando **tácticas propias del cibercrimen organizado** y ampliando de forma explícita su foco hacia **entornos OT e infraestructuras críticas**.

En el ámbito de los **ataques DDoS**, los grupos hacktivistas han adoptado **TTPs más avanzados**, combinando técnicas como el carpet bombing (DDoS), el uso masivo de routers comprometidos y, de forma creciente, **capacidades apoyadas en IA** para incrementar la intensidad, persistencia y alcance de los ataques. Los datos de Netscout para el primer semestre de 2024 muestran un **incremento del 50 % en dispositivos infectados**, impulsado principalmente por la aparición del Botnet Zergeca y la evolución del Botnet DDoSia, empleado por NoName057(16), que destaca por el uso **de DNS over HTTPS (DoH)** como canal de mando y control, dificultando su detección.

Un fenómeno especialmente relevante **es la convergencia entre hacktivismo y ransomware**, particularmente entre grupos prorrusos. Colectivos como **CyberVolk's, Azzasec, Funksec o Lapsus$** pasaron de campañas ideológicas a **modelos de ransomware-as-a-service (RaaS)**, mientras que **KillSecurity**, originalmente alineado con Anonymous, se consolidó como actor relevante tras lanzar su propia plataforma RaaS en junio de 2024. Desde entonces, este grupo dirigió ataques contra múltiples Estados miembros de la UE, con picos de actividad observados en 2025. Esta evolución confirma que el hacktivismo ya no se limita a la disrupción simbólica, sino que busca **beneficios económicos y persistencia operativa**.

En paralelo, los **ataques contra OT** se han convertido en un elemento central del discurso y la actividad hacktivista. Destaca el caso **de Z-PST-ALLIANCE**, que reivindicó ataques contra **interfaces de gestión OT expuestas a Internet** en sectores como **energía y agua**, con un alcance geográfico amplio en la UE. Países como **Italia, Chequia, Francia y España** figuran entre los más afectados. Aunque estos incidentes no provocarían impactos operativos significativos, la **difusión de vídeos mostrando la manipulación de sistemas OT** apunta claramente a un objetivo de **impacto psicológico, propagandístico y disuasorio**, más que a la interrupción efectiva de procesos.

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

Z-PENTEST-ALLIANCE se situó como el **principal grupo hacktivista en el targeting de infraestructuras críticas en la UE,** con un énfasis creciente en sistemas energéticos. Desde comienzos de 2025, el grupo intensificó su retórica y sus declaraciones de intenciones contra OT, llegando incluso a **atribuirsele vínculos con el grupo Sandworm**. Sin embargo, estas afirmaciones no han podido verificarse y, por el momento, se consideran dudosas, lo que sugiere posibles estrategias de **inflado reputacional o "faketivismo"**.

Finalmente, emerge un nuevo vector de riesgo con la aparición en junio de 2025 del grupo **Infrastructure Destruction Squad (IDS)**, que afirma desarrollar **VoltRuptor**, un malware específico para ICS con **soporte multiprotocolo, capacidades avanzadas de persistencia y técnicas antiforenses**. La supuesta disponibilidad de VoltRuptor en mercados clandestinos y la reivindicación de un compromiso contra una empresa italiana de automatización de edificios exponen un **escenario de especial preocupación**, aunque la amenaza es aún demasiado reciente para una evaluación concluyente. Aun así, la hipótesis de una **instrumentalización de este actor por intereses estatales** se considera plausible y refuerza la tendencia **de difuminación entre hacktivismo, cibercrimen y operaciones de influencia con trasfondo geopolítico**, con implicaciones directas para la seguridad de entornos ICS/OT.

3.1.3.2 TTPs

Los **TTPs (Tactics, Techniques and Procedures)** de las matrices MITRE ATT&CK describen cómo operan los adversarios: **las tácticas** reflejan sus objetivos, las **técnicas** los métodos generales empleados, y los **procedimientos** los pasos concretos o herramientas utilizadas [4][5].

A partir de fuentes abiertas, el conjunto de datos de ENISA se centra principalmente en **actividades posteriores al compromiso**, destacando especialmente las fases de **reconocimiento**, **mantenimiento del acceso y ejecución de cargas maliciosas** tras la intrusión inicial. En comparación, las tácticas asociadas a **impacto**, **exfiltración y colección** aparecen con menor frecuencia.

A nivel de técnicas, el análisis revela **patrones recurrentes de uso conjunto**, que se reflejan en una **visualización agrupada de TTPs**. Un primer bloque claramente definido corresponde a las técnicas **de descubrimiento**, como la identificación de procesos, configuración de red, información del sistema, ficheros, directorios y recursos

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

compartidos, lo que evidencia la fase sistemática de inventariado que realizan los atacantes una vez dentro del entorno.

Un segundo grupo relevante se concentra en las técnicas **de ejecución**, dominadas por el uso de **intérpretes de comandos y scripting**, junto con mecanismos como WMI, APIs nativas, ejecución mediante servicios y acciones iniciadas por el usuario. Estas técnicas reflejan la preferencia de los adversarios por **mecanismos legítimos del sistema operativo**, que facilitan la evasión y reducen la detección.

La **persistencia** aparece como otro bloque cohesionado, combinando el uso de servicios de Windows, modificaciones en el registro, mecanismos de autoarranque y **la creación o abuso de cuentas válidas**, lo que demuestra cómo los atacantes **superponen múltiples métodos de permanencia** para asegurar el acceso a largo plazo.

Finalmente, aunque con menor peso, se identifican bloques coherentes asociados a **exfiltración de información** y **técnicas de impacto**, que incluyen distintos métodos de transferencia de datos y acciones orientadas a la interrupción, degradación o manipulación de sistemas.

En este punto resulta pertinente **insertar la gráfica de TTPs que proporciona ENISA**, que permite apreciar de forma intuitiva cómo estas técnicas tienden a agruparse alrededor de fases concretas del ciclo de ataque, proporcionando la comprensión de los patrones operativos más habituales observados en este análisis.

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

TTPs más vistos en los incidentes analizados. Fuente: ENISA (2025)

Cabe destacar que en el anexo 12.1 de este informe de ENISA, se incluye **una tabla con todas las tácticas, técnicas y mitigaciones asociadas**, para referencia del lector que quiera profundizar en la cuestión.

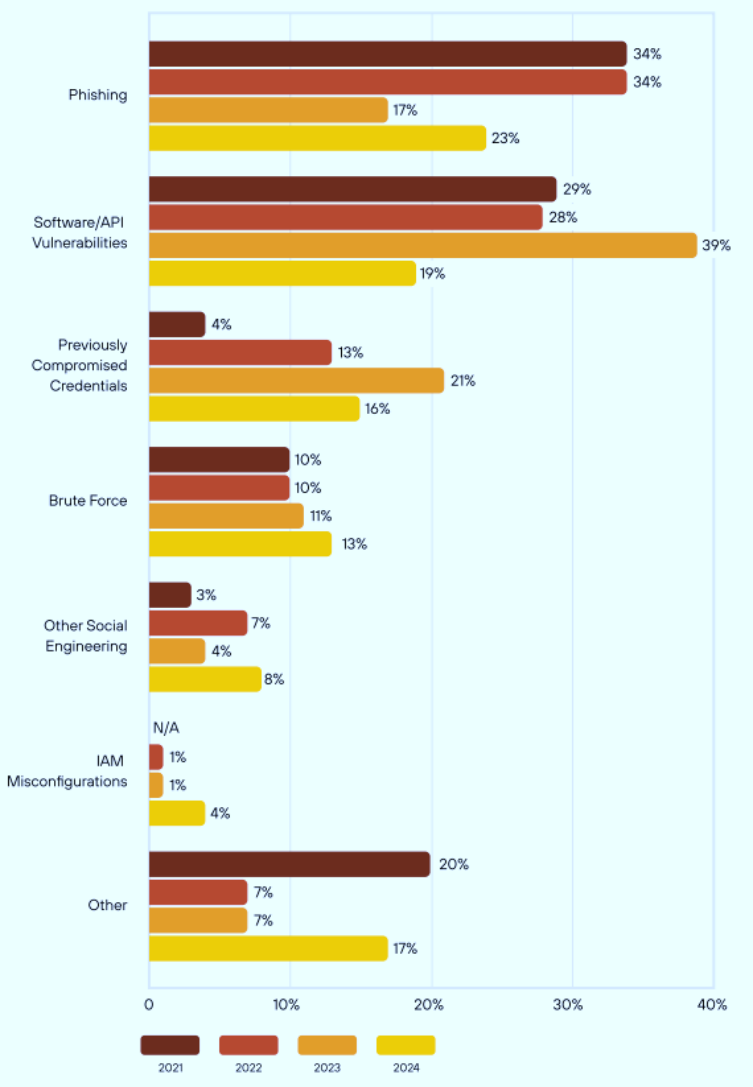
3.1.4 Unit 42 Palo Alto Networks

En el informe **de Unit 42 de Palo Alto** [6], aparecen un par de figuras interesantes relativas al punto inicial de ataque de los adversarios, así como una tendencia a este respecto en los últimos cuatro años:

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

Fronts of Attack	Percentage of Cases
Endpoints	72%
Human	65%
Identity	63%
Network	58%
Email	28%
Cloud	27%
Application	21%
SecOps	14%
Database	1%

Punto de ataque en incidentes. Fuente: Palo Alto Networks (2025)

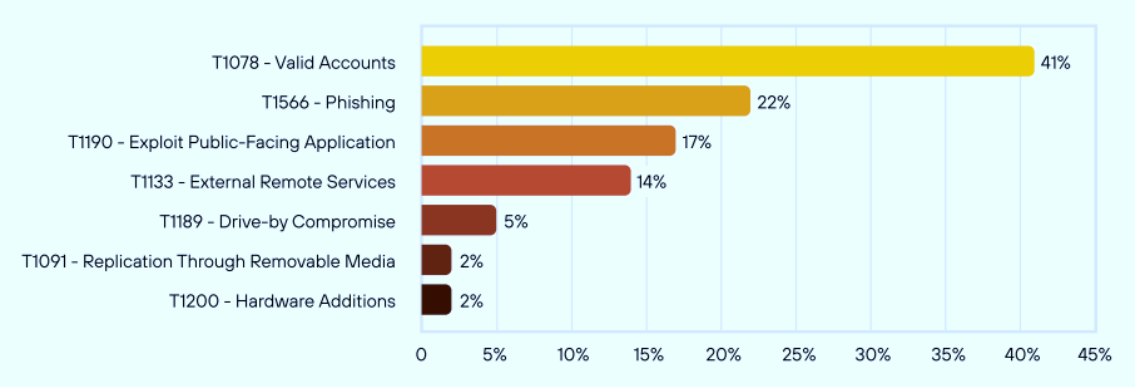


Tendencia del punto de entrada inicial de los ataques. Fuente: Palo Alto Networks (2025)

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

Identifican además una consolidación **de TTPs "living off the land"**, donde los atacantes priorizan el abuso de **mecanismos legítimos** frente al uso de malware complejo, reduciendo así la detección y facilitando la persistencia.

Una de las tendencias más destacadas es el uso **de T1078 – Valid Accounts** como **vector principal de acceso inicial**, representando más del 40 % de las técnicas asociadas a esta táctica (más detalle en la figura siguiente). Este patrón se ve favorecido por **debilidades estructurales en la gestión de identidades y accesos**, como la ausencia de MFA, el uso de contraseñas débiles o recicladas, controles insuficientes frente a fuerza bruta **y permisos excesivos** en cuentas comprometidas. Esta técnica es especialmente relevante en entornos híbridos IT/OT, donde las credenciales válidas permiten pivotar hacia redes industriales mal segmentadas.



Prevalencia de las técnicas observadas respecto de la táctica de acceso inicial. Fuente: Palo Alto (2025)

En la fase de ejecución, la técnica dominante es **T1059 – Command and Scripting Interpreter**, presente en más del 60 % de los casos asociados a la táctica de ejecución. Los adversarios abusan **de PowerShell**, intérpretes nativos **de Windows y Unix**, así como shells específicos de aplicaciones y dispositivos de red, para realizar tareas de reconocimiento, movimiento lateral y despliegue de cargas, aprovechando herramientas ya disponibles en los sistemas.

Para el **movimiento lateral,** la técnica más observada es **T1021 – Remote Services**, que aparece en más del 86 % de los casos analizados para esta táctica. Los atacantes reutilizan credenciales legítimas para autenticarse mediante **RDP**, **SMB** y **SSH**, reforzando la tendencia de explotación de servicios remotos internos en lugar de técnicas más ruidosas.

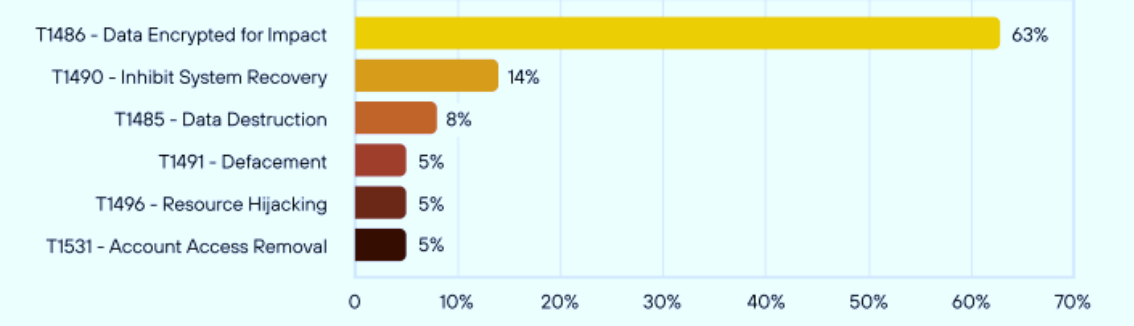
En paralelo, Unit 42 observa un aumento significativo de técnicas orientadas a la **evasión de defensas**, especialmente **T1562 – Impair Defenses**, presente en cerca del

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

30 % de los casos analizados. Estas actividades incluyen **deshabilitar o modificar herramientas de seguridad**, **firewalls del sistema y registro de eventos de Windows**, con el objetivo de operar de forma más sigilosa y acelerar la exfiltración de datos.

Finalmente, se consolida el uso del enfoque **BYOVD (Bring Your Own Vulnerable Driver)**, mediante el cual los atacantes introducen controladores vulnerables para obtener privilegios elevados y **eludir EDR y otras protecciones**. Este patrón se relaciona estrechamente con técnicas como **T1543.003 – Create or Modify System Process: Windows Service** y **T1068 – Exploitation for Privilege Escalation**, evidenciando una profesionalización creciente en la manipulación del propio entorno defensivo.

Con respecto a las estrategias observadas asociadas a la **táctica de impacto**, tenemos los siguientes resultados, que denotan la **prevalencia clara del ransomware sobre otros efectos maliciosos**:



Prevalencia de las técnicas observadas respecto de la táctica de impacto. Fuente: Palo Alto (2025)

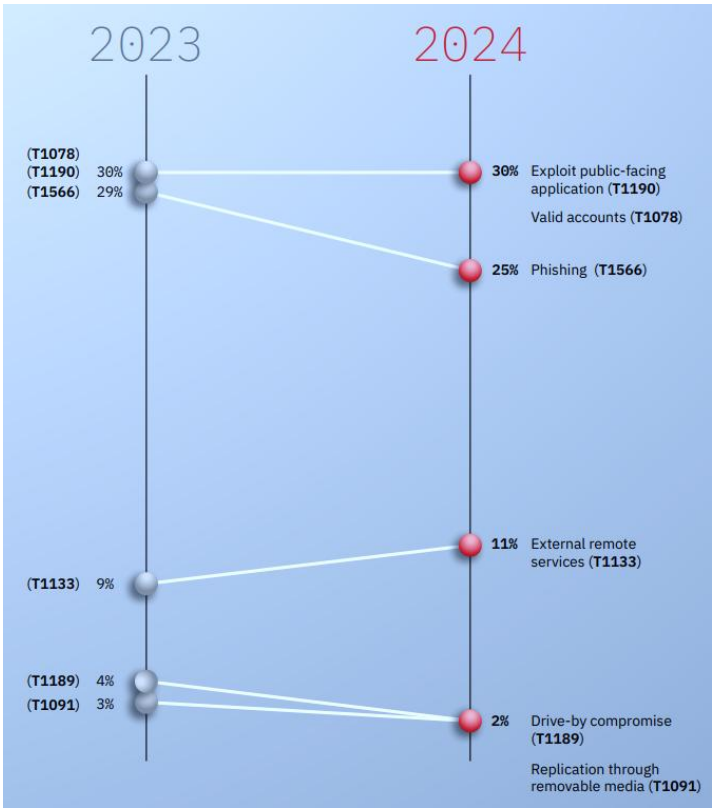
Estas tendencias muestran que en 2024 los atacantes priorizan **credenciales válidas, herramientas nativas y técnicas de evasión**, combinándolas para alcanzar intrusiones más persistentes, rápidas y difíciles de detectar, con implicaciones directas para organizaciones con entornos IT e ICS interconectados.

3.1.5 IBM X-Force

En 2024, **IBM observa** en el informe vinculado **una consolidación clara de los accesos iniciales basados en identidades y vulnerabilidades**, hasta el punto de que los **dos principales vectores de acceso inicial** fueron, en igualdad de peso, la **explotación de aplicaciones expuestas a Internet (T1190)** y el **uso de cuentas válidas (T1078)**, **ambos con un 30** % de los casos de respuesta a incidentes [7]. Esta realidad refuerza la

tendencia ya apuntada en años anteriores: *los atacantes ya no "entran por la fuerza", sino que acceden con credenciales legítimas*.

En el gráfico que se muestra a continuación, se refleja la evolución de técnicas de 2024 frente a 2023 en cuanto a acceso inicial.



Métodos utilizados por los actores de amenaza para obtener acceso. Fuente: IBM X-Force (2025)

El **abuso de credenciales** sigue alimentándose de un ecosistema criminal muy activo. Los actores de amenaza obtienen cuentas válidas principalmente mediante **malware infostealer**, ampliamente distribuido en campañas de phishing, así como a través de su **compra y venta masiva en mercados clandestinos**. A pesar del crecimiento en la adopción de **MFA**, X-Force detectó en 2024 un aumento de **kits y servicios de phishing adversary-in-the-middle (AiTM)** diseñados específicamente para **eludir MFA,** lo que confirma la madurez de un **mercado criminal de** "**access-as-a-service**".

El **phishing clásico (T1566)** continúa siendo relevante, pero pierde peso relativo como vector directo de compromiso, representando **el 25 % de los incidentes en 2024**, frente al 29 % en 2023 y el 46 % en 2022. Esta caída se atribuye a la mejora de las capacidades defensivas de las organizaciones, que logran bloquear con mayor eficacia

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

correos maliciosos, incluso cuando incorporan contenidos generados con IA. Sin embargo, el phishing no desaparece, **sino que evoluciona hacia un papel indirecto**, actuando como **vector "sombra" para el robo de credenciales**.

En este contexto, X-Force identifica un **cambio estratégico clave**: el descenso de campañas masivas de malware persistente entregado por correo electrónico (como Emotet, TrickBot o Qakbot) y un **fuerte aumento del uso de infostealers**, menos visibles y más rápidos. En 2024, el número medio semanal **de infostealers distribuidos por phishing creció un 84 % respecto de 2023**, y los primeros datos de 2025 apuntan a incrementos aún mayores. Familias como **AgentTesla, FormBook, SnakeKeylogger y PureLogs** destacan entre las más utilizadas.

Especial relevancia tiene la actividad **de Hive0145**, un **initial access broker** centrado en Europa, que distribuye **Strela Stealer** con el objetivo específico de robar credenciales de correo electrónico y facilitar **Business Email Compromise (BEC)**. En la segunda mitad de 2024, este actor ha introducido técnicas más sofisticadas, como el "**attachment hijacking**" o secuestro de archivos adjuntos, reutilizando correos legítimos previamente robados para aumentar la credibilidad y eficacia de sus campañas.

En conjunto, el análisis de X-Force muestra un **desplazamiento definitivo hacia ataques centrados en identidades**, con menos dependencia de malware persistente y una mayor explotación de **credenciales válidas, infostealers y técnicas de evasión de MFA**, configurando un escenario especialmente preocupante para organizaciones con superficies de ataque amplias y entornos híbridos IT/OT.

A modo de cierre de esta sección, podemos decir que la observación sistemática de TTPs recurrentes —especialmente en acceso inicial, persistencia y evasión— evidencia que **muchos incidentes podrían haberse contenido de forma temprana si existiera visibilidad adecuada sobre comportamientos anómalos en IT con impacto potencial en OT, como el abuso de credenciales válidas, el uso de herramientas legítimas de modo malicioso o la manipulación de servicios y cuentas.**

Además, el cruce de información procedente de fuentes diversas y reputadas, permite **identificar qué técnicas están siendo más utilizadas** en Europa y cuáles afectan con mayor frecuencia a sectores industriales. **Esto facilita priorizar inversiones y esfuerzos** —por ejemplo, en gestión de identidades, endurecimiento de accesos remotos, detección de movimientos laterales o protección de activos ICS críticos— y

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

avanzar hacia una defensa basada en comportamiento y contexto operativo, más **resiliente frente a la reutilización constante de TTPs por actores muy distintos entre sí.**

3.1.6 Dragos

3.1.6.1 Introducción y Cyber Kill Chain

El análisis de los **grupos de amenaza específicos para entornos industriales (OT/ICS)** constituye uno de los elementos diferenciales más relevantes de la inteligencia especializada aportada por Dragos en su informe anual OT Cybersecurity Year in Review 2025 [8]. A diferencia de otros informes de carácter más transversal —centrados en IT o en amenazas globales—, Dragos mantiene una metodología propia orientada a la identificación, seguimiento y caracterización de actores con **capacidad demostrada o intención explícita de afectar a sistemas de control industrial**, ofreciendo así una lectura particularmente valiosa para operadores de infraestructuras críticas.

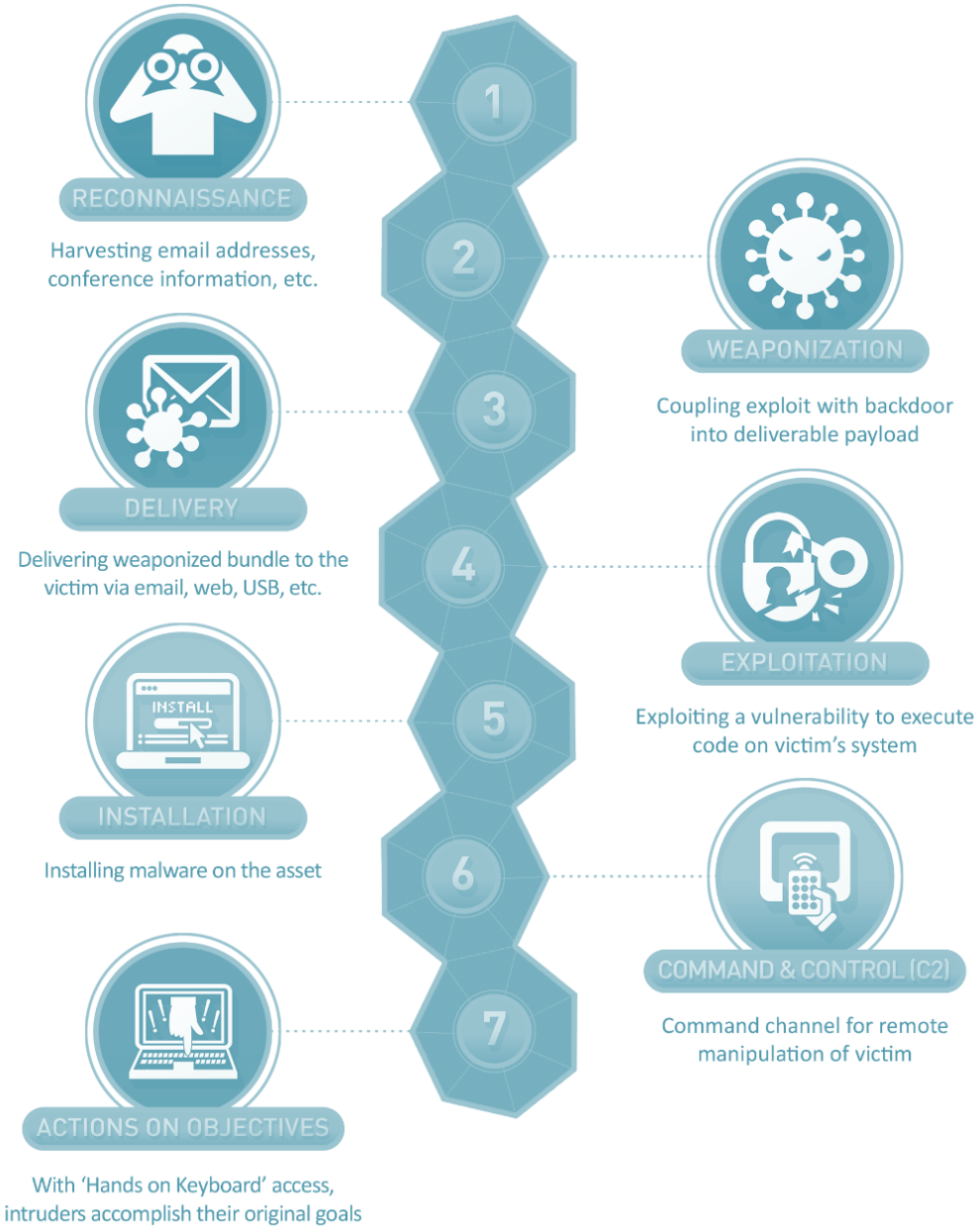
En el período analizado, Dragos identifica **nueve grupos de amenaza activos con relevancia para ICS/OT,** de nombre clave: KAMACITE, MAGNALLIUM, PARISITE, VOLTZITE, WASSONITE, CHERNOVITE, ELECTRUM, GRAPHITE, BAUXITE. Los dos últimos son considerados **nuevas incorporaciones en 2024**, lo que evidencia la evolución dinámica del ecosistema de amenazas industriales y la entrada de nuevos actores con interés específico en sistemas ciberfísicos.

Además, el informe destaca que **tres de estos grupos presentan capacidad en la denominada "ICS Cyber Kill Chain Stage 2"**, es decir, han demostrado habilidades más allá del acceso inicial a entornos IT, alcanzando fases de interacción directa o impacto potencial sobre procesos industriales.

Grupos de amenaza en ICS/OT identificados. Fuente: Dragos (2025)

La Cyber Kill Chain aplicada a ICS

El concepto de **Cyber Kill Chain** fue formulado inicialmente por Lockheed Martin como un **modelo estructurado para describir las fases de un ataque dirigido (APT, Advanced Persistent Threat)**, desde la preparación hasta la consecución del objetivo final, como se ve en la siguiente figura [9][10].



Cyber Kill Chain. Fuente: Lockheed Martin (2011)

A nivel operativo, el significado de cada fase es el siguiente:

1. **Reconocimiento (Reconnaissance)**: recopilación de información sobre la organización objetivo, activos expuestos, personal clave y tecnologías empleadas.
2. **Armamento (Weaponization)**: preparación del artefacto malicioso que combinará vulnerabilidad y carga útil.
3. **Entrega (Delivery)**: transmisión del vector de ataque (correo electrónico, explotación web, acceso remoto, etc.).
4. **Explotación (Exploitation)**: ejecución de la vulnerabilidad para obtener acceso inicial.
5. **Instalación (Installation)**: establecimiento de persistencia mediante malware o modificaciones del sistema.
6. **Comando y Control (C2)**: comunicación con el atacante para recibir instrucciones adicionales.
7. **Acciones sobre el objetivo (Actions on Objectives)**: ejecución del propósito final, como exfiltración, sabotaje o destrucción.

Este modelo, ampliamente adoptado en el ámbito IT, fue posteriormente complementado por marcos como **MITRE ATT&CK** [4] y su adaptación específica para sistemas industriales, **MITRE ATT&CK for ICS** [5], que detallan tácticas y técnicas propias de entornos de control.

En el ámbito industrial, la progresión del ataque no se detiene en la exfiltración de información. Por el contrario, puede evolucionar hacia la interacción directa con PLCs, RTUs, HMIs o sistemas SCADA. Dragos, en su trabajo de **mapeo específico sobre ATT&CK para ICS** [11]**, introduce una diferenciación relevante al identificar lo que denomina Stage 2 Capability dentro de la ICS Cyber Kill Chain.**

Desde una perspectiva metodológica, la adaptación al ámbito ICS puede resumirse en dos grandes fases operativas:

- **Stage 1 – Compromiso IT/Perímetro**: incluye las etapas tradicionales de acceso inicial, movimiento lateral, escalada de privilegios y consolidación de presencia dentro de la red corporativa. Muchos actores se quedan en esta fase, limitándose al espionaje o extorsión.

- **Stage 2 – Interacción con el proceso industrial**: implica la capacidad de pivotar hacia la red OT, identificar activos de control, comprender protocolos industriales (Modbus, OPC UA, DNP3, S7, etc.) y ejecutar acciones que alteren el funcionamiento físico del proceso. Esta fase puede incluir manipulación de lógica de control, modificación de parámetros operativos, degradación de sistemas de seguridad o interrupción deliberada del servicio.

La relevancia de la Stage 2 radica en que supone un salto cualitativo desde el impacto digital **al impacto ciberfísico**, afectando directamente a la disponibilidad, integridad o seguridad de las operaciones industriales. No todos los actores con acceso IT poseen conocimiento técnico suficiente sobre ingeniería de procesos o protocolos industriales para completar esta fase.

Desde el punto de vista de la defensa, la desagregación de la Kill Chain permite:

- **Identificar** en qué **fase puede interrumpirse el ataque**.
- **Priorizar medidas de segmentación** entre IT y OT.
- **Implementar detección específica basada** en comportamiento en redes industriales.
- **Alinear controles técnicos con las técnicas más empleadas según ATT&CK for ICS.**

Esta aproximación estructurada refuerza los modelos de defensa en profundidad y permite evaluar con mayor precisión el nivel de madurez de un actor de amenaza.

En la presente subsección se abordan ahora los **nueve grupos identificados por Dragos, describiendo su perfil y orientación, sectores y geografía objetivo, actividad subrayable y TTPs más relevantes junto a nivel de madurez operativa en entornos ICS.** Esta aproximación complementa la visión general ofrecida por otras fuentes analizadas previamente, incorporando una dimensión especializada **de interés para las organizaciones gallegas con exposición directa a sistemas industriales que hayan alcanzado un nivel de madurez que les permita desarrollar actividades de caza de amenazas** (threat hunting).

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

3.1.6.2 Grupos de amenaza

3.1.6.2.1 KAMACITE

- **Perfil y orientación.** KAMACITE se describe como un actor particularmente relevante por actuar, en múltiples operaciones, como **proveedor de acceso inicial**: establece pie en redes corporativas (IT) y **cede el control** a equipos con orientación más destructiva en OT, como ELECTRUM. El informe también sitúa su trayectoria en campañas disruptivas dirigidas contra infraestructura eléctrica en Ucrania, y destaca una evolución reciente hacia nuevas familias de malware y un foco más amplio.
- **Foco sectorial y geográfico.** En el período analizado, Dragos encuadra su objetivo principal en **Ucrania** y también en **Europa Oriental y Central**, con especial atención a organizaciones de **electricidad y petróleo y gas**, así como entidades de **manufactura** y de la **base industrial de defensa**.
- **Actividad y campañas destacables.** El informe recoge, entre otras, una campaña asociada al backdoor **Kapeka** (observada en 2022-2023 e identificada en 2024) contra operadores ucranianos de infraestructura crítica, incluyendo entidades que abastecen **calor, agua y electricidad**. En paralelo, Dragos señala el uso continuado de malware de naturaleza "commodity" en campañas de ingeniería social dirigida o spear-phishing (p.ej., **DarkCrystal RAT**) para **vigilancia** y **robo de información**.

  Adicionalmente, se describe una campaña de 2024 con temática vinculada a la **Gas Infrastructure Europe (GIE)** en Alemania, en la que KAMACITE combinó *loaders y stealers* (p.ej., **LummaStealer**) con una cadena de infección más compleja que culmina en un backdoor Windows desarrollado a medida (**Edam**), interpretada como un **giro** desde un enfoque casi exclusivo en Ucrania hacia objetivos europeos en el ámbito de petróleo y gas.
- **TTPs y capacidades observadas.** El patrón operativo subrayado combina **ingeniería social** (spear-phishing y cebos temáticos), cadenas de ejecución basadas en **PowerShell** y artefactos de *loader/dropper*, y el uso de infraestructura de intermediación (p.ej., *proxies*). El informe llama la atención sobre la necesidad de disponer de telemetría suficiente para observar **tráfico norte–sur** (de entrada y salida en la red ICS/OT) y señales de actividad anómala en entornos industriales.

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

- **Implicaciones defensivas en OT/ICS.** Dragones vincula la mitigación efectiva a:
    1. **formación y concienciación** frente al phishing,
    2. **segmentación robusta IT/OT** para impedir la escalada hacia eventos disruptivos,
    3. y mejora de la **visibilidad y detección** de patrones anómalos en redes de control (p.ej., interrupciones inusuales de conexiones entre centros de control o sondajes anómalos sobre subestaciones y estados de interruptores).

3.1.6.2.2 MAGNALLIUM

La ficha de este grupo se elabora a partir de la info disponible en la web [26], pues no se muestra detalle en el informe anual antes mencionado.

- **Perfil y orientación.** MAGNALLIUM se cuenta como un actor activo desde al menos 2013, centrado principalmente en **operaciones de acceso inicial y recogida de información** contra organizaciones industriales. Aunque su actividad impacta en sectores críticos, no se identifica capacidad demostrada para interactuar directamente con sistemas ICS ni para ejecutar acciones de impacto físico en procesos industriales. Su perfil encaja en un actor orientado a la intrusión en entornos IT con potencial de pivotaje, pero sin evidencia de progresión a fases avanzadas de la ICS Cyber Kill Chain.
- **Foco sectorial y geográfico.** MAGNALLIUM ha dirigido históricamente sus campañas contra **fabricantes petroquímicos y organizaciones del sector energético**, con foco inicial en **Arabia Saudita** y posterior expansión hacia **Europa** y **Norteamérica**. También se observaron actividades contra entidades industriales y del ámbito aeroespacial.
- **Actividad y campañas destacables.** Las campañas atribuidas a MAGNALLIUM incluyen operaciones de phishing dirigido empleando cebos relacionados con ofertas laborales y comunicaciones corporativas, así como el uso de kits de phishing de terceros. En etapas anteriores empleó familias de malware como variantes no destructivas asociadas a StoneDrill y TURNEDUP, y desde 2018 se observó una transición hacia el uso de herramientas basadas en PowerShell para

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

tareas de post-explotación y mantenimiento de acceso. No existen indicios en el informe, de interacción directa con redes de control industrial.

- **TTPs y capacidades observadas.** El patrón operativo descrito incluye:
    - **Phishing dirigido** con cebos personalizados.
    - **Password spraying** para comprometer credenciales corporativas.
    - Uso de herramientas públicas o semi-públicas para **captura de credenciales.**
    - Empleo de **scripts PowerShell para ejecución remota y persistencia** en entornos IT.

  No se documentan técnicas específicas orientadas a protocolos industriales ni acciones asociadas a Stage 2 en la ICS Cyber Kill Chain.

- **Implicaciones defensivas en OT/ICS.** La mitigación frente a MAGNALLIUM se centra en reforzar controles en la capa IT para evitar escaladas hacia OT:
    1. **autenticación robusta y monitorización** de intentos de password spraying,
    2. **formación frente a phishing** dirigido,
    3. **segmentación efectiva** IT/OT,
    4. y **registro de actividad anómala** asociada a **herramientas de administración remota y ejecución de scripts**.

3.1.6.2.3 PARISITE

La ficha de este grupo se elabora a partir de la info disponible en la web [27], pues no se muestra detalle en el informe anual antes mencionado.

- **Perfil y orientación.** PARISITE se introduce como un actor con actividad sostenida contra organizaciones industriales, con un enfoque principal en **operaciones de espionaje y recogida de información**. A diferencia de otros grupos con capacidad disruptiva, no se atribuyen a PARISITE capacidades demostradas de impacto directo sobre procesos industriales ni progresión a fases avanzadas de la ICS Cyber Kill Chain. Su comportamiento encaja en un actor orientado a la obtención de acceso y a la extracción de datos estratégicos.

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

- **Foco sectorial y geográfico.** Las campañas atribuidas a PARISITE se dirigieron principalmente contra **sectores industriales y de infraestructura crítica**, incluyendo **electricidad y petróleo y gas**, con actividad observada en **América del Norte, Europa y Oriente Medio**.
- **Actividad y campañas destacables.** PARISITE emplea campañas de intrusión que combinan técnicas de phishing dirigido y explotación de servicios expuestos para obtener acceso inicial. Una vez dentro, se centra en la **recogida de información técnica, credenciales y documentación interna**, sin evidencias de manipulación directa de sistemas de control.
- **TTPs y capacidades observadas.** Las técnicas documentadas incluyen:
    - **Phishing dirigido** con anexos o enlaces maliciosos.
    - Explotación de **servicios accesibles desde internet**.
    - Uso de **herramientas legítimas del sistema para movimiento lateral y** ejecución remota.
    - **Actividades de reconocimiento interno orientadas a inventariar activos** e identificar sistemas industriales.

  No se observan técnicas asociadas a la manipulación de PLCs, alteración de lógica de control ni acciones clasificables como Stage 2.
- **Implicaciones defensivas en OT/ICS.** La defensa frente a PARISITE requiere reforzar controles en la capa de acceso inicial:
    1. **protección** frente a **phishing,**
    2. **endurecimiento de servicios expuestos,**
    3. **monitorización** de movimiento lateral,
    4. **y visibilidad sobre** intentos de **recogida masiva de documentación técnica.**

  La segmentación efectiva entre redes IT y OT continúa siendo un mecanismo clave para impedir que intrusiones orientadas al espionaje evolucionen hacia impactos operativos.

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

3.1.6.2.4 VOLTZITE

- **Perfil y orientación.** Dragos califica VOLTZITE como uno de los grupos más relevantes a seguir en infraestructura crítica por su foco persistente en **datos OT** y por su trayectoria en intrusiones en red con componentes de inteligencia operativa. El informe indica también **solapamientos técnicos** con Volt Typhoon según la nomenclatura de otros equipos de inteligencia.
- **Foco sectorial y geográfico.** Las actividades descritas afectan a organizaciones vinculadas a infraestructura crítica y sectores con dependencia de información geoespacial y operaciones distribuidas; en el informe aparecen, entre otros, **electricidad**, **petróleo y gas**, **agua y saneamiento**, así como telecomunicaciones, elementos satelitales o de defensa, y otras **entidades gubernamentales**. Su foco principal es **Norteamérica, Europa, Asia, África y Nueva Zelanda.**
- **Actividad y campañas destacables.** El documento describe un conjunto de campañas en las que VOLTZITE comprometió **routers de pequeñas empresas** y empleó infraestructuras de terceros como puntos de **pivotaje**, con el objetivo de enumerar y alcanzar activos expuestos en infraestructura crítica. En campañas específicas, se destaca la interacción con **GIS** (sistemas de información geográfica) y **el robo/exfiltración** de datos GIS, así como la obtención de **diagramas de red OT** e instrucciones operativas.
- **TTPs y capacidades observadas.** El patrón resaltado combina:
    - **compromiso de dispositivos periféricos** para construir redes de *proxy/relay* por el adversario,
    - **uso de esas redes para scanning y enumeración** de superficie expuesta,
    - **y colección de información OT de alto valor** (GIS, topologías, instrucciones), que potencialmente permitiría diseñar herramientas específicas con capacidad disruptiva.
- **Implicaciones defensivas en OT/ICS.** La defensa frente a VOLTZITE requiere especial énfasis en:
    1. visibilidad sobre **pasarelas de acceso remoto**,
    2. detección de **exfiltración de GIS** y documentación sensible,

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

3. y control de la exposición a internet de dispositivos y servicios susceptibles de ser reutilizados como pivot (incluyendo dispositivos de red y accesos remotos en cadenas de suministro).

3.1.6.2.5 WASSONITE

La ficha de este grupo se elabora a partir de la información disponible en la web [28], pues no se muestra detalle en el informe anual antes mencionado.

- **Perfil y orientación.** WASSONITE se menciona como un grupo de amenaza con actividad dirigida a organizaciones industriales y de infraestructura crítica, con un enfoque predominante en **intrusión y recogida de información**. Según la característica publicada, no se le atribuye capacidad demostrada para ejecutar acciones disruptivas directas sobre procesos industriales (no consta progresión confirmada a Stage 2 en la ICS Cyber Kill Chain).
- **Foco sectorial y geográfico.** La actividad asociada a WASSONITE abarca organizaciones de **infraestructura crítica**, incluyendo sectores como **electricidad, nuclear y manufactura**, con víctimas identificadas en diferentes regiones, especialmente en India, Corea del Sur y Japón.
- **Actividad y campañas destacables.** Las operaciones atribuidas a WASSONITE se centran en compromisos de acceso inicial a través de vectores tradicionales (como phishing o explotación de servicios expuestos) y posterior actividad de reconocimiento interno. El objetivo principal observado es la **obtención de información técnica y credenciales**, así como la cartografía de redes con componentes industriales.
- **TTPs y capacidades observadas.** Entre los patrones descritos por Dragos se incluyen:
    - Uso de **phishing dirigido** para capturar credenciales.
    - Explotación de **servicios accesibles desde internet**.
    - Empleo de herramientas legítimas del sistema para mantener persistencia y realizar movimiento lateral.
    - Actividad de **reconocimiento interno** orientada a la identificación de activos OT y documentación asociada.

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

No se documentan interacciones directas con PLC ni manipulación de lógica de control.

- **Implicaciones defensivas en OT/ICS.** La mitigación frente a WASSONITE se focaliza en:

    1. **reforzar controles de acceso** inicial (protección frente a phishing y endurecimiento de servicios expuestos),
    2. incrementar la **visibilidad sobre movimiento lateral** en redes corporativas,
    3. y **mantener una segmentación efectiva IT/OT** que limite la progresión hacia sistemas de control.

3.1.6.2.6 GRAPHITE

- **Perfil y orientación.** GRAPHITE es uno de los dos grupos **introducidos como novedad** en 2024. El informe se vincula con campañas de interés geopolítico relacionadas con la situación militar en Ucrania y señala **solapamientos técnicos** con el clúster conocido como APT28 en otras nomenclaturas. Su relevancia para OT/ICS deriva de su foco en entidades industriales y energéticas, aunque Dragos indica que **no mostró capacidad Stage 2**.
- **Foco sectorial y geográfico.** Las víctimas confirmadas y objetivos se sitúan en **Europa Oriental**, **Oriente Medio** y también en **Asia**, con afectación de sectores como **electricidad**, **petróleo y gas**, **logística ferroviaria y de mercancías**, **logística aeronáutica** y **base industrial de defensa**, así como entidades gubernamentales.
- **Actividad y campañas destacables.** El informe documenta campañas de *spear-phishing* prolongadas (desde 2022 y especialmente a lo largo de 2023-2024) dirigidas, entre otros, a operadores de **oleoductos/gasoductos** y a instalaciones de **generación hidroeléctrica**, con un objetivo recurrente de **robo de credenciales**. En una fase inicial, GRAPHITE explotó una vulnerabilidad en **Microsoft Outlook** que permitía capturar datos de autenticación de Windows, y en paralelo mantuvo operaciones de phishing con malware basado en *scripts*.

    En otras campañas descritas, el grupo utilizó sitios web maliciosos y herramientas específicas para **phishing de credenciales**, incluyendo portales

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

que imitaban servicios populares, y también combinó diferentes piezas de malware (p.ej., backdoors basados en *batch* y C#) para mantener ejecución remota y persistencia.

- **TTPs y capacidades observadas.** Dragos subraya el uso de una red de **routers Ubiquiti Edge** comprometidos para distribuir malware y mantener canales de **C2**, infraestructura que permaneció activa hasta su interrupción en febrero de 2024 por los americanos. A partir de 2024, observa un desplazamiento hacia el uso de **servicios legítimos de internet** para preparación de ataques (staging) y comunicaciones.
- **Implicaciones defensivas en OT/ICS.** Dado que el vector dominante es la intrusión en *Stage 1*, la prioridad defensiva se centra en:
    1. endurecer y detectar **phishing dirigido**,
    2. **elevar la higiene de identidad** (incluyendo monitorización de robos de credenciales y abuso de sesiones),
    3. y **reducir la exposición y confianza implícita en infraestructura de red de terceros** que pueda ser reutilizada para distribución de *payloads* y C2.

3.1.6.2.7 BAUXITE

- **Perfil y orientación.** BAUXITE es el segundo grupo **novedoso en 2024** y se dispone como un actor con campañas centradas en OT/ICS y en dispositivos específicos. El informe señala una **alineación técnica sustancial** con el ente hacktivista pro-iraní **CyberAv3ngers**. Recoge que este último fue vinculado explícitamente con el **gobierno iraní,** cuyos miembros han sido sancionados, según el reporte de la Administración de los Estados Unidos. BAUXITE aparece, además, como un actor que **investiga activamente: participa en foros orientados a OT/ICS y muestra interés por hardware OEM y avisos de seguridad.**
- **Foco sectorial y geográfico.** Se sitúan víctimas confirmadas en **Estados Unidos**, **Europa**, **Australia y Asia Occidental**, e identifica afectación en múltiples sectores: **electricidad**, **petróleo y gas**, **agua y saneamiento**, **químico**, **alimentación y bebidas** y **manufactura**.

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

- **Actividad y campañas destacables.** Desde finales de 2023, Dragos observa **cuatro campañas** asociadas a BAUXITE, incluyendo operaciones con **impacto Stage 2** en la ICS Cyber Kill Chain mediante compromisos triviales de dispositivos expuestos. El documento destaca una pauta consistente de aprovechar **superficie expuesta** y condiciones de autenticación débiles, con acciones orientadas a interrumpir o degradar entornos industriales.
- **TTPs y capacidades observadas.** El informe refleja un comportamiento de reconocimiento y explotación apoyado en:
    - **seguimiento intensivo de avisos de seguridad y vulnerabilidades** conocidas en entornos industriales (más detalle en otros informes del Observatorio [29]),
    - **interés por protocolos y ecosistemas OT/ICS**,
    - y **capacidad para ejecutar acciones disruptivas** cuando existen accesos triviales (p.ej., servicios expuestos y credenciales débiles).
- **Implicaciones defensivas en OT/ICS.** La propuesta prioriza controles directamente ligados a la exposición:
    1. identificar activos con **SSH** accesible desde internet y **ocultar el acceso tras VPN**,
    2. verificar que cuando existan accesos SSH, no se empleen **contraseñas por defecto** o fácilmente adivinables,
    3. y **auditar claves SSH** (eliminar las innecesarias y rotar las existentes cuando hubo exposición).

    Esta línea de mitigación es coherente con la naturaleza oportunista de parte de las campañas descritas.

3.1.6.2.8 CHERNOVITE

La ficha de este grupo se elabora a partir de la info disponible en la web [30], pues no se muestra detalle en el informe anual antes mencionado. CHERNOVITE se incluye en el conjunto de grupos destacados por Dragos y aparece asociado a la **capacidad Stage 2 en** la **ICS Cyber Kill Chain** según la clasificación empleada.

- **Perfil y orientación.** CHERNOVITE es un grupo de amenaza identificado por Dragos con capacidad para desarrollar **malware específico para sistemas de**

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

control industrial (ICS), orientado a la **disrupción, degradación y potencial destrucción de entornos industriales y procesos físicos**. El grupo está asociado al desarrollo de **PIPEDREAM**, un marco modular de malware diseñado específicamente para atacar a sistemas ICS. El sexto malware ICS conocido tras STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE y TRISIS.

- **Foco sectorial y geográfico.** Según Dragos, CHERNOVITE dirige su actividad contra sectores críticos como **electricidad y gas natural licuado (LNG)**, así como otros entornos industriales que emplean PLC y tecnologías industriales ampliamente implantadas. La naturaleza transversal de PIPEDREAM permite adaptar sus capacidades a múltiples arquitecturas industriales.
- **Actividad y campañas destacables.** El elemento distintivo atribuible a CHERNOVITE es como se indicó anteriormente, el desarrollo de la herramienta **PIPEDREAM**, considerada como una de las primeras plataformas de malware ICS específicamente diseñadas para manipular dispositivos de control industrial más allá de herramientas IT tradicionales. Observaron este marco malicioso en laboratorio y evaluaron sus capacidades, pero no está confirmado su uso en operaciones reales en el momento de la publicación, por lo que podría ser diseñado por algún Estado Nación para posicionarse de cara a movimientos futuros.
- **TTPs y capacidades observadas.** Las capacidades descritas incluyen:
    - Desarrollo de una plataforma de malware modular capaz de interactuar con protocolos industriales como **OPCUA**, **Modbus y** entornos **basados en CoDeSys**.
    - Capacidad de **escanear e interactuar con dispositivos PLC**, incluyendo captura de credenciales, intentos de fuerza bruta y potencial denegación de servicio.
    - **Herramientas para intrusión e interacción con sistemas Windows y software de ingeniería industrial** como parte de la cadena de ataque.

  Estas capacidades permitirían manipular o afectar PLCs y sistemas de control, situando a CHERNOVITE dentro del conjunto de actores con **potencial de progresión hacia Stage 2 en la ICS Cyber Kill Chain.**

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

- **Implicaciones defensivas en OT/ICS.** La existencia de un **grupo con capacidades de desarrollo de malware ICS como CHERNOVITE** refuerza la necesidad de:
    1. **telemetría y detección de comportamiento anómalo** en protocolos industriales,
    2. **inventario exhaustivo y visibilidad** sobre PLC y dispositivos de control,
    3. **segmentación estricta IT/OT y limitación de accesos** remotos,
    4. **y monitorización de actividad inusual en herramientas de ingeniería y software** asociado a control industrial.

3.1.6.2.9 ELECTRUM

- **Perfil y orientación.** ELECTRUM es uno de los grupos más veteranos descritos, **responsable de múltiples ataques contra ICS y vinculado a un historial de operaciones disruptivas**. El informe destaca su relación técnica con Sandworm en otras nomenclaturas y subraya que, aunque en 2024 tuvo menor volumen de actividad que KAMACITE, mantuvo una capacidad destructiva subrayable y recurrió a **personas hackivistas** para ocultar operaciones.
- **Foco sectorial y geográfico.** Su foco principal se encuadra en **Ucrania**, aunque también se observa interés por **empresas energéticas en Alemania**. El sector **eléctrico** es central en su perfil de riesgo.
- **Actividad y campañas destacables.** El informe describe un ciberataque contra el operador de telecomunicaciones **Kyivstar** (diciembre de 2023) que provocó interrupciones de servicio a escala nacional. Dos personas hacktivistas pro-rusas reivindicaron la autoría con mensajes prácticamente idénticos; el análisis de Dragos atribuye la operación a ELECTRUM e interpreta esa reivindicación como un mecanismo de **ofuscación** apoyado en la reputación y recursos de una de esas personas.
- **TTPs y capacidades observadas.** La principal novedad técnica destacada es **AcidPour**, un wiper para sistemas Linux capaz de buscar y borrar directorios **UBI** en dispositivos embebidos, incluidos dispositivos presentes en entornos OT. Se contextualiza como una extensión de **AcidRain** (wiper empleado en 2022), destacando diferencias de arquitectura objetivo y su aptitud para causar

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

disrupción operativa. **El informe también enfatiza que ELECTRUM ha demostrado capacidad para alcanzar Stage 2 (ejecución de ataque ICS) dentro de la Kill Chain.**

- **Implicaciones defensivas en OT/ICS.** Las recomendaciones asociadas se centran en:

    1. reducir y monitorizar la capacidad de ejecutar binarios en entornos de control: **limitar instalación de nuevos servicios, impedir cambios no autorizados,**
    2. **aplicar listas blancas de aplicaciones** cuando sea viable,
    3. **monitorizar transferencias de ficheros** hacia la red ICS
    4. **y, sobre todo, garantizar copias de seguridad robustas y probadas** (lógica de proyecto, configuraciones de IED e instaladores de aplicaciones ICS) almacenadas fuera de línea para acelerar la recuperación.

3.1.6.2.10 Cuadro resumen

Tras abordar el detalle individual de cada grupo, se presenta a continuación un **cuadro resumen comparativo** que sintetiza las características más destacables de los actores identificados por el fabricante desde una perspectiva contextualizada para la industria gallega. El objetivo de esta matriz no es reiterar la descripción técnica ya expuesta en las fichas, sino ofrecer una **lectura priorizada en términos de capacidad OT real, exposición sectorial en Galicia y nivel de riesgo estimado**, facilitando así una interpretación ejecutiva y orientada a la toma de decisiones.

La clasificación propuesta integra tres dimensiones fundamentales:

(i) la capacidad demostrada o potencial de progresión en la ICS Cyber Kill Chain, especialmente en relación con el Stage 2,

(ii) la coincidencia entre los sectores objetivo descritos por Dragos y los sectores industriales presentes en Galicia, y

(iii) la naturaleza del impacto observable (espionaje, preparación de capacidades o disrupción directa). De esta forma, la matriz permite distinguir entre actores con riesgo estratégico a medio plazo y aquellos con un impacto más limitado o circunscrito a la capa IT.

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

Grupo	Capacidad OT	Exposición sectorial Galicia	Nivel de riesgo
KAMACITE	Broker IT (facilitador de pivotaje)	Transversal (energía, industria)	Medio
MAGNALLIUM	IT (sin capacidad OT demostrada)	Limitado	Bajo
PARISITE	Espionaje IT	Limitado	Bajo
VOLTZITE	Espionaje OT y preparación de capacidades	Infraestructuras críticas (energía, agua, telecom.)	Medio
WASSONITE	IT con foco en infraestructura crítica	Limitado	Bajo
GRAPHITE	IT avanzado con foco energético	Energía	Medio
BAUXITE	Stage 2 oportunista	Agua, alimentación, manufactura	Medio-Alto
CHERNOVITE	Malware ICS avanzado (potencial Stage 2)	Energía	Estratégico
ELECTRUM	Alta (Stage 2 demostrado)	Energía eléctrica	Alto

Resumen de características principales de los actores de amenaza en ICS/OT identificados. Fuente: Dragos (2025)

3.2 Inteligencia propia

Los servicios de inteligencia de amenazas permiten anticipar, detectar y responder eficazmente a ciberataques. En esta sección se presentan algunos elementos que permiten construir una base de inteligencia operativa utilizando soluciones abiertas y colaborativas, especialmente orientadas a entornos ICS/OT.

La combinación de fuentes públicas como ThreatFox, plataformas como MISP y OpenCTI, **y mecanismos de captura directa** de inteligencia como honeypots, **permite estructurar un ecosistema propio de vigilancia y análisis que alimenta la defensa industrial de manera bidireccional** (i.e. desde la comunidad de inteligencia a la organización y en sentido opuesto).

A continuación, iremos introduciendo conceptos y servicios asociados a esta capacidad.

Indicadores de compromiso (IoCs)

Los IoCs son evidencias técnicas que indican que un sistema, red o dispositivo puede ser comprometido por una amenaza informática. En esencia, **un IoC es cualquier dato que revela actividad maliciosa**, como direcciones IP sospechosas, dominios maliciosos,

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

URLs, hashes de archivos o patrones anómalos de red. En entornos industriales (ICS/OT), los IoCs pueden incluir hashes de malware dirigido a PLCs, dominios de C2 asociados a ataques a sistemas SCADA o anomalías en protocolos industriales.

ThreatFox

ThreatFox [12] es un proyecto de abuse.ch dedicado a **recopilar y compartir IoCs asociados a malware**. Funciona como una plataforma donde investigadores y analistas publican indicadores como hashes, direcciones IP o dominios, consultables vía web o APIs. Su utilidad radica en que permite a las organizaciones reforzar sus sistemas defensivos y detectar actividades maliciosas en fases tempranas. ThreatFox puede integrarse con otras plataformas de inteligencia, como MISP y OpenCTI, que veremos a continuación.

MISP

MISP (Malware Information Sharing Platform) [13] **es una plataforma de código abierto para el intercambio estructurado de información de amenazas**. Permite almacenar, correlacionar y distribuir indicadores de compromiso, enriquecidos con contexto adicional. A través de MISP, los analistas pueden automatizar el envío de datos hacia otras herramientas (como un SIEM o IDS), gestionar eventos de seguridad y visualizar relaciones entre incidentes.

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

Captura de pantalla de MISP. Fuente: misp-project.org (2025)

Un recurso útil para familiarizarse con la plataforma, es la sesión formativa publicada en You Tube por el equipo de CIRCL (Computer Incident Response Center Luxembourg), pues son quienes desarrollaron y mantienen la solución [14].

MISP fomenta la colaboración mediante **comunidades sectoriales** [15], donde los miembros comparten inteligencia de forma privada. En el ámbito industrial, destaca la comunidad **ICS-CSIRT.io**, un nodo dedicado a inteligencia de entornos ICS, al que se recomienda adherirse.

Estas comunidades permiten recibir y aportar conocimiento útil en tiempo real, fortaleciendo así la defensa colectiva.

MISP Galaxy

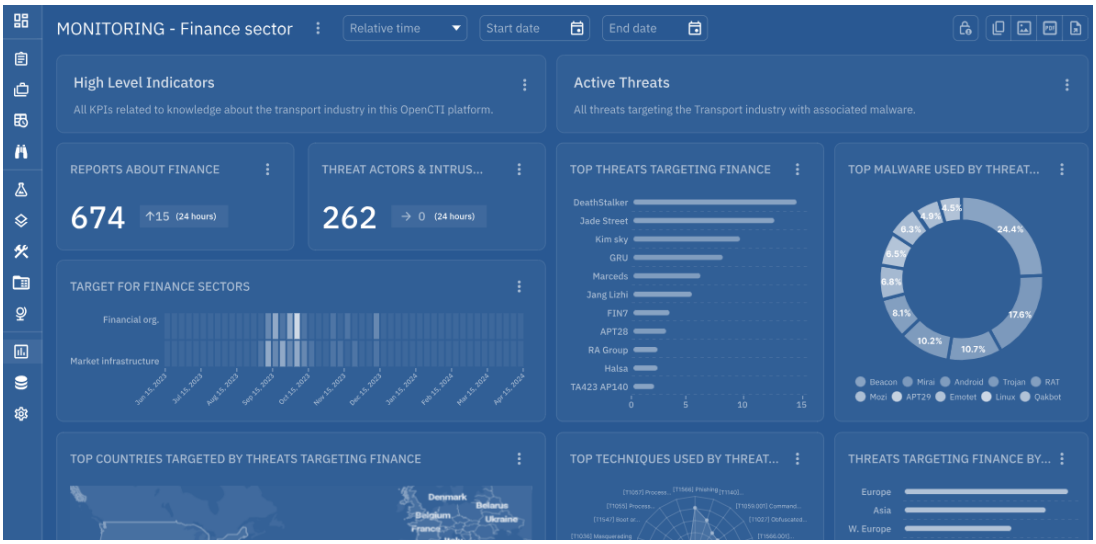
MISP Galaxy [16] es un componente adicional de MISP que facilita el **etiquetado semántico de los eventos** mediante taxonomías predefinidas. Permite, por ejemplo, asociar un IoC a un actor de amenaza conocido, a un malware específico o a una técnica MITRE ATT&CK. Esta estructura facilita la agregación de conocimiento y la identificación de patrones.

OpenCTI

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

OpenCTI [17] es una plataforma de código abierto diseñada para **gestionar, analizar y visualizar conocimiento estructurado sobre amenazas**. A diferencia de MISP, que se centra en eventos técnicos e IoCs, OpenCTI permite representar relaciones entre actores, campañas, técnicas, malware y vulnerabilidades en un grafo de conocimiento basado en el estándar STIX2.

Existen versiones comunitaria y comercial (esta última bajo la denominación comercial de filigran.io). En ambas se habilita la integración con otras fuerzas y plataformas (incluidas MISP, TheHive o MITRE ATT&CK), lo que permite crear un núcleo de inteligencia contextual en tiempo real.



Captura de pantalla de OpenCTI. Fuente: filigran.io (2025)

Conviene aclarar que OpenCTI y MISP son altamente complementarios dentro de un sistema de inteligencia de amenazas.

- **MISP** se centra en la **gestión técnica de eventos e indicadores de compromiso (IoCs)**, facilitando su almacenamiento, compartición y correlación estructurada. Es ideal para automatizar la defensa basada en señales técnicas concretas.
- Por su parte, **OpenCTI** va un paso más allá al permitir **modelar y visualizar el conocimiento contextual**: relaciones entre actores, campañas, malware, técnicas y vulnerabilidades, siguiendo el estándar STIX2.

Mientras que MISP es más operativo y centrado en la detección, **OpenCTI aporta profundidad analítica y estratégica**. Ambas plataformas pueden integrarse,

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

beneficiándose mutuamente: MISP alimenta OpenCTI con datos técnicos, y OpenCTI enriquece esos datos con contexto.

Integración con captura directa de inteligencia: honeypots

Las plataformas anteriores se nutren de fuentes externas, pero también pueden integrarse con **inteligencia propia capturada en campo**. Una forma efectiva de generar esta inteligencia es mediante honeypots: sistemas trampa que simulan infraestructuras reales para atraer y estudiar ataques [18].

En entornos industriales, **Conpot** [19] es uno de tantos posibles honeypots "out of the box" (empleables sin modificaciones). Simula dispositivos industriales como PLCs y protocolos como Modbus, s7comm o HTTP. Permite registrar patrones de acceso, intentos de explotación y comandos maliciosos dirigidos a infraestructuras críticas.

Mencionar que se prevé que futuras ediciones de este informe puedan apoyarse en **tres honeypots desplegados en la infraestructura de AMTEGA**, accesibles desde Internet y simulando ser equipos bajo diferentes protocolos de comunicación presentes en entornos industriales, con el objetivo de **capturar indicadores en tiempo real**, analizar patrones de ataque y enriquecer el conocimiento de los informes con estadísticas propias de actividad dirigida contra sistemas ICS reales.

IoCs, ataques y TTPs: de la detección a la atribución

La detección de un IoC aporta la señal; los TTPs (Tácticas, Técnicas y Procedimientos) explican el comportamiento del atacante. La **matriz MITRE ATT&CK for ICS** [5] categoriza las técnicas ofensivas utilizadas específicamente contra sistemas industriales. Dragos, por su parte, extendió esta lógica con su propia matriz [11], donde cruza los IoCs observados con los TTPs documentados y los grupos criminales que identificaron con sus fuentes de inteligencia, facilitando así la atribución de ataques y la priorización de defensas.

Como se mostró, es posible **establecer un sistema eficaz de inteligencia de amenazas con herramientas abiertas y colaborativas**. La combinación de plataformas como ThreatFox, MISP y OpenCTI, junto con mecanismos de captura directa como honeypots, permite construir un ecosistema operativo que no sólo consume, sino que también genera y distribuye inteligencia, y puede formar parte perfectamente del SOC de la organización.

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

La clave está en entender que **la inteligencia es un proceso vivo**, que se retroalimenta de fuentes internas y externas. Participar en comunidades MISP, mantener activos honeypots y enriquecer los eventos con contexto TTP/MITRE son acciones que no sólo elevan el nivel de protección, sino que contribuyen a mejorar la seguridad de todo el ecosistema industrial gallego y global.

4 Recomendaciones

Tras el análisis de los múltiples informes de referencia y estudios sectoriales de la bibliografía, se puede concluir que las recomendaciones técnicas y estratégicas emitidas por los diferentes fabricantes y organismos coinciden, en gran medida, en su enfoque hacia una ciberdefensa más proactiva, adaptativa y resiliente. Aunque muchas de estas orientaciones provienen de proveedores de soluciones de seguridad y ello introduce

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

cierto sesgo de autopromoción, es posible extraer principios universales que trascienden las herramientas concretas y se centran en **prácticas, procesos y prioridades de seguridad**.

Este apartado recopila y sintetiza esas indicaciones, con el objetivo de presentar **recomendaciones aplicables y accionables**, especialmente en entornos con componentes OT/ICS. Comenzaremos con las recomendaciones de los informes de fabricantes de manera agregada, pondremos especial énfasis en las propuestas de entidades neutrales y de prestigio como **ENISA** y **CISA**, y las complementaremos con recursos técnicos seleccionados por su utilidad práctica, con independencia de la solución tecnológica implementada.

A continuación, por tanto, se presentan las principales líneas de actuación recomendadas.

4.1.1 Fabricantes de soluciones de ciberseguridad

Los informes de fabricantes analizados a lo largo de este estudio, ofrecen un amplio abanico de recomendaciones para mejorar la postura defensiva de las organizaciones. A pesar de la heterogeneidad de los enfoques, se pueden extraer **líneas estratégicas comunes**.

1. **Refuerzo de la identidad y el acceso**

Una constante en todos los informes es la **importancia crítica de proteger las identidades**. Se insiste en aplicar autenticación multifactor robusta y resistente al phishing (como llaves físicas), eliminar cuentas con privilegios innecesarios, consolidar plataformas de gestión de identidad, y reducir la proliferación de credenciales. IBM sugiere avanzar hacia un "tejido de identidad" unificado que integre todos los dominios y sistemas. Microsoft y CrowdStrike, por su parte, recalcan que la identidad sigue siendo el vector de ataque principal, por lo que debe priorizarse su defensa. Este principio cobra aún más importancia en entornos industriales, donde accesos privilegiados a interfaces de programación de autómatas o consolas de ingeniería deben estar debidamente controlados

2. **Visibilidad unificada y respuesta avanzada**

La detección efectiva depende de una **visión unificada del entorno de IT y OT**. Palo Alto destaca que muchas intrusiones podrían haberse detectado si los sistemas estuvieran bien integrados y las evidencias centralizadas. Se recomienda integrar

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

telemetrías de endpoints, red, nube, identidad y aplicaciones en una vista común, y complementar con analítica avanzada y detección basada en IA para reducir el tiempo medio de detección (MTTD) y respuesta (MTTR). En redes industriales, cruzar la telemetría generada por sensores, controladores lógicos programables (PLC) y sistemas SCADA con datos del entorno IT permite detectar comportamientos anómalos e intrusiones híbridas.

3. **Automatización y ciberinteligencia**

Para contrarrestar la rapidez con la que operan los atacantes, **la automatización de la respuesta es esencial**. CrowdStrike y Palo Alto coinciden en recomendar la integración de capacidades de automatización en el SOC, así como el uso de inteligencia de amenazas en tiempo real. Microsoft añade que esta inteligencia debe fluir hacia los procesos del equipo de seguridad para anticipar técnicas emergentes. IBM subraya la importancia del uso proactivo de la inteligencia mediante intercambio con terceros y comunidades. En entornos ICS, el uso de plataformas *de Threat intelligence* especializadas puede facilitar la respuesta anticipada ante *malware* dirigido a protocolos industriales.

4. **Reducción de complejidad y confianza implícita**

Uno de los principales enemigos de una defensa eficaz es la **complejidad tecnológica y organizativa**. Palo Alto indica que el uso de múltiples herramientas no integradas impide detectar señales clave. Se recomienda consolidar tecnologías, eliminar silos y aplicar los principios de Zero Trust para reducir la confianza implícita. Esto incluye segmentar redes, verificar continuamente usuarios y dispositivos, y aplicar el principio de mínimo privilegio. En entornos OT, esta segmentación lógica es fundamental para aislar zonas críticas de producción de las redes corporativas o de mantenimiento remoto.

5. **Protección de entornos cloud y de desarrollo**

Los entornos cloud siguen siendo un objetivo prioritario. Microsoft, Palo Alto y CrowdStrike destacan la necesidad de **integrar desde el desarrollo ("shift-left") hasta la ejecución**. Esto implica auditar la infraestructura cloud, proteger APIs, controlar accesos, aplicar detección y respuesta en tiempo real, y automatizar la contención de incidentes. También se propone reforzar la seguridad en la cadena de suministro

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

software. Esta recomendación es extensible a sistemas OT modernos que incorporan servicios en la nube para telemetría, actualizaciones o gestión de dispositivos remotos.

6. **Gestión de vulnerabilidades con enfoque basado en riesgo**

Los atacantes priorizan vulnerabilidades conocidas y accesibles publicamente. CrowdStrike aconseja adoptar un enfoque de **gestión de vulnerabilidades centrado en el adversario**, combinando inteligencia externa, escaneo continuo, priorización basada en criticidad y superficie expuesta. Se sugiere también integrar señales sobre explotación activa y encadenamiento de fallos para actuar de forma proactiva. En ICS, donde muchos sistemas son sensibles a actualizaciones, este enfoque debe combinarse con medidas compensatorias como la detección basada en firmas específicas o el aislamiento de activos vulnerables. Y recordemos el enfoque Now-Next-Never propuesto por Dragos.

7. **Concienciación y preparación organizativa**

Todos los informes coinciden en que el **factor humano sigue siendo un eslabón débil**. Se recomienda invertir en formación periódica, ejercicios de simulación, red teams y cultura de seguridad transversal. Microsoft recordó que la ciberseguridad debe ser un tema tratado al más alto nivel de Dirección. Estar preparado para incidentes incluye contar con planes actualizados, ensayar su ejecución y conocer las debilidades propias antes de que lo hagan los adversarios. En fábricas y entornos OT, donde el tiempo de reacción puede determinar el impacto físico de un ataque, la coordinación entre ciberseguridad, producción y mantenimiento es vital.

8. **Consideraciones emergentes: IA y post-cuantum**

IBM y Microsoft alertan sobre los **riesgos emergentes de la IA y la computación cuántica**. Se recomienda establecer gobernanza sobre los sistemas de IA, proteger sus modelos y datos, auditar su funcionamiento y anticipar escenarios de uso indebido. También se insta a comenzar a planificar la transición a criptografía post-cuántica mediante inventario de algoritmos y sistemas afectados. Para entornos industriales críticos, donde los sistemas pueden tener ciclos de vida muy largos, anticipar esta transición es crucial para evitar futuros riesgos de confidencialidad o integridad.

Estas recomendaciones, aunque diversas en matices, convergen en la necesidad de adoptar un enfoque proactivo, integrado y basado en inteligencia para **anticiparse a las amenazas y resistir sus impactos**.

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

4.1.2 ENISA

ENISA, la Agencia de la Unión Europea para la Ciberseguridad, presenta un conjunto de recomendaciones concisas de índole general. Éstas se dirigen principalmente a los responsables de formular políticas, reguladores y operadores de servicios esenciales, especialmente en sectores incluidos en la Directiva NIS2.

- En primer lugar, aboga por **reducir la superficie de exposición** a amenazas de ciberseguridad, tanto conocidas como emergentes, con una atención especial al papel de la inteligencia artificial. Subraya la necesidad de abordar los desafíos legales, técnicos y operativos que expone la IA, recomendando medidas como la integración de evaluaciones de impacto de seguridad en sistemas que la emplean.
- En segundo lugar, insiste en la importancia de la **resiliencia operativa frente a interrupciones prolongadas**, como las observadas en campañas de ransomware recientes. Esto implica mejorar las capacidades de respuesta, contener los ataques y mantener la continuidad de negocio ante amenazas disruptivas.
- También destaca el refuerzo del **marco de ciberseguridad para sectores críticos**. Ello pasa por aumentar la adopción de controles de seguridad avanzados, reforzar las capacidades técnicas de supervisión, y promover el intercambio de información entre los operadores. En línea con esto, se recomienda a los CERTs nacionales reforzar su visibilidad técnica y apoyar a las organizaciones menos maduras.
- Se señala la necesidad de **adaptar los planes de gestión de crisis** a amenazas complejas como la combinación de campañas de desinformación con ciberataques. Se propone desarrollar manuales y simulacros de crisis que contemplen estos escenarios híbridos, especialmente en momentos críticos como elecciones o conflictos geopolíticos.
- Por último, ENISA sugiere consolidar mecanismos que faciliten una **coordinación efectiva entre los Estados miembros de la UE**, tanto a nivel operativo como político. Esto permitiría una respuesta más ágil y cohesionada ante incidentes de ciberseguridad de gran escala que afecten a varios países al mismo tiempo.

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

Además, en su informe "*Threat Landscape 2025*", sintetiza sus **recomendaciones de defensa en base a los TTPs observados, agrupándolos en cinco cimientos fundamentales** que consolidan buenas prácticas de higiene de ciberseguridad. Estas recomendaciones tienen como objetivo prevenir el compromiso inicial, contener el impacto y dificultar el acceso persistente a largo plazo.

Nótese que las referencias a códigos M que se indican a continuación, corresponden al MITRE D3FEND Framework [20] y al MITRE ATT&CK para controles defensivos.

1. **Endurecimiento del sistema (System Hardening)**

   Fortalecer la configuración del entorno operativa es esencial para reducir la superficie de ataque. ENISA propone medidas como:

   - Prevención de ejecución (M1038) y control de comportamiento en endpoints (M1040).
   - Configuración segura de sistemas operativos (M1028), software (M1054) y Active Directory (M1015).
   - Restricción de permisos en el registro (M1024), archivos y directorios (M1022), y carga de librerías (M1044).
   - Mecanismos de convalidación como firma de código (M1045) y deshabilitado de funciones innecesarias (M1042).

2. **Control de acceso y privilegios (Access & Privilege)**

   Las buenas prácticas en la gestión de identidades ayudan a prevenir abusos:

   - Gestión de cuentas de usuario (M1018), cuentas privilegiadas (M1026) y control de cuentas (M1052).
   - Limitación de instalación de software (M1033).
   - Políticas de contraseñas robustas (M1027), autenticación multifactor (M1032) y uso controlado de cuentas (M1035).

3. **Protecciones de red (Network Protections)**

   Estas medidas buscan evitar la comunicación maliciosa y los movimientos laterales:

   - Prevención de intrusión en red (M1031) y filtrado de tráfico (M1037).
   - Segmentación de red (M1030) y restricción de contenido web (M1021).

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

- Limitación del acceso a recursos a través de red (M1048).

4. Monitorización (Monitoring)

La supervisión efectiva permite detectar amenazas de forma temprana:

- Auditoría de sistemas y actividades (M1047).
- Buenas prácticas en el desarrollo seguro (M1013).

Políticas de uso de cuentas y control de acceso en red complementan la detección de análisis de comportamiento.

5. Resiliencia (Resilience)

Dado que algunos ataques tendrán éxito, la capacidad de recuperación es clave:

- Copias de seguridad (M1053) y almacenamiento remoto de datos (M1029).
- Prevención de pérdida de datos (M1057) y cifrado de información sensible (M1041).
- Actualización de software (M1051) y uso de antivirus/antimalware (M1049)
- Formación de usuarios para identificar ataques de ingeniería social (M1017).

Estas medidas forman una estrategia integral que puede adaptarse tanto a entornos corporativas tradicionales como a contextos OT/ICS.

4.1.3 CISA

La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) es el organismo federal de EE. UU. encargado de coordinar la protección de infraestructuras críticas frente a amenazas físicas y digitales. A través de su iniciativa de Seguridad en Sistemas de Control Industrial (ICS), **CISA proporciona orientación técnica, alertas y recomendaciones específicas para operadores de infraestructuras OT**, basadas en años de experiencia y colaboración con los sectores público y privado.

Uno de sus recursos más interesantes es el repositorio **de ICS Recommended Practices** [21], donde se agrupan **buenas prácticas diseñadas para aumentar la resiliencia de entornos industriales.** Esta colección está compuesta por documentos relativamente breves y accionables, que pueden servir como base para fortalecer la seguridad desde distintos enfoques:

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

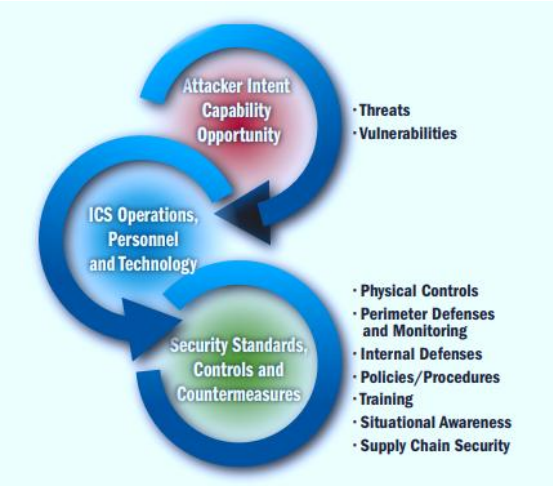
- **Updating Antivirus in an Industrial Control System**: buenas prácticas para actualizar motores y firmas antivirus en entornos ICS sin comprometer la disponibilidad de los sistemas.
- **Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies**: guía para aplicar una estrategia multicapa que combine medidas físicas, técnicas y organizativas para proteger infraestructuras industriales.
- **Creating Cyber Forensics Plans for Control Systems**: orientaciones para definir planes de forense adaptados a ICS, preservando evidencias ante incidentes sin interrumpir procesos críticos.
- **Developing an Industrial Control Systems Cybersecurity Incident Response Capability**: pasos para establecer una capacidad efectiva de respuesta ante incidentes de ciberseguridad en sistemas de control.
- **Case Study: Cross-Site Scripting**: análisis práctico de un incidente real de XSS en un entorno industrial, con lecciones aprendidas y medidas de mitigación.
- **Patch Management of Control Systems**: pautas para la planificación, evaluación, convalidación e implementación segura de parches en entornos de control.
- **Securing Control System Modems**: recomendaciones específicas para proteger los módems conectados a sistemas ICS, que suelen representar vectores de entrada críticos.
- **Configuring and Managing Remote Access for Industrial Control Systems**: estrategias para habilitar el acceso remoto seguro a sistemas de control sin comprometer la integridad de los activos.
- **Cyber Security Procurement Language for Control Systems**: ejemplos de cláusulas y requerimientos de ciberseguridad que pueden incluirse en contratos de adquisición de tecnología industrial.
- **Mitigations for Security Vulnerabilities Found in Control System Networks**: estrategias generales para las mitigaciones sin afectar a la continuidad operativa.

4.1.3.1 Estrategias de Defensa en Profundidad

Dado su carácter transversal y aplicabilidad general, analizaremos con mayor profundidad el documento sobre **Estrategias de Defensa en Profundidad para mejorar la ciberseguridad de sistemas ICS** [22], por constituir una referencia fundamental tanto para organizaciones que inician su camino en la protección de

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

sistemas de control como para aquellas que buscan consolidar un marco de defensa multicapa sólido.



Planificación de Defensa en Profundidad. Fuente: CISA (2016)

A continuación, describiremos los elementos principales de la propuesta: las estrategias de defensa en profundidad, y las recomendaciones finales.

Estrategias Defense-in-Depth

- **Estrategia 1. Gestión de riesgos en ICS:** integrar la gestión de riesgo específica de los sistemas de control industrial en todos los niveles de la organización. Esto implica entender los riesgos de negocio asociados al entorno ICS y alinearlos con la tolerancia de riesgo empresarial. Conocer las amenazas, procesos operativos y requerimientos únicos permite implantar un enfoque multinivel de monitorización y defensa continua en las operaciones diarias. Como ilustra la figura siguiente, las organizaciones deben aplicar controles al nivel de seguridad adecuado y después **monitorizar y ajustar** esos controles continuamente contra amenazas emergentes.

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

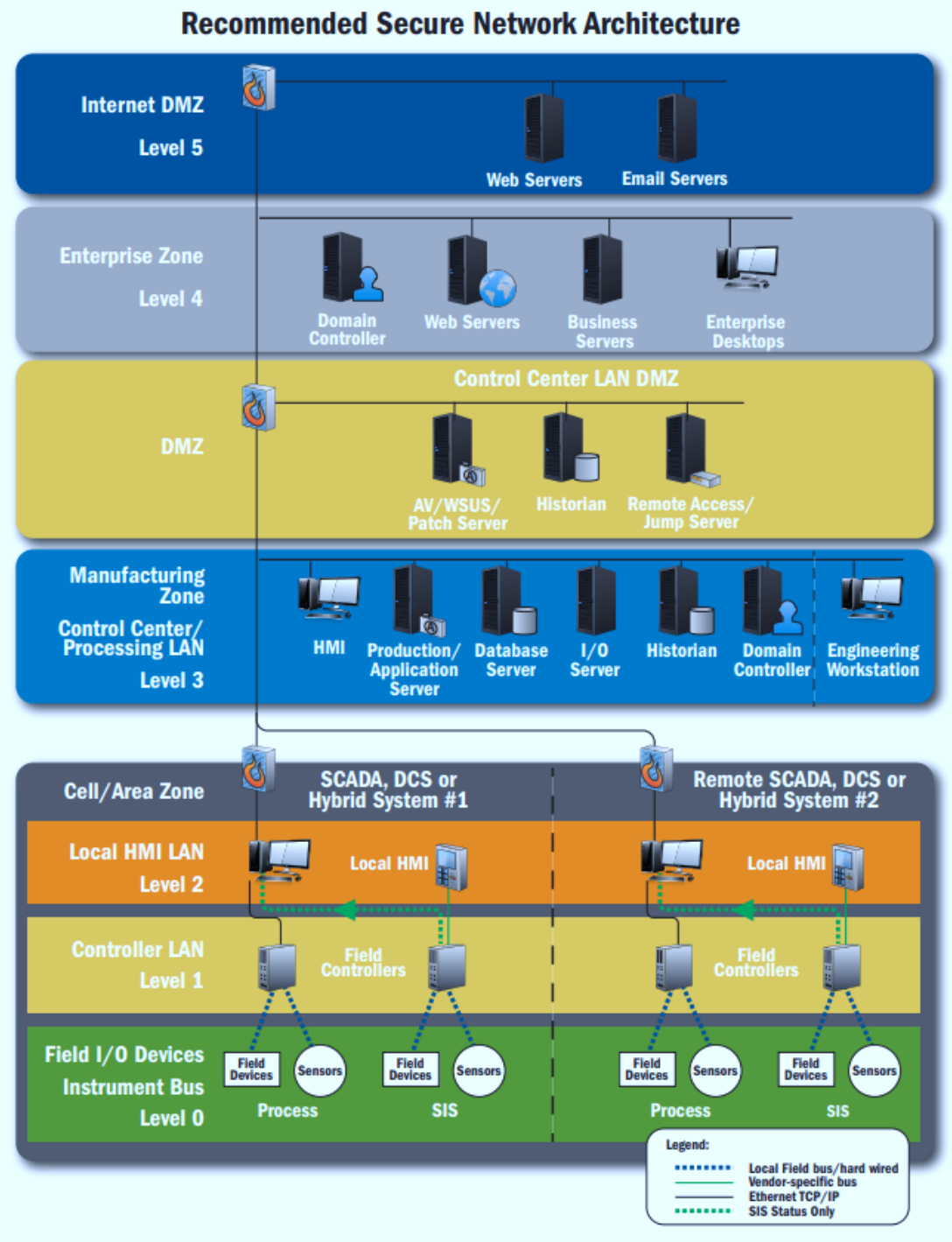
Enfoque de gestión del riesgo. Fuente: CISA (2016)

Este modelo obliga a adoptar un ciclo iterativo de mejora, reforzando las defensas a medida que evoluciona el panorama de riesgo.

- **Estrategia 2. Inventario de activos y caracterización de riesgo:** identificar y clasificar exhaustivamente los activos ICS (equipos, software, redes, datos y personal) para saber qué debe protegerse y por qué. Este inventario incluye sistemas de proceso, redes de control y el apoyo de infraestructura (IT y OT). Conociendo el contexto de negocio y la criticidad de cada activo, la organización puede priorizar las defensas según el impacto potencial. Una "lista de activos actualizada y caracterizada por criticidad" proporciona una base sólida para aplicar contramedidas adecuadas y asegurarse de que no quede ningún dispositivo crítico desprotegido.
- **Estrategia 3. Seguridad física:** aplicar controles físicos para impedir el acceso no autorizado o la interferencia con activos ICS. Esto abarca asegurar instalaciones y equipos (cableado, armarios, salas de control), restringir entradas mediante autenticación multifactor físico (tarjetas, biometría), instalar cámaras y sensores de movimiento, y controlar estrictamente los medios extraíbles (USB, CD). En otras palabras, se refuerza el perímetro físico del sistema (vallas, barreras, guardias) y se adapta según los requisitos de seguridad industrial y regulatoria, con el fin de evitar manipulaciones o robo de equipos y datos sensibles en el entorno ICS.
- **Estrategia 4. Arquitectura de red ICS:** diseñar una topología de red segura y segmentada para los sistemas de control. Se recomienda colocar los equipos de

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

campo y centros de control en zonas lógicas separadas, delimitadas por **zonas desmilitarizadas (DMZ),** VLANs y diodos unidireccionales. De este modo, la red ICS queda aislada de la red corporativa externa; por ejemplo, sólo una DMZ intermedia permitiría conexiones controladas entre IT y OT (ver figura).



Arquitectura de red segura recomendada. Fuente: CISA (2016)

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

Además, hay que asegurar el perímetro de red con accesos remotos controlados (pasarelas, VPNs con autenticación fuerte) y mantener una gestión estricta de parches y vulnerabilidades para cada segmento. Este diseño segmentado aumenta el coste y la complejidad de cualquier intento de intrusión.

- **Estrategia 5. Arquitecturas de seguridad:** implantar un marco de políticas y procedimientos de seguridad específicos para ICS, complementado con medidas de aislamiento técnico. Por ejemplo, definir normas operativas rigurosas **y bloquear electrónicamente los componentes de campo críticos** (firmware y configuraciones protegidos). Este nivel estructural implica combinar seguridad lógica (configuración de dispositivos y permisos) con seguridad física, asegurando que los sistemas más sensibles estén bastionados y que exista supervisión del cumplimiento de políticas en el ciclo de vida ICS.
- **Estrategia 6. Seguridad en hosts ICS:** asegurar los dispositivos finales y servidores que operan en el dominio ICS. Esto incluye endurecer cada host (p.ej. controladores, HMI y servidores SCADA) reduciendo al mínimo el software instalado, empleando máquinas virtuales seguras o sistemas de respaldo dedicados, y activando detección de intrusiones a nivel local (HIDS) cuando sea viable. La idea es minimizar las funciones expuestas de cada equipo ICS y contar con avisos tempranos de comportamientos anómalos en los equipos de control.
- **Estrategia 7. Monitorización de seguridad:** establecer vigilancia continua de eventos de seguridad en el entorno ICS. Esto supone registrar y analizar logs de auditoría críticos, **desplegar soluciones tipo NDR o CPS PP**, implementar soluciones de correlación y **SIEM** orientadas a OT, y supervisar de forma permanente la red ICS. Incluye también vigilar la cadena de suministro y el ciclo de vida de los componentes (para detectar anomalías en actualizaciones o configuraciones). La monitorización proactiva detecta indicios de intrusión y garantiza ajustar las defensas según la información del comportamiento real de la red.
- **Estrategia 8. Gestión de proveedores y outsourcing:** incluir a la cadena de suministro en la estrategia de seguridad ICS. Esto abarca revisar proveedores de servicios gestionados y soluciones cloud para asegurarse de que cumplen los niveles de seguridad exigidos, así como aplicar políticas contractuales claras. Por ejemplo, al usar servicios en la nube o consultores externos, deben definirse

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

controles específicos (acceso restringido, cifrado, supervisión) y asegurarse de que existan protocolos de respuesta ante incidentes de proveedores. De este modo se minimizan los riesgos introducidos por enlaces en la cadena de valor.

- **Estrategia 9. El elemento humano:** no podía faltar. Reconocer que el factor humano es parte integral y fundamental de la defensa. Se destaca establecer procedimientos claros de operación y emergencia, y sobre todo capacitar al personal continuamente en seguridad ICS: operadores, ingenieros y equipo de IT/OT deben recibir adiestramiento y concienciación específicos. Un personal bien formado y alertado podrá aplicar las capas de defensa con disciplina y detectar comportamientos sospechosos (phishing, accesos inusuales, etc.), reduciendo el riesgo de errores o ataques dirigidos a usuarios internos.

Recomendaciones finales

Para cerrar con esta guía de CISA, recogemos las cuatro recomendaciones que se derivan de la misma:

1. **Adoptar un modelo de seguridad proactivo:** el informe destaca la necesidad de moverse de un esquema reactivo a uno proactivo e iterativo. Es decir, no sólo aplicar controles puntuales tras un incidente, sino integrar la mejora continua: diseñar el sistema con seguridad desde el inicio, probar escenarios de intrusión, y ajustar periódicamente las defensas.

Modelo de seguridad proactivo. Fuente: CISA (2016)

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

Este modelo implica practicar ciberseguridad preventiva (ejercicios de respuesta, análisis de amenazas futuras) y aprovechar automatización para detectar y cazar ataques antes de que causen daños.

2. **Implementar contramedidas clave específicas:** el documento propone un conjunto de cinco contramedidas esenciales para ICS, enfocadas en mitigar los vectores más comunes (por ejemplo, segmentación estricta de la red, autenticación multifactor, gestión de parches priorizada, monitorización OT especializada, etc.). En resumen, se aconseja combinar técnicas probadas –como controles de acceso robustos, comunicación cifrada y sandboxing de dispositivos– para cubrir las necesidades únicas de un entorno de control. Aunque el informe no las enumera explícitamente, sugiere centrar los esfuerzos en las defensas más efectivas para entornos industriales críticos, gestionando internamente los riesgos residuales.
3. **Seguir estándares y marcos de referencia**: se recomienda alinear la ciberseguridad ICS con marcos reconocidos (en este caso propone los empleados en el mundo anglosajón, p. ej. NIST CSF, ISO/IEC 62443, NERC CIP, entre otros) y las políticas de ciberseguridad del sector. Esto incluye adoptar guías de buenas prácticas que aborden tanto la tecnología como la gestión del riesgo. Usar estos estándares ayuda a estandarizar los controles en todas las capas (técnica, organizativa y procedimental) y facilita auditorías, cumplimiento regulatorio y mejora continua del programa de seguridad industrial.
4. **Emplear herramientas y servicios adecuados:** el informe aconseja aprovechar herramientas especializadas en ICS para implementar defensa en profundidad. Por ejemplo, utilizar evaluaciones de seguridad y simuladores, software de gestión de vulnerabilidades enfocadas en ICS, y servicios de monitorización OT avanzados. También sugiere programas de apoyo técnico y colaboración público-privada. Estas herramientas permiten automatizar la identificación de brechas, validar la arquitectura de red y mantenerse al día con las amenazas emergentes.

En conjunto, son componentes prácticos para reforzar los nueve niveles de defensa anteriores. Mencionar que en [23] CISA ofrece una infografía interesante y totalmente alineada con esta estrategia de defensa en profundidad, que aconsejamos tomar como referencia.

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

4.1.4 Resiliencia ciberfísica

La resiliencia ciberfísica es uno de los pilares emergentes más relevantes en la protección de infraestructuras OT, particularmente ante amenazas persistentes, fallos inevitables y disrupciones ciberfísicas complejas. Lejos de limitarse a una visión tradicional de prevención o robustez estática, las tendencias internacionales promueven un enfoque dinámico, centrado en la continuidad del servicio bajo condiciones adversas. Este cambio de paradigma se articula alrededor de dos referencias fundamentales:

El informe americano del ***President's Council of Advisors on Science and Technology (PCAST) sobre resiliencia ciberfísica*** [24] establece un marco estratégico de primer nivel para el diseño de políticas de seguridad industrial en infraestructuras críticas. Este documento promueve un **cambio conceptual claro: de la ciberseguridad orientada a evitar intrusiones ("keep attackers out")** a la resiliencia operativa enfocada en **garantizar la funcionalidad mínima** de los servicios esenciales incluso bajo condiciones de fallo o ataque **("keep essential services running").**

Menciona también ***Minimum Viable Operating Capabilities*** (capacidades mínimas operativas), los modelos de ***bounded impact*** (fallos acotados) y de ***degraded but functioning*** (servicio degradado pero continuo). Además, defiende que la resiliencia es una responsabilidad compartida que afecta no sólo a los operadores técnicos, sino también a fabricantes, entidades reguladoras y órganos ejecutivos de dirección. **A través de casos reales como los incidentes del Colonial Pipeline o el apago en Texas, se ilustra cómo una gestión anticipada y transversal de la resiliencia puede mitigar severamente el impacto de un ataque OT exitoso.**

Adicionalmente, **el estudio académico de Largo et al. sobre la evolución de la resiliencia ciberfísica, métricas e integración normativa** [25] complementa la perspectiva del PCAST con una aproximación más técnico-metodológica. Este trabajo rastrea la evolución del concepto de resiliencia —desde su enfoque en robustez estática hacia una visión adaptativa y sistémica— e introduce criterios medibles aplicables a sistemas ICS. **Clasifica indicadores, modelos de evaluación y frameworks operativos, y propone un conjunto de métricas útiles para diseñar KPIs, evaluar controles de continuidad o realizar auditorías y simulaciones de fallo.**

Además, el estudio **integra la dimensión regulatoria europea**, incluyendo marcos como la directiva NIS2 o el Reglamento CER, aportando así una visión complementaria al enfoque estadounidense. Para entornos OT en Europa, **esta doble referencia**

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

permite armonizar criterios técnicos con obligaciones normativas, mejorando la alineación entre los objetivos de resiliencia operativa y los requerimientos regulatorios aplicables.

Ambas fuentes permiten a operadores industriales y administraciones públicas adoptar una visión avanzada de la resiliencia en entornos ciberfísicos, para anticiparse a ataques inevitables y reducir su impacto operativo (algo crítico en servicios esenciales).

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

5 Conclusiones

La segunda versión del **Informe de Inteligencia de amenazas OT – II** consolida y amplía el trabajo iniciado en el Informe I, incorporando una lectura más focalizada sobre **actores de amenaza** y sobre su capacidad real de progresar desde intrusiones en IT hacia escenarios de impacto en OT/ICS. A lo largo del documento se confirma una idea central: en ciberseguridad industrial, el riesgo no viene definido sólo por la existencia de una campaña o de una vulnerabilidad, sino por la combinación de **capacidad del adversario**, **exposición del operador**, **madurez operativa** y **posibilidad de progresión hacia el proceso físico**.

Una primera conclusión transversal es que el panorama OT/ICS actual debe leerse desde una perspectiva **multi-fuente y** no desde una única lente. Las evidencias recopiladas muestran patrones recurrentes que se repiten entre estudios: la persistencia de intrusiones basadas en **identidad y acceso** (phishing, abuso de credenciales, accesos remotos mal gobernados), la importancia creciente de la **cadena de suministro e infraestructura de terceros** como vector y amplificador de riesgo, y la consolidación de escenarios de **disrupción operativa** como resultado plausible cuando confluyen debilidades técnicas y procedimentales. El valor del informe reside, precisamente, en **triangular** estas señales y traducirlos a prioridades defensivas adaptables al tejido industrial gallego.

En segundo lugar, el análisis de actores y TTPs —incluyendo la visión especializada que distingue fases del ciclo de ataque— refuerza que la prioridad no es sólo impedir intrusiones, sino **reducir la capacidad de progresión y acortar el tiempo de permanencia** del adversario. Incluso cuando los incidentes comienzan en IT, la experiencia agregada muestra que el impacto real en industria suele depender de dos factores:

(i) la **existencia de caminos de tránsito IT→OT insuficientemente controlados**, y

(ii) la **falta de visibilidad y procedimientos para detectar y contener movimientos laterales**, reconocimiento interno y extracción de información técnica.

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

Un tercer hallazgo de fondo es el carácter estratégico de la **información OT** (diagramas, topologías, instrucciones operativas, configuraciones y datos generales cuando aplique). Su protección no puede considerarse un asunto documental menor: cuando esa información es accesible sin gobernanza, se convierte en un multiplicador de riesgo que reduce la fricción para el adversario y acelera la preparación de acciones más dañinas. En consecuencia, el informe sugiere tratar la documentación técnica como **activo crítico**, equiparando su protección a la de credenciales y accesos.

Desde una perspectiva territorial, la exposición de Galicia no se limita a sectores estrictamente críticos: abarca entre otros **energía, agua, alimentación, manufactura y logística**, así como proveedores y subcontratas que operan tecnología industrial y mantenimiento. Ello implica que la mejora de la postura de seguridad debe formularse como programa continuado y no como proyecto puntual: combinar **prevención** (reducción de exposición y endurecimiento) con **resiliencia** (detección, respuesta y recuperación), asumiendo que el objetivo realista es **reducir probabilidad e impacto**, y no eliminar por completo la amenaza.

Una conclusión especialmente práctica, que complementa el análisis técnico, es la pertinencia de establecer —o fortalecer— **programas internos de inteligencia de amenazas** adaptados a OT/ICS. El informe sugiere que las organizaciones industriales pueden mitigar riesgos de manera más eficiente cuando disponen de capacidades internas para:

- Definir un **ciclo de inteligencia** (requisitos, recopilación, análisis, difusión y retroalimentación) orientado a decisiones operativas.
- Integrar señales de fuentes externas con su propia telemetría (SOC/OT-SOC, registros de acceso remoto, eventos de red industrial, inventario y cambios), generando **hipótesis verificables**.
- Traducir TTPs a **casos de uso de detección**, reglas de monitorización y mejoras procedimentales, evitando depender sólo de indicadores puntuales.
- Evaluar de forma recurrente la exposición y la capacidad de recuperación mediante **métricas** (p.ej., cobertura de activos críticos, tiempos de detección/contención, robustez de copias, eficacia de segmentación) y ejercicios controlados.

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

Finalmente, las recomendaciones de seguridad formuladas a lo largo del documento no se fundamentan en un único marco, sino **en una convergencia de buenas prácticas procedentes de guías y estudios de referencia, informes de inteligencia y lecciones aprendidas en operaciones reales**. Esto refuerza un mensaje de gobernanza: la seguridad OT/ICS requiere un enfoque de **defensa en profundidad**, apoyado por arquitectura y operación (segmentación, control de identidades, acceso remoto), por capacidades de observación y respuesta (detección basada en comportamiento, procedimientos de contención), y por preparación para continuidad y recuperación (copias probadas, planes y ejercicios).

En síntesis, esta versión II consolida una recomendación transversal: **alinear la inteligencia de actores y TTPs con decisiones de arquitectura, operación, personas y recuperación, creando un ciclo de mejora continuo que aumente la resiliencia ciberfísica**.

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

Bibliografía

[1] 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

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

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

[4] MITRE (2013). *MITRE ATT&CK® — Adversarial Tactics, Techniques & Procedures*. Recuperado de https://attack.mitre.org/

[5] MITRE (2020). *MITRE ATT&CK® for ICS — Knowledge Base for Industrial Control System Threats*. Recuperado de https://attack.mitre.org/matrices/ics/

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

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

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

[9] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Recuperado de https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[10] Lockheed Martin (n.d.). *Cyber Kill Chain®. The Seven Steps of Cyber Intrusion*. Recuperado de https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[11] Dragos (2021). *MITRE ATT&CK for ICS Mapping by Dragos*. Recuperado de https://www.dragos.com/mitre-attack-for-ics

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

[12] ThreatFox (2021). *Share Indicators Of Compromise (IOCs)*. Recuperado de https://threatfox.abuse.ch

[13] MISP Project (2011). *Open Source Threat Intelligence Platform*. Recuperado de https://www.misp-project.org

[14] CIRCL (2023). *Introducción a MISP*. Recuperado de https://www.youtube.com/watch?v=ttfWq_V4cLc

[15] MISP Project (2012). *MISP Communities*. Recuperado de https://www.misp-project.org/communities

[16] MISP Galaxy (2016). *A simple method to express threat actor information*. Recuperado de https://www.misp-project.org/galaxy.html

[17] OpenCTI Platform (2019). *Open Cyber Threat Intelligence Platform*. Recuperado de https://github.com/OpenCTI-Platform/opencti

[18] TheHackerNews (2023). *Honeypot Factory: The Use of Deception in ICS/OT Environments*. Recuperado de https://thehackernews.com/2023/02/honeypot-factory-use-of-deception-in.html

[19] Conpot Project (2013). *ICS/SCADA honeypot with the capability to simulate industrial control protocols*. Recuperado de https://github.com/mushorg/conpot

[20] MITRE Corporation (2021). *MITRE D3FEND: A knowledge graph of cybersecurity countermeasures*. Recuperado de https://d3fend.mitre.org/

[21] CISA (2023). *Cross-Sector ICS Recommended Practices*. Recuperado de https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

[22] CISA (2016). *Defense in Depth Strategies for Industrial Control Systems*. Recuperado de https://www.cisa.gov/sites/default/files/2023-01/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[23] CISA (2016). *Cybersecurity Best Practices for Industrial Control Systems*. Recuperado de https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

[24] President's Council of Advisors on Science and Technology (PCAST) (2024). *Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital*

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

World. Recuperado de https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf

[25] Longo, A.; Aghazadeh Ardebili, A.; Lazari, A.; Ficarella, A. (2025). *Cyber–Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks*. Electronics, 14(8), 1684. Recuperado de https://www.mdpi.com/2079-9292/14/8/1684

[26] Dragos (2017). *MAGNALLIUM Threat Activity Group Profile*. Recuperado de https://www.dragos.com/threat/magnallium

[27] Dragos (2017). *PARISITE Threat Activity Group Profile*. Recuperado de https://www.dragos.com/threat/parisite

[28] Dragos (2018). *WASSONITE Threat Activity Group Profile*. Recuperado de https://www.dragos.com/threat/wassonite

[29] Observatorio de Ciberseguridad Industrial de Galicia (2025). *Informes de Ciberalertas.* Recuperados de https://ciberseguridadegalicia.gal/es

[30] Dragos (2021). *CHERNOVITE Threat Activity Group Profile*. Recuperado de https://www.dragos.com/threat/chernovite

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

Glosario

ABYSSWORKER

Familia de malware citada en el informe en el contexto de amenazas y herramientas empleadas en campañas de intrusión.

AcidPour

Wiper para Linux orientado a borrar contenidos en dispositivos embebidos (p.ej., mediante búsqueda de directorios UBI), empleado como capacidad disruptiva en entornos industriales.

AcidRain

Wiper observado previamente y empleado como referencia comparativa para contextualizar capacidades destructivas en entornos embebidos.

AMTEGA (Agencia para la Modernización Tecnológica de Galicia)

Organismo de la Xunta de Galicia responsable de iniciativas y coordinación tecnológica, incluyendo líneas de ciberseguridad.

APT (Advanced Persistent Threat / Amenaza Persistente Avanzada)

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

ATT&CK (MITRE ATT&CK)

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

AuKill

Herramientas/malware citado en el informe en el contexto de capacidades empleadas por actores de amenaza.

AvNeutralizer

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

Herramientas/malware citado en el informe en el contexto de técnicas de evasión y neutralización de defensas.

BAUXITE

Grupo de amenaza identificado por Dragos con foco en OT/ICS y casos asociados a impacto en fases avanzadas (Stage 2) mediante compromisos oportunistas de activos expuestos.

Backdoor (Puerta trasera)

Mecanismo (software o configuración) que permite acceso persistente y no autorizado a un sistema, normalmente con capacidad de ejecución remota.

BEC (Business Email Compromise / Compromiso de correo empresarial)

Fraude basado en suplantación (o compromiso real) de cuentas de correo para inducir transferencias, cambios de cuenta bancaria o acceso a información sensible.

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.

C2 (Command and Control / Comando e control)

Cauce e infraestructura empleadas por el atacante para comunicarse con sistemas comprometidos, emitir instrucciones y recibir datos.

CAPTCHA

Mecanismo de verificación para distinguir humanos de automatización; puede aparecer en campañas maliciosas como control de acceso o evasión.

CCN-CERT

Centro Criptológico Nacional – CERT (España). Entidad de referencia para alertas, guías e información técnica sobre amenazas e incidentes.

CER (Critical Entities Resilience Directive)

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

Directiva europea orientada a reforzar la resiliencia de entidades críticas frente a riesgos, incluyendo dimensiones tecnológicas y operativas.

CHERNOVITE

Grupo de amenaza identificado por Dragos asociado al desarrollo de capacidades avanzadas para ICS, incluyendo el marco PIPEDREAM.

CIP (Critical Infrastructure Protection / Protección de infraestructuras críticas)

Conjunto de políticas y prácticas para proteger infraestructuras críticas frente a amenazas físicas y digitales (incluyendo marcos específicos como NERC CIP).

CISA (Cybersecurity and Infrastructure Security Agency)

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

CoDeSys

Plataforma de desarrollo/ejecución para PLCs y sistemas industriales, citada en el contexto de interacción con ecosistemas de control.

CRASHOVERRIDE

Malware orientado a entornos industriales (también referido como Industroyer en otros contextos) asociado a impactos sobre infraestructura eléctrica.

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.

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

DarkCrystal RAT

Herramienta del tipo RAT (Remote Access Trojan) empleada en campañas de intrusión para control remoto y robo de información.

DLL (Dynamic Link Library)

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

DMZ (Zona desmilitarizada)

Segmento de red intermedio diseñado para aislar servicios expuestos y reducir el riesgo de tránsito hacia redes internas críticas.

DNS (Domain Name System)

Sistema de nombres de dominio; puede ser empleado por los atacantes para resolución de infraestructura C2 o técnicas de evasión.

EDR (Endpoint Detection and Response)

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

ELECTRUM

Grupo de amenaza con historial disruptivo en OT/ICS, asociado a operaciones con capacidad Stage 2 y uso de herramientas destructivas (p.ej., wipers).

ENISA (European Union Agency for Cybersecurity)

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

Exfiltración

Extracción no autorizada de datos desde una organización hacia el exterior (p.ej., documentación OT, GIS, credenciales).

FormBook

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

Familia de infostealer citada como ejemplo de malware empleado en campañas de robo de información.

GDPR (Reglamento General de Protección de Datos)

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

GIE (Gas Infrastructure Europe)

Entidad/ámbito sectorial citado como temática de lure en campañas relacionadas con petróleo y gas.

GIS (Geographic Information System / Sistema de información geográfica)

Herramientas y datos geoespaciales críticos para operaciones (p.ej., infraestructura y activos), citados como objetivo de exfiltración.

GRAPHITE

Grupo de amenaza identificado por Dragos (nuevo en la clasificación 2024) con campañas de espionaje y foco en sectores industriales/energéticos.

GRU

Dirección Principal de Inteligencia (Rusia), citada en el informe en relación con contextos de atribución y actividad geopolítica.

HART (Highway Addressable Remote Transducer)

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

HAVEX

Malware asociado históricamente a campañas contra entornos industriales, citado como referencia en el contexto de amenazas ICS.

HIDS (Host-based Intrusion Detection System)

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

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

HMI (Human-Machine Interface)

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

HTTP / HTTPS

Protocolos web empleados para comunicación. En contexto de amenaza, pueden utilizarse para C2, staging o exfiltración camuflada en tráfico legítimo.

IA (Inteligencia Artificial)

Tecnologías de automatización y análisis basadas en modelos de aprendizaje; en el informe aparece como elemento contextual y de riesgo/uso transversal.

IBM X-Force

Equipo/servicio de inteligencia de amenazas citado como fuente de contexto y tendencias.

ICS (Industrial Control Systems / Sistemas de control industrial)

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

ICS Cyber Kill Chain

Adaptación del ciclo de ataque a entornos industriales, empleada para describir la progresión desde intrusión inicial hasta interacción con el proceso físico.

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.

IED (Intelligent Electronic Device / Dispositivo electrónico inteligente)

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

Dispositivos empleados en automatización y subestaciones (p.ej., protección y control), críticos en entornos eléctricos.

IDS (Intrusion Detection System)

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

IEC (International Electrotechnical Commission)

Organismo de normalización en el ámbito electrotécnico e industrial, citado como referencia de estándares.

IIoT (Industrial Internet of Things)

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

Industroyer

Denominación asociada a CRASHOVERRIDE en otros contextos; referencia a malware orientado a sistemas industriales.

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.

IT (Information Technology / Tecnologías de la información)

Infraestructura digital corporativa (sistemas de información, servidores, endpoints, identidad), frecuentemente punto de entrada en ataques a OT.

Kapeka

Backdoor citado en el informe en el contexto de campañas e intrusiones contra organizaciones industriales.

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

KEV (Known Exploited Vulnerabilities)

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

Kill Chain (Cyber Kill Chain)

Modelo de fases de un ataque dirigido (reconocimiento, armamento, entrega, explotación, instalación, C2 y acciones sobre el objetivo).

Lista blanca de aplicaciones (Application allowlisting)

Control que permite ejecutar sólo software previamente autorizado, reduciendo el riesgo de ejecución de malware y movimiento lateral.

LLM (Large Language Model / Modelo de lenguaje de gran escala)

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

Loader

Componente de malware que prepara el sistema y descarga/ejecuta payloads posteriores (p.ej., stealers o backdoors).

LockBit

Grupo/familia de ransomware citada como ejemplo de amenaza criminal con impacto operativo y económico.

LNG (Liquefied Natural Gas / Gas natural licuado)

Sector/ámbito industrial citado como objetivo/entorno de relevancia para amenazas OT.

LummaStealer

Stealer citado en el informe en el contexto de campañas de robo de información y credenciales.

MAGNALLIUM

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

Grupo de amenaza descrito por Dragos con actividad centrada en intrusión y espionaje en IT contra sectores industriales, sin capacidad OT demostrada.

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 D3FEND

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

Modbus

Protocolo industrial empleado en automatización; relevante por ser un vector de visibilidad/detección y potencial abuso si existe acceso indebido.

Movimiento lateral

Técnicas para desplazarse dentro de una red tras el acceso inicial, buscando sistemas de mayor privilegio o proximidad a OT.

MS Threat Intelligence / Microsoft Threat Intelligence

Capacidad/servicios de inteligencia de amenazas citados como fuente de contexto y tendencias.

MTTD (Mean Time To Detect / Tiempo medio de detección)

Métrica para medir cuánto tarda una organización en detectar un incidente.

MTTR (Mean Time To Respond/Recover / Tempo medio de respuesta/recuperación)

Métrica para medir cuanto tarda una organización en responder y recuperar tras un incidente.

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

MuddyWater / OilRig

Denominaciones citadas en el informe en contexto de actividad de amenazas asociadas a determinados perfiles de actor.

NDR (Network Detection and Response)

Tecnologías y capacidades de detección y respuesta basadas en red, relevantes para visibilidad en OT e IT.

NERC / NERC CIP

Marco de estándares (especialmente en el ámbito eléctrico) orientado a requisitos de seguridad para infraestructura crítica.

NIS2 (Network and Information Security Directive 2)

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

NIST (National Institute of Standards and Technology)

Instituto estadounidense de referencia en estándares y guías de ciberseguridad, citado como marco transversal.

Nozomi Networks

Fabricante y fuente de observabilidad OT citada como referencia para contexto y tendencias en entornos industriales.

OPC / OPC-UA (OPC Unified Architecture)

Tecnología/protocolo industrial empleado para interoperabilidad y comunicación; relevante en amenazas por visibilidad y potencial abuso cuando hay acceso indebido.

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)

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

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

OTAN

Organización del Tratado del Atlántico Norte, citada en el informe como referencia contextual.

OEM (Original Equipment Manufacturer / Fabricante original)

Fabricante de equipos industriales; relevante por cadena de suministro, firmware, actualizaciones y soporte.

PARISITE

Grupo de amenaza descrito por Dragos con foco en espionaje y recogida de información contra organizaciones industriales.

Password spraying

Técnica de ataque a credenciales que prueba pocas contraseñas comunes contra muchas cuentas para evitar bloqueos y aumentar la tasa de éxito.

PCAST

Referencia a informes y análisis (p.ej., resiliencia ciberfísica) citadas en el informe como contexto.

PIPEDREAM

Marco modular de malware diseñado para interacción con entornos ICS, asociado a CHERNOVITE.

PLC (Programmable Logic Controller)

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

Proxy / Relay (Relé)

Infraestructura intermedia empleada para redirigir tráfico (p.ej., C2, staging), ocultando origen y dificultando detección.

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

RAT (Remote Access Trojan)

Malware que habilita control remoto del sistema comprometido (captura de pantalla, ejecución de comandos, extracción de datos).

RDP (Remote Desktop Protocol)

Protocolo de acceso remoto a escritorios Windows; frecuente como vector de intrusión si está expuesto o con credenciales débiles.

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.

SMB (Server Message Block)

Protocolo de compartición en Windows; relevante como vector de movimiento lateral o abuso en redes mal segmentadas.

SOC (Security Operations Center)

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

SOHO (Small Office / Home Office)

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

Categoría de dispositivos y redes de pequeña oficina/hogar; en el informe aparece en el contexto de compromisos de routers usados como relés.

Spear-phishing

Phishing altamente dirigido, con cebos personalizados para una persona/organización concreta, orientado a obtener acceso inicial.

SSH (Secure Shell)

Protocolo de administración remota cifrada; crítico en exposición a internet y gobernanza de credenciales.

Stage 1 / Stage 2 (ICS Cyber Kill Chain)

Clasificación por fases: Stage 1 (intrusión/espionaje en IT y preparación) y Stage 2 (interacción con el proceso industrial e impacto OT).

STUXNET

Malware ICS histórico citado como referencia por ser un punto de inflexión en ataques ciberfísicos.

Staging (Preparación de payloads)

Uso de infraestructura intermedia (a veces servicios legítimos) para alojar, preparar y servir cargas maliciosas antes de la ejecución final.

Stealer

Malware diseñado para robar información (credenciales, cookies, wallets, datos de navegador) y facilitar accesos posteriores.

Telemetría

Conjunto de datos de observación (red, endpoints, protocolos industriales, registros) empleados para detección y respuesta.

ThreatConnect / ThreatStream / ThreatFox / TheHive

Herramientas/plataformas citadas en el informe para gestión, intercambio y operación de inteligencia de amenazas.

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

TRISIS

Malware orientado a sistemas de seguridad industrial, citado como referencia en el contexto de amenazas ICS avanzadas.

TrickBot

Malware/capacidad criminal citada en el informe como ejemplo de herramienta empleada en campañas de intrusión.

TTP (Tactics, Techniques and Procedures)

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

TURNEDUP

Denominación de malware citada en el informe asociada a campañas de intrusión y espionaje.

UBI (Unsorted Block Images)

Formato/estructura típica en almacenamiento de dispositivos embebidos; relevante por técnicas de borrado destructivo en wipers.

UE (Unión Europea)

Ámbito institucional citado en relación con normativa, contexto de amenazas y marcos de referencia.

USB (Universal Serial Bus)

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

VOLTZITE

Grupo de amenaza descrito por Dragos con foco en espionaje y recogida de información OT (p.ej., GIS y documentación técnica), y uso de infraestructura de relé.

VPN (Virtual Private Network)

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

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

WASSONITE

Grupo de amenaza descrito por Dragos, con actividad orientada a la intrusión y recogida de información en sectores industriales e infraestructura crítica.

Wiper

Malware diseñado para destruir datos e impedir la recuperación (borrado, corrupción de ficheros/particiones), con impacto disruptivo.

WMI (Windows Management Instrumentation)

Conjunto de herramientas de Microsoft para la administración y monitorización 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.

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

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial
Informe de Inteligencia de Amenazas - I

AMTEGA – Xunta de Galicia 2026

CC BY-SA 4.0

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