CIBER SEGURIDADE GALICIA

# Observatorio de Ciberseguridade Industrial

## Informe de Intelixencia de Ameazas - II

Maio 2026

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

**Edita:** Xunta de Galicia

**Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA)**

**Lugar:** Santiago de Compostela

**Ano:** 2026

# Índice





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

# 1 Introdución

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

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

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

--

A evolución cara aos modelos de **Industria 4.0 e 5.0**, caracterizados pola automatización avanzada, integración de sistemas ciberfísicos, analítica de datos en tempo real e maior interacción entre persoas e tecnoloxía, está a transformar profundamente o ecosistema industrial. Esta transformación incrementa a complexidade técnica das infraestruturas produtivas e introduce novas dependencias dixitais que deben ser xestionadas desde unha perspectiva de risco. Neste contexto, a intelixencia de ameazas orientada a OT/ICS convértese nun instrumento esencial para a **priorización de riscos**, o apoio á **toma de decisións** e o fortalecemento da **resiliencia operativa** do tecido industrial galego.

Este **Informe de intelixencia de ameazas OT – II** concíbese como unha evolución natural do Informe inicial do Observatorio, co que comparte enfoque e vocación práctica, mais **actualiza e amplía** o contido para incorporar unha caracterización máis completa de actores, campañas e patróns operativos observados recentemente.

Mentres o Informe I establecía unha base metodolóxica e unha visión consolidada do panorama (marco teórico, alertas e recomendacións), esta segunda versión reforza de

maneira explícita a dimensión de **atribución e perfilado de grupos**, con especial atención á intelixencia especializada de Dragos e ao seu marco de lectura da progresión adversaria en contornos industriais.

O propósito fundamental do documento é ofrecer **intelixencia accionable** para organizacións con exposición a sistemas industriais —dende infraestruturas críticas e servizos esenciais ata manufactura e cadeas de subministración—, transformando a actividade adversaria global en implicacións operativas aplicables a Galicia. Para iso, o informe inclúe:

(i) a recompilación de **actores de ameaza** con interese ou capacidade en OT/ICS,

(ii) a identificación das **Tácticas, Técnicas e Procedementos (TTPs)** máis recorrentes na intrusión e na persistencia do atacante,

(iii) e a **interpretación do risco segundo a posibilidade de progresión** desde intrusións en IT cara a impactos sobre OT.

Un elemento diferencial desta versión é a incorporación do marco **ICS Cyber Kill Chain** empregado por Dragos para distinguir niveis de madurez operativa do adversario. En particular, préstase atención aos grupos con capacidade confirmada para avanzar máis aló do acceso inicial e do espionaxe en IT, acadando fases de **interacción co proceso industrial** (capacidade *Stage 2*), que constitúen o salto cualitativo cara ao impacto ciberfísico. Esta distinción resulta clave para orientar investimentos defensivos en sectores galegos con alta dependencia de continuidade de operación, onde un incidente pode traducirse en **paradas de produción**, degradación de servizo, riscos de seguridade e custos de recuperación elevados.

A estrutura do informe mantén unha progresión didáctica: inicia cunha introdución e un resumo executivo orientado a decisores, continúa cun bloque central de **intelixencia de ameazas** que consolida fontes de referencia e perfís de actores (incluíndo a análise de grupos e TTPs), e complétase cun apartado de **intelixencia propia** e recomendacións de carácter técnico e organizativo.

O obxectivo final é proporcionar unha visión coherente e operativa que permita **anticipar**, **detectar** e **mitigar** ameazas con impacto potencial sobre contornos industriais no contexto galego.



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

# 2 Resumo executivo

A continuación sintetizamos os elementos máis relevantes do **Informe de intelixencia de ameazas OT – II**, co obxectivo de facilitar a **toma de decisións** por parte de responsables de ciberseguridade, operacións industriais e dirección. Recórdase que a versión II dá continuidade ao enfoque do Informe I, mantendo a visión integrada por fontes, e **reforza de maneira específica a análise de actores con relevancia OT/ICS**, especialmente aqueles con capacidade de progresar cara a impactos ciberfísicos.

En canto a **fontes principais empregadas.** A elaboración deste estudo baséase nunha combinación de fontes de intelixencia e referencia amplamente recoñecidas no eido OT/ICS, co obxectivo de equilibrar evidencias técnicas de campo, tendencias agregadas, e marcos metodolóxicos.

En particular, esta versión II apoia o seu bloque central de actores na intelixencia especializada de **Dragos** (informe anual OT Cybersecurity Year in Review 2025 e perfís públicos de grupos de ameaza), e complétase con informes e guías de alcance máis transversal que permiten contextualizar tendencias e priorización defensiva, incluíndo, entre outros, **ENISA** (panorama de ameazas), **Microsoft Digital Defense Report**, **IBM X-Force**, informes de fabricantes e observabilidade OT (p.ex., **Crowdstrike**) e análise de madurez e prácticas (p.ex., **CISA**), así como fontes institucionais e sectoriais dispoñibles no marco do Observatorio.

**Mensaxes clave para a toma de decisións**

**1) A ameaza relevante non é só "intrusión en IT", senón a progresión cara a OT.** O criterio diferencial que debe guiar a priorización é a capacidade do adversario para avanzar no ciclo de ataque ata fases de **interacción co proceso industrial** (capacidade Stage 2 na ICS Cyber Kill Chain). No corpus analizado, isto materialízase con claridade en actores como **ELECTRUM** (capacidade demostrada de executar ataque ICS e desenvolvemento de wipers destructivos), **BAUXITE** (impactos Stage 2 por compromisos triviais de dispositivos expostos) e **CHERNOVITE** (malware ICS avanzado asociado a PIPEDREAM).

**2) A actividade adversaria está a combinar sofisticación (malware ICS) con oportunismo (exposición e credenciais débiles).** O mesmo 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 ou wipers orientados a entornos embebidos) como operacións de baixo custo baseadas en **phishing**, **password spraying**, **servizos expostos** e abuso de infraestrutura de terceiros. Isto implica que o risco non depende só do perfil do actor, senón tamén do **nivel de hixiene e exposición** do operador.

**3) O sector eléctrico e os servizos esenciais continúan como obxectivo prioritario, con impactos reais e observables.** O caso do ataque a **Kyivstar** exemplifica que a disrupción pode materializarse en degradación de servizos a gran escala, e que os adversarios poden empregar "mecanismos de cobertura" (p. ex., actores hacktivistas) para dificultar a atribución e a resposta. En paralelo, o histórico de ELECTRUM (CRASHOVERRIDE/Industroyer) e a aparición de **AcidPour** reforzan que a disrupción deliberada segue sendo unha ameaza prioritaria en ecosistemas eléctricos.

**4) A información OT (GIS, topoloxías, instrucións) é un activo estratéxico que está a ser buscado de forma persistente.** En campañas como as asociadas a **VOLTZITE**, a exfiltración de **datos GIS** e documentación OT (diagramas, instrucións operativas) aparece como obxectivo central. Para infraestruturas galegas (enerxía, auga, transporte e portos), isto obriga a tratar a documentación técnica como activo crítico, con controis equivalentes aos aplicados a credenciais e acceso remoto.

**5) Europa non é un espectador: obsérvase selección explícita de obxectivos e desprazamento cara a obxectivos europeos.** A campaña de **KAMACITE** relacionada coa **Gas Infrastructure Europe (GIE)** en Alemaña, combinando loaders/stealers e un backdoor a medida (**Edam**), ilustra un desprazamento desde un foco case exclusivo en Ucraína cara a **obxectivos europeos no ámbito de petróleo e gas**. Isto é relevante para Galicia polo peso de cadeas de subministración industriais e pola dependencia de servizos esenciais.

Inclúese unha clasificación de actores de amenaza que pode empregarse como guía práctica para decidir **onde investir primeiro**: non só en tecnoloxía, senón en políticas de acceso, operación e recuperación.

### Decisións defensivas recomendadas a curto e medio prazo

As evidencias recompiladas apuntan a un conxunto de decisións de alto impacto para organizacións industriais:



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

**a) Blindar a ponte IT/OT como prioridade número 1.** A **segmentación efectiva**, o control de fluxos e a limitación do movemento lateral son a medida máis determinante para impedir que intrusións en IT evolucionen cara a impactos OT.

**b) Tratar accesos remotos e exposición como risco operativo.** Deben priorizarse accións como: restrinxir o acceso **SSH e servizos críticos tras VPN**, eliminar credenciais por defecto, auditar e rotar **credenciais SSH**, e revisar a exposición de dispositivos e servizos que poidan ser reutilizados como relés.

**c) Protexer documentación OT e sistemas GIS como activos críticos.** Establecer clasificación, control de acceso, rexistro de accesos e detección de exfiltración sobre diagramas de rede, instrucións operativas e información xeoespacial.

**d) Asegurar capacidade de recuperación fronte a disrupción e wipers.** Para escenarios tipo ELECTRUM, é imprescindible dispoñer de **copias de seguridade fóra de liña, probadas**, incluíndo lóxica de proxecto, configuracións de IED e instaladores de aplicacións ICS, así como controis que impidan ou alerten sobre **execución de binarios** e cambios non autorizados.

**e) Mellorar visibilidade e detección en OT con enfoque a comportamento.** Ademais de IoCs, é necesario observar patróns como comunicacións anómalas cara a internet desde activos inesperados, uso inusual de protocolos e sinais de movemento lateral ou acceso a repositorios de documentación técnica.

### Implicación para gobernanza e investimento

A lectura agregada do informe reforza unha conclusión práctica: a mellora de ciberseguridade industrial en Galicia require combinar **medidas de prevención** (exposición, identidades, segmentación) con **medidas de resiliencia** (capacidade de detección e recuperación). Isto é especialmente relevante en sectores con dependencia de continuidade de operación —enerxía, auga, alimentación, manufactura e loxística— onde o impacto dun incidente transcende o ámbito tecnolóxico e pode derivar en custos operativos, reputacionais e de prestación de servizos esenciais.



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

# 3 Intelixencia de ameazas

## 3.1 Actores de ameaza e TTPs

A comprensión do risco en OT/ICS require ir máis aló da enumeración de vulnerabilidades ou do rexistro de incidentes: cómpre identificar **quen** opera (actores de ameaza), **como** opera (Tácticas, Técnicas e Procedementos – **TTPs**) e **con que intención e capacidade** pode progresar cara ao impacto sobre o proceso industrial. Nesta sección introdúcese unha lectura estruturada do panorama de ameazas, combinando fontes institucionais e de intelixencia (p.ex., organismos nacionais e equipos de *threat intelligence*) con marcos técnicos que permiten describir de forma consistente as accións do adversario ao longo do ciclo de ataque.

Preséntanse por tanto, as principais achegas das fontes seleccionadas (CCN-CERT, intelixencia de fabricantes e provedores, e análises especializadas), para culminar nunha síntese orientada a contornos industriais: **que vectores predominan**, que técnicas se repiten, e que sinais permiten anticipar unha posible evolución desde intrusións en IT cara a escenarios de **impacto ciberfísico** en OT/ICS.

### 3.1.1 CCN-CERT

Esta sección sintetiza a visión do **CCN-CERT** [1] en base ao informe xa vinculado en bibliografía, sobre actores de ameaza, combinando **a perspectiva estratéxica por Estado coa identificación dos principais grupos de ciberameaza (APT, clusters e colectivos)** que operan aliñados ou en apoio de devanditos Estados. Mantense así unha dobre lectura: por unha banda, os **obxectivos, motivacións e patróns xerais por país**, e por outro, os **grupos concretos** que materializan estas campañas, con especial atención ao seu impacto potencial en **contornos ICS/OT**. Comezaremos cos actores estatais.

**Federación Rusa**

Desde unha perspectiva estratéxica, Rusia mantén unha **actividade sostida e multifacética** no ciberespazo, combinando **ciberespionaxe, operacións de influencia, sabotaxe e apoio a campañas de hacktivismo**. O CCN-CERT subliña que o foco ruso diríxese de forma recorrente a **infraestruturas críticas, administracións públicas, defensa, enerxía, transporte e industria**, especialmente no contexto do conflito en Ucraína e as tensións coa UE e a OTAN.



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

Esta estratexia materialízase a través de **grupos de ciberamenaza ben establecidos**, entre os que destacan:

- **APT28 (Fancy Bear)** e **APT29 (Cozy Bear)**, con campañas de espionaxe dirixidas a gobernos, organismos internacionais e sectores estratéxicos.
- **Turla** e **Snake**, orientados a intrusións persistentes e de alto sixilo.
- **Sandworm (Unidade 74455 do GRU)**, especialmente relevante para contornos **ICS/OT**, polo seu historial de ataques disruptivos contra redes eléctricas, sistemas industriais e servizos esenciais.

No eido OT, o risco non se limita a ataques destrutivos directos, senón tamén a **intrusións previas, recoñecemento e preposicionamento** en redes industriais, que poden activarse en momentos de escalada xeopolítica.

**República Popular China**

China centra a súa actividade no **ciberespionaxe a gran escala**, cunha clara énfase na **obtención de propiedade intelectual, segredos industriais e vantaxe tecnolóxica**. O informe do CCN-CERT sinala que os sectores máis afectados inclúen **industria avanzada, enerxía, telecomunicacións, transporte e tecnoloxías estratéxicas**, o que sitúa ás contornos ICS/OT como obxectivos de alto valor.

Esta estratexia articúlase a través de múltiples grupos, entre os que destacan:

- **APT41**, coñecido por combinar espionaxe estatal con actividades de cibercrime.
- **APT31** e **APT17**, activos contra administracións públicas e empresas tecnolóxicas.
- **Mustang Panda**, con campañas persistentes contra gobernos e sectores industriais.

No contexto industrial, estas campañas adoitan buscar **acceso prolongado e silencioso**, explotando vulnerabilidades en produtos amplamente despregados, cadeas de subministración e provedores tecnolóxicos, máis que causar disrupcións inmediatas.

**Corea do Norte**

Corea do Norte combina **ciberespionaxe, cibercrime financeiro e operacións encubertas** como ferramenta de financiamento do réxime e evasión de sancións. O CCN-CERT destaca o seu interese en **sector financeiro, industria, enerxía e defensa**, con implicacións indirectas para contornos OT.



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

Os principais grupos asociados inclúen:

- **Lazarus Group**, coñecido por ataques de alto impacto, ransomware e sabotaxe selectiva.
- **Kimsuky** e **Andariel**, orientados a espionaxe e obtención de credenciais.

Aínda que moitas campañas se orixinan en contornos IT, o acceso a **redes corporativas de organizacións industriais** pode facilitar movementos laterais cara a sistemas OT mal segmentados.

**Irán**

Irán mantén unha actividade crecente, caracterizada por **espionaxe rexional, sabotaxe selectiva e operacións de represalia**. O CCN-CERT identifica como obxectivos prioritarios os sectores de **enerxía, auga, transporte e industria**, o que confire a OT un papel central.

Entre os grupos máis representativos atópanse:

- **APT33**, historicamente vinculado a ataques contra enerxía e aviación.
- **APT34 (OilRig)** e **APT35**, con campañas de espionaxe prolongadas.
- **MuddyWater**, especialmente relevante pola súa actividade contra organismos gobernamentais e empresas industriais.

Estes actores demostraron interese en **sistemas de control industrial e redes híbridas IT/OT**, combinando técnicas relativamente simples cunha alta persistencia.

**Outros actores estatais**

O informe tamén recolle actividade atribuída a outros Estados, como **India** ou **Israel**, xeralmente cun alcance máis limitado e focalizado en **espionaxe estratéxica e rexional**. A continuación, un gráfico para ilustrar quen son maioritariamente o obxectivo destes ataques:



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


*Obxectivo de campañas de espionaxe. Fonte: CCN-CERT (2024)*

Aínda que o seu impacto directo en OT é menor, estas operacións poden afectar a **provedores tecnolóxicos e cadeas de subministración industriais**.

**Hacktivismo**

O **hacktivismo** ocupa un papel destacado no panorama actual, especialmente dende 2022. O CCN-CERT diferenza entre campañas de **baixo impacto técnico pero alta visibilidade** e outras con maior capacidade de disrupción.

Desde unha visión xeral, o hacktivismo caracterízase por:

- **Motivación ideolóxica e xeopolítica**.
- Emprego intensivo **de DDoS, defacement e filtracións de información**.
- Coordinación a través de canles públicas (Telegram, foros).

Nos últimos anos emerxeron colectivos claramente aliñados con intereses estatais, entre eles:

- **Killnet** e **NoName057(16)**, activos contra países europeos e sectores críticos en apoio a narrativas prorrusas.
- Alianzas temporais entre grupos, que incrementan a escala e frecuencia dos ataques.

Aínda que estas campañas adoitan dirixirse a **servizos dixitais e portais web**, a súa relevancia para ICS/OT radica en varios factores: dependencia de **servizos IT para a operación industrial**, impacto reputacional e presión social, e risco de **efectos colaterais** cando os ataques afectan a provedores ou infraestruturas compartidas.



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

En conxunto, a combinación de **estratexias estatais** e **grupos de ameaza concretos** reforza a idea de que as contornos industriais deben considerarse obxectivos lexítimos dentro do ciberconflicto moderno, non só polo seu valor operativo, senón tamén pola súa importancia económica, social e xeopolítica.

### 3.1.2 Microsoft Threat Intelligence

A continuación, a referencia máis actualizada de MS na súa Digital Report 2025 [2], sobre as consideracións anteriores dos estados nación que achegaba o CCN-CERT.

**Rusia**

Microsoft confirma que **Rusia mantén un uso intensivo do ciberespazo como ferramenta estratéxica**, combinando espionaxe, operacións de influencia e actividades disruptivas. En liña co CCN-CERT, obsérvase unha **priorización de infraestruturas críticas, administracións públicas, defensa e sectores enerxéticos e de transporte**, especialmente no contexto do conflito en Ucraína e os seus efectos colaterais sobre Europa.

Desde a óptica de Microsoft, resulta relevante a **crecente converxencia entre operacións de ciberseguridade e obxectivos cinéticos**, así como o uso de **grupos con distintos niveis de sofisticación**, desde APT altamente capacitados até colectivos hacktivistas ou criminais que actúan como forza de presión complementaria. Para contornos ICS/OT, esta combinación incrementa o risco de **ataques oportunistas e disruptivos** contra servizos esenciais, mesmo cando o obxectivo principal non sexa industrial.

**China**

Microsoft describe a China como un actor **altamente persistente e orientado ao ciberespionaxe estratéxica a longo prazo**. O foco principal segue a ser a **obtención de información sensible, propiedade intelectual e coñecemento tecnolóxico**, con campañas prolongadas e de baixa visibilidade.

O valor engadido do informe de Microsoft reside en subliñar a **amplitude sectorial dos obxectivos**, incluíndo telecomunicacións, administracións públicas, provedores de servizos dixitais e sectores industriais avanzados. No eido ICS/OT, este enfoque reforza a idea de que **o acceso a redes IT pode ser un paso intermedio** cara a contornos industriais, especialmente en organizacións con forte dependencia tecnolóxica ou cadeas de subministración complexas.



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

**Corea do Norte**

Actor singular, onde **a motivación económica e a evasión de sancións** teñen un peso comparable á espionaxe. Mantense o uso de campañas dirixidas contra sectores financeiros, tecnolóxicos e empresas con capacidade de xerar ingresos directos ou indirectos.

O informe de Microsoft achega contexto adicional sobre a **profesionalización destas operacións** e a súa escalabilidad, o que incrementa o risco de efectos colaterais en contornos industriais, especialmente cando organizacións OT dependen de servizos IT, provedores externos ou infraestruturas dixitais compartidas.

**Irán**

Caracterízase a Irán como un actor **máis orientado a operacións disruptivas, de influencia e de presión política**, cun nivel técnico xeralmente inferior ao de Rusia ou China, mais compensado por un uso intensivo de técnicas coñecidas e ataques oportunistas.

Para ICS/OT, esta converxencia de análise reforza a percepción de risco fronte a **ataques de baixa sofisticación técnica pero alto impacto operativo**, especialmente en sectores enerxéticos, transporte e servizos públicos, onde a dispoñibilidade é un factor crítico.

### 3.1.3 ENISA

#### 3.1.3.1 Panorama xeral

No informe Threat Landscape 2025 de ENISA, recóllense as **Tácticas, Técnicas e Procedementos (TTPs) máis comunmente observados**, de maneira informal (i.e. sen asignar código da matriz de MITRE) [3].

Durante o período analizado, **os grupos de cibercrime evolucionaron de forma continua as súas TTPs**, cunha énfase clara na **madurez dos ecosistemas ransomware** e no **endurecemento das tácticas de presión sobre as vítimas**. Mantense a reutilización de builders filtrados, como no caso de SafePay —derivado de LockBit 3—, e prevese que a publicación do código fonte de VanHelsing RaaS reduza aínda máis as barreiras de entrada ao cibercrime, facilitando a aparición de novos operadores.



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

En paralelo, os **mecanismos de distribución de malware**, especialmente infostealers, diversificáronse. Aos vectores clásicos (software pirata, phishing ou repositorios públicos de código) súmanse **métodos de baixo custo e alto alcance**, como falsos CAPTCHA, servizos de aloxamento na nube ou enlaces embebidos en plataformas de vídeo, o que incrementa notablemente a superficie de exposición, tamén para organizacións con contornos OT conectados indirectamente a IT.

Un cambio especialmente relevante é o **uso sistemático de ferramentas deseñadas para desactivar solucións EDR**, co obxectivo de realizar intrusións máis sigilosas e centradas na exfiltración rápida de datos. Ferramentas como AvNeutralizer (AuKill), EDRKillShifter ou técnicas baseadas en drivers asinados —como ABYSSWORKER— foron adoptadas progresivamente por múltiples esquemas RaaS activos na UE. Esta tendencia reforza o risco para contornos industriais Windows-based, habituais en capas de supervisión e operación.

En canto á **extorsión**, novas familias como Fog e Qilin intensificaron tácticas agresivas, incorporando contadores regresivos, perfís públicos de vítimas, mostras descargables e, no caso de Qilin, mesmo funcionalidades que simulan escaladas a procedementos legais ("call lawyer"). No contexto europeo, estas tácticas resultan especialmente eficaces debido ás **obrigacións regulatorias e de notificación (GDPR, NIS2)**, que incrementan a presión para pagar rescates.

Máis aló do ransomware, obsérvase unha **diversificación do cibercrime cara a fraudes complexas**, como os esquemas de pig-butchering (estafas traballadas no tempo), que creceron preto dun 40% interanual e xeran entre 9,1 e 11,4 millóns de euros a escala global. Estas campañas combinan **enxeñaría social prolongada, criptomonedas, IA xerativa e deepfakes**, e xa afectan de forma significativa a cidadáns e organizacións da UE. As operacións policiais recentes mostran a escala industrial destas redes, con millóns de dispositivos e credenciais comprometidas.

Finalmente, emerxe unha dimensión especialmente preocupante: a **translación do impacto dixital ao plano físico**, con ataques directos —incluídos secuestros— contra titulares de criptoactivos e as súas familias, vinculados a filtracións de datos de plataformas centralizadas. Casos documentados en varios Estados membros evidencian como o cibercrime está cruzando a fronteira entre o dixital e o físico, un risco que resulta particularmente crítico para sectores industriais e operadores de infraestruturas esenciais.



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

Nunha sección posterior refírense aos TTPs asociados a hacktivismo. Durante o período analizado, o **hacktivismo mostrou unha clara evolución desde campañas principalmente disruptivas cara a modelos híbridos**, incorporando **tácticas propias do cibercrime organizado** e ampliando de forma explícita o seu foco cara a **contornos OT e infraestruturas críticas**.

No ámbito dos **ataques DDoS**, os grupos hacktivistas adoptaron **TTPs máis avanzadas**, combinando técnicas como o carpet bombing, o uso masivo de routers comprometidos e, de forma crecente, **capacidades apoiadas en IA** para incrementar a intensidade, persistencia e alcance dos ataques. Os datos de Netscout para o primeiro semestre de 2024 mostran un **incremento do 50 % en dispositivos infectados**, impulsado principalmente pola aparición do botnet Zergeca e a evolución do botnet DDoSia, empregado por NoName057(16), que destaca polo uso **de DNS over HTTPS (DoH)** como canle de mando e control, dificultando a súa detección.

Un fenómeno especialmente relevante é a **converxencia entre hacktivismo e ransomware**, particularmente entre grupos prol-rusos. Colectivos como **CyberVolk's, Azzasec, Funksec ou Lapsus**$ pasaron de campañas ideolóxicas a **modelos de ransomware-as-a-service (RaaS)**, mentres que **KillSecurity**, orixinalmente aliñado con Anonymous, consolidouse como actor relevante tras lanzar a súa propia plataforma RaaS en xuño de 2024. Desde entón, este grupo dirixiu ataques contra múltiples Estados membros da UE, con picos de actividade observados en 2025. Esta evolución confirma que o hacktivismo xa non se limita á disrupción simbólica, senón que procura **beneficios económicos e persistencia operativa**.

En paralelo, os **ataques contra OT** convertéronse nun elemento central do discurso e a actividade hacktivista. Destaca o caso **de Z-PENTEST-ALLIANCE**, que reivindicou ataques contra **interfaces de xestión OT expostas a Internet** en sectores como **enerxía e auga**, cun alcance xeográfico amplo na UE. Países como **Italia, Chequia, Francia e España** figuran entre os máis afectados. Aínda que estes incidentes non provocarían impactos operativos significativos, a **difusión de vídeos mostrando a manipulación de sistemas OT** apunta claramente a un obxectivo de **impacto psicolóxico, propagandístico e disuasorio**, máis que á interrupción efectiva de procesos.

Z-PENTEST-ALLIANCE situouse como o **principal grupo hacktivista no targeting de infraestruturas críticas na UE**, cunha énfase crecente en sistemas enerxéticos. Dende



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

comezos de 2025, o grupo intensificou a súa retórica e as súas declaracións de intención contra OT, chegando mesmo a **atribuírse vínculos co grupo Sandworm**. No entanto, estas afirmacións non puideron verificarse e, polo momento, considéranse dubidosas, o que suxire posibles estratexias de **inflado reputacional ou** "**faketivismo**".

Finalmente, emerxe un novo vector de risco coa aparición en xuño de 2025 do grupo **Infrastructure Destruction Squad (IDS)**, que afirma desenvolver **VoltRuptor**, un malware específico para ICS con **soporte multiprotocolo, capacidades avanzadas de persistencia e técnicas antiforenses**. A suposta dispoñibilidade de VoltRuptor en mercados clandestinos e a reivindicación dun compromiso contra unha empresa italiana de automatización de edificios expoñen un **escenario de especial preocupación**, aínda que a ameaza é aínda demasiado recente para unha avaliación concluínte. Aínda así, a hipótese dunha **instrumentalización deste actor por intereses estatais** considérase plausible e reforza a tendencia **de difuminación entre hacktivismo, cibercrime e operacións de influencia con trasfondo xeopolítico**, con implicacións directas para a seguridade de contornos ICS/OT.

#### 3.1.3.2 TTPs

As **TTPs (Tactics, Techniques and Procedures)** das matrices MITRE ATT&CK describen como operan os adversarios: as **tácticas** reflicten os seus obxectivos, as **técnicas** os métodos xerais empregados e os **procedementos** os pasos concretos ou ferramentas utilizadas [4][5].

A partir de fontes abertas, o conxunto de datos de ENISA céntrase principalmente en **actividades posteriores ao compromiso**, destacando especialmente as fases de **recoñecemento**, **mantemento do acceso** e **execución de cargas maliciosas** tras a intrusión inicial. En comparación, as tácticas asociadas a **impacto**, **exfiltración** e **colección** aparecen con menor frecuencia.

A nivel de técnicas, a análise revela **patróns recorrentes de uso conxunto**, que se reflicten nunha **visualización agrupada de TTPs**. Un primeiro bloque claramente definido corresponde ás **técnicas de descubrimento**, como a identificación de procesos, configuración de rede, información do sistema, ficheiros, directorios e recursos compartidos, o que evidencia a fase sistemática de inventariado que realizan os atacantes unha vez dentro do contorno.

Un segundo grupo relevante concéntrase nas **técnicas de execución**, dominadas polo uso de **intérpretes de comandos e scripting**, xunto con mecanismos como WMI, APIs



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

nativas, execución mediante servizos e accións iniciadas polo usuario. Estas técnicas reflicten a preferencia dos adversarios por **mecanismos lexítimos do sistema operativo**, que facilitan a evasión e reducen a detección.

A **persistencia** aparece como outro bloque cohesionado, combinando o uso de servizos de Windows, modificacións no rexistro, mecanismos de autoarranque e a **creación ou abuso de contas válidas**, o que demostra como os atacantes **superpoñen múltiples métodos de permanencia** para asegurar o acceso a longo prazo.

Finalmente, aínda que con menor peso, identifícanse bloques coherentes asociados a **exfiltración de información** e **técnicas de impacto**, que inclúen distintos métodos de transferencia de datos e accións orientadas á interrupción, degradación ou manipulación de sistemas.

Neste punto resulta pertinente **inserir a gráfica de TTPs que proporciona ENISA**, que permite apreciar de forma intuitiva como estas técnicas tenden a se agrupar arredor de fases concretas do ciclo de ataque, permitindo comprender os patróns operativos máis habituais observados nesta análise.


*TTPs máis vistos nos incidentes analizados. Fonte: ENISA (2025)*



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

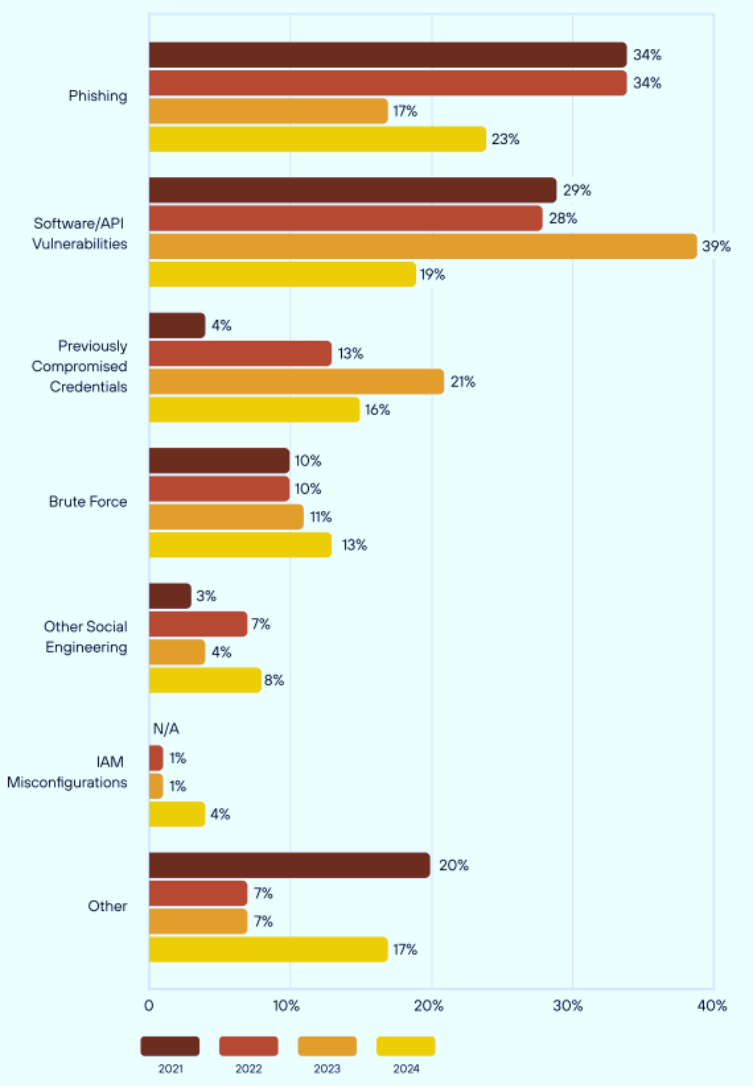
Cabe destacar que no anexo 12.1 deste informe de ENISA, inclúese **unha táboa con todas as tácticas, técnicas e mitigacións asociadas**, para referencia do lector que queira profundar na cuestión.

### 3.1.4 Unit 42 Palo Alto Networks

No informe **de Unit 42 de Palo Alto** [6], aparecen un par de figuras interesantes relativas ao punto inicial de ataque dos adversarios, así como unha tendencia a este respecto para os últimos catro anos:

| 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. Fonte: Palo Alto Networks (2025)*



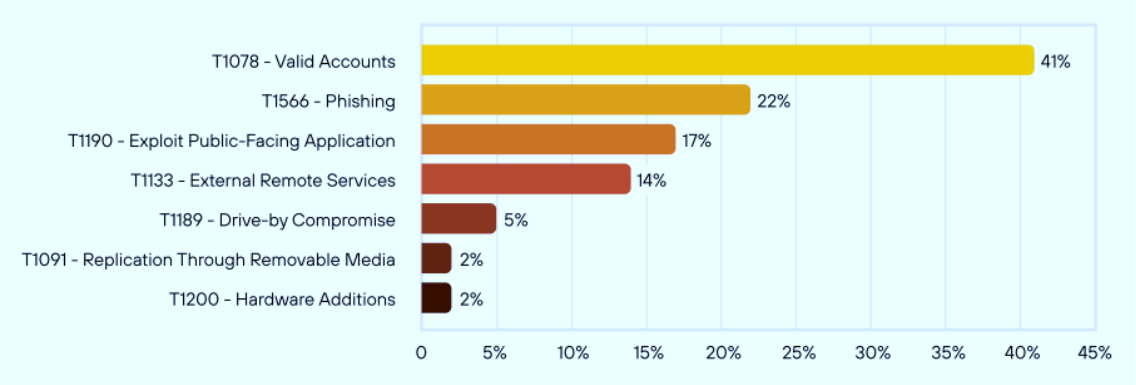

*Tendencia do punto de entrada inicial dos ataques. Fonte: Palo Alto Networks (2025)*

Identifican ademais unha consolidación **de TTPs** "**living off the land**", onde os atacantes priorizan o abuso de **mecanismos lexítimos** fronte ao uso de malware complexo, reducindo así a detección e facilitando a persistencia.

Unha das tendencias máis destacadas é o uso **de T1078 – Valid Accounts** como **vector principal de acceso inicial**, representando máis do 40 % das técnicas asociadas a esta táctica (máis detalle na figura seguinte). Este patrón vese favorecido por **debilidades estruturais na xestión de identidades e accesos**, como a ausencia de MFA, o uso de contrasinais débiles ou reciclados, controis insuficientes fronte a forza bruta e **permisos excesivos** en contas comprometidas. Esta técnica é especialmente relevante en contornos híbridos IT/OT, onde as credenciais válidas permiten pivotar cara a redes industriais mal segmentadas.



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




*Prevalencia das técnicas observadas respecto da táctica de acceso inicial. Fonte: Palo Alto (2025)*

Na fase de execución, a técnica dominante é **T1059 – Command and Scripting Interpreter**, presente en máis do 60 % dos casos asociados á táctica de execución. Os adversarios abusan **de PowerShell**, intérpretes nativos **de Windows e Unix**, así como shells específicos de aplicacións e dispositivos de rede, para realizar tarefas de recoñecemento, movemento lateral e despregamento de cargas, aproveitando ferramentas xa dispoñibles nos sistemas.

Para o **movemento lateral**, a técnica máis observada é **T1021 – Remote Services**, que aparece en máis do 86 % dos casos analizados para esta táctica. Os atacantes reutilizan credenciais lexítimas para autenticarse mediante **RDP**, **SMB** e **SSH**, reforzando a tendencia de explotación de servizos remotos internos en lugar de técnicas máis ruidosas.

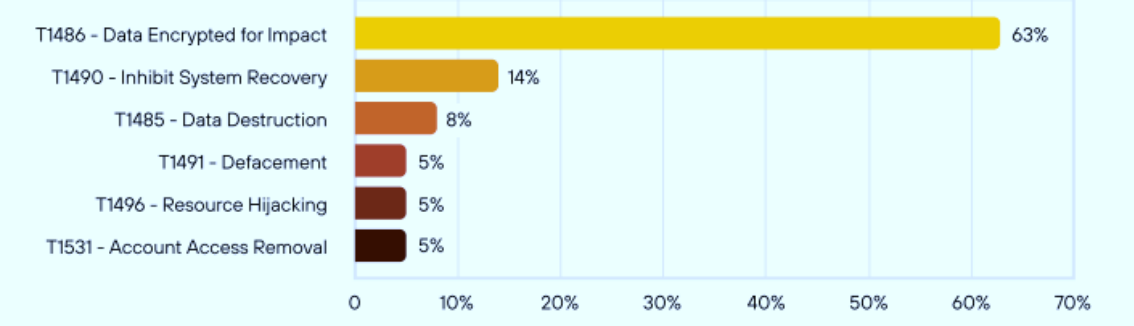
En paralelo, Unit 42 observa un aumento significativo de técnicas orientadas á **evasión de defensas**, especialmente **T1562 – Impair Defenses**, presente en cerca do 30 % dos casos analizados. Estas actividades inclúen **deshabilitar ou modificar ferramentas de seguridade**, **firewalls do sistema** e **rexistro de eventos de Windows**, co obxectivo de operar de forma máis sigilosa e acelerar a exfiltración de datos.

Finalmente, consolídase o uso do enfoque **BYOVD (Bring Your Own Vulnerable Driver)**, mediante o cal os atacantes introducen controladores vulnerables para obter privilexios elevados e **eludir EDR e outras proteccións**. Este patrón relaciónase estreitamente con técnicas como **T1543.003 – Create or Modify System Process: Windows Service** e **T1068 – Exploitation for Privilege Escalation**, evidenciando unha profesionalización crecente na manipulación do propio contorno defensivo.



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

Con respecto ás estratexias observadas asociadas á **táctica de impacto**, temos os seguintes resultados, que denotan a **prevalencia clara do ransomware sobre outros efectos maliciosos**:



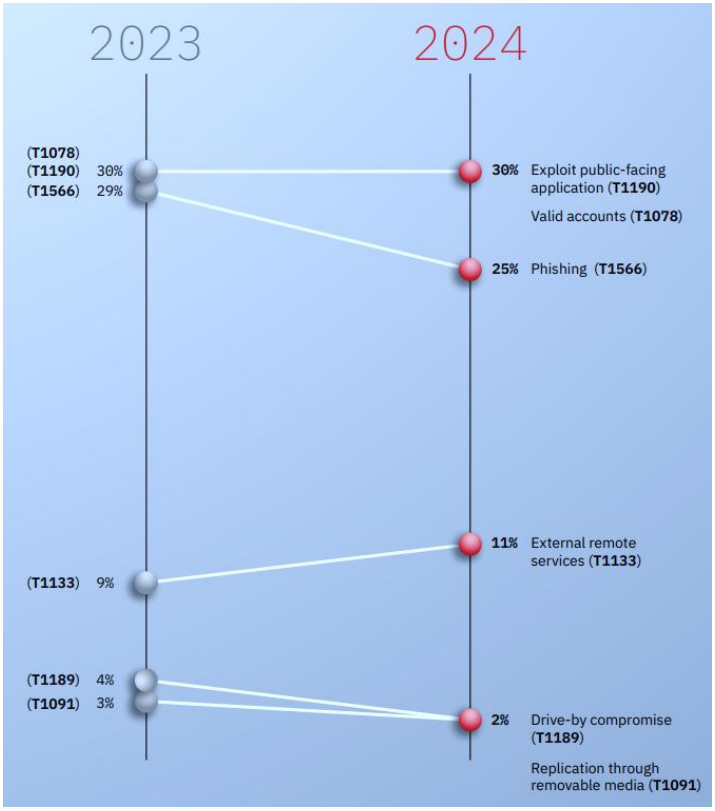

*Prevalencia das técnicas observadas respecto da táctica de impacto. Fonte: Palo Alto (2025)*

Estas tendencias mostran que en 2024 os atacantes priorizan **credenciais válidas, ferramentas nativas e técnicas de evasión**, combinándoas para acadar intrusións máis persistentes, rápidas e difíciles de detectar, con implicacións directas para organizacións con contornos IT e ICS interconectados.

### 3.1.5 IBM X-Force

En 2024, **IBM observa** no informe vinculado **unha consolidación clara dos accesos iniciais baseados en identidades e vulnerabilidades**, até o punto de que os **dous principais vectores de acceso inicial** foron, en igualdade de peso, a **explotación de aplicacións expostas a Internet (T1190)** e o **uso de contas válidas (T1078)**, **ambos cun 30** % dos casos de resposta a incidentes [7]. Esta realidade reforza a tendencia xa apuntada en anos anteriores: *os atacantes xa non "entran pola forza", senón que acceden con credenciais lexítimas*.

No gráfico que se mostra a continuación, reflíctese a evolución de técnicas de 2024 fronte a 2023 en canto a acceso inicial.




*Métodos utilizados polos actores de ameaza para obter acceso. Fonte: IBM X-Force (2025)*

O **abuso de credenciais** segue alimentándose dun ecosistema criminal moi activo. Os actores de ameaza obteñen contas válidas principalmente mediante **malware infostealer**, amplamente distribuído en campañas de phishing, así como a través da súa **compra e venda masiva en mercados clandestinos**. A pesar do crecemento na adopción **de MFA**, X-Force detectou en 2024 un aumento de **kits e servizos de phishing adversary-in-the-middle (AiTM)** deseñados especificamente para **eludir MFA**, o que confirma a madurez dun **mercado criminal de** "**access-as-a-service**".

O **phishing clásico (T1566)** continúa sendo relevante, pero perde peso relativo como vector directo de compromiso, representando **o 25 % dos incidentes en 2024**, fronte ao 29 % en 2023 e o 46 % en 2022. Esta caída atribúese á mellora das capacidades defensivas das organizacións, que logran bloquear con maior eficacia correos maliciosos, mesmo cando incorporan contidos xerados con IA. No entanto, o phishing non desaparece, senón que **evoluciona cara a un papel indirecto**, actuando como **vector** "**sombra**" **para o roubo de credenciais**.

Neste contexto, X-Force identifica un **cambio estratéxico clave**: o descenso de campañas masivas de malware persistente entregado por correo electrónico (como Emotet, TrickBot ou Qakbot) e un **forte aumento do uso de infostealers**, menos



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

visibles e máis rápidos. En 2024, o número medio semanal **de infostealers distribuídos por phishing creceu un 84 % respecto de 2023**, e os primeiros datos de 2025 apuntan a incrementos aínda maiores. Familias como **AgentTesla, FormBook, SnakeKeylogger e PureLogs** destacan entre as máis utilizadas.

Especial relevancia ten a actividade **de Hive0145**, un **initial access broker** centrado en Europa, que distribúe **Strela Stealer** co obxectivo específico de roubar credenciais de correo electrónico e facilitar **Business Email Compromise (BEC)**. Na segunda metade de 2024, este actor introduciu técnicas máis sofisticadas, como o "**attachment hijacking**" o secuestro de anexos, reutilizando correos lexítimos previamente roubados para aumentar a credibilidade e eficacia das súas campañas.

En conxunto, a análise de X-Force mostra un **desprazamento definitivo cara a ataques centrados en identidades**, con menos dependencia de malware persistente e unha maior explotación de **credenciais válidas, infostealers e técnicas de evasión de MFA**, configurando un escenario especialmente preocupante para organizacións con superficies de ataque amplas e contornos híbridos IT/OT.

A modo de peche desta sección, podemos dicir que a observación sistemática de TTPs recorrentes —especialmente en acceso inicial, persistencia e evasión— evidencia que **moitos incidentes poderían haberse contido de forma temperá se existise visibilidade axeitada sobre comportamentos anómalos en IT con impacto potencial en OT, como o abuso de credenciais válidas, o uso de ferramentas lexítimas de modo malicioso ou a manipulación de servizos e contas.**

Ademais, o cruzamento de información procedente de fontes diversas e reputadas, permite **identificar que técnicas están** a **ser máis utilizadas** en Europa e cales afectan con maior frecuencia a sectores industriais. **Isto facilita priorizar investimentos e esforzos** —por exemplo, en xestión de identidades, endurecemento de accesos remotos, detección de movementos laterais ou protección de activos ICS críticos— e avanzar cara a unha defensa baseada en comportamento e contexto operativo, máis **resiliente fronte á reutilización constante de TTPs por actores moi distintos entre si.**

### 3.1.6 Dragos

#### 3.1.6.1 Introdución e Cyber Kill Chain

A análise dos **grupos de ameaza específicos para contornos industriais (OT/ICS)** constitúe un dos elementos diferenciais máis relevantes da intelixencia especializada



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

achegada por Dragos no seu informe anual OT Cybersecurity Year in Review 2025 [8]. A diferenza doutros informes de carácter máis transversal —centrados en IT ou en ameazas globais—, Dragos mantén unha metodoloxía propia orientada á identificación, seguimento e caracterización de actores con **capacidade demostrada ou intención explícita de afectar sistemas de control industrial**, ofrecendo así unha lectura particularmente valiosa para operadores de infraestruturas críticas.

No período analizado, Dragos identifica **nove grupos de ameaza activos con relevancia para ICS/OT,** de nome clave: KAMACITE, MAGNALLIUM, PARISITE, VOLTZITE, WASSONITE, CHERNOVITE, ELECTRUM, GRAPHITE, BAUXITE. Os dous últimos son considerados **novas incorporacións en 2024**, o que evidencia a evolución dinámica do ecosistema de ameazas industriais e a entrada de novos actores con interese específico en sistemas ciberfísicos.

Ademais, o informe destaca que **tres destes grupos presentan capacidade na denominada "ICS Cyber Kill Chain Stage 2"**, é dicir, demostraron habilidades máis aló do acceso inicial a contornos IT, acadando fases de interacción directa ou impacto potencial sobre procesos industriais.

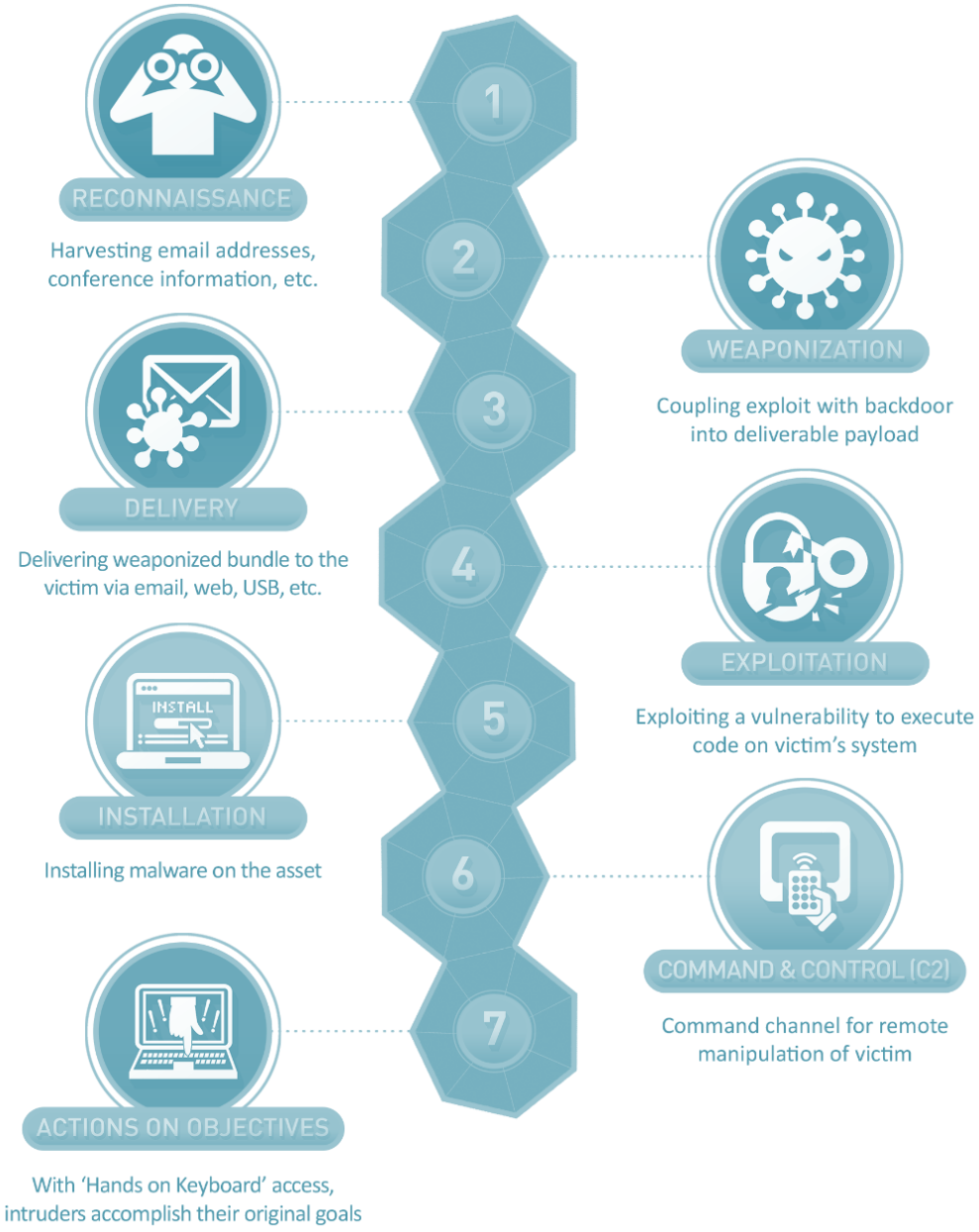

*Grupos de ameaza en ICS/OT identificados. Fonte: Dragos (2025)*

**A Cyber Kill Chain aplicada a ICS**

O concepto de **Cyber Kill Chain** foi formulado inicialmente por Lockheed Martin como un **modelo estruturado para describir as fases dun ataque dirixido (APT, Advanced Persistent Threat)**, desde a preparación ata a consecución do obxectivo final, como se ve na seguinte figura [9][10].



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




*Cyber Kill Chain. Fonte: Lockheed Martin (2011)*

A nivel operativo, o significado de cada fase é o seguinte:

1. **Recoñecemento (Reconnaissance)**: recompilación de información sobre a organización obxectivo, activos expostos, persoal clave e tecnoloxías empregadas.
2. **Armamento (Weaponization)**: preparación do artefacto malicioso que combinará vulnerabilidade e carga útil.



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

3. **Entrega (Delivery)**: transmisión do vector de ataque (correo electrónico, explotación web, acceso remoto, etc.).
4. **Explotación (Exploitation)**: execución da vulnerabilidade para obter acceso inicial.
5. **Instalación (Installation)**: establecemento de persistencia mediante malware ou modificacións do sistema.
6. **Comando e Control (C2)**: comunicación co atacante para recibir instrucións adicionais.
7. **Accións sobre o obxectivo (Actions on Objectives)**: execución do propósito final, como exfiltración, sabotaxe ou destrución.

Este modelo, amplamente adoptado no ámbito IT, foi posteriormente complementado por marcos como **MITRE ATT&CK** [4] e a súa adaptación específica para sistemas industriais, **MITRE ATT&CK for ICS** [5], que detallan tácticas e técnicas propias de contornos de control.

No ámbito industrial, a progresión do ataque non se detén na exfiltración de información. Pola contra, pode evolucionar cara á interacción directa con PLCs, RTUs, HMIs ou sistemas SCADA. Dragos, no seu traballo de **mapeo específico sobre ATT&CK para ICS** [11]**, introduce unha diferenciación relevante ao identificar o que denomina Stage 2 Capability dentro da ICS Cyber Kill Chain.**

Desde unha perspectiva metodolóxica, a adaptación ao ámbito ICS pode resumirse en dúas grandes fases operativas:

- **Stage 1 – Compromiso IT/Perímetro**: inclúe as etapas tradicionais de acceso inicial, movemento lateral, escalada de privilexios e consolidación de presenza dentro da rede corporativa. Moitos actores quedan nesta fase, limitándose a espionaxe ou extorsión.
- **Stage 2 – Interacción co proceso industrial**: implica a capacidade de pivotar cara á rede OT, identificar activos de control, comprender protocolos industriais (Modbus, OPC, DNP3, S7, etc.) e executar accións que alteren o funcionamento físico do proceso. Esta fase pode incluír manipulación de lóxica de control, modificación de parámetros operativos, degradación de sistemas de seguridade ou interrupción deliberada do servizo.



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

A relevancia da Stage 2 radica en que supón un salto cualitativo desde o impacto dixital ao **impacto ciberfísico**, afectando directamente á dispoñibilidade, integridade ou seguridade das operacións industriais. Non todos os actores con acceso IT posúen coñecemento técnico suficiente sobre enxeñaría de procesos ou protocolos industriais para completar esta fase.

**Desde o punto de vista da defensa, a desagregación da Kill Chain permite**:

- **Identificar** en que **fase pode interromperse o ataque**.
- **Priorizar medidas de segmentación** entre IT e OT.
- **Implementar detección específica** baseada en comportamento en redes industriais.
- **Aliñar controis técnicos coas técnicas máis empregadas segundo ATT&CK for ICS.**

Esta aproximación estrutural reforza os modelos de defensa en profundidade e permite avaliar con maior precisión o nivel de madurez dun actor de ameaza.

Na presente subsección abordanse agora os **nove grupos identificados por Dragos, describindo o seu perfil e orientación, sectores e xeografía obxectivo, actividad salientable e TTPs máis relevantes xunto a nivel de madurez operativa en contornos ICS.** Esta aproximación complementa a visión xeral ofrecida por outras fontes analizadas previamente, incorporando unha dimensión especializada **de interese para as organizacións galegas con exposición directa a sistemas industriais acaden un nivel de madurez que lles permita desenvolver actividades de caza de ameazas** (threat hunting).

#### 3.1.6.2 Grupos de ameaza

##### 3.1.6.2.1 KAMACITE

- **Perfil e orientación.** KAMACITE descríbese como un actor particularmente relevante por actuar, en múltiples operacións, como **provedor de acceso inicial**: establece pé en redes corporativas (IT) e **cede o control** a equipos con orientación máis destrutiva en OT, como ELECTRUM. O informe tamén sitúa a súa traxectoria en campañas disruptivas dirixidas contra infraestrutura eléctrica en Ucraína, e destaca unha evolución recente cara a novas familias de malware e un foco máis amplo.



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

- **Foco sectorial e xeográfico.** No período analizado, Dragos encadra o seu obxectivo principal en **Ucraína** e tamén en **Europa Oriental e Central**, con especial atención a organizacións de **electricidade** e **petróleo e gas**, así como entidades de **manufactura** e da **base industrial de defensa**.
- **Actividade e campañas salientables.** O informe recolle, entre outras, unha campaña asociada ao backdoor **Kapeka** (observada en 2022-2023 e identificada en 2024) contra operadores ucraínos de infraestrutura crítica, incluíndo entidades que fornecen **calor, auga e electricidade**. En paralelo, Dragos sinala o uso continuado de malware de natureza "commodity" en campañas de enxeñería social dirixida ou spear-phishing (p.ex., **DarkCrystal RAT**) para **vixilancia** e **roubo de información**.

  Adicionalmente, descríbese unha campaña de 2024 con temática vinculada á conferencia **Gas Infrastructure Europe (GIE)** en Alemaña, na que KAMACITE combinou *loaders* e *stealers* (p.ex., **LummaStealer**) cunha cadea de infección máis complexa que culmina nun backdoor Windows desenvolvido a medida (**Edam**), interpretada como un **xiro** desde un enfoque case exclusivo en Ucraína cara a obxectivos europeos no ámbito de petróleo e gas.
- **TTPs e capacidades observadas.** O patrón operativo salientado combina **enxeñería social** (spear-phishing e cebos temáticos), cadeas de execución baseadas en **PowerShell** e artefactos de *loader*/*dropper*, e o uso de infraestrutura de intermediación (p.ex., *proxies*). O informe chama a atención sobre a necesidade de dispoñer de telemetría suficiente para observar **tráfico norte–sur** (de entrada e saída na rede ICS/OT) e sinais de actividade anómala en contornos industriais.
- **Implicacións defensivas en OT/ICS.** Dragos vincula a mitigación efectiva a:
  1. **formación e concienciación** fronte ao phishing,
  2. **segmentación robusta IT/OT** para impedir a escalada cara a eventos disruptivos,
  3. e mellora da **visibilidade e detección** de patróns anómalos en redes de control (p.ex., interrupcións inusuais de conexións entre centros de control ou sondaxes anómalas sobre subestacións e estados de interruptores).



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

#### 3.1.6.2.2 MAGNALLIUM

A ficha deste grupo elabórase a partir da información dispoñible na web [26], pois non se amosa detalle no informe anual antes mencionado.

- **Perfil e orientación.** MAGNALLIUM preséntase como un actor activo dende polo menos 2013, centrado principalmente en **operacións de acceso inicial e recollida de información** contra organizacións industriais. Aínda que a súa actividade impacta en sectores críticos, non se identifica capacidade demostrada para interactuar directamente con sistemas ICS nin para executar accións de impacto físico en procesos industriais. O seu perfil encaixa nun actor orientado á intrusión en contornos IT con potencial de pivote, pero sen evidencia de progresión a fases avanzadas da ICS Cyber Kill Chain.
- **Foco sectorial e xeográfico.** MAGNALLIUM dirixiu historicamente as súas campañas contra **fabricantes petroquímicos e organizacións do sector enerxético**, con foco inicial en **Arabia Saudita** e posterior expansión cara a **Europa** e **Norteamérica**. Tamén se observaron actividades contra entidades industriais e do ámbito aeroespacial.
- **Actividade e campañas salientables.** As campañas atribuídas a MAGNALLIUM inclúen operacións de phishing dirixido empregando cebos relacionados con ofertas laborais e comunicacións corporativas, así como o uso de kits de phishing de terceiros. En etapas anteriores empregou familias de malware como variantes non destrutivas asociadas a StoneDrill e TURNEDUP, e dende 2018 observouse unha transición cara ao uso de ferramentas baseadas en PowerShell para tarefas de pos-explotación e mantemento de acceso. Non existen indicios no informe de interacción directa con redes de control industrial.
- **TTPs e capacidades observadas.** O patrón operativo descrito por Dragos inclúe:
    - **Phishing dirixido** con cebos personalizados.
    - **Password spraying** para comprometer credenciais corporativas.
    - Uso de ferramentas públicas ou semi-públicas para **captura de credenciais.**
    - Emprego de **scripts PowerShell para execución remota e persistencia** en contornos IT.

Non se documentan técnicas específicas orientadas a protocolos industriais nin accións asociadas a Stage 2 na ICS Cyber Kill Chain.

- **Implicacións defensivas en OT/ICS.** A mitigación fronte a MAGNALLIUM céntrase en reforzar controis na capa IT para evitar escaladas cara a OT:
    1. **autenticación robusta e monitorización** de intentos de password spraying,
    2. **formación fronte a phishing** dirixido,
    3. **segmentación efectiva** IT/OT,
    4. e **rexistro de actividade anómala** asociada a **ferramentas de administración remota e execución de scripts**.

#### 3.1.6.2.3 PARISITE

A ficha deste grupo elabórase a partir da información dispoñible na web [27], pois non se amosa detalle no Informe anual antes mencionado.

- **Perfil e orientación.** PARISITE introdúcese como un actor con actividade sostida contra organizacións industriais, cun enfoque principal en **operacións de espionaxe e obtención de información**. A diferenza doutros grupos con capacidade disruptiva, Dragos non atribúe a PARISITE capacidades demostradas de impacto directo sobre procesos industriais nin progresión a fases avanzadas da ICS Cyber Kill Chain. O seu comportamento encaixa nun actor orientado á obtención de acceso e á extracción de datos estratéxicos.
- **Foco sectorial e xeográfico.** As campañas atribuídas a PARISITE dirixíronse principalmente contra **sectores industriais e de infraestrutura crítica**, incluíndo **electricidade e petróleo e gas**, con actividade observada en **América do Norte, Europa e Oriente Medio**.
- **Actividade e campañas salientables.** PARISITE emprega campañas de intrusión que combinan técnicas de phishing dirixido e explotación de servizos expostos para obter acceso inicial. Unha vez dentro, céntrase na **recollida de información técnica, credenciais e documentación interna**, sen evidencias de manipulación directa de sistemas de control.
- **TTPs e capacidades observadas.** As técnicas documentadas inclúen:
    - **Phishing dirixido** con anexos ou ligazóns maliciosas.



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

- Explotación de **servizos accesibles desde internet**.
- Uso de **ferramentas lexítimas do sistema para movemento lateral** e execución remota.
- **Actividades de recoñecemento interno orientadas a inventariar activos** e identificar sistemas industriais.

Non se observan técnicas asociadas a manipulación de PLC, alteración de lóxica de control nin accións clasificables como Stage 2.

- **Implicacións defensivas en OT/ICS.** A defensa fronte a PARISITE require reforzar controis na capa de acceso inicial:
  1. **protección** fronte a **phishing,**
  2. **endurecemento de servizos expostos,**
  3. **monitorización** de movemento lateral,
  4. **e visibilidade sobre** intentos de **recollida masiva de documentación técnica.**

  A segmentación efectiva entre redes IT e OT continúa sendo un mecanismo clave para impedir que intrusións orientadas a espionaxe evolucionen cara a impactos operativos.

#### 3.1.6.2.4 VOLTZITE

- **Perfil e orientación.** Dragos cualifica VOLTZITE como un dos grupos máis relevantes a seguir en infraestrutura crítica polo seu foco persistente en **datos OT** e pola súa traxectoria en intrusións en rede con compoñentes de intelixencia operativa. O informe indica tamén **solapamentos técnicos** con Volt Typhoon segundo a nomenclatura doutros equipos de intelixencia.
- **Foco sectorial e xeográfico.** As actividades descritas afectan organizacións vinculadas a infraestrutura crítica e sectores con dependencia de información xeoespacial e operacións distribuídas; no informe aparecen, entre outros, **electricidade**, **petróleo e gas**, **auga e saneamento**, así como telecomunicacións, elementos satelitais ou de de defensa, así como outras **entidades gobernamentais**. O seu foco principal é **Norteamérica, Europa, Asia, África e Nova Zelandia.**



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

- **Actividade e campañas salientables.** O documento describe un conxunto de campañas nas que VOLTZITE comprometeu **routers de pequenas empresas** e empregou infraestrutura de terceiros como puntos de **pivotaxe**, co obxectivo de enumerar e alcanzar activos expostos en infraestrutura crítica. En campañas específicas, Dragos destaca a interacción con **GIS** (sistemas de información xeográfica) e o **roubo/exfiltración** de datos GIS, así como a obtención de **diagramas de rede OT** e instrucións operativas.
- **TTPs e capacidades observadas.** O patrón salientado combina:
    - **compromiso de dispositivos periféricos** para construír redes de *proxy/relay* controladas polo adversario,
    - **uso de esas redes para scanning e enumeración** de superficie exposta,
    - **e colección de información OT de alto valor** (GIS, topoloxías, instrucións), que potencialmente permitiría deseñar ferramentas específicas con capacidade disruptiva.
- **Implicacións defensivas en OT/ICS.** A defensa fronte a VOLTZITE require especial énfase en:
    1. visibilidade sobre **pasarelas de acceso remoto**,
    2. detección de **exfiltración de GIS** e documentación sensible,
    3. e control da exposición a internet de dispositivos e servizos susceptibles de seren reutilizados como pivote (incluíndo dispositivos de rede e accesos remotos en cadeas de subministración).

#### 3.1.6.2.5 WASSONITE

A ficha deste grupo elabórase a partir da información dispoñible na web [28], pois non se amosa detalle no Informe anual antes mencionado.

- **Perfil e orientación.** WASSONITE mencionase como un grupo de ameaza con actividade dirixida a organizacións industriais e de infraestrutura crítica, cun enfoque predominante en **intrusión e recollida de información**. Segundo a caracterización publicada, non se lle atribúe capacidade demostrada para executar accións disruptivas directas sobre procesos industriais (non consta progresión confirmada a Stage 2 na ICS Cyber Kill Chain).

- **Foco sectorial e xeográfico.** A actividade asociada a WASSONITE abrangue organizacións de **infraestrutura crítica**, incluíndo sectores como **electricidade, nuclear e manufactura**, con vítimas identificadas en diferentes rexións, especialmente en India, Corea do Sur e Xapón.
- **Actividade e campañas salientables.** As operacións atribuídas a WASSONITE céntranse en compromisos de acceso inicial a través de vectores tradicionais (como phishing ou explotación de servizos expostos) e posterior actividade de recoñecemento interno. O obxectivo principal observado é a **obtención de información técnica e credenciais**, así como a cartografía de redes con compoñentes industriais.
- **TTPs e capacidades observadas.** Entre os patróns descritos por Dragos inclúense:
    - Uso de **phishing dirixido** para capturar credenciais.
    - Explotación de **servizos accesibles desde internet**.
    - Emprego de ferramentas lexítimas do sistema para manter persistencia e realizar movemento lateral.
    - Actividade de **recoñecemento interno** orientada á identificación de activos OT e documentación asociada.

  Non se documentan interaccións directas con PLC nin manipulación de lóxica de control.
- **Implicacións defensivas en OT/ICS.** A mitigación fronte a WASSONITE céntrase en:
    1. **reforzar controis de acceso** inicial (protección fronte a phishing e endurecemento de servizos expostos),
    2. incrementar a **visibilidade sobre movemento lateral** en redes corporativas,
    3. e **manter unha segmentación efectiva IT/OT** que limite a progresión cara a sistemas de control.

#### 3.1.6.2.6 GRAPHITE

- **Perfil e orientación.** GRAPHITE é un dos dous grupos **introducidos como novidade** por Dragos en 2024. O informe vincúlao con campañas de interese

xeopolítico relacionadas coa situación militar en Ucraína e sinala **solapamentos técnicos** co clúster coñecido como APT28 noutras nomenclaturas. A súa relevancia para OT/ICS deriva do seu foco en entidades industriais e enerxéticas, aínda que Dragos indica que **non amosou capacidade Stage 2**.

- **Foco sectorial e xeográfico.** As vítimas confirmadas e obxectivos observados sitúanse en **Europa Oriental**, **Oriente Medio** e tamén en **Asia**, con afectación de sectores como **electricidade**, **petróleo e gas**, **loxística ferroviaria e de mercadorías**, **loxística aeronáutica** e **base industrial de defensa**, así como entidades gobernamentais.
- **Actividade e campañas salientables.** O informe documenta campañas de *spear-phishing* prolongadas (desde 2022 e especialmente ao longo de 2023-2024) dirixidas, entre outros, a operadores de **oleodutos/gasodutos** e a instalacións de **xeración hidroeléctrica**, cun obxectivo recorrente de **roubo de credenciais**. Nunha fase inicial, GRAPHITE explotou unha vulnerabilidade en **Microsoft Outlook** que permitía capturar datos de autenticación de Windows mediante anexos maliciosos, e en paralelo mantivo operacións de phishing con malware baseado en *scripts*.

  Noutras campañas descritas, o grupo utilizou sitios web maliciosos e ferramentas específicas para **phishing de credenciais**, incluíndo portais que imitaban servizos populares, e tamén combinou diferentes pezas de malware (p.ex., backdoors baseados en *batch* e backdoors en C#) para manter execución remota e persistencia.
- **TTPs e capacidades observadas.** Dragos subliña o uso dunha rede de **routers Ubiquiti Edge** comprometidos para distribuír malware e manter canles de **C2**, infraestrutura que permaneceu activa ata a súa interrupción en febreiro de 2024 polas autoridades americanas. A partir de 2024, observa un desprazamento cara ao uso de **servizos lexítimos de internet** para preparación de ataques (staging) e comunicacións.
- **Implicacións defensivas en OT/ICS.** Dado que o vector dominante é a intrusión en *Stage 1*, a prioridade defensiva céntrase en:

  1. endurecer e detectar **phishing dirixido**,



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

2. **elevar a hixiene de identidade** (incluíndo monitorización de roubos de credenciais e abuso de sesións),
3. e **reducir a exposición e confianza implícita en infraestrutura de rede de terceiros** que poida ser reutilizada para distribución de *payloads* e C2.

#### 3.1.6.2.7 BAUXITE

- **Perfil e orientación.** BAUXITE é o segundo grupo **novidoso en 2024** e preséntase como un actor con campañas centradas en OT/ICS e en dispositivos específicos. O informe sinala unha **aliñación técnica substancial** co ente hacktivista pro-iraniano **CyberAv3ngers**. Recolle que este último foi vinculada explicitamente co **goberno iraní,** cuxos membros foron sancionados, segundo o reporte da Administración dos Estados Unidos. BAUXITE aparece, ademais, como un actor que **investiga activamente: participa en foros orientados a OT/ICS e amosa interese por dispositivos OEM e por avisos de seguridade.**
- **Foco sectorial e xeográfico.** Sitúanse vítimas confirmadas en **Estados Unidos**, **Europa**, **Australia** e **Asia Occidental**, e identifica afectación en múltiples sectores: **electricidade**, **petróleo e gas**, **auga e saneamento**, **químico**, **alimentación e bebidas** e **manufactura**.
- **Actividade e campañas salientables.** Desde finais de 2023, Dragos observa **catro campañas** asociadas a BAUXITE, incluíndo operacións con **impacto Stage 2** na ICS Cyber Kill Chain mediante compromisos triviais de dispositivos expostos. O documento destaca unha pauta consistente de aproveitar **superficie exposta** e condicións de autenticación débiles, con accións orientadas a interromper ou degradar contornos industriais.
- **TTPs e capacidades observadas.** O informe reflicte un comportamento de recoñecemento e explotación apoiado en:
  - **seguimento intensivo de avisos de seguridade e vulnerabilidades** coñecidas en contornos industriais (máis detalle noutros informes do Observatorio [29]),
  - **interese por protocolos e ecosistemas OT/ICS**,
  - e **capacidade para executar accións disruptivas** cando existen accesos triviais (p.ex., servizos expostos e credenciais febles).



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

- **Implicacións defensivas en OT/ICS.** A proposta priorizaría controis directamente ligados á exposición:

    1. identificar activos con **SSH** accesible desde internet e **ocultar o acceso tras VPN**,
    2. verificar que cando existan accesos SSH, non se empreguen **contrasinais por defecto** ou doadamente adiviñables,
    3. e **auditar chaves SSH** (eliminar chaves innecesarias e rexerar as existentes cando houbo exposición).

    Esta liña de mitigación é coherente coa natureza oportunista de parte das campañas descritas.

#### 3.1.6.2.8 CHERNOVITE

A ficha deste grupo elabórase a partir da información dispoñible na web [30], pois non se mostran detalles no informe anual antes mencionado. CHERNOVITE inclúese no conxunto de grupos destacados por Dragos e aparece asociado a **capacidade Stage 2** na ICS Cyber Kill Chain segundo a clasificación empregada.

- **Perfil e orientación.** CHERNOVITE é un grupo de ameaza identificado por Dragos con capacidade para desenvolver **malware específico para sistemas de control industrial (ICS)**, orientado á **disrupción, degradación e potencial destrución de contornos industriais e procesos físicos**. O grupo está asociado ao desenvolvemento de **PIPEDREAM**, un marco modular de malware deseñado especificamente para atacar sistemas ICS. O sexto malware ICS coñecido tras STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, e TRISIS.
- **Foco sectorial e xeográfico.** Segundo Dragos, CHERNOVITE dirixe a súa actividade contra sectores críticos como **electricidade** e **gas natural licuado (LNG)**, así como outros contornos industriais que empregan PLC e tecnoloxías industriais amplamente implantadas. A natureza transversal de PIPEDREAM permite adaptar as súas capacidades a múltiples arquitecturas industriais.
- **Actividade e campañas salientables.** O elemento distintivo atribuíble a CHERNOVITE é como se indicou anteriormente, o desenvolvemento da ferramenta **PIPEDREAM**, considerada como unha das primeiras plataformas de malware ICS especificamente deseñadas para manipular dispositivos de control industrial máis aló de ferramentas IT tradicionais. Observaron este marco



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

malicioso en laboratorio e avaliaron as súas capacidades, mais non está confirmado o seu uso en operacións reais no momento da publicación, polo que podería ser deseñado por algún Estado Nación para posicionarse de cara a movementos futuros.

- **TTPs e capacidades observadas.** As capacidades descritas inclúen:
    - Desenvolvemento dunha plataforma de malware modular capaz de interactuar con protocolos industriais como **OPC-UA**, **Modbus** e contornos baseados en **CoDeSys**.
    - Capacidade de **escanear e interactuar con dispositivos PLC**, incluíndo captura de credenciais, intentos de forza bruta e potencial denegación de servizo.
    - **Ferramentas para intrusión e interacción con sistemas Windows e software de enxeñaría industrial** como parte da cadea de ataque.

  Estas capacidades permitirían manipular ou afectar PLCs e sistemas de control, situando a CHERNOVITE dentro do conxunto de actores con **potencial de progresión cara a Stage 2 na ICS Cyber Kill Chain.**
- **Implicacións defensivas en OT/ICS.** A existencia dun **grupo con capacidades de desenvolvemento de malware ICS como CHERNOVITE** reforza a necesidade de:
    1. **telemetría e detección de comportamento anómalo** en protocolos industriais,
    2. **inventario exhaustivo e visibilidade** sobre PLC e dispositivos de control,
    3. **segmentación estrita IT/OT e limitación de accesos** remotos,
    4. **e monitorización de actividade inusual en ferramentas de enxeñaría e software** asociado a control industrial.

#### 3.1.6.2.9 ELECTRUM

- **Perfil e orientación.** ELECTRUM é un dos grupos máis veteranos descritos, **responsable de múltiples ataques contra ICS e vinculado a un historial de operacións disruptivas**. O informe destaca a súa relación técnica con Sandworm noutras nomenclaturas e subliña que, aínda que en 2024 tivo menor

volume de actividade que KAMACITE, mantivo unha capacidade destrutiva salientable e recorreu a **personas hacktivistas** para ocultar operacións.

- **Foco sectorial e xeográfico.** Dragos encadra o seu foco principal en **Ucraína**, aínda que tamén observa interese por **empresas enerxéticas en Alemaña**. O sector **eléctrico** é central no seu perfil de risco.
- **Actividade e campañas salientables.** O informe describe un ciberataque contra o operador de telecomunicacións **Kyivstar** (decembro de 2023) que provocou interrupcións de servizo a escala nacional. Dúas personas hacktivistas pro-rusas reivindicaron a autoría con mensaxes practicamente idénticas; a análise de Dragos atribúe a operación a ELECTRUM e interpreta esa reivindicación como un mecanismo de **obfuscación** apoiado na reputación e recursos dunha desas personas.
- **TTPs e capacidades observadas.** A principal novidade técnica salientada é **AcidPour**, un wiper para sistemas Linux capaz de buscar e borrar directorios **UBI** en dispositivos embebidos, incluídos dispositivos presentes en contornos OT. Contextualízase como unha extensión de **AcidRain** (wiper empregado en 2022), salientando diferenzas de arquitectura obxectivo e a súa aptitude para causar **disrupción operativa**. **O informe tamén enfatiza que ELECTRUM demostrou capacidade para acadar Stage 2 (execución de ataque ICS) dentro da Kill Chain.**
- **Implicacións defensivas en OT/ICS.** As recomendacións asociadas céntranse en:

    1. limitar e monitorizar a capacidade de executar binarios en contornos de control: **limitar instalación de novos servizos, impedir cambios non autorizados,**
    2. **aplicar listas brancas de aplicacións** cando sexa viable,
    3. **monitorizar transferencias de ficheiros** cara á rede ICS
    4. **e, sobre todo, garantir copias de seguridade robustas e probadas** (lóxica de proxecto, configuracións de IED e instaladores de aplicacións ICS) almacenadas fóra de liña para acelerar a recuperación.



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

#### 3.1.6.2.10 Cadro resumo

Tras abordar o detalle individual de cada grupo, preséntase a continuación un **cadro resumo comparativo** que sintetiza as mais salientables características dos actores identificados polo fabricante desde unha perspectiva contextualizada para a industria galega. O obxectivo desta matriz non é reiterar a descrición técnica xa exposta nas fichas, senón ofrecer unha **lectura priorizada en termos de capacidade OT real, exposición sectorial en Galicia e nivel de risco estimado**, facilitando así unha interpretación executiva e orientada á toma de decisións.

A clasificación proposta integra tres dimensións fundamentais:

(i) a capacidade demostrada ou potencial de progresión na ICS Cyber Kill Chain, especialmente en relación co Stage 2,

(ii) a coincidencia entre os sectores obxectivo descritos por Dragos e os sectores industriais presentes en Galicia, e

(iii) a natureza do impacto observable (espionaxe, preparación de capacidades ou disrupción directa). Deste xeito, a matriz permite distinguir entre actores con risco estratéxico a medio prazo e aqueles cun impacto máis limitado ou circunscrito á capa IT.

| Grupo | Capacidade OT | Exposición sectorial Galicia | Nivel risco |
|---|---|---|---|
| **KAMACITE** | Broker IT (facilitador de pivote) | Transversal (enerxía, industria) | Medio |
| **MAGNALLIUM** | IT (sen capacidade OT demostrada) | Limitado | Baixo |
| **PARISITE** | IT espionaxe | Limitado | Baixo |
| **VOLTZITE** | Espionaxe OT e preparación de capacidades | Infraestruturas críticas (enerxía, auga, telecom.) | Medio |
| **WASSONITE** | IT con foco en infraestrutura crítica | Limitado | Baixo |
| **GRAPHITE** | IT avanzado con foco enerxético | Enerxía | Medio |
| **BAUXITE** | Stage 2 oportunista | Auga, alimentación, manufactura | Medio-Alto |
| **CHERNOVITE** | Malware ICS avanzado (potencial Stage 2) | Enerxía | Estratéxico |
| **ELECTRUM** | Alta (Stage 2 demostrado) | Enerxía eléctrica | Alto |

*Resumo de características principais dos actores de ameaza en ICS/OT identificados. Fonte: Dragos (2025)*



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

## 3.2 Intelixencia propia

**Os servizos de intelixencia de ameazas permiten anticipar, detectar e responder eficazmente a ciberataques.** Nesta sección preséntanse algúns elementos que permiten construír unha base de intelixencia operativa utilizando solucións abertas e colaborativas, especialmente orientadas a contornos ICS/OT.

**A combinación de fontes públicas** como ThreatFox, plataformas como MISP e OpenCTI, **e mecanismos de captura directa** de intelixencia como honeypots, **permite estruturar un ecosistema propio de vixilancia e análise que alimenta a defensa industrial de maneira bidireccional** (i.e. dende a comunidade de intelixencia á organización, e en sentido oposto).

A continuación, iremos introducindo conceptos e servizos asociados a esta capacidade.

**Indicadores de compromiso (IoCs)**

Os IoCs son evidencias técnicas que indican que un sistema, rede ou dispositivo pode ser comprometido por unha ameaza informática. En esencia, **un IoC é calquera dato que revela actividade maliciosa**, como direccións IP sospeitosas, dominios maliciosos, URLs, hashes de arquivos ou patróns anómalos de rede. En contornos industriais (ICS/OT), os IoCs poden incluír hashes de malware dirixido a PLCs, dominios de C2 asociados a ataques a sistemas SCADA ou anomalías en protocolos industriais.

**ThreatFox**

ThreatFox [12] é un proxecto de abuse.ch dedicado a **recompilar e compartir IoCs asociados a malware**. Funciona como unha plataforma onde investigadores e analistas publican indicadores como hashes, direccións IP ou dominios, consultables vía web ou APIs. A súa utilidade radica en que permite ás organizacións reforzar os seus sistemas defensivos e detectar actividades maliciosas en fases temperás. ThreatFox pode integrarse con outras plataformas de intelixencia, como MISP e OpenCTI, que veremos a continuación.

**MISP**

MISP (Malware Information Sharing Platform) [13] é unha **plataforma de código aberto para o intercambio estruturado de información de ameazas**. Permite almacenar, correlacionar e distribuír indicadores de compromiso, enriquecidos con contexto adicional. A través de MISP, os analistas poden automatizar o envío de datos

cara a outras ferramentas (como un SIEM ou IDS), xestionar eventos de seguridade e visualizar relacións entre incidentes.


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

Un recurso útil para familiarizarse coa plataforma, é a sesión formativa publicada en You Tube polo equipo de CIRCL (Computer Incident Response Center Luxembourg), pois son quen desenvolveron e manteñen a solución [14].

MISP fomenta a colaboración mediante **comunidades sectoriais** [15], onde os membros comparten intelixencia de forma privada. No ámbito industrial, destaca a comunidade **ICS-CSIRT.io**, un nodo dedicado a intelixencia de contornos ICS, ao que se recomenda adherirse.

Estas comunidades permiten recibir e achegar coñecemento útil en tempo real, fortalecendo así a defensa colectiva.

**MISP Galaxy**

MISP Galaxy [16] é un compoñente adicional de MISP que facilita a **etiquetación semántica dos eventos** mediante taxonomías predefinidas. Permite, por exemplo, asociar un IoC a un actor de ameaza coñecido, a un malware específico ou a unha técnica MITRE ATT&CK. Esta estrutura facilita a agregación de coñecemento e a identificación de patróns.

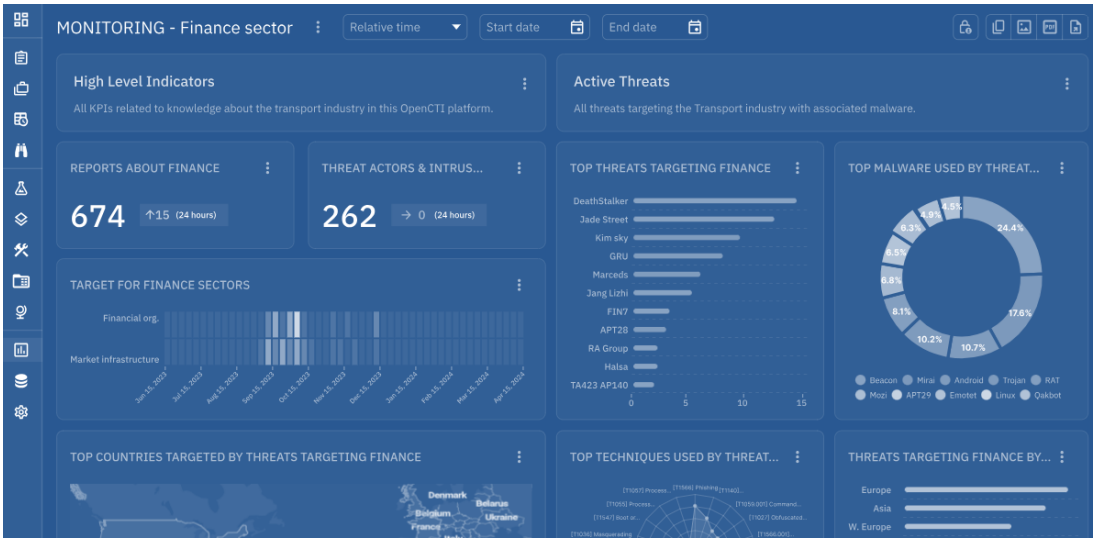


Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA
Xacobeo 2027

### OpenCTI

OpenCTI [17] é unha plataforma de código aberto deseñada para **xestionar, analizar e visualizar coñecemento estruturado sobre ameazas**. A diferenza de MISP, que se centra en eventos técnicos e IoCs, OpenCTI permite representar relacións entre actores, campañas, técnicas, malware e vulnerabilidades nun grafo de coñecemento baseado no estándar STIX2.

Existen versións comunitaria e comercial (esta última baixo a denominación comercial de filigran.io). En ambas as habilítase a integración con outras fontes e plataformas (incluídas MISP, TheHive ou MITRE ATT&CK), o que permite crear un núcleo de intelixencia contextual en tempo real.




*Captura de pantalla de OpenCTI. Fonte: filigran.io (2025)*

Cómpre aclarar que OpenCTI e MISP son altamente complementarios dentro dun sistema de intelixencia de ameazas.

- **MISP** céntrase na **xestión técnica de eventos e indicadores de compromiso (IoCs)**, facilitando o seu almacenamento, compartición e correlación estruturada. É ideal para automatizar a defensa baseada en sinais técnicos concretas.
- Pola súa banda, **OpenCTI** vai un paso máis aló ao permitir **modelar e visualizar o coñecemento contextual**: relacións entre actores, campañas, malware, técnicas e vulnerabilidades, seguindo o estándar STIX2.

Mentres que MISP é máis operativo e centrado na detección, **OpenCTI achega profundidade analítica e estratéxica**. Ambas as plataformas poden 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 a OpenCTI con datos técnicos, e OpenCTI enriquece eses datos con contexto.

**Integración con captura directa de intelixencia: honeypots**

As plataformas anteriores nútrense de fontes externas, pero tamén poden integrarse con **intelixencia propia capturada en campo**. Unha forma efectiva de xerar esta intelixencia é mediante honeypots: sistemas trampa que simulan infraestruturas reais para atraer e estudar ataques [18].

En contornos industriais, **Conpot** [19] é un de tantos posibles honeypots "out of the box" (empregables sen modificacións). Simula dispositivos industriais como PLCs e protocolos como Modbus, s7comm ou HTTP. Permite rexistrar patróns de acceso, intentos de explotación e comandos maliciosos dirixidos a infraestruturas críticas.

Mencionar que se prevé que futuras edicións deste informe poidan apoiarse en **tres honeypots despregados na infraestrutura de AMTEGA**, accesibles desde Internet e simulando ser equipos baixo diferentes protocolos de comunicación presentes en contornos industriais, co obxectivo de **capturar indicadores en tempo real**, analizar patróns de ataque e enriquecer o coñecemento dos informes con estatísticas propias de actividade dirixida contra sistemas ICS reais.

**IoCs, ataques e TTPs: da detección á atribución**

A detección dun IoC achega o sinal; os TTPs (Tácticas, Técnicas e Procedementos) explican o comportamento do atacante. A **matriz MITRE ATT&CK for ICS** [5] categoriza as técnicas ofensivas utilizadas especificamente contra sistemas industriais. Dragos, pola súa banda, estendeu esta lóxica coa súa propia matriz [11], onde cruza os IoCs observados cos TTPs documentados e os grupos criminais que identificaron coas súas fontes de intelixencia, facilitando así a atribución de ataques e a priorización de defensas.

Como se amosou, é posible **establecer un sistema eficaz de intelixencia de ameazas con ferramentas abertas e colaborativas**. A combinación de plataformas como ThreatFox, MISP e OpenCTI, xunto con mecanismos de captura directa como honeypots, permite construír un ecosistema operativo que non só consome, senón que tamén xera e distribúe intelixencia, e pode formar parte perfectamente do SOC da organización.

A clave está en entender que a **intelixencia é un proceso vivo**, que se retroalimenta de fontes internas e externas. Participar en comunidades MISP, manter activos honeypots



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

e enriquecer os eventos con contexto TTP/MITRE son accións que non só elevan o nivel de protección, senón que contribúen a mellorar a seguridade de todo o ecosistema industrial galego e global.



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

# 4 Recomendacións

Tras a análise dos múltiples informes de referencia e estudos sectoriais da bibliografía, pódese concluír que as recomendacións técnicas e estratéxicas emitidas polos diferentes fabricantes e organismos coinciden, en gran medida, no seu enfoque cara a unha ciberdefensa máis proactiva, adaptativa e resiliente. Aínda que moitas destas orientacións proveñen de provedores de solucións de seguridade e iso introduce certo sesgo de autopromoción, é posible extraer principios universais que transcenden as ferramentas concretas e céntranse en **prácticas, procesos e prioridades de seguridade**.

Este apartado recompila e sintetiza esas indicacións, co obxectivo de presentar **recomendacións aplicables e accionables**, especialmente en contornos con compoñentes OT/ICS. Comezaremos coas recomendacións dos informes de fabricantes de maneira agregada, poremos especial énfase nas propostas de entidades neutrais e de prestixio como **ENISA** e **CISA**, e complementarémolas con recursos técnicos seleccionados pola súa utilidade práctica, con independencia da solución tecnolóxica implementada.

A continuación, por tanto, preséntanse as principais liñas de actuación recomendadas.

### 4.1.1 Fabricantes de solucións de ciberseguridade

Os informes de fabricantes analizados ao longo deste estudo, ofrecen un amplo abanico de recomendacións para mellorar a postura defensiva das organizacións. A pesar da heteroxeneidade dos enfoques, pódense extraer **liñas estratéxicas comúns**.

1. **Reforzo da identidade e o acceso**

Unha constante en todos os informes é a **importancia crítica de protexer as identidades**. Insístese en aplicar autenticación multifactor robusta e resistente ao phishing (como chaves físicas), eliminar contas con privilexios innecesarios, consolidar plataformas de xestión de identidade, e reducir a proliferación de credenciais. IBM suxire avanzar cara a un "tecido de identidade" unificado que integre todos os dominios e sistemas. Microsoft e CrowdStrike, pola súa banda, recalcan que a identidade segue sendo o vector de ataque principal, polo que debe priorizarse o seu defensa. Este principio cobra aínda máis importancia en contornos industriais, onde accesos



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

privilexiados a interfaces de programación de autómatas ou consolas de enxeñaría deben estar debidamente controlados

2. **Visibilidade unificada e resposta avanzada**

A detección efectiva depende dunha **visión unificada do contorno de IT e OT**. Palo Alto destaca que moitas intrusións puideron haberse detectado se os sistemas estivesen ben integrados e as evidencias centralizadas. Recoméndase integrar telemetrías de endpoints, rede, nube, identidade e aplicacións nunha vista común, e complementar con analítica avanzada e detección baseada en IA para reducir o tempo medio de detección (MTTD) e resposta (MTTR). En redes industriais, cruzar a telemetría xerada por sensores, controladores lóxicos programables (PLC) e sistemas SCADA con datos do contorno IT permite detectar comportamentos anómalos e intrusións híbridas.

3. **Automatización e ciberintelixencia**

Para contrarrestar a rapidez coa que operan os atacantes, **a automatización da resposta é esencial**. CrowdStrike e Palo Alto coinciden en recomendar a integración de capacidades de automatización no SOC, así como o uso de intelixencia de ameazas en tempo real. Microsoft engade que esta intelixencia debe fluír cara aos procesos do equipo de seguridade para anticipar técnicas emerxentes. IBM subliña a importancia do uso proactivo da intelixencia mediante intercambio con terceiros e comunidades. En contornos ICS, o uso de plataformas *de threat intelligence* especializadas pode facilitar a resposta anticipada ante *malware* dirixido a protocolos industriais.

4. **Redución de complexidade e confianza implícita**

Un dos principais inimigos dunha defensa eficaz é a **complexidade tecnolóxica e organizativa**. Palo Alto indica que o uso de múltiples ferramentas non integradas impide detectar sinais clave. Recoméndase consolidar tecnoloxías, eliminar silos e aplicar os principios de Zero Trust para reducir a confianza implícita. Isto inclúe segmentar redes, verificar continuamente usuarios e dispositivos, e aplicar o principio de mínimo privilexio. En contornos OT, esta segmentación lóxica é fundamental para illar zonas críticas de produción das redes corporativas ou de mantemento remoto.

5. **Protección de contornos cloud e de desenvolvemento**

Os contornos cloud seguen sendo un obxectivo prioritario. Microsoft, Palo Alto e CrowdStrike destacan a necesidade de **integrar seguridade desde o desenvolvemento ("shift-left") até a execución**. Isto implica auditar a infraestrutura

cloud, protexer APIs, controlar accesos, aplicar detección e resposta en tempo real, e automatizar a contención de incidentes. Tamén se propón reforzar a seguridade na cadea de subministración software. Esta recomendación é extensible a sistemas OT modernos que incorporan servizos na nube para telemetría, actualizacións ou xestión de dispositivos remotos.

6. **Xestión de vulnerabilidades con enfoque baseado en risco**

Os atacantes priorizan vulnerabilidades coñecidas e accesibles publicamente. CrowdStrike aconsella adoptar un enfoque de **xestión de vulnerabilidades centrado no adversario**, combinando intelixencia externa, escaneo continuo, priorización baseada en criticidade e superficie exposta. Suxírese tamén integrar sinais sobre explotación activa e encadeamento de fallos para actuar de forma proactiva. En ICS, onde moitos sistemas son sensibles a actualizacións, este enfoque debe combinarse con medidas compensatorias como a detección baseada en sinaturas específicas ou o illamento de activos vulnerables. E lembremos o enfoque Now-Next-Never proposto por Dragos.

7. **Concienciación e preparación organizativa**

Todos os informes coinciden en que **o factor humano segue sendo un elo débil**. Recoméndase investir en formación periódica, exercicios de simulación, red teams e cultura de seguridade transversal. Microsoft lembra que a ciberseguridade debe ser un tema tratado ao máis alto nivel de Dirección. Estar preparado para incidentes inclúe contar con plans actualizados, ensaiar a súa execución e coñecer as debilidades propias antes de que o fagan os adversarios. En fábricas e contornos OT, onde o tempo de reacción pode determinar o impacto físico dun ataque, a coordinación entre ciberseguridade, produción e mantemento é vital.

8. **Consideracións emerxentes: IA e post-cuantum**

IBM e Microsoft alertan sobre os **riscos emerxentes da IA e a computación cuántica**. Recoméndase establecer gobernanza sobre os sistemas de IA, protexer os seus modelos e datos, auditar o seu funcionamento e anticipar escenarios de uso indebido. Tamén se insta a comezar a planificar a transición a criptografía post-cuántica mediante inventario de algoritmos e sistemas afectados. Para contornos industriais críticos, onde os sistemas poden ter ciclos de vida moi longos, anticipar esta transición é crucial para evitar futuros riscos de confidencialidade ou integridade.



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

Estas recomendacións, aínda que diversas en matices, converxen na necesidade de adoptar un enfoque proactivo, integrado e baseado en intelixencia para **anticiparse ás ameazas e resistir os seus impactos**.

### 4.1.2 ENISA

**ENISA, a Axencia da Unión Europea para a Ciberseguridade**, presenta un conxunto de recomendacións concisas de índole xeral. Estas diríxense principalmente aos responsables de formular políticas, reguladores e operadores de servizos esenciais, especialmente en sectores incluídos na Directiva NIS2.

- En primeiro lugar, avoga por **reducir a superficie de exposición** a ameazas de ciberseguridade, tanto coñecidas como emerxentes, cunha atención especial ao papel da intelixencia artificial. Subliña a necesidade de abordar os desafíos legais, técnicos e operativos que expón a IA, recomendando medidas como a integración de avaliacións de impacto de seguridade en sistemas que a empregan.
- En segundo lugar, insiste na importancia da **resiliencia operativa fronte a interrupcións prolongadas**, como as observadas en campañas de ransomware recentes. Isto implica mellorar as capacidades de resposta, conter os ataques e manter a continuidade de negocio ante ameazas disruptivas.
- Tamén salienta o reforzo do **marco de ciberseguridade para sectores críticos**. Isto pasa por aumentar a adopción de controis de seguridade avanzados, reforzar as capacidades técnicas de supervisión, e promover o intercambio de información entre os operadores. En liña con esta idea, recoméndase aos CERTs nacionais reforzar a súa visibilidade técnica e apoiar ás organizacións menos maduras.
- Sinálase a necesidade de **adaptar os plans de xestión de crise** a ameazas complexas como a combinación de campañas de desinformación con ciberataques. Proponse desenvolver manuais e simulacros de crises que contemplen estes escenarios híbridos, especialmente en momentos críticos como eleccións ou conflitos xeopolíticos.
- Por último, ENISA suxire consolidar mecanismos que faciliten unha **coordinación efectiva entre os Estados membros da UE**, tanto a nivel operativo como político. Isto permitiría unha resposta máis áxil e cohesionada

ante incidentes de ciberseguridade de gran escala que afecten a varios países asemade.

Alén, no seu informe "*Threat Landscape 2025*", sintetiza as súas **recomendacións de defensa en base ás TTPs observadas, agrupándoas en cinco alicerces fundamentais** que consolidan boas prácticas de hixiene de ciberseguridade. Estas recomendacións teñen como obxectivo previr o compromiso inicial, conter o impacto e dificultar o acceso persistente a longo prazo.

Nótese que as referencias a códigos M que se indican a continuación, corresponden ao MITRE D3FEND Framework [20] e ao MITRE ATT&CK para controis defensivos.

1. **Endurecemento do sistema (System Hardening)**

   Fortalecer a configuración do contorno operativa é esencial para reducir a superficie de ataque. ENISA propón medidas como:

   - Prevención de execución (M1038) e control de comportamento en endpoints (M1040).
   - Configuración segura de sistemas operativos (M1028), software (M1054) e Active Directory (M1015).
   - Restrición de permisos no rexistro (M1024), arquivos e directorios (M1022), e carga de librarías (M1044).
   - Mecanismos de validación como sinatura de código (M1045) e deshabilitación de funcións innecesarias (M1042).

2. **Control de acceso e privilexios (Access & Privilege)**

   As boas prácticas na xestión de identidades axudan a previr abusos:

   - Xestión de contas de usuario (M1018), contas privilexiadas (M1026) e control de contas (M1052).
   - Limitación de instalación de software (M1033).
   - Políticas de contrasinais robustas (M1027), autenticación multifactor (M1032) e uso controlado de contas (M1035).

3. **Protección de rede (Network Protections)**

   Estas medidas buscan evitar a comunicación maliciosa e os movementos laterais:



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

- Prevención de intrusión en rede (M1031) e filtrado de tráfico (M1037).
- Segmentación de rede (M1030) e restrición de contido web (M1021).
- Limitación do acceso a recursos a través de rede (M1048).

**4. Monitorización (Monitoring)**

A supervisión efectiva permite detectar ameazas de forma temperá:

- Auditoría de sistemas e actividades (M1047).
- Boas prácticas no desenvolvemento seguro (M1013).

Políticas de uso de contas e control de acceso en rede complementan a detección de análise de comportamento.

**5. Resiliencia (Resilience)**

Dado que algúns ataques terán éxito, a capacidade de recuperación é clave:

- Copias de seguridade (M1053) e almacenamento remoto de datos (M1029).
- Prevención de perda de datos (M1057) e cifrado de información sensible (M1041).
- Actualización de software (M1051) e uso de antivirus/antimalware (M1049)
- Formación de usuarios para identificar ataques de enxeñaría social (M1017).

Estas medidas forman unha estratexia integral que pode adaptarse tanto a contornos corporativas tradicionais como a contextos OT/ICS.

### 4.1.3 CISA

A Axencia de Ciberseguridade e Seguridade das Infraestruturas (CISA) é o organismo federal de EE. UU. encargado de coordinar a protección de infraestruturas críticas fronte a ameazas físicas e dixitais. A través da súa iniciativa de Seguridade en Sistemas de Control Industrial (ICS), **CISA proporciona orientación técnica, alertas e recomendacións específicas para operadores de infraestruturas OT**, baseadas en anos de experiencia e colaboración cos sectores público e privado.

Un dos seus recursos máis interesantes é o repositorio **de ICS Recommended Practices** [21], onde se agrupan **boas prácticas deseñadas para aumentar a resiliencia de contornos industriais.** Esta colección está composta por documentos relativamente

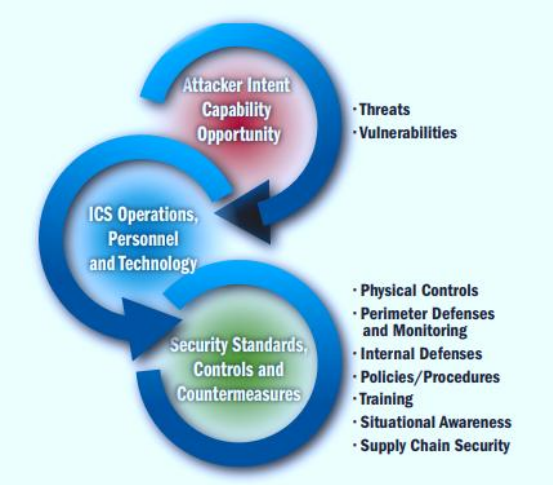
breves e accionables, que poden servir como base para fortalecer a seguridade desde distintos enfoques:

- **Updating Antivirus in an Industrial Control System**: boas prácticas para actualizar motores e asinas antivirus en contornos ICS sen comprometer a dispoñibilidade dos sistemas.
- **Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies**: guía para aplicar unha estratexia multicapa que combine medidas físicas, técnicas e organizativas para protexer infraestruturas industriais.
- **Creating Cyber Forensics Plans for Control Systems**: orientacións para definir plans de análise forense adaptados a ICS, preservando evidencias ante incidentes sen interromper procesos críticos.
- **Developing an Industrial Control Systems Cybersecurity Incident Response Capability**: pasos para establecer unha capacidade efectiva de resposta ante incidentes de ciberseguridade en sistemas de control.
- **Case Study: Cross-Site Scripting**: análise práctica dun incidente real de XSS nun contorno industrial, con leccións apresas e medidas de mitigación.
- **Patch Management of Control Systems**: pautas para a planificación, avaliación, validación e implementación segura de parches en contornos de control.
- **Securing Control System Modems**: recomendacións específicas para protexer os módems conectados a sistemas ICS, que adoitan representar vectores de entrada críticos.
- **Configuring and Managing Remote Access for Industrial Control Systems**: estratexias para habilitar o acceso remoto seguro a sistemas de control sen comprometer a integridade dos activos.
- **Cyber Security Procurement Language for Control Systems**: exemplos de cláusulas e requerimentos de ciberseguridade que poden incluírse en contratos de adquisición de tecnoloxía industrial.
- **Mitigations for Security Vulnerabilities Found in Control System Networks**: estratexias xerais para as mitigacións sen afectar á continuidade operativa.

#### 4.1.3.1 Estratexias de Defensa en Profundidade

Dado o seu carácter transversal e aplicabilidade xeral, analizaremos con maior profundidade o documento sobre **Estratexias de Defensa en Profundidade para mellorar a ciberseguridade de sistemas ICS** [22], por constituír unha referencia

fundamental tanto para organizacións que inician o seu camiño na protección de sistemas de control como para aquelas que buscan consolidar un marco de defensa multicapa sólido.




*Planificación de Defensa en Profundidade. Fonte: CISA (2016)*

Deseguido, describiremos os elementos principais da proposta: as estratexias de defensa en profundidade, e as recomendacións finais.

**Estratexias Defense-in-Depth**

- **Estratexia 1. Xestión de riscos en ICS:** integrar a xestión de risco específica dos sistemas de control industrial en todos os niveis da organización. Isto implica entender os riscos de negocio asociados ó contorno ICS e aliñalos coa tolerancia de risco empresarial. Coñecer as ameazas, procesos operativos e requirimentos únicos permite implantar un enfoque multinivel de monitorización e defensa continua nas operacións diarias. Como ilustra a figura seguinte, as organizacións deben aplicar controis ao nivel de seguridade axeitado e despois **monitorizar e axustar** eses controis continuamente contra ameazas emerxentes.



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


*Enfoque de xestión do risco. Fonte: CISA (2016)*

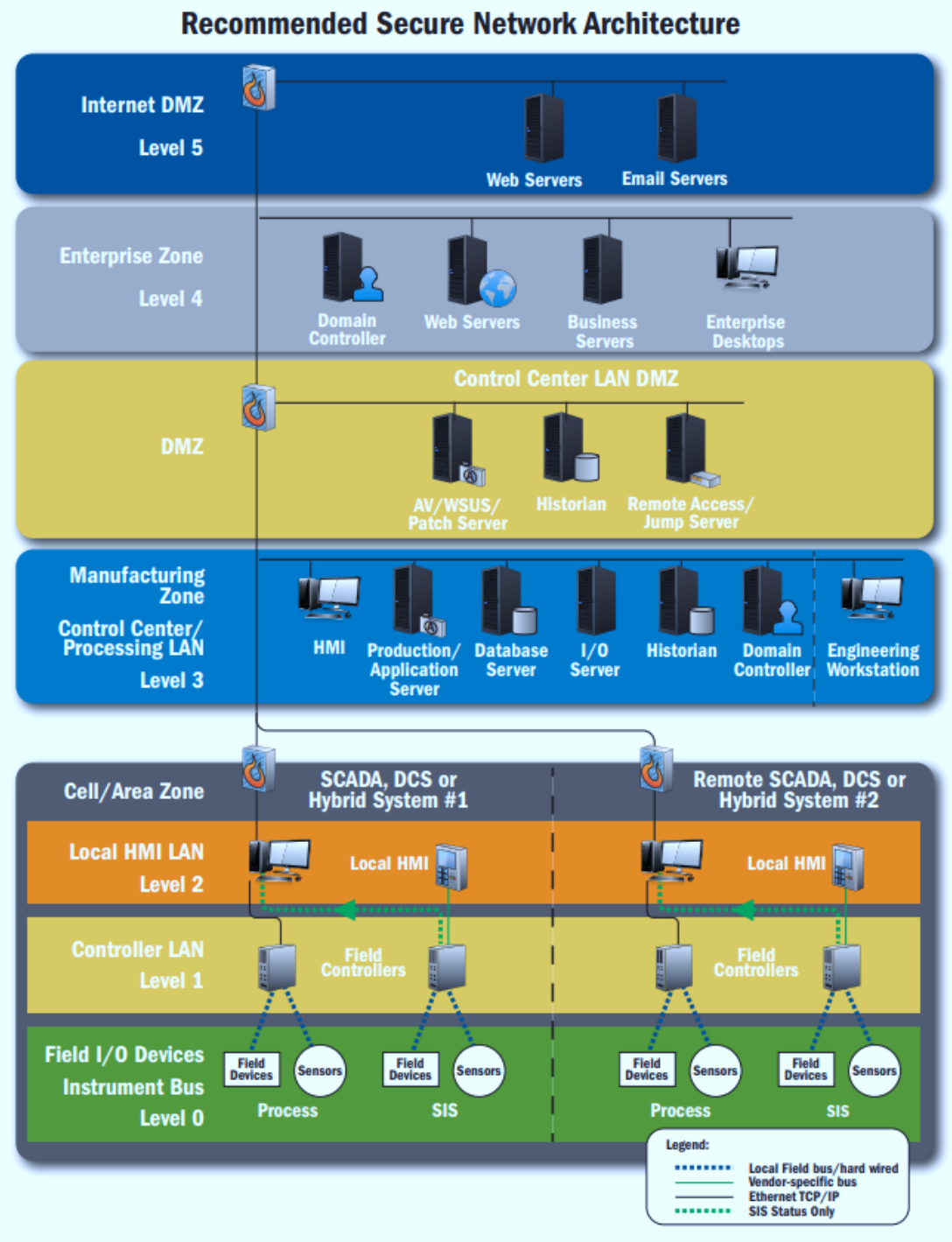
Este modelo obriga a adoptar un ciclo iterativo de mellora, reforzando as defensas a medida que evoluciona o panorama de risco.

- **Estratexia 2. Inventario de activos e caracterización de risco:** identificar e clasificar exhaustivamente os activos ICS (equipos, software, redes, datos e persoal) para saber que debe protexerse e por que. Este inventario inclúe sistemas de proceso, redes de control e o apoio de infraestrutura (IT e OT). Coñecendo o contexto de negocio e a criticidade de cada activo, a organización pode priorizar as defensas segundo o impacto potencial. Unha "lista de activos actualizada e caracterizada por criticidade" proporciona unha base sólida para aplicar contramedidas axeitadas e asegurarse de que non quede ningún dispositivo crítico desprotexido.
- **Estratexia 3. Seguridade física:** aplicar controis físicos para impedir o acceso non autorizado ou a interferencia con activos ICS. Isto abarca asegurar instalacións e equipos (cableado, armarios, salas de control), restrinxir entradas mediante autenticación multifactor física (tarxetas, biometría), instalar cámaras e sensores de movemento, e controlar estritamente os medios extraíbles (USB, CD). Noutras palabras, refórzase o perímetro físico do sistema (valos, barreiras, gardas) e adáptase segundo os requisitos de seguridade industrial e regulatoria, coa fin de evitar manipulacións ou roubo de equipos e datos sensibles no contorno ICS.
- **Estratexia 4. Arquitectura de rede ICS:** deseñar unha topoloxía de rede segura e segmentada para os sistemas de control. Recoméndase colocar os equipos de



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

campo e centros de control en zonas lóxicas separadas, delimitadas por **zonas desmilitarizadas (DMZ)**, VLANs e diodos unidireccionais. Deste modo, a rede ICS queda illada da rede corporativa externa; por exemplo, só unha DMZ intermedia permitiría conexións controladas entre IT e OT (ver figura).




*Arquitectura de rede segura recomendada. Fonte: CISA (2016)*

Ademais, hai que asegurar o perímetro de rede con accesos remotos controlados (pasarelas, VPNs con autenticación forte) e manter unha xestión estrita de parches e vulnerabilidades para cada segmento. Este deseño segmentado aumenta o custo e a complexidade de calquera intento de intrusión.

- **Estratexia 5. Arquitecturas de seguridade:** implantar un marco de políticas e procedementos de seguridade específicos para ICS, complementado con medidas de illamento técnico. Por exemplo, definir normas operativas rigorosas e **bloquear electrónicamente os compoñentes de campo críticos** (firmware e configuracións protexidos). Este nivel estrutural implica combinar seguridade lóxica (configuración de dispositivos e permisos) con seguridade física, asegurando que os sistemas máis sensibles estean bastionados e que exista supervisión do cumprimento de políticas no ciclo de vida ICS.
- **Estratexia 6. Seguridade en hosts ICS:** asegurar os dispositivos finais e servidores que operan no dominio ICS. Isto inclúe endurecer cada host (p.ex. controladores, HMI e servidores SCADA) reducindo ao mínimo o software instalado, empregando máquinas virtuais seguras ou sistemas de respaldo dedicados, e activando detección de intrusións a nivel local (HIDS) cando sexa viable. A idea é minimizar as funcións expostas de cada equipo ICS e contar con avisos temperáns de comportamentos anómalos nos equipos de control.
- **Estratexia 7. Monitorización de seguridade:** establecer vixilancia continua de eventos de seguridade no contorno ICS. Isto supón rexistrar e analizar logs de auditoría críticos, **despregar solucións tipo NDR ou CPS PP**, implementar solucións de correlación e **SIEM** orientadas a OT, e supervisar de forma permanente a rede ICS. Inclúe tamén vixiar a cadea de subministración e o ciclo de vida dos compoñentes (para detectar anomalías en actualizacións ou configuracións). A monitorización proactiva detecta indicios de intrusión e garante axustar as defensas segundo a información do comportamento real da rede.
- **Estratexia 8. Xestión de provedores e outsourcing:** incluír á cadea de subministración na estratexia de seguridade ICS. Isto abarca revisar provedores de servizos xestionados e solucións cloud para asegurarse de que cumpren os niveis de seguridade esixidos, así como aplicar políticas contractuais claras. Por exemplo, ao usar servizos na nube ou consultores externos, débense definir



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

controis específicos (acceso restrinxido, cifrado, supervisión) e asegurarse de que existan protocolos de resposta ante incidentes de provedores. Deste modo minimízanse os riscos introducidos por enlaces na cadea de valor.

- **Estratexia 9. O elemento humano:** non podía faltar. Recoñecer que o factor humano é parte integral e fundamental da defensa. Saliéntase establecer procedementos claros de operación e emerxencia, e sobre todo capacitar ao persoal continuamente en seguridade ICS: operadores, enxeñeiros e equipo de TI/OT deben recibir adestramento e concienciación específicos. Un persoal ben formado e alertado poderá aplicar as capas de defensa con disciplina e detectar comportamentos sospeitosos (phishing, accesos inusuais, etc.), reducindo o risco de erros ou ataques dirixidos a usuarios internos.

**Recomendacións finais**

Para pechar con esta guía de CISA, recollemos as catro recomendacións que se derivan da mesma:

1. **Adoptar un modelo de seguridade proactivo:** o informe destaca a necesidade de moverse dun esquema reactivo a un proactivo e iterativo. É dicir, non só aplicar controis puntuais tras un incidente, senón integrar a mellora continua: deseñar o sistema con seguridade desde o inicio, probar escenarios de intrusión, e axustar periodicamente as defensas.


*Modelo de seguridade proactivo. Fonte: 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 ciberseguridade preventiva (exercicios de resposta, análise de ameazas futuras) e aproveitar automatización para detectar e cazar ataques antes de que causen danos.

2. **Implementar contramedidas clave específicas:** o documento propón un conxunto de cinco contramedidas esenciais para ICS, enfocadas en mitigar os vectores máis comúns (por exemplo, segmentación estrita da rede, autenticación multifactor, xestión de parches priorizada, monitorización OT especializada, etc.). En resumo, aconséllase combinar técnicas probadas –como controis de acceso robustos, comunicación cifrada e sandboxing de dispositivos– para cubrir as necesidades únicas dun contorno de control. Aínda que o informe non as enumera explicitamente, suxire centrar os esforzos nas defensas máis efectivas para contornos industriais críticos, xestionando internamente os riscos residuais.
3. **Seguir estándares e marcos de referencia**: recoméndase aliñar a ciberseguridade ICS con marcos recoñecidos (neste caso propón os empregados no mundo anglosaxón, p. ex. NIST CSF, ISO/IEC 62443, NERC CIP, entre outros) e as políticas de ciberseguridade do sector. Isto inclúe adoptar guías de boas prácticas que aborden tanto a tecnoloxía como a xestión do risco. Usar estes estándares axuda a estandarizar os controis en todas as capas (técnica, organizativa e procedimental) e facilita auditorías, cumprimento regulatorio e mellora continua do programa de seguridade industrial.
4. **Empregar ferramentas e servizos axeitados:** o informe aconsella aproveitar ferramentas especializadas en ICS para implementar defensa en profundidade. Por exemplo, utilizar avaliacións de seguridade e simuladores, software de xestión de vulnerabilidades enfocadas en ICS, e servizos de monitorización OT avanzados. Tamén suxire programas de apoio técnico e colaboración público-privada. Estas ferramentas permiten automatizar a identificación de brechas, validar a arquitectura de rede e manterse ao día coas ameazas emerxentes.

En conxunto, son compoñentes prácticos para reforzar os nove niveis de defensa anteriores. Mencionar que en [23] CISA ofrece unha infografía interesante e totalmente aliñada con esta estratexia de defensa en profundidade, que aconsellamos tomar como referencia.

### 4.1.4 Resiliencia ciberfísica

**A resiliencia ciberfísica é un dos alicerces emerxentes máis relevantes na protección de infraestruturas OT**, particularmente ante ameazas persistentes, fallos inevitables e disrupcións ciberfísicas complexas. Lonxe de limitarse a unha visión tradicional de prevención ou robustez estática, as tendencias internacionais promoven un enfoque dinámico, centrado na continuidade do servizo baixo condicións adversas. Este cambio de paradigma articúlase ao redor de dúas referencias fundamentais:

O informe americano do ***President's Council of Advisors on Science and Technology (PCAST) sobre resiliencia ciberfísica*** [24] establece un marco estratéxico de primeiro nivel para o deseño de políticas de seguridade industrial en infraestruturas críticas. Este documento promove un **cambio conceptual claro: da ciberseguridade orientada a evitar intrusións ("keep attackers out") á** resiliencia operativa enfocada en **garantir a funcionalidade mínima** dos servizos esenciais mesmo baixo condicións de fallo ou ataque **("keep essential services running").**

Menciona tamén ***Minimum Viable Operating Capabilities*** (capacidades mínimas operativas), os modelos de ***bounded impact*** (fallos acoutados) e de ***degraded but functioning*** (servizo degradado pero continuo). Ademais, defende que a resiliencia é unha responsabilidade compartida que afecta non só aos operadores técnicos, senón tamén a fabricantes, entidades reguladoras e órganos executivos de dirección. **A través de casos reais como os incidentes do Colonial Pipeline ou o apagamento en Texas, ilústrase como unha xestión anticipada e transversal da resiliencia pode mitigar severamente o impacto dun ataque OT exitoso.**

Adicionalmente, **o estudo académico de Longo et ao. sobre a evolución da resiliencia ciberfísica, métricas e integración normativa** [25] complementa a perspectiva do PCAST cunha aproximación máis técnico-metodolóxica. Este traballo rastrexa a evolución do concepto de resiliencia —desde o seu enfoque en robustez estática cara a unha visión adaptativa e sistémica— e introduce criterios medibles aplicables a sistemas ICS. **Clasifica indicadores, modelos de avaliación e frameworks operativos, e propón un conxunto de métricas útiles para deseñar KPIs, avaliar controis de continuidade ou realizar auditorías e simulacións de fallo.**

Ademais, o estudo **integra a dimensión regulatoria europea**, incluíndo marcos como a directiva NIS2 ou o regulamento CER, achegando así unha visión complementaria ao

enfoque estadounidense. Para contornos OT en Europa, **esta dobre referencia permite harmonizar criterios técnicos con obrigacións normativas**, mellorando a aliñación entre os obxectivos de resiliencia operativa e os requerimentos regulatorios aplicables.

Ambas fontes permiten a operadores industriais e administracións públicas adoptar unha visión avanzada da resiliencia en contornos ciberfísicos, para anticiparse a ataques inevitables e reducir o seu impacto operativo (algo crítico en servizos esenciais).

# 5 Conclusións

A segunda versión do **Informe de intelixencia de ameazas OT – II** consolida e amplía o traballo iniciado no Informe I, incorporando unha lectura máis focalizada sobre **actores de ameaza** e sobre a súa capacidade real de progresar desde intrusións en IT cara a escenarios de impacto en OT/ICS. Ao longo do documento confírmase unha idea central: en ciberseguridade industrial, o risco non vén definido só pola existencia dunha campaña ou dunha vulnerabilidade, senón pola combinación de **capacidade do adversario**, **exposición do operador**, **madurez operativa** e **posibilidade de progresión cara ao proceso físico**.

Unha primeira conclusión transversal é que o panorama OT/ICS actual debe lerse desde unha perspectiva **multi-fonte** e non desde unha única lente. As evidencias recompiladas mostran patróns recorrentes que se repiten entre estudos: a persistencia de intrusións baseadas en **identidade e acceso** (phishing, abuso de credenciais, accesos remotos mal gobernados), a importancia crecente da **cadea de subministración e infraestrutura de terceiros** como vector e amplificador de risco, e a consolidación de escenarios de **disrupción operativa** como resultado plausible cando conflúen debilidades técnicas e procedementais. O valor do informe reside, precisamente, en **triangular** estes sinais e traducilos a prioridades defensivas adaptables ao tecido industrial galego.

En segundo lugar, a análise de actores e TTPs —incluíndo a visión especializada que distingue fases do ciclo de ataque— reforza que a prioridade non é só impedir intrusións, senón **reducir a capacidade de progresión** e **acurtar o tempo de permanencia** do adversario. Mesmo cando os incidentes comezan en IT, a experiencia agregada amosa que o impacto real en industria adoita depender de dous factores:

> (i) a **existencia de camiños de tránsito IT→OT insuficientemente controlados**, e
>
> (ii) **a falta de visibilidade e procedementos para detectar e conter movementos laterais**, recoñecemento interno e extracción de información técnica.

Un terceiro achado de fondo é o carácter estratéxico da **información OT** (diagramas, topoloxías, instrucións operativas, configuracións e datos xeoespaciais cando aplique). A súa protección non pode considerarse un asunto documental menor: cando esa



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

información é accesible sen gobernanza, convértese nun multiplicador de risco que reduce a fricción para o adversario e acelera a preparación de accións máis daniñas. En consecuencia, o informe suxire tratar a documentación técnica como **activo crítico**, equiparando a súa protección á de credenciais e accesos.

Desde unha perspectiva territorial, a exposición de Galicia non se limita a sectores estritamente críticos: abrangue entre outros **enerxía, auga, alimentación, manufactura e loxística**, así como provedores e subcontratas que operan tecnoloxía industrial e mantemento. Isto implica que a mellora da postura de seguridade debe formularse como programa continuado e non como proxecto puntual: combinar **prevención** (redución de exposición e endurecemento) con **resiliencia** (detección, resposta e recuperación), asumindo que o obxectivo realista é **reducir probabilidade e impacto**, e non eliminar por completo a ameaza.

Unha conclusión especialmente práctica, que complementa a análise técnica, é a pertinencia de establecer —ou fortalecer— **programas internos de intelixencia de ameazas** adaptados a OT/ICS. O informe suxire que as organizacións industriais poden mitigar riscos de maneira máis eficiente cando dispoñen de capacidades internas para:

- Definir un **ciclo de intelixencia** (requisitos, recompilación, análise, difusión e retroalimentación) orientado a decisións operativas.
- Integrar sinais de fontes externas coa súa propia telemetría (SOC/OT-SOC, rexistros de acceso remoto, eventos de rede industrial, inventario e cambios), xerando **hipóteses verificables**.
- Traducir TTPs a **casos de uso de detección**, regras de monitorización e melloras procedementais, evitando depender só de indicadores puntuais.
- Avaliar de forma recorrente a exposición e a capacidade de recuperación mediante **métricas** (p.ex., cobertura de activos críticos, tempos de detección/contención, robustez de copias, eficacia de segmentación) e exercicios controlados.

Finalmente, as recomendacións de seguridade formuladas ao longo do documento non se fundamentan nun único marco, senón nunha **converxencia de boas prácticas procedentes de guías e estudos de referencia, informes de intelixencia e leccións aprendidas en operacións reais**. Isto reforza unha mensaxe de gobernanza: a seguridade OT/ICS require un enfoque de **defensa en profundidade**, apoiado por



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

arquitectura e operación (segmentación, control de identidades, acceso remoto), por capacidades de observación e resposta (detección baseada en comportamento, procedementos de contención), e por preparación para continuidade e recuperación (copias probadas, plans e exercicios).

En síntese, esta versión II consolida unha recomendación transversal: **aliñar a intelixencia de actores e TTPs con decisións de arquitectura, operación, persoas e recuperación, creando un ciclo de mellora continuo que aumente a 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 Ciberameazas e Tendencias 2024*. Recuperado de https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html

[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

[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). *Introdución 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*

*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 Ciberseguridade 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

# Glosario

**ABYSSWORKER**

Familia de malware citada no informe no contexto de ameazas e ferramentas empregadas en campañas de intrusión.

**AcidPour**

Wiper para Linux orientado a borrar contidos en dispositivos embebidos (p.ex., mediante procura de directorios UBI), empregado como capacidade disruptiva en contornos industriais.

**AcidRain**

Wiper observado previamente e empregado como referencia comparativa para contextualizar capacidades destrutivas en contornos embebidos.

**AMTEGA (Axencia para a Modernización Tecnolóxica de Galicia)**

Organismo da Xunta de Galicia responsable de iniciativas e coordinación tecnolóxica, incluíndo liñas de ciberseguridade.

**APT (Advanced Persistent Threat / Ameaza Persistente Avanzada)**

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

**ATT&CK (MITRE ATT&CK)**

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

**AuKill**

Ferramenta/malware citada no informe no contexto de capacidades empregadas por actores de ameaza.

**AvNeutralizer**

Ferramenta/malware citada no informe no contexto de técnicas de evasión e neutralización de defensas.

**BAUXITE**

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

**Backdoor (Porta traseira)**

Mecanismo (software ou configuración) que permite acceso persistente e non autorizado a un sistema, normalmente con capacidade de execución remota.

**BEC (Business Email Compromise / Compromiso de correo empresarial)**

Fraude baseado en suplantación (ou compromiso real) de contas de correo para inducir transferencias, cambios de conta bancaria ou acceso a información sensible.

**BYOVD (Bring Your Own Vulnerable Driver)**

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

**C2 (Command and Control / Comando e control)**

Canle e infraestrutura empregadas polo atacante para comunicarse con sistemas comprometidos, emitir instrucións e recibir datos.

**CAPTCHA**

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

**CCN-CERT**

Centro Criptolóxico Nacional – CERT (España). Entidade de referencia para alertas, guías e información técnica sobre ameazas 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 a resiliencia de entidades críticas fronte a riscos, incluíndo dimensións tecnolóxicas e operativas.

**CHERNOVITE**

Grupo de ameaza identificado por Dragos asociado ao desenvolvemento de capacidades avanzadas para ICS, incluíndo o marco PIPEDREAM.

**CIP (Critical Infrastructure Protection / Protección de infraestruturas críticas)**

Conxunto de políticas e prácticas para protexer infraestruturas críticas fronte a ameazas físicas e dixitais (incluíndo marcos específicos como NERC CIP).

**CISA (Cybersecurity and Infrastructure Security Agency)**

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

**CoDeSys**

Plataforma de desenvolvemento/execución para PLCs e sistemas industriais, citada no contexto de interacción con ecosistemas de control.

**CRASHOVERRIDE**

Malware orientado a contornos industriais (tamén referido como Industroyer noutros contextos) asociado a impactos sobre infraestrutura eléctrica.

**CPS (Cyber-Physical Systems / Sistemas ciberfísicos)**

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

**CVE (Common Vulnerabilities and Exposures)**

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

**CWE (Common Weakness Enumeration)**

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

**DarkCrystal RAT**

Ferramenta do tipo RAT (Remote Access Trojan) empregada en campañas de intrusión para control remoto e roubo de información.

**DLL (Dynamic Link Library)**

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

**DMZ (Zona desmilitarizada)**

Segmento de rede intermedio deseñado para illar servizos expostos e reducir o risco de tránsito cara a redes internas críticas.

**DNS (Domain Name System)**

Sistema de nomes de dominio; pode ser empregado polos atacantes para resolución de infraestrutura C2 ou técnicas de evasión.

**EDR (Endpoint Detection and Response)**

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

**ELECTRUM**

Grupo de ameaza con historial disruptivo en OT/ICS, asociado a operacións con capacidade Stage 2 e uso de ferramentas destrutivas (p.ex., wipers).

**ENISA (European Union Agency for Cybersecurity)**

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

**Exfiltración**

Extracción non autorizada de datos desde unha organización cara ao exterior (p.ex., documentación OT, GIS, credenciais).

**FormBook**

Familia de infostealer citada como exemplo de malware empregado en campañas de roubo de información.

**GDPR (Regulamento Xeral de Protección de Datos)**

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

**GIE (Gas Infrastructure Europe)**

Entidade/ámbito sectorial citado como temática de lure en campañas relacionadas con petróleo e gas.

**GIS (Geographic Information System / Sistema de información xeográfica)**

Ferramentas e datos xeoespaciais críticos para operacións (p.ex., infraestrutura e activos), citados como obxectivo de exfiltración.

**GRAPHITE**

Grupo de ameaza identificado por Dragos (novo na clasificación 2024) con campañas de espionaxe e foco en sectores industriais/enerxéticos.

**GRU**

Dirección Principal de Intelixencia (Rusia), citada no informe en relación con contextos de atribución e actividade xeopolítica.

**HART (Highway Addressable Remote Transducer)**

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

**HAVEX**

Malware asociado historicamente a campañas contra contornos industriais, citado como referencia no contexto de ameazas ICS.

**HIDS (Host-based Intrusion Detection System)**

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



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)**

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

**HTTP / HTTPS**

Protocolos web empregados para comunicación. En contexto de ameaza, poden utilizarse para C2, staging ou exfiltración camuflada en tráfico lexítimo.

**IA (Intelixencia Artificial)**

Tecnoloxías de automatización e análise baseadas en modelos de aprendizaxe; no informe aparece como elemento contextual e de risco/uso transversal.

**IBM X-Force**

Equipo/servizo de intelixencia de ameazas citado como fonte de contexto e tendencias.

**ICS (Industrial Control Systems / Sistemas de control industrial)**

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

**ICS Cyber Kill Chain**

Adaptación do ciclo de ataque a contornos industriais, empregada para describir a progresión desde intrusión inicial ata interacción co proceso físico.

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

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

**ICS-CSIRT (ICS Computer Security Incident Response Team)**

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

**IED (Intelligent Electronic Device / Dispositivo electrónico intelixente)**

Dispositivos empregados en automatización e subestacións (p.ex., protección e control), críticos en contornos eléctricos.

**IDS (Intrusion Detection System)**

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

**IEC (International Electrotechnical Commission)**

Organismo de normalización no ámbito electrotécnico e industrial, citado como referencia de estándares.

**IIoT (Industrial Internet of Things)**

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

**Industroyer**

Denominación asociada a CRASHOVERRIDE noutros contextos; referencia a malware orientado a sistemas industriais.

**IoC (Indicator of Compromise / Indicador de compromiso)**

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

**IoT (Internet of Things)**

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

**IT (Information Technology / Tecnoloxías da información)**

Infraestrutura dixital corporativa (sistemas de información, servidores, endpoints, identidade), frecuentemente punto de entrada en ataques a OT.

**Kapeka**

Backdoor citado no informe no contexto de campañas e intrusións contra organizacións industriais.

**KEV (Known Exploited Vulnerabilities)**

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

**Kill Chain (Cyber Kill Chain)**

Modelo de fases dun ataque dirixido (recoñecemento, armamento, entrega, explotación, instalación, C2 e accións sobre o obxectivo).

**Lista branca de aplicacións (Application allowlisting)**

Control que permite executar só software previamente autorizado, reducindo o risco de execución de malware e movemento lateral.

**LLM (Large Language Model / Modelo de linguaxe de gran escala)**

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

**Loader**

Compoñente de malware que prepara o sistema e descarga/executa payloads posteriores (p.ex., stealers ou backdoors).

**LockBit**

Grupo/familia de ransomware citada como exemplo de ameaza criminal con impacto operativo e económico.

**LNG (Liquefied Natural Gas / Gas natural licuado)**

Sector/ámbito industrial citado como obxectivo/contorno de relevancia para ameazas OT.

**LummaStealer**

Stealer citado no informe no contexto de campañas de roubo de información e credenciais.

**MAGNALLIUM**

Grupo de ameaza descrito por Dragos con actividade centrada en intrusión e espionaxe en IT contra sectores industriais, sen capacidade OT demostrada.

**MFA (Multi-Factor Authentication / Autenticación multifactor)**

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

**MISP (Malware Information Sharing Platform)**

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

**MITRE D3FEND**

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

**Modbus**

Protocolo industrial empregado en automatización; relevante por ser un vector de visibilidade/detección e potencial abuso se existe acceso indebido.

**Movemento lateral**

Técnicas para desprazarse dentro dunha rede tras o acceso inicial, buscando sistemas de maior privilexio ou proximidade a OT.

**MS Threat Intelligence / Microsoft Threat Intelligence**

Capacidade/servizos de intelixencia de ameazas citados como fonte de contexto e tendencias.

**MTTD (Mean Time To Detect / Tempo medio de detección)**

Métrica para medir canto tarda unha organización en detectar un incidente.

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

Métrica para medir canto tarda unha organización en responder e 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**

Denominacións citadas no informe en contexto de actividade de ameazas asociadas a determinados perfís de actor.

**NDR (Network Detection and Response)**

Tecnoloxías e capacidades de detección e resposta baseadas en rede, relevantes para visibilidade en OT e IT.

**NERC / NERC CIP**

Marco de estándares (especialmente no ámbito eléctrico) orientado a requisitos de seguridade para infraestrutura crítica.

**NIS2 (Network and Information Security Directive 2)**

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

**NIST (National Institute of Standards and Technology)**

Instituto estadounidense de referencia en estándares e guías de ciberseguridade, citado como marco transversal.

**Nozomi Networks**

Fabricante e fonte de observabilidade OT citada como referencia para contexto e tendencias en contornos industriais.

**OPC / OPC-UA (OPC Unified Architecture)**

Tecnoloxía/protocolo industrial empregado para interoperabilidade e comunicación; relevante en ameazas por visibilidade e potencial abuso cando hai acceso indebido.

**OpenCTI (Open Cyber Threat Intelligence)**

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

**OT (Operational Technology / Tecnoloxías de operación)**

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

**OTAN**

Organización do Tratado do Atlántico Norte, citada no informe como referencia contextual.

**OEM (Original Equipment Manufacturer / Fabricante orixinal)**

Fabricante de equipos industriais; relevante por cadea de subministración, firmware, actualizacións e soporte.

**PARISITE**

Grupo de ameaza descrito por Dragos con foco en espionaxe e recollida de información contra organizacións industriais.

**Password spraying**

Técnica de ataque a credenciais que proba poucas contrasinais comúns contra moitas contas para evitar bloqueos e aumentar a tasa de éxito.

**PCAST**

Referencia a informes e análises (p.ex., resiliencia ciberfísica) citadas no informe como contexto.

**PIPEDREAM**

Marco modular de malware deseñado para interacción con contornos ICS, asociado a CHERNOVITE.

**PLC (Programmable Logic Controller)**

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

**Proxy / Relay (Relé)**

Infraestrutura intermedia empregada para redirixir tráfico (p.ex., C2, staging), ocultando orixe e dificultando detección.

**RAT (Remote Access Trojan)**

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

**RDP (Remote Desktop Protocol)**

Protocolo de acceso remoto a escritorios Windows; frecuente como vector de intrusión se está exposto ou con credenciais débiles.

**RTU (Remote Terminal Unit)**

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

**SBOM (Software Bill of Materials)**

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

**SCADA (Supervisory Control and Data Acquisition)**

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

**SIEM (Security Information and Event Management)**

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

**SMB (Server Message Block)**

Protocolo de compartición en Windows; relevante como vector de movemento lateral ou abuso en redes mal segmentadas.

**SOC (Security Operations Center)**

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

**SOHO (Small Office / Home Office)**

Categoría de dispositivos e redes de pequena oficina/fogar; no informe aparece no contexto de compromisos de routers usados como relés.

**Spear-phishing**

Phishing altamente dirixido, con cebos personalizados para unha persoa/organización concreta, orientado a obter acceso inicial.

**SSH (Secure Shell)**

Protocolo de administración remota cifrada; crítico en exposición a internet e gobernanza de credenciais.

**Stage 1 / Stage 2 (ICS Cyber Kill Chain)**

Clasificación por fases: Stage 1 (intrusión/espionaxe en IT e preparación) e Stage 2 (interacción co 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 infraestrutura intermedia (ás veces servizos lexítimos) para aloxar, preparar e servir cargas maliciosas antes da execución final.

**Stealer**

Malware deseñado para roubar información (credenciais, cookies, wallets, datos de navegador) e facilitar accesos posteriores.

**Telemetría**

Conxunto de datos de observación (rede, endpoints, protocolos industriais, rexistros) empregados para detección e resposta.

**ThreatConnect / ThreatStream / ThreatFox / TheHive**

Ferramentas/plataformas citadas no informe para xestión, intercambio e operación de intelixencia de ameazas.



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 seguridade industrial, citado como referencia no contexto de ameazas ICS avanzadas.

**TrickBot**

Malware/capacidade criminal citada no informe como exemplo de ferramenta empregada en campañas de intrusión.

**TTP (Tactics, Techniques and Procedures)**

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

**TURNEDUP**

Denominación de malware citada no informe asociada a campañas de intrusión e espionaxe.

**UBI (Unsorted Block Images)**

Formato/estrutura típica en almacenamento de dispositivos embebidos; relevante por técnicas de borrado destrutivo en wipers.

**UE (Unión Europea)**

Ámbito institucional citado en relación con normativa, contexto de ameazas e marcos de referencia.

**USB (Universal Serial Bus)**

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

**VOLTZITE**

Grupo de ameaza descrito por Dragos con foco en espionaxe e recollida de información OT (p.ex., GIS e documentación técnica), e uso de infraestrutura de relé.

**VPN (Virtual Private Network)**

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

**WASSONITE**

Grupo de ameaza descrito por Dragos, con actividade orientada a intrusión e recollida de información en sectores industriais e infraestrutura crítica.

**Wiper**

Malware deseñado para destruír datos e impedir a recuperación (borrado, corrupción de ficheiros/particións), con impacto disruptivo.

**WMI (Windows Management Instrumentation)**

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

**XSS (Cross-Site Scripting)**

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



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

CIBER SEGURIDADE GALICIA

# Observatorio de Ciberseguridade Industrial
# **Informe de Intelixencia de Ameazas - II**

**AMTEGA – Xunta de Galicia 2026**



Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Xacobeo 2027