CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial

Informe de ciberalertas - I

Xaneiro 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 progresiva dixitalización do tecido industrial, xunto coa consolidación de arquitecturas cada vez máis interconectadas, **continúa a ampliar de xeito significativo a superficie de exposición dos sistemas OT**. Este fenómeno, observado desde hai varios anos, intensificouse a medida que a **converxencia entre tecnoloxías de operación e tecnoloxías da información se converteu nun elemento estrutural** de sectores como a enerxía, a auga, a automoción, a alimentación ou a loxística. O medre desa interdependencia tecnolóxica xerou un ecosistema operativo máis eficiente, pero tamén **máis vulnerable fronte a actores maliciosos con capacidade técnica, motivación económica ou interese estratéxico**.

Os datos recollidos no informe **ENISA Threat Landscape 2025** [1] amosan que a explotación de vulnerabilidades continúa a ser un dos vectores de intrusión máis relevantes no panorama europeo, representando o **21,3 %** dos casos analizados. Destaca, ademais, que **case o 70 % dos incidentes baseados en vulnerabilidades derivan nunha intrusión efectiva**, o que evidencia a eficacia deste vector para os actores maliciosos e a rapidez coa que se aproveitan erros recentemente publicados.

Alén, ENISA (Axencia da Unión Europea para a Ciberseguridade) subliña a crecente capacidade das campañas automatizadas para armar vulnerabilidades en cuestión de días desde a súa divulgación pública, incrementando a presión sobre organizacións que dependen de sistemas industriais e servizos críticos. Desta circunstancia e do contexto OT específico falaremos na sección seguinte.

De forma complementaria, o **Balance de Ciberseguridade 2024 do Instituto de Ciberseguridade de España (INCIBE)** [2] —o último dispoñible na data de elaboración deste informe— indica que se xestionaron máis de 97.000 incidentes nesa anualidade, con **máis de 31.500 afectando directamente a empresas e máis de 183.000 sistemas vulnerables identificados** no territorio nacional. Estes datos subliñan a persistencia de eivas de seguridade e a necesidade de adoptar medidas preventivas robustas para minguar riscos que poden traducirse en impactos operacionais severos.

Neste contexto, o **presente informe adopta un dobre enfoque** coa fin de reforzar o seu carácter didáctico e facilitar unha comprensión progresiva dos elementos clave relacionados coa xestión de vulnerabilidades e alertas en contornas OT:

- Cada edición incluirá **un bloque conceptual orientado a clarificar aspectos teóricos de interese** —conceptos, modelos, prácticas de referencia e fundamentos metodolóxicos— que sirvan como base para interpretar adecuadamente os riscos e as medidas asociadas.
- Manterase unha análise estruturada e orientada á acción, centrada **nas vulnerabilidades e alertas máis relevantes do trimestre**, co obxectivo de proporcionar información práctica e directamente aplicable por parte de empresas e administracións públicas.

No primeiro informe, este bloque conceptual centrarase en **definir formalmente que é unha vulnerabilidade**, **analizar os tempos de explotación** desde diversas perspectivas (incluíndo estudos de diferentes entidades e organismos) e examinar o retorno do investimento asociado á súa correcta xestión. En edicións posteriores abordaranse outros aspectos esenciais do proceso de xestión de vulnerabilidades, entre os que poderían atoparse:

- **Estratexias de priorización baseadas no risco** —considerando fontes como o catálogo KEV da CISA—;
- **A importancia da visibilidade e do inventario OT** como base para a priorización e aliñamento con marcos como IEC 62443;

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

- **A aplicación de controis compensatorios cando o parcheo non é viable**: segmentación, filtrado avanzado, *whitelisting* e outras técnicas de mitigación propias de contornas industriais.

Deste xeito, o informe combina **orientación didáctica e utilidade operativa**, proporcionando tanto unha base conceptual sólida como unha análise actualizada que permita **fornecer a resiliencia do ecosistema industrial galego fronte a ameazas que evolúen axiña e complexidade crecente**.

Entre os avisos máis relevantes do trimestre, destaca o emitido por Siemens, que afecta a un número especialmente elevado de produtos e compoñentes amplamente despregados en sectores industriais e de infraestruturas críticas. Este feito subliña a importancia de manter unha vixilancia continua sobre os fabricantes estratéxicos e de reforzar os procesos internos de identificación e avaliación de impacto.

Alén deste caso, apréciase unha intensificación de vulnerabilidades relacionadas con accesos remotos, erros de autenticación e exposicións non intencionadas, ademais dunha dependencia crecente e anunciada entre redes IT e OT.

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

2 Metodoloxía e fontes

Este boletín apóiase nun conxunto amplo e contrastado de **fontes oficiais, bases de datos de vulnerabilidades, informes especializados e avisos de fabricantes industriais**, coa fin de ofrecer unha visión clara, actualizada e útil para empresas e administracións públicas.

O enfoque adoptado combina dous elementos esenciais:

- **Consulta sistemática de fontes fiables e recoñecidas**, tanto nacionais como internacionais, que inclúen CERTs (Computer Emergency Response Teams, ou Equipos de Resposta ante Emerxencias Informáticas), axencias europeas, bases de datos de vulnerabilidades, publicacións de referencia, informes sectoriais e avisos oficiais de fabricantes OT/ICS.
- **Escolla e organización da información** para que resulte relevante e práctica, priorizando aquela relacionada con vulnerabilidades e alertas que afectan a tecnoloxías industriais empregadas en sectores estratéxicos galegos, como os representados no Laboratorio de Ciberseguridade Industrial de AMTEGA [3].

Este boletín non pretende por agora realizar análises avanzadas como a extracción de tendencias, a correlación entre fontes ou a avaliación comparada de criticidades. O propósito é garantir unha **visión clara, estruturada e fundamentada** en fontes consolidadas, con alertas comprensibles e accionables polo ecosistema galego para a protección dos seus activos.

As fontes empregadas abranguen diferentes categorías relevantes para a construción do informe. Entre elas destacan:

- **CERT nacionais e internacionais**, como INCIBE-CERT, CCN-CERT (do Centro Criptolóxico Nacional), CISA (Axencia de Ciberseguridade e Seguridade de Infraestructuras estadounidense) ou CERT@VDE (CERT alemán especializado en sistemas industriais e de control).
- **Axencias e organismos europeos e internacionais**, como ENISA ou NIST (Instituto Nacional de Estándares e Tecnoloxía estadounidente).
- **Bases de datos de vulnerabilidades amplamente recoñecidas**, como NVD, CVE.org ou ou EUVD (norteamericanas e europea, respectivamente).

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

- **Informes e/ou laboratorios de investigación en ciberseguridade industrial**, de orixes como Nozomi Networks, Claroty Team82, Dragos, SANS, ICS STRIVE e Kaspersky ICS CERT.
- **Os paneis de avisos oficiais de seguridade publicados por fabricantes industriais**, como por exemplo Siemens, Schneider Electric, Rockwell Automation, ABB, B&R, Mitsubishi Electric, Omron, Beckhoff e Festo.
- **Documentos e guías metodolóxicas** aplicables á xestión de vulnerabilidades en contornas OT, como as publicadas por CISA.

No seu conxunto, esta agrupación de fontes proporciona unha **base sólida, actualizada e orientada á práctica**, que asegura que o seu contido sexa de utilidade para o tecido empresarial e as administracións públicas ligadas ao sector industrial.

3 Vulnerabilidades

3.1 Marco teórico

3.1.1 Definición

No eido da ciberseguridade, enténdese por **vulnerabilidade** calquera **debilidade, erro ou deficiencia** presente nun sistema, rede, aplicación, dispositivo ou configuración, que **puidese aproveitar un atacante para comprometer a confidencialidade, integridade ou dispoñibilidade** da información ou dos servizos que o devandito activo proporciona. Esta definición, amplamente aceptada na literatura especializada, resulta igualmente aplicable tanto a contornas puramente TI como a infraestruturas OT e industriais.

As vulnerabilidades poden ter a súa orixe en múltiples factores: **erros de deseño** (arquitecturas que non contemplan axeitadamente a seguridade), **erros de programación** (por exemplo, ausencia de validación de entradas, desbordamentos de memoria ou condicións de carreira), **configuracións incorrectas ou inseguras** (servizos innecesarios expostos, contrasinais por defecto, regras de cortalumes permisivas de máis), **software ou firmware desactualizados** que non incorporan correccións coñecidas, ou **procedementos organizativos deficientes** que non establecen controis efectivos sobre cambios, accesos ou xestión de parches.

As consecuencias derivadas da explotación dunha **vulnerabilidade** poden ser moi diversas, pero adoitan materializarse en accesos non autorizados a sistemas ou datos, **interrupcións do servizo**, alteración ou destrución de información, **escalada de privilexios** dentro dunha rede, instalación de malware ou emprego da infraestrutura comprometida como punto de apoio para lanzar ataques contra terceiros. En contornas industriais, estas consecuencias poden trasladarse mesmo ao plano físico: modificación de parámetros de proceso, parada de liñas de produción, danos en equipamento ou impacto sobre a seguridade das persoas.

No caso dos sistemas OT, unha vulnerabilidade nun PLC, unha HMI, unha RTU, unha pasarela de comunicacións industrial ou un servidor SCADA non afecta unicamente a un activo lóxico, senón que pode comprometer a capacidade de controlar válvulas, motores, bombas, robots ou sistemas de climatización industrial. Deste xeito, unha simple debilidade técnica pode converterse na orixe dun incidente con repercusións directas sobre a continuidade operativa, a calidade do produto ou a seguridade física.

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

3.1.2 Vulnerabilidades e a súa clasificación

Antes de abordar as distintas clasificacións, resulta útil considerar os cinco **factores que permiten identificar unha vulnerabilidade**:

1. **Exposición**: o activo vulnerable debe estar accesible para un atacante, xa sexa de forma remota, local ou física.
2. **Emprego dunha técnica de ataque coñecida**: a vulnerabilidade debe poder explotarse mediante un método documentado ou comprendido.
3. **Impacto demostrable**: a súa explotación debe ter consecuencias medibles sobre o sistema, proceso ou información.
4. **Condicións de explotación**: deben existir os requisitos necesarios (privilexios, acceso, interacción do usuario, etc.).
5. **Existencia dun axente capaz de a explotar**: un adversario con motivación, intención e medios.

Estes factores permiten xulgar entre unha simple debilidade teórica e unha **vulnerabilidade real e explotable**, o que é esencial para a súa correcta priorización operativa.

Clasificacións de vulnerabilidades

A literatura técnica e os marcos de referencia internacionais propoñen distintas formas de **clasificar as vulnerabilidades**, en función de aspectos como o tipo de activo afectado, a causa raíz, a forma de explotación ou o impacto potencial.

a) Segundo o tipo de activo afectado

- **Vulnerabilidades de software**: eivas presentes no código de aplicacións, sistemas operativos, servizos ou firmware. Por exemplo, un desbordamento de búfer no firmware dun PLC ou un fallo de validación nunha API de xestión dun SCADA.
- **Vulnerabilidades de hardware**: defectos no deseño ou implementación de compoñentes físicos que permiten comportamentos non previstos ou inseguros. Aínda que menos frecuentes, poden atoparse en controladores específicos, tarxetas de comunicación ou módulos criptográficos.
- **Vulnerabilidades de rede e comunicacións**: configuracións inseguras en routers, switches, cortalumes ou dispositivos industriais de comunicación; uso

de protocolos sen cifrado nin autenticación (como Modbus/TCP ou DNP3 na súa versión clásica); servizos innecesarios expostos a redes non confiables.

- **Vulnerabilidades en aplicacións web**: debilidades en portais de administración, paneis de monitorización ou interfaces web de enxeñaría, que permiten ataques de inxección SQL, cross-site scripting (XSS) ou eludir mecanismos de autenticación. En contornas OT, é habitual que a consola de xestión dun SCADA ou dun historiador de datos expóñase mediante unha interface web.
- **Vulnerabilidades en dispositivos IoT/IIoT**: firmware non actualizable, credenciais por defecto, servizos embebidos inseguros ou falta de mecanismos de actualización, moi frecuentes en sensores, cámaras ou dispositivos auxiliares conectados a redes industriais.
- **Vulnerabilidades específicas de sistemas OT**: afectan a PLC, HMI, sistemas SCADA, sistemas de control distribuído (DCS) ou gateways industriais, e inclúen desde falta de autenticación en funcións críticas ata ausencia de rexistros de auditoría ou mecanismos febles de integridade de firmware.

b) Segundo a causa raíz

- **Erros de programación**: fallos no código que permiten executar instrucións non previstas, provocar condicións de erro explotables ou manipular datos sen os controis adecuados.
- **Deseño inseguro do sistema**: arquitecturas que non contemplan segmentación de redes, separación de funcións ou principios básicos de mínima exposición e mínimo privilexio.
- **Emprego de compoñentes obsoletos**: bibliotecas, sistemas operativos ou firmware que deixaron de recibir soporte e acumulan vulnerabilidades coñecidas.
- **Configuracións defectuosas ou por defecto**: servizos innecesarios activos, portos abertos sen xustificación, credenciais predeterminadas ou regras de cortalumes excesivamente permisivas.
- **Dependencias vulnerables**: inclusión de compoñentes de terceiros (por exemplo, bibliotecas nunha aplicación industrial) que presentan vulnerabilidades xa documentadas.

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

c) Segundo a súa explotabilidade

Outro xeito habitual de clasificar as vulnerabilidades é atendendo ás condicións necesarias para a súa explotación:

- **Explotables remotamente**: permiten a un atacante comprometer o sistema a través da rede, sen necesidade de acceso físico (por exemplo, execución remota de código nun servidor SCADA exposto).
- **Explotación local ou con acceso físico**: requiren que o atacante teña acceso directo ao sistema ou á rede interna (por exemplo, conexión a un porto serie dun PLC en planta).
- **Requiren autenticación previa**: só poden explotarse tras obter ou eludir credenciais válidas.
- **Explotables de xeito automatizado**: a súa explotación pode integrarse facilmente en ferramentas e kits, facilitando campañas de ataque a gran escala.

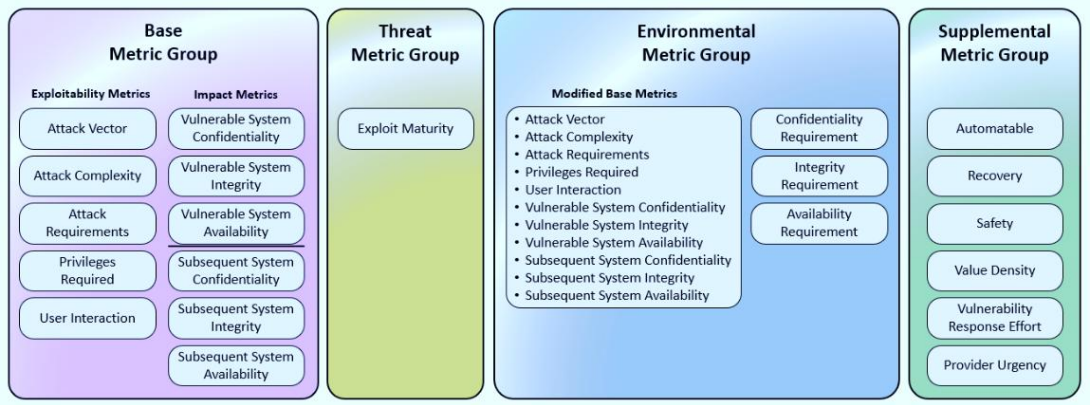
d) Segundo estándares e esquemas de referencia

Na práctica, a clasificación de vulnerabilidades adoita apoiarse en **estándares consolidados**:

- **CVE (Common Vulnerabilities and Exposures)** proporciona un identificador único para cada vulnerabilidade coñecida, o que facilita o seu seguimento e referencia [4].
- **CVSS (Common Vulnerability Scoring System)** asigna unha puntuación de criticidade (por xeral de 0 a 10) baseada en factores como a facilidade de explotación, o impacto sobre confidencialidade, integridade e dispoñibilidade, ou a necesidade de interacción do usuario [5].

  CVSS 4.0 constitúe a versión máis recente do estándar internacional utilizado para medir a gravidade dunha vulnerabilidade, achegando un modelo máis preciso e flexible ca os seus predecesores. O seu obxectivo é ofrecer unha valoración que reflicta tanto a natureza intrínseca da vulnerabilidade como a súa explotación real e o seu impacto nunha contorna concreta. Establece a súa valoración de severidade a partir de catro grupos de métricas que permiten describir con precisión o risco asociado a unha vulnerabilidade.

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



Grupos de métricas de CVSS 4.0. Fonte: first.org (2023)

O primeiro grupo, as **métricas Base**, representa as características intrínsecas da vulnerabilidade que non dependen do tempo nin da contorna onde se atope o sistema afectado. Estas métricas divídense en dous subconxuntos: as de **Explotabilidade**, que describen a facilidade técnica coa que pode explotarse o fallo no sistema vulnerable —como o vector de ataque, a complexidade, os privilexios requiridos ou a interacción do usuario—, e as de **Impacto**, que avalían as consecuencias directas dunha explotación exitosa. Estas últimas consideran tanto o impacto sobre o propio sistema vulnerable como o impacto sobre sistemas subseguintes, podendo incluír mesmo implicacións sobre a seguridade física, un aspecto inserido orixinariamente con CVSS v3 ao se ampliar o concepto de alcance (scope en inglés) máis alá do compoñente técnico afectado.

O segundo grupo, as **métricas de Ameaza (Threat)**, incorpora información relativa ao estado de explotación coñecido da vulnerabilidade. Dado que estas condicións poden variar no tempo, este grupo permite axustar a severidade en función de se existen probas públicas de explotación, código dispoñible ou incidentes confirmados. Así, unha vulnerabilidade con alto impacto teórico pero sen evidencia de explotación pode recibir unha valoración diferente respecto doutra activamente explotada por actores maliciosos.

O terceiro grupo, as **métricas Ambientais (Environmental)**, adapta a puntuación ao contexto específico de cada organización. Este axuste ten en conta a criticidade do sistema afectado, a existencia de controis que mitiguen os impactos ou a importancia relativa de atributos como a confidencialidade, a integridade ou a dispoñibilidade. En contornas OT ou CPS, onde a

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

dispoñibilidade e a seguridade física poden ser prioritarias, estas métricas permiten reflectir de forma máis realista a severidade operativa dunha vulnerabilidade.

Finalmente, CVSS 4.0 incorpora un cuarto grupo denominado **métricas Suplementarias (Supplemental),** que proporciona descritores adicionais sobre características externas da vulnerabilidade —como requisitos regulamentarios, aspectos relacionados coa seguridade humana ou a posibilidade de explotación automatizada—. Estas métricas **non afectan ao cálculo da puntuación CVSS**, pero permiten a cada organización incorporar factores que resulten relevantes no seu propio modelo de priorización, enriquecendo a interpretación do risco sen modificar a puntuación estándar.

A escala continúa medindo de 0 a 10. As categorías de severidade son as seguintes: de 0,0 a 3,9 considérase baixa, de 4,0 a 6,9 media, de 7,0 a 8,9 alta e de 9,0 a 10 crítica.

No seu conxunto, CVSS 4.0 proporciona unha visión máis axustada do risco, especialmente útil en contextos OT e industriais onde a explotación dunha vulnerabilidade pode transcender o plano dixital e afectar á continuidade operativa ou á seguridade física.

- O **catálogo KEV (Known Exploited Vulnerabilities)** da CISA [6][7] recolle vulnerabilidades que se sabe que están a ser **explotadas activamente**, constituíndo un subconxunto especialmente prioritario á hora de planificar medidas de mitigación.

En contornas OT decote atópanse vulnerabilidades asociadas ao uso de protocolos sen cifrado nin autenticación robusta, lóxicas de control expostas sen controis de acceso, firmware desactualizado ou paneis de administración accesibles desde redes non segmentadas. Nestes casos, a correcta clasificación e comprensión do contexto operativo é crucial para determinar a súa verdadeira criticidade.

3.1.3 Organismos e marcos de referencia

A xestión de vulnerabilidades apóiase no traballo de diversos **organismos e comunidades de referencia**, que proporcionan marcos conceptuais, listaxes de debilidades e modelos de ataque. Entre os máis relevantes destacan **OWASP** [8] e **MITRE** [9].

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

3.1.3.1 OWASP

O **Open Worldwide Application Security Project (OWASP)** é unha organización internacional sen ánimo de lucro dedicada a mellorar a seguridade do software. Estrutúrase como unha comunidade aberta na que participan profesionais de desenvolvemento, auditoría e operación de sistemas, que colaboran na creación de guías, ferramentas e boas prácticas.

O seu proxecto máis coñecido é o **OWASP Top 10** [10], un informe que se actualiza periodicamente e que recolle os dez riscos máis críticos en seguridade de aplicacións web. Este documento consolidouse como un **estándar de concienciación** para desenvolvedores e responsables de seguridade, ao ofrecer unha síntese das vulnerabilidades máis frecuentes e de maior impacto observadas na práctica.

Aínda que o foco orixinal de OWASP se sitúa no ámbito das aplicacións web corporativas, moitos dos riscos identificados son plenamente aplicables a **interfaces de xestión e supervisión industrial**. Por exemplo:

- Consolas web utilizadas para administrar sistemas SCADA ou historiadores de planta.
- Portais de mantemento remoto de equipos industriais.
- APIs (interfaces de programación de aplicacións) expostas que permiten interactuar con dispositivos OT ou recompilar datos de proceso.

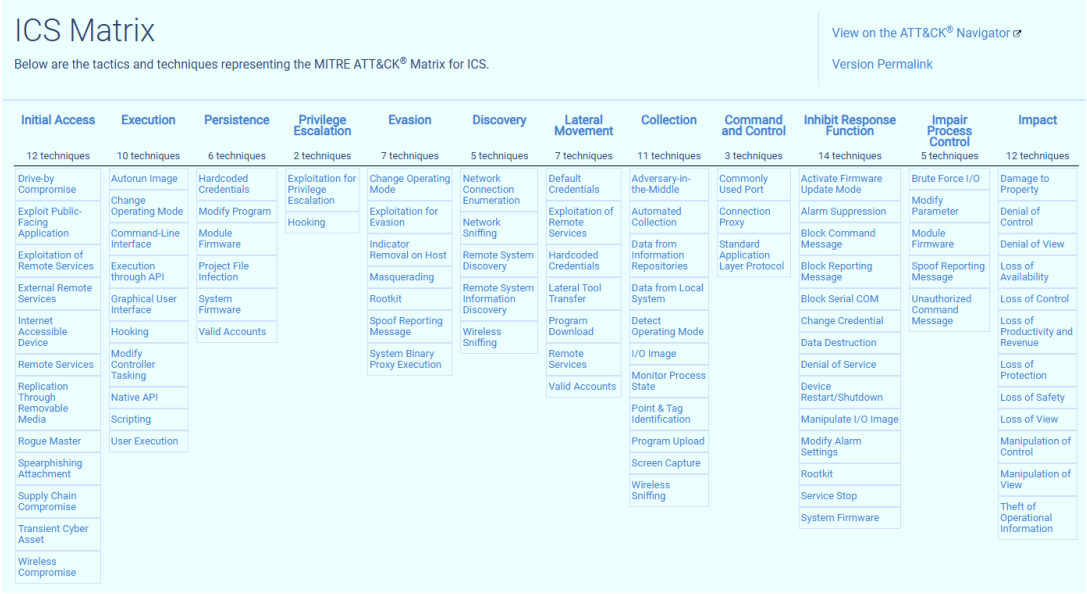
En todos estes casos, erros como a **inxección de código**, a **falta de control de acceso**, a **xestión deficiente de sesións** ou a **exposición de información sensible** poden facilitar a un atacante o acceso a sistemas industriais que, en principio, non deberían ser alcanzables desde o exterior.

3.1.3.2 MITRE ATT&CK, CWE e CAPEC

A entidade **MITRE** é unha organización estadounidense sen ánimo de lucro que provee enxeñería de sistemas, I+D e soporte sobre tecnoloxías da información ao goberno de Estados Unidos de América, e mantén varios catálogos de coñecemento esenciais para comprender e xestionar vulnerabilidades e ataques:

- **MITRE ATT&CK** é unha matriz que documenta técnicas e procedementos utilizados por atacantes reais, organizados por tácticas (obxectivos) e fases da intrusión. Ofrece unha taxonomía práctica para entender como se encadean distintas accións maliciosas en campañas reais [11].

- **MITRE ATT&CK for ICS** amplía este modelo ao ámbito industrial, recollendo técnicas específicas utilizadas contra sistemas de control industrial (ICS), como a manipulación de lóxicas de PLC, a inserción de comandos maliciosos en protocolos industriais ou a modificación de parámetros de control [12].



Matriz MITRE ATT&CK para ICS. Fonte: mitre.org (2025)

- **CWE (Common Weakness Enumeration)** fornece un catálogo estruturado de **debilidades de software**, é dicir, patróns de erros que poden dar lugar a vulnerabilidades (por exemplo, "validación insuficiente de entradas" ou "xestión insegura de recursos") [13].

- **CAPEC (Common Attack Pattern Enumeration and Classification)** clasifica patróns de ataque recorrentes, facilitando a comprensión de como se explotan na práctica as debilidades recollidas en CWE [14].

No contexto OT, estes marcos permiten relacionar **vulnerabilidades técnicas concretas** (por exemplo, un fallo de autenticación na interface web dun PLC) con **técnicas de ataque documentadas** (como o abuso de servizos remotos ou a modificación de lóxicas de control), proporcionando unha linguaxe común para analistas, operadores e equipos de resposta ante incidentes.

Ademais de OWASP e MITRE, existen outros marcos e estándares relevantes para a caracterización formal e o intercambio de información sobre vulnerabilidades.

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

3.1.3.3 NVD – National Vulnerability Database

A **NVD (National Vulnerability Database)** [15], mantida por NIST [16], constitúe a base de datos de referencia para a clasificación e consulta de vulnerabilidades. Amplía o rexistro CVE con:

- métricas CVSS oficiais,
- análises de severidade,
- puntuacións temporais e contextuais,
- ligazóns a recursos adicionais.

En contornas OT, a NVD é particularmente útil para identificar firmware vulnerable, bibliotecas afectadas ou compoñentes obsoletos incluídos en equipos industriais. Recentemente, por cuestións de soberanía tecnolóxica en Europa impulsouse a creación da **alternativa EUVD (EU Vulnerability Database)** [17].

3.1.3.4 MITRE Top 25

O **MITRE CWE Top 25 Most Dangerous Software Weaknesses** [18] identifica cada ano as 25 debilidades máis perigosas en software, baseadas na súa prevalencia e severidade. Moitas delas están presentes tamén en dispositivos industriais, incluíndo:

- validación insuficiente de entradas (CWE-20)
- erros de xestión de memoria (CWE-119),
- exposición de información sensible (CWE-200),
- configuracións inseguras (CWE-16).

A súa utilidade radica en que permite prever que erros son máis probables en software industrial, especialmente en firmware de PLC ou aplicacións de enxeñaría.

3.1.3.5 CVRF – Common Vulnerability Reporting Framework

O **CVRF (Common Vulnerability Reporting Framework)** [19] é un estándar de estruturación de informes de vulnerabilidades promovido por OASIS (un consorcio internacional de estándares tecnolóxicos). Permite a fabricantes e CERT publicar avisos de forma consistente, incluíndo:

- descrición técnica da vulnerabilidade,
- impacto,

- produtos afectados,
- ligazóns CVE e métricas CVSS,
- recomendacións de mitigación

Fabricantes industriais como Siemens, Schneider Electric ou Rockwell Automation empregan formatos compatibles con CVRF para distribuír avisos de seguridade, o que facilita a súa integración en ferramentas automáticas de xestión de vulnerabilidades.

3.1.4 Ferramentas de análise de vulnerabilidades

As ferramentas de análise de vulnerabilidades constitúen un elemento central do proceso, xa que permiten automatizar a detección dun gran número de debilidades coñecidas. Porén, o seu uso debe entenderse sempre como un complemento —e non como substituto— dunha análise experta.

3.1.4.1 Escáneres tradicionais

Entre as ferramentas máis estendidas atópanse:

- **OpenVAS / Greenbone**: OpenVAS [20] naceu como un proxecto de software libre para a análise de vulnerabilidades, que co tempo deu lugar a solucións comerciais como as de Greenbone [21]. Aínda que OpenVAS segue sendo unha ferramenta útil con fins didácticos e en determinados escenarios, en contornas profesionais considérase preferible empregar versións soportadas e con bases de sinaturas actualizadas regularmente.
- **Nessus (Tenable)** [22]: un dos escáneres de vulnerabilidades máis recoñecidos. Dispón dunha ampla base de datos de plugins mantida por Tenable e ofrece capacidades avanzadas para detectar debilidades en sistemas, aplicacións e redes. Adoita destacarse pola súa precisión na detección e pola dispoñibilidade de documentación e soporte.
- **Qualys** [23]: plataforma baseada na nube que combina avaliación de vulnerabilidades con outras capacidades (análise de configuración, cumprimento normativo, monitorización continua). A súa arquitectura distribuída e a súa orientación a grandes contornas convértena nunha opción axeitada para organizacións con infraestruturas complexas e heteroxéneas.

En todos os casos, estas ferramentas permiten xerar informes estruturados nos que as vulnerabilidades se clasifican por criticidade, o que facilita a súa priorización.

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

3.1.4.2 Solucións específicas para OT (CPS PP)

Gartner define as **plataformas de protección para sistemas ciberfísicos** (CPS PP, Cyber-Physical Systems Protection Platform [24], polas súas siglas en inglés) como aquelas solucións que utilizan o coñecemento dos protocolos industriais, o tráfico de rede operacional ou de produción, e o comportamento dos activos físicos, coa fin de **descubrir, categorizar, mapear e protexer os CPS en contornas de produción ou críticos que quedan fóra do ámbito tradicional de TI**.

No contexto da **ciberseguridade industrial**, xurdiron estas solucións especializadas que, entre outras cousas, permiten **identificar vulnerabilidades e debilidades en sistemas OT sen interferir co seu funcionamento**. Estas ferramentas, entre as que se inclúen plataformas como **Nozomi** [25], **Claroty** [26], **Dragos** [27] ou a galega **InprOTech Guardian** [28], baséanse habitualmente na monitorización activo-pasiva do tráfico de rede industrial e na análise da configuración de dispositivos.

As súas principais achegas neste ámbito son:

- Descubrimento automático de **activos OT** (PLC, HMI, variadores, sensores, gateways, etc.).
- Identificación de **versións de firmware** e correlación con bases de vulnerabilidades coñecidas.
- Detección de **protocolos e servizos expostos** que poidan supoñer un risco.
- Análise de **anomalías no comportamento** da rede ou dos dispositivos, que pode revelar tanto vulnerabilidades como incidentes en curso.

Este enfoque resulta especialmente valioso en redes onde o uso de escáneres tradicionais podería ser demasiado intrusivo ou supor riscos para a dispoñibilidade do proceso.

Cómpre destacar que no Laboratorio de Ciberseguridade Industrial de AMTEGA dispóñense tanto de escáneres de vulnerabilidades como de plataformas CPS PP para analizar e avaliar por parte de calquera entidade interesada en comprender os beneficios destas tecnoloxías.

3.1.5 Limitacións e retos da análise de vulnerabilidades

Malia a súa importancia, a análise de vulnerabilidades presenta diversas **limitacións e retos** que cómpre ter en conta á hora de interpretar os seus resultados.

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

Falsos positivos

En primeiro lugar, as ferramentas automatizadas poden xerar tanto **falsos positivos** (vulnerabilidades inexistentes, ou que en realidade non son explotables no contexto concreto) como **falsos negativos** (debilidades que pasan inadvertidas). Iso implica que os resultados deben ser revisados criticamente e, en caso necesario, validados mediante análise manual.

Necesidade de recursos

En segundo lugar, a implementación dun programa de análise de vulnerabilidades eficaz require **recursos especializados** (tempo, persoal, ferramentas), cousa que non sempre está ao alcance de todas as organizacións. Esta situación acentúase en contornas industriais, onde a coordinación entre equipos de TI, equipos OT e provedores externos engade complexidade.

Dinamismo das vulnerabilidades

Ademais, o propio dinamismo do panorama de ameazas fai que o conxunto de vulnerabilidades relevantes estea en constante evolución. Novas debilidades descóbrense de forma continua, mentres que outras pasan a ser especialmente críticas cando se constata a súa explotación activa en campañas reais.

Dispoñibilidade

En redes industriais, súmase un reto adicional: a **prioridade outorgada historicamente á dispoñibilidade** fronte a outros atributos de seguridade. Esta realidade fai que, en moitos casos, exista reticencia a introducir cambios —como actualizacións de firmware ou aplicación de parches— por medo a afectar ao funcionamento dos procesos.

Limitacións da contorna

Así mesmo, en determinados dispositivos IoT ou IIoT empregados en contornas industriais, as vulnerabilidades detectadas non poden corrixirse de forma directa, ben por limitacións de hardware, ben por ausencia de mecanismos de actualización, o que obriga a recorrer a controis compensatorios.

Volume de defectos

Por último, o elevado volume de información xerado polos escaneos esixe contar con criterios claros de **priorización**, de modo que os esforzos se concentren naquelas

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

vulnerabilidades cuxo tratamento achega un maior beneficio en termos de redución do risco. Disto falarase con maior profundidade noutros informes.

3.1.6 Pentesting vs análise de vulnerabilidades

No discurso habitual sobre ciberseguridade empréganse decote de xeito indistinto os termos **análise de vulnerabilidades** e **probas de penetración (pentesting)**, a pesar de que se trata de actividades con obxectivos, alcances e metodoloxías claramente diferenciadas (aínda que complementarias).

A **análise de vulnerabilidades** céntrase en **identificar e catalogar debilidades** mediante ferramentas automatizadas e revisións sistemáticas. O seu alcance adoita ser amplo: analízase un conxunto significativo de sistemas, servizos e dispositivos, xerando un inventario de vulnerabilidades que se clasifican por criticidade. Non se busca, en xeral, explotar esas debilidades, senón coñecer a súa existencia e valorar o seu impacto potencial.

As **probas de penetración**, pola contra, consisten na **simulación controlada de ataques reais**, levada a cabo por profesionais especializados. Partindo, en moitos casos, da información obtida nunha análise de vulnerabilidades, o obxectivo do pentest é **explotar de forma controlada** as debilidades detectadas para demostrar que podería lograr un atacante nun escenario real: acceder a datos sensibles, escalar privilexios, moverse lateralmente pola rede ou alterar o funcionamento dun sistema.

No contexto industrial, un exemplo ilustrativo sería o seguinte: mentres que unha análise de vulnerabilidades podería revelar que a interface web de administración dun PLC usa credenciais por defecto e executa unha versión de firmware vulnerable, unha proba de penetración podería demostrar que, aproveitando estas debilidades, é posible modificar a lóxica de control do PLC e alterar a secuencia de funcionamento dunha liña de produción.

As diferenzas entre ambos enfoques poden sintetizarse do seguinte xeito:

- **Propósito**: a análise de vulnerabilidades busca **detectar e clasificar**; o pentesting pretende **demostrar a explotabilidade e impacto real**.
- **Profundidade**: a análise de vulnerabilidades é tipicamente **máis ampla pero menos profunda**, mentres que o pentesting é **máis focalizado e detallado**.

- **Metodoloxía**: a análise apóiase fortemente en **ferramentas automatizadas**; o pentesting combina ferramentas e técnicas manuais, creatividade do analista e coñecemento específico da contorna.
- **Frecuencia**: a análise de vulnerabilidades plántase como unha actividade periódica e recorrente, mentres que as probas de penetración adoitan realizarse de forma máis puntual, asociadas a fitos (por exemplo, posta en produción dunha nova planta, cambios relevantes na arquitectura ou requisitos normativos).

Lonxe de seren excluíntes, ambas actividades **refórzanse mutuamente**. Un programa maduro de xestión de vulnerabilidades benefíciase da capacidade dos escáneres e solucións especializadas para identificar debilidades a gran escala, mentres que as probas de penetración achegan evidencia tanxible do risco que estas debilidades supoñen, axudando a priorizar esforzos e a sensibilizar aos responsables de negocio e operación sobre a necesidade de abordalas de forma sistemática.

3.2 Xestión e explotación

3.2.1 Etapas da análise de vulnerabilidades

A **análise de vulnerabilidades** (tamén denominada avaliación ou xestión de vulnerabilidades) é un proceso estruturado orientado a i**dentificar, analizar, priorizar e tratar** as debilidades presentes nos sistemas dunha organización. Aínda que existen variacións segundo o marco metodolóxico adoptado, pódense distinguir varias etapas comúns.

a) Identificación e clasificación de activos

O primeiro paso consiste en determinar **que activos se van protexer**. Isto implica elaborar e manter un inventario actualizado de sistemas, aplicacións, dispositivos e servizos, identificando aqueles que resultan máis críticos para o negocio. Nunha contorna industrial, isto inclúe non só servidores e equipos de rede, senón tamén PLC, HMI, RTU, gateways, sensores, robots, variadores de frecuencia ou sistemas de supervisión e adquisición de datos.

Unha clasificación axeitada dos activos —por criticidade, función, dependencia doutros sistemas ou impacto potencial en caso de fallo— permite orientar os esforzos de análise cara aqueles elementos cuxa vulnerabilidade suporía un maior risco.

b) Descubrimento e escaneo de vulnerabilidades

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

Unha vez definidos os activos, procédese á súa análise mediante **ferramentas automatizadas de escaneo**, que comparan a configuración e o software instalado con bases de datos de vulnerabilidades coñecidas. Estas ferramentas permiten detectar, entre outros aspectos, versións desactualizadas, servizos innecesarios, configuracións febles ou parámetros inseguros.

En contornas puramente TI, o escaneo pode levarse a cabo de forma relativamente intensiva. Porén, en contornas OT debe actuarse con **especial cautela**, xa que algúns tipos de escaneo poderían afectar a dispositivos sensibles ou a comunicacións de control en tempo real. Por este motivo, resulta habitual complementar ou substituír o escaneo activo por solucións de monitorización pasiva específicas para ICS.

c) Análise e priorización de resultados

Os achados obtidos na fase de escaneo deben ser **analizados e priorizados**, tendo en conta tanto a criticidade técnica da vulnerabilidade como o contexto operacional no que se atopa. Aínda que a puntuación CVSS proporciona unha referencia útil, en contornas industriais é necesario considerar factores adicionais, como o impacto sobre a seguridade das persoas, a dispoñibilidade da instalación ou o potencial efecto na calidade do produto.

Nesta etapa, resulta especialmente útil dispoñer de información sobre se unha vulnerabilidade está a ser **explotada activamente** (por exemplo, a través do catálogo KEV de CISA mencionado [7]) ou se forma parte de incidentes reais no ámbito industrial, o que reforza a necesidade de priorizar o seu tratamento.

d) Mitigación, remediación e verificación

Unha vez priorizadas as vulnerabilidades, defínense e implementan **accións de mitigación ou remediación**. Idealmente, isto implica a aplicación de parches de seguridade ou a actualización de firmware e configuracións. Non obstante, en contornas OT con restricións operativas ou tecnolóxicas, non sempre é posible aplicar parches de forma inmediata.

Nestes casos, recórrese a **controis compensatorios**, tales como a segmentación de redes, a aplicación de regras específicas en cortalumes industriais, o reforzo de mecanismos de autenticación ou a limitación de accesos remotos. Tras a implementación destas medidas, realízase unha **verificación** —mediante novos escaneos ou revisións— para confirmar que a vulnerabilidade foi corrixida ou que o seu risco se reduciu a un nivel aceptable.

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

e) Documentación e mellora continua

O proceso conclúe coa **documentación dos resultados**, as decisións adoptadas e as medidas implementadas. Esta documentación non só permite deixar constancia do traballo realizado, senón que facilita a mellora de políticas e procedementos, contribuíndo a consolidar un enfoque de **mellora continua** na xestión de vulnerabilidades.

3.2.2 Xestión das vulnerabilidades

A xestión de vulnerabilidades constitúe un proceso esencial dentro de calquera programa de ciberseguridade e, como se dicía, é un reto pola gran cantidade de defectos que aparecen nunha contorna. O nivel de risco non depende unicamente da presenza da vulnerabilidade, senón do **tempo que permanece sen mitigar**, do **momento do ciclo de vida** no que se atopa e da **capacidade real de explotación** por parte dun adversario. En contornas industriais e de operación (OT), onde a dispoñibilidade e a seguridade física son aspectos críticos, a falta de mitigación pode traducirse non só en incidentes dixitais, senón en disrupcións de proceso, danos sobre equipamento ou consecuencias para a seguridade física das persoas (safety en inglés).

Neste marco conceptual resulta imprescindible comprender dous parámetros fundamentais: o **tempo de explotación** e o **tempo de remediación**.

O **tempo de explotación** (time-to-exploit en inglés) describe a rapidez coa que un adversario consegue explotar unha vulnerabilidade desde a súa divulgación inicial. As investigacións do informe **ENISA State of Cybersecurity Vulnerabilities 2018–2019** [29] (o único especializado neste eido atopado), revelan que este intervalo se reduciu de forma significativa nos últimos anos, chegando a observarse casos nos que a explotación se produce en **cuestión de horas ou días**.

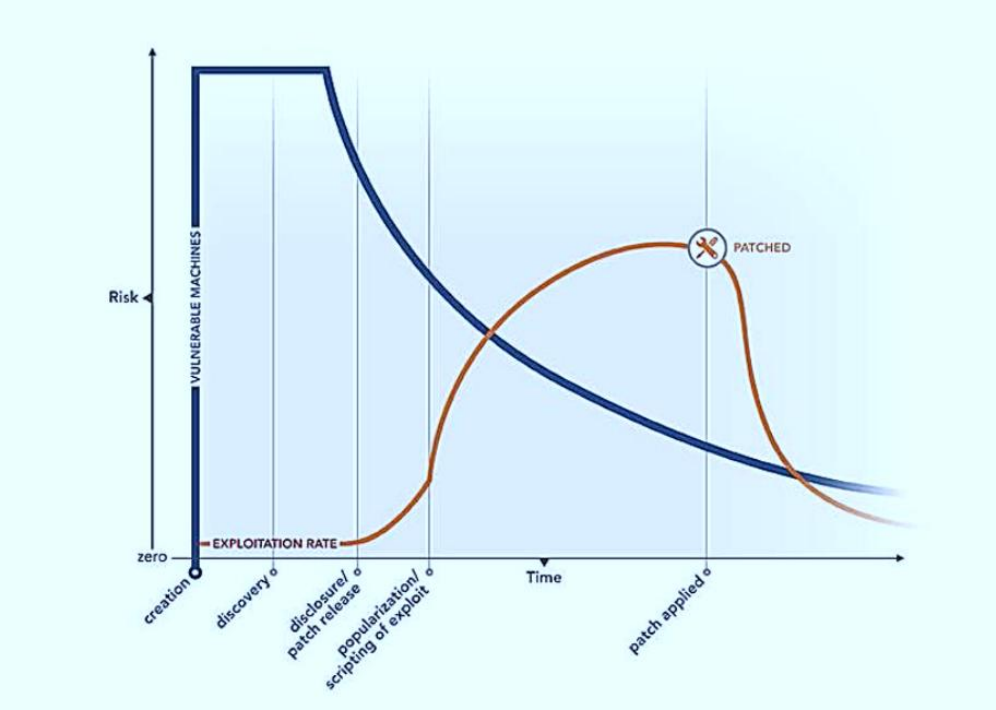
Os ataques dirixidos mediante APT (Advanced Persistent Threat, técnicas avanzadas), patrocinados en moitos casos por estados nación por motivos xeopolíticos ou estratéxicos, caerían dentro da categoría dos non parcheables, pois nin sequera terían sido divulgadas as vulnerabilidades (concepto coñecido como vulnerabilidades de día cero, ou zero-day).

Pola súa banda, o **tempo de remediación** (time-to-remediate en inglés) mide canto tarda unha organización en aplicar a medida correctiva recomendada. En contornas OT, este tempo adoita ser considerablemente maior que no ámbito TI debido á necesidade

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

de planificar xanelas de mantemento, validar os parches en sistemas críticos ou cumprir con restricións de certificación de equipos industriais.

Cando o tempo de explotación é menor que o tempo de remediación, a vulnerabilidade transita por unha fase especialmente delicada na que o risco se amplifica. Ese risco asociado a unha vulnerabilidade pode entenderse como o resultado da interacción entre **probabilidade de explotación** e **impacto potencial**. E o risco non é constante, senón que evoluciona co tempo, como se pode ver na seguinte figura.



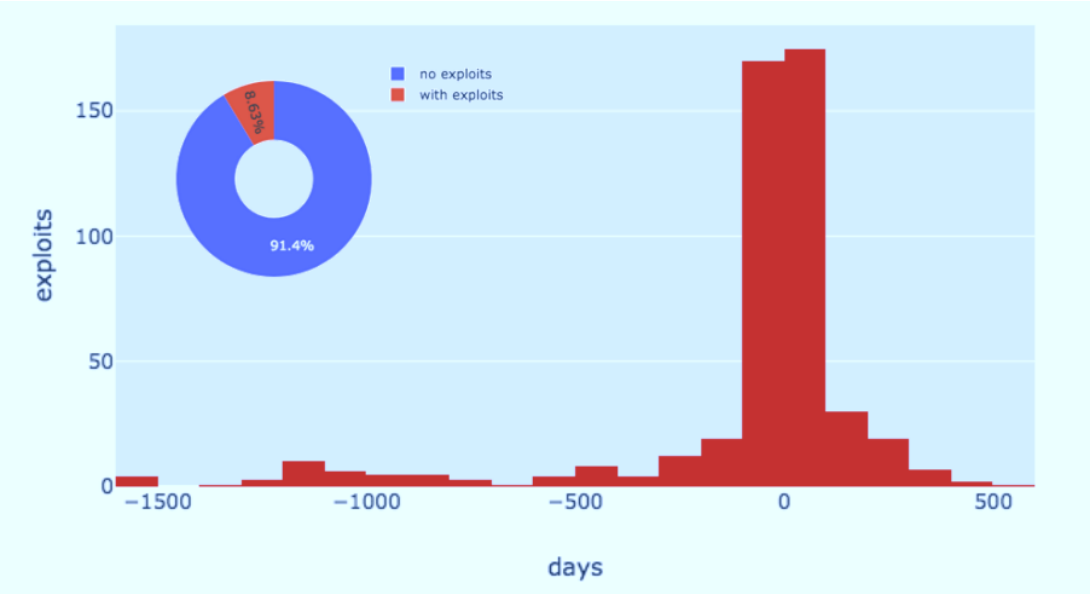
Risco dunha vulnerabilidade fronte ao tempo. Fonte: Alert Logic (2014)

A medida que avanza o ciclo de vida da vulnerabilidade —desde a súa descoberta ata a súa explotación activa en campañas reais— as condicións cambian tanto para atacantes como para defensores. Polo lado ofensivo, a dispoñibilidade de información técnica, probas de concepto ou exploits automatizados reduce o esforzo necesario para comprometer un sistema. Polo lado defensivo, cada día que pasa sen aplicar un parche, unha actualización de firmware ou unha mitigación alternativa amplía a xanela de exposición, especialmente cando a vulnerabilidade é amplamente coñecida ou figura en catálogos como o KEV de CISA [7].

Os estudos especializados que analizan a evolución do risco reforzan esta idea. O informe de ENISA State of Cybersecurity Vulnerabilities 2018–2019 [29] mostra como o tempo desempeña un papel determinante na probabilidade de explotación: **polo menos o 8,65 % de todas as vulnerabilidades analizadas eran explotables no**

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

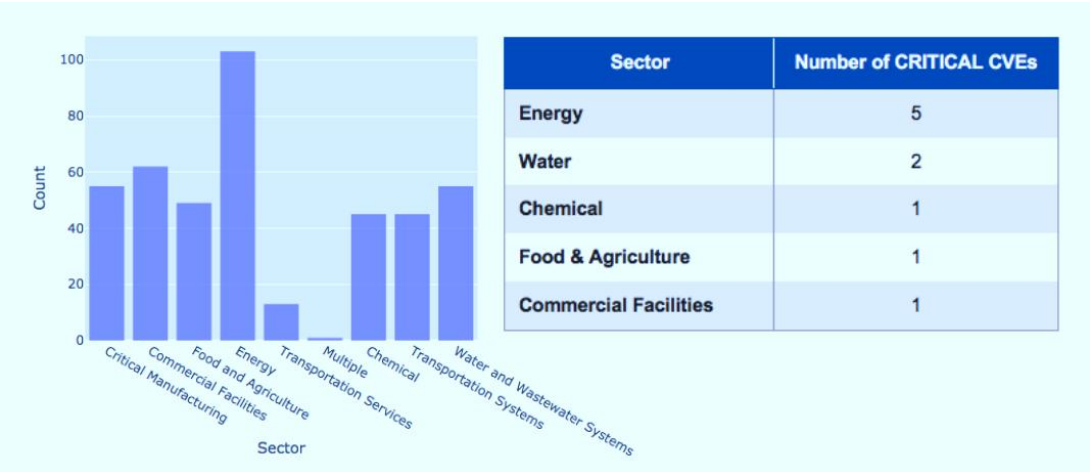
momento do estudo, e as vulnerabilidades **CRÍTICAS presentaban un tempo medio de aparición do exploit de só 24,83 días** respecto da súa data de publicación, significativamente menor que en vulnerabilidades doutras categorías.



Tempo de aparición do exploit desde a publicación da vulnerabilidade (t=0). Fonte: ENISA (2019)

Como se ve, as vulnerabilidades nalgúns casos comezan a explotarse mesmo varios anos antes da publicación das mesmas.

A continuación amósanse os datos do informe de ENISA en canto a vulnerabilidades detectadas por sector de actividade:



Sector	Number of CRITICAL CVEs
Energy	5
Water	2
Chemical	1
Food & Agriculture	1
Commercial Facilities	1

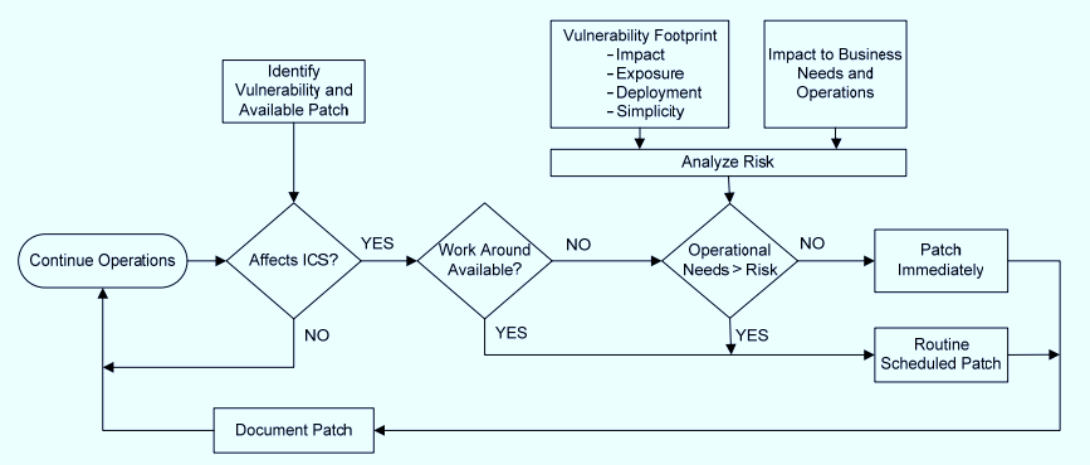
Vulnerabilidades por sector. Fonte: ENISA (2019)

A investigación revela ademais que, en numerosas ocasións, os atacantes desenvolven comprobacións automatizadas para detectar activos vulnerables pouco despois da divulgación dunha vulnerabilidade, acelerando o proceso de explotación.

Moitas vulnerabilidades alcanzan o seu punto crítico semanas ou meses despois de facerse públicas, cando os exploits maduraron e se incorporan a ferramentas automatizadas e kits de ataque. Este comportamento explica por que vulnerabilidades antigas continúan a ser explotadas durante anos cando non se aplican medidas correctivas.

Unha dinámica semellante dedúcese das guías operativas de CISA para xestión de parches en contornas ICS [30], que describen a **xanela de remediación** como o período máis crítico do ciclo de vida da vulnerabilidade. Tras a publicación dun parche ou mitigación oficial, os atacantes poden analizar os cambios introducidos para comprender o fallo subxacente e xerar exploits funcionais. CISA sinala que os sistemas que non aplican parches se converten en obxectivos preferentes, e subliña que **a maioría dos ataques exitosos se apoian en vulnerabilidades coñecidas para as que xa existía parche**. Neste contorna, cada día de atraso incrementa a probabilidade de explotación, especialmente cando a vulnerabilidade pasou a formar parte do catálogo KEV [7] ou dispón dun exploit público totalmente funcional.

Para facilitar a priorización por parte dos xestores de redes OT, CISA propón unha árbore de decisión de urxencia de parcheo:



Árbore de decisión de urxencia de parcheo. Fonte: CISA (2008)

Por último, a análise de Qualys sobre as vulnerabilidades máis explotadas en 2023 [31] mostra que **varias das dez vulnerabilidades máis explotadas tiñan máis de cinco anos desde a súa divulgación**, e aínda así continuaban a rexistrar actividade maliciosa

significativa. Ademais, o estudo destaca, aliñado con ENISA, que **as vulnerabilidades con exploits dispoñibles tardan unha media de menos de 30 días en seren explotadas activamente**, consolidando a idea de que a dispoñibilidade de código público acelera a explotación a escala industrial.

Polo tanto, a xestión eficaz de vulnerabilidades non se limita a identificar debilidades nos sistemas, senón que esixe unha comprensión profunda de como evoluciona o risco ao longo do tempo e de como estes factores se combinan para crear oportunidades de ataque. En contornas OT, onde a seguridade está estreitamente vinculada á dispoñibilidade e á integridade do proceso produtivo, adoptar esta visión resulta esencial para reducir a exposición efectiva fronte a adversarios cada vez máis rápidos en aproveitar vulnerabilidades coñecidas.

3.3 ROI (Retorno do Investimento)

Para comprender plenamente o impacto económico da xestión de vulnerabilidades, resulta útil complementar a explicación conceptual cun **método estruturado de cálculo do ROI** (Return of Investment en inglés), amplamente utilizado en análises de riscos e baseado nun enfoque cuantitativo [32][33][34][35]. Isto permite non só estimar as perdas esperadas, senón tamén cuantificar os beneficios económicos derivados de aplicar medidas correctivas ou mitigadoras.

Deseguido preséntase o procedemento teórico, seguido dun exemplo práctico aplicado a unha contorna industrial.

1. Identificación de activos e o seu valor económico (Asset Value, AV)

O primeiro paso consiste **en determinar que activos están en risco e cal é o seu valor**. Nunha contorna industrial, un activo pode ser un PLC, un sistema SCADA, unha liña de produción, un robot ou mesmo un servidor de enxeñaría. O valor do activo (AV) inclúe non só o seu custo de substitución, senón tamén os custos de indispoñibilidade, perda de produción e efectos colaterais derivados do seu fallo.

2. Identificación de ameazas relevantes (pares activo–ameaza)

A cada activo asígnanselle ameazas plausibles: explotación remota dunha vulnerabilidade do PLC, manipulación de parámetros nunha HMI, caída do servidor SCADA por ransomware, etc. Cada par activo–ameaza permite cuantificar o risco de maneira illada.

3. Cálculo do Factor de Exposición (Exposure Factor, EF)

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

O EF expresa a **porcentaxe de perda que sufriría o activo se a ameaza se materializa**. Por exemplo, unha parada de liña causada polo compromiso dun PLC podería representar un EF do 25%, mentres que a corrupción total dun sistema SCADA podería acadar un EF do 80%.

4. Cálculo da perda por evento (Single Loss Expectancy, SLE)

Obtense mediante a fórmula seguinte, e **expresa a perda asociada a un evento individual**:

$$\mathbf{SLE = AV \times EF}$$

Se o activo ten un valor de 200.000 € e o EF é do 40%, entón:

$$\mathbf{SLE = 200.000\ € \times 0{,}40 = 80.000\ €}$$

5. Probabilidade anual de materialización (Annual Rate of Occurrence, ARO)

O ARO **expresa cantas veces ao ano se espera que se materialice a ameaza.** Pode estimarse mediante estatísticas históricas, información do sector, análise experta ou intelixencia de ameazas. Un ARO de 0,5 indica que o incidente podería producirse aproximadamente unha vez cada dous anos.

6. Cálculo da perda anual esperada (Annual Loss Expectancy, ALE)

Calcúlase como:

$$\mathbf{ALE = SLE \times ARO}$$

Seguindo o exemplo anterior:

$$\mathbf{ALE = 80.000\ € \times 0{,}5 = 40.000\ €/ano}$$

7. Avaliación de contramedidas e do seu impacto

Analízanse controis técnicos ou organizativos: segmentación de rede, actualización de firmware, despregamento de cortalumes industriais, hardening do PLC, monitorización OT, etc. Cada contramedida pode reducir o EF (menor impacto), o ARO (menor probabilidade) ou ambos.

Supoñamos que a aplicación de parches e a segmentación reducen:

- o EF do 40% ao **10%,**
- o ARO de 0,5 a **0,1.**

Os novos valores serían:

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

$$\mathbf{SLE_2 = AV \times EF_2 = 200.000\ € \times 0{,}10 = 20.000\ €}$$

$$\mathbf{ALE_2 = SLE_2 \times ARO_2 = 20.000\ € \times 0{,}1 = 2.000\ €/ano}$$

8. Cálculo do ROI das contramedidas

Se o custo de aplicar as medidas é de 15.000 €, o ROI sería:

$$\mathbf{ROI = (ALE_1 - ALE_2 - custo\ das\ medidas)}$$

$$\mathbf{ROI = (40.000\ € - 2.000\ € - 15.000\ €) = 23.000\ €}$$

Un ROI positivo indicaría que o investimento compensa economicamente, ademais de reducir de forma significativa o risco operacional.

3.3.1 Exemplo práctico aplicado a unha contorna OT

Para ilustrar o valor do ROI en contornas industriais, consideremos agora un activo de alto valor económico: un **sistema SCADA central** que supervisa varios procesos críticos dentro dunha instalación industrial. O seu valor operativo (AV), considerando perdas de produción, penalizacións contractuais, riscos de calidade e potencial impacto físico, estímase en **5.000.000 €**.

O fabricante publica unha vulnerabilidade crítica que permite execución remota de código. Baseándonos en estudos de ENISA e CISA, sabemos que vulnerabilidades críticas poden dispoñer dun exploit funcional en **menos de 25 días**, e que as vulnerabilidades coñecidas sen parche aplicado figuran entre os vectores máis explotados a escala global.

Se estimamos un EF do **40%** (impacto severo sobre a operación) e un ARO de **0,35**, a perda anual esperada antes de mitigación sería:

$$\mathbf{SLE = 5.000.000\ € \times 0{,}40 = 2.000.000\ €}$$

$$\mathbf{ALE = 2.000.000\ € \times 0{,}35 = 700.000\ €/ano}$$

Aplicar segmentación avanzada, parcheo de vulnerabilidades do SCADA, endurecemento de accesos remotos e monitorización OT reduce o EF ao **10%** e o ARO a **0,1**:

$$\mathbf{SLE_2 = 5.000.000\ € \times 0{,}10 = 500.000\ €}$$

$$\mathbf{ALE_2 = 500.000\ € \times 0{,}1 = 50.000\ €/ano}$$

Se o custo conxunto destas medidas ascende a **150.000 €**, entón:

$$\mathbf{ROI = (700.000 - 50.000 - 150.000) = 500.000\ €}$$

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

Este resultado demostra que, para activos industriais de alto valor, a mitigación de vulnerabilidades ofrece un retorno económico moi elevado e constitúe un elemento clave para garantir a continuidade operativa e reducir o risco global.

4 Alertas

4.1 Panorama de ataques

O panorama de ameazas contra sistemas de control industrial (ICS) e tecnoloxías de operación (OT) mostra, nos últimos anos, un **medre sostido no volume de ataques, na súa sofisticación técnica e na amplitude de sectores afectados**. A información dispoñible procede en gran medida de informes de intelixencia de fabricantes especializados, enquisas sectoriais e repositorios de incidentes, polo que debe interpretarse sempre tendo en conta unha limitación clave: **os datos dispoñibles representan só unha fracción dos incidentes reais**, xa que moitas organizacións optan por non facelos públicos por motivos de confidencialidade, impacto reputacional ou ausencia de obrigas regulamentarias de notificación.

Neste apartado sintetízanse algunhas das fontes máis relevantes —SANS Institute, Dragos, Nozomi, Kaspersky ICSCERT ou ICSStrive— co obxectivo de ofrecer unha visión integrada de:

- **Tendencias xerais de ameazas e ataques.**
- **Evolución cuantitativa** (volume de incidentes e sistemas afectados).
- **Técnicas predominantes** empregadas polos atacantes.
- **Sectores e rexións máis impactados**, con referencias específicas a Europa e, cando é posible, a datos que afectan indirectamente ao contexto español.

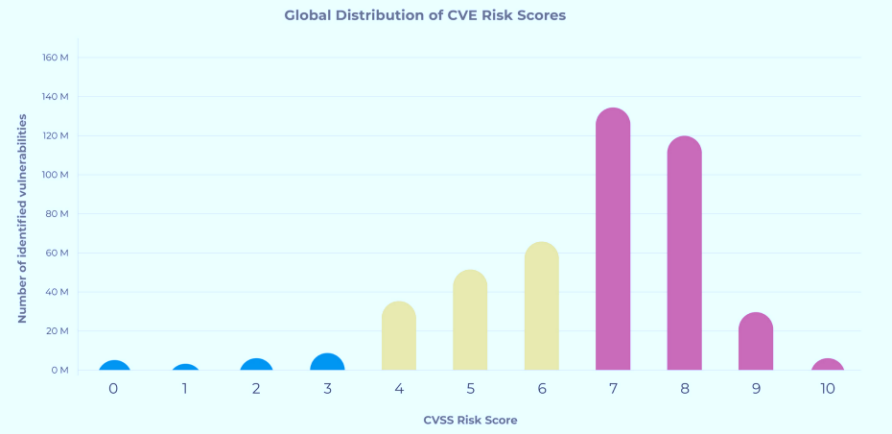
Algúns destes aspectos trataranse con máis profundidade en futuros entregables do Observatorio de Ciberseguridade Industrial, como o Informe de Intelixencia de Ameazas.

4.1.1 Tendencias xerais

Os informes de Nozomi Networks Labs **Trends e Insights 2025** [36] revelan un crecemento continuo na cantidade e gravidade de vulnerabilidades ICS. A súa última análise recolle **241 novos avisos de CISA** aplicables a contornas industriais e **619 vulnerabilidades ICS divulgadas**, afectando a uns **70 fabricantes distintos**. De particular relevancia é que **a maioría presenta puntuacións CVSS ≥ 7**, o que confirma un risco elevado de explotación.

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

Así mesmo, Nozomi identifica **catro vulnerabilidades catalogadas como KEV** (Known Exploited Vulnerabilities) por CISA, e **unhas vinte cun EPSS superior ao 1 %**, o que implicaba unha probabilidade realista de explotación a curto prazo (EPSS ou Exploit Prediction Scoring System é un sistema de ciberseguridade que usa aprendizaxe automático para predecir qué vulnerabilidades (CVEs) teñen maior probabilidad de seren explotadas nos próximos 30 días). A distribución sectorial mostra maior concentración en **Manufactura Crítica e Enerxía**, seguida de Comunicacións, sectores todos eles con forte presenza en Galicia.



Distribución de CVE por severidade. Fonte: Nozomi Networks (2025)

Distribution of CVEs by Exploitability and Severity

Exploitability \ Severity	Low	Medium	High	Critical
Very High (75–100%)	0%	1%	2%	10%
High (50–75%)	0%	0%	1%	9%
Medium (25–50%)	0%	1%	2%	9%
Low (0–25%)	99%	97%	95%	72%

Explotabilidade das vulnerabilidades fronte a severidade. Fonte: Nozomi Networks (2025)

Pola súa banda, o informe **2025 OT Cyber Threat Report** de **ICSStrive** [37] reflicte unha intensificación substancial dos ataques que xeran **impacto físico en procesos industriais** (indispoñibilidade de produción). A análise longitudinal da súa base de datos mostra un **incremento acumulado do 146 % nos ataques con repercusión física directa** en sedes operativas desde o ano anterior. Este patrón indica unha escalada progresiva na agresividade e consecuencias das intrusións en OT, observándose casos nos que unha brecha inicial permite comprometer múltiples plantas ou centros de produción.

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

Número de sedes impactadas por incidentes con impacto físico en contornas ICS. Fonte: ICSStrive (2025)

É destacable que a base de datos de ICSStrive, activa desde 2017, contén **centos de incidentes documentados**, incluídos ataques que derivaron en paradas de planta, danos a equipos, alteracións na calidade do produto ou interrupcións graves de procesos críticos. Pódese consultar o detalle agregado no propio informe enlazado.

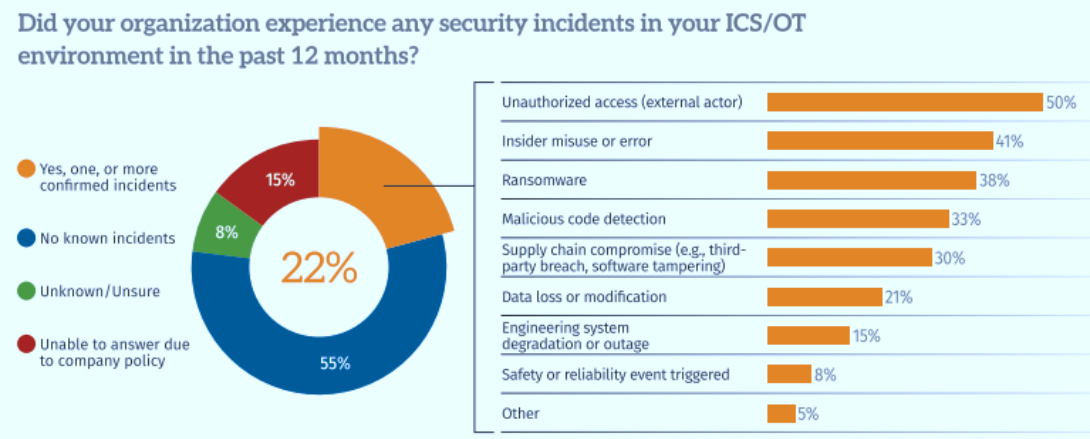
4.1.2 Detalles

4.1.2.1 Ransomware, accesos remotos e velocidade de execución

Os datos agregados de **SANS State of ICS/OT Security 2025** [38] confirman que as contornas ICS/OT seguen a enfrontarse a ameazas de alto impacto. Segundo a súa enquisa internacional, o **22 % das organizacións experimentou polo menos un incidente ICS/OT nos últimos 12 meses**. Os principais vectores foron:

- **Acceso externo non autorizado (50 %)**
- **Ransomware (38 %)**

Ademais, preto do **40 % dos incidentes provocaron interrupcións operativas** e arredor do 20 % implicaron perdas financeiras, exposición de datos ou riscos para a seguridade física.



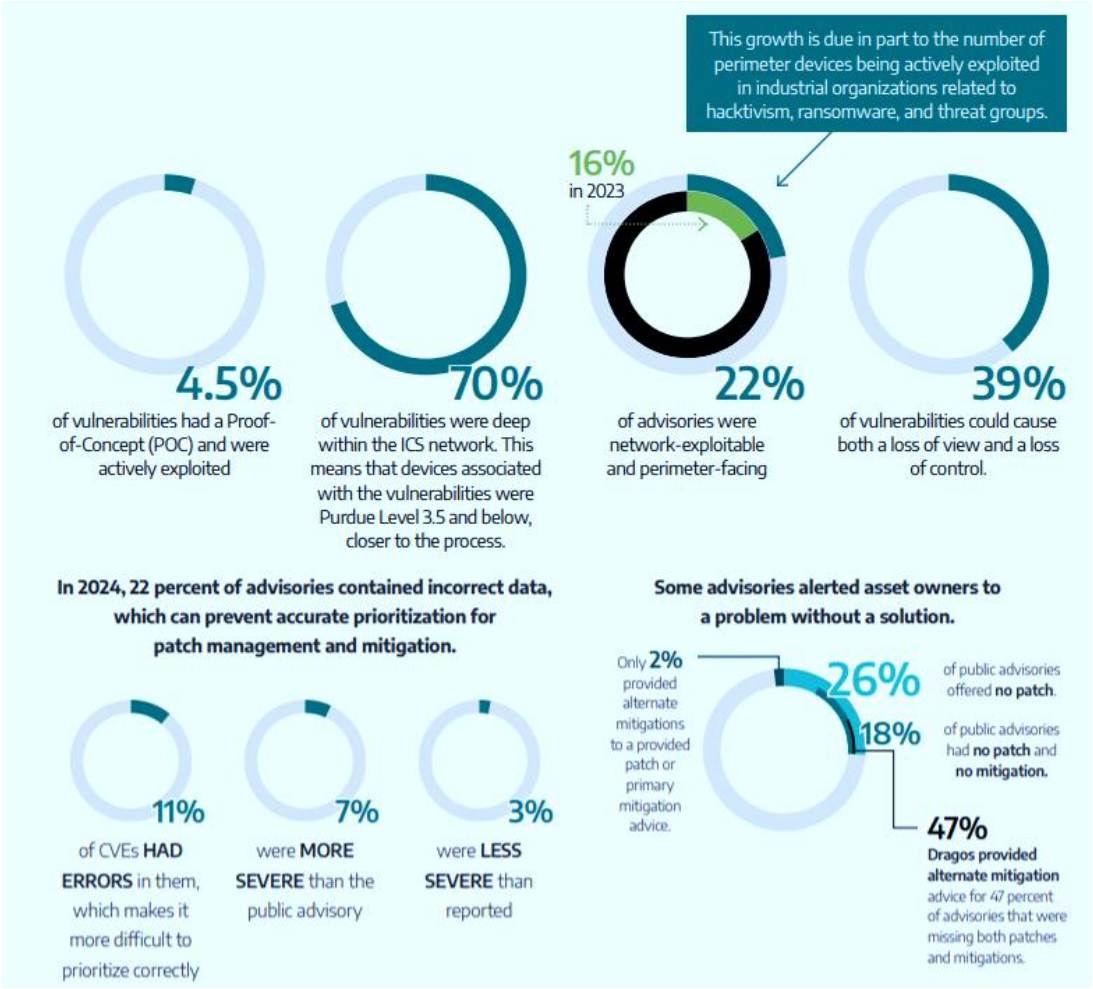
Enquisa de incidentes en contornas ICS/OT. Fonte: SANS (2025)

O informe de ICSStrive complementa estes datos coa observación de que, en incidentes de ransomware contra organizacións industriais, o **tempo medio entre a intrusión e a activación do cifrado é duns 16 horas**, sendo moitos casos considerablemente máis rápidos. Esta xanela tan reducida incrementa a necesidade de capacidades de **detección temperá, vixilancia 24x7 e resposta automatizada en OT**.

4.1.2.2 Vulnerabilidades analizadas

O informe **Dragos – Year in Review 2025** [39] sinala que, na comunicación pública das vulnerabilidades, o CVSS por si só non reflicte ben o risco real en contornas OT. Ademais, en 2024 un 22 % dos advisories incluían datos incorrectos e un 26 % non ofrecían parche, polo que a priorización debe complementarse con contexto operativo e medidas alternativas.

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



Detalle de vulnerabilidades OT de 2024 analizadas. Fonte: Dragos (2025)

4.1.2.3 Sectores e rexións máis afectados

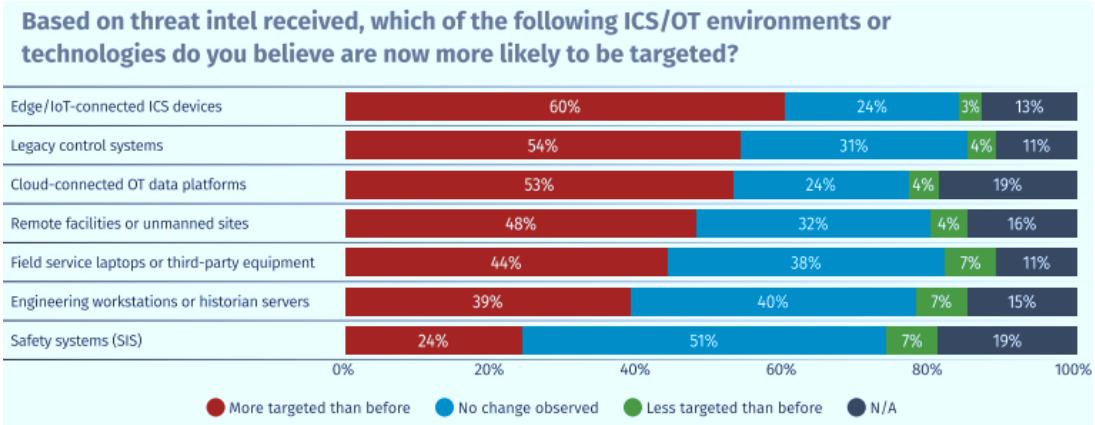
Os sectores máis impactados de forma consistente nas distintas fontes inclúen **enerxía, manufactura, auga, alimentación e loxística**, todos eles con forte peso en Galicia.

Segundo **Kaspersky ICS CERT** [40][41][42], aproximadamente **un de cada cinco equipos ICS bloqueou obxectos maliciosos** durante o segundo trimestre de 2025. A proporción global situouse arredor do **21,32%** con incrementos notorios en rexións como **Australia/Nova Zelandia e Europa do Norte**.

No referente a **vectores de ataque**, destaca un aumento continuado das ameazas procedentes do **correo electrónico**, con **picos próximos ao 7 % de equipos ICS afectados en Europa do Sur**, rexión que inclúe España. Este dato pon de manifesto a relevancia de reforzar políticas de filtrado e segmentación para evitar que accesos IT deriven en compromisos OT.

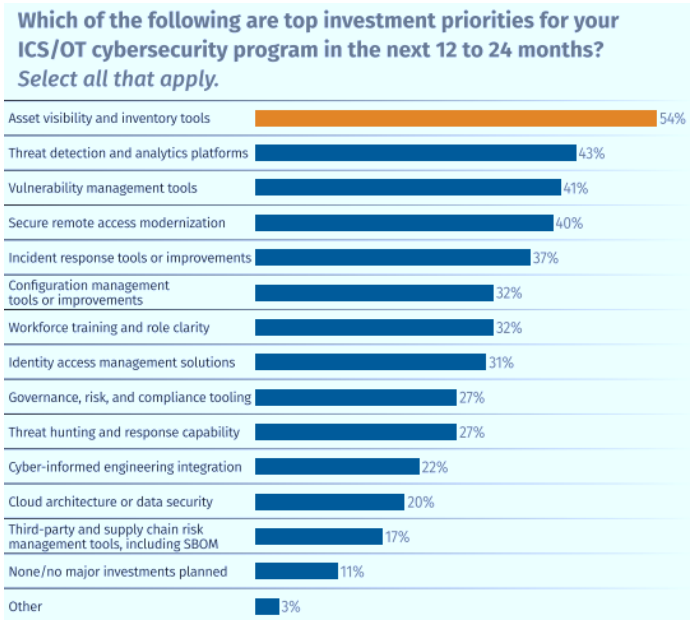
O informe rexional **Kaspersky – Threat landscape for industrial automation systems (Europe, Q2 2025)** sitúa **Europa do Sur e do Este** entre as áreas europeas con **maior risco de ataques dirixidos**, debido á combinación de campañas de phishing, spyware e outros tipos de malware orientados a contornas industriais.

En canto á percepción do risco e prioridades de investimento, **SANS** sinala en [38] que máis do **50 % das organizacións** considera que os sistemas en **legacy, no Edge/IoT e conectados á nube** se volveron os máis atractivos para os atacantes:



Probabilidade de sufrir un ataque por tipo de activo segundo os enquisados. Fonte: SANS (2025)

Ao mesmo tempo, as prioridades de investimento para os próximos 12–24 meses céntranse en **visibilidade de activos, detección de ameazas e xestión de vulnerabilidades**, reflectindo unha maduración progresiva na estratexia defensiva industrial.



Prioridade de investimento en ciberseguridade OT segundo os enquisados. Fonte: SANS (2025)

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

4.1.2.4 Limitacións dos datos e relevancia para Galicia

A pesar do valor que achegan os informes analizados, é necesario interpretar as súas conclusións con cautela.

O **subrexistro de incidentes** segue a ser un factor determinante, xa que moitas organizacións optan por non facer públicos os ataques que sofren, ben por medo ao impacto reputacional, ben pola ausencia de obrigas regulamentarias que lles esixan notificar eses incidentes. A isto súmase un **sesgo rexional significativo**: as rexións con marcos normativos máis estritos ou con maior cultura de reporte tenden a amosar cifras máis completas, mentres que outras áreas permanecen infrarrepresentadas. Tamén cómpre considerar a **dependencia de telemetría** propia de fabricantes como Nozomi ou Kaspersky, cuxas análises se basean en datos procedentes de organizacións que empregan as súas solucións, o que deixa fóra sectores ou xeografías que non dispoñen destas tecnoloxías.

Estas limitacións non restan relevancia ás tendencias observadas, especialmente no caso de Galicia. A comunidade conta cunha **elevada concentración de sectores intensivos en OT**, como enerxía, auga, automoción, naval, alimentación ou loxística, todos eles amplamente mencionados como obxectivos recorrentes nos informes internacionais. Ademais, España forma parte de **Europa do Sur**, unha rexión que Kaspersky identifica de maneira sistemática como unha das máis expostas a ameazas dirixidas contra sistemas industriais. A combinación de **ransomware, accesos remotos inseguros, vulnerabilidades ICS de alta severidade e a crecente superficie IoT** encaixa de maneira precisa coa estrutura tecnolóxica de boa parte do tecido industrial galego.

No seu conxunto, este panorama constitúe un insumo para **priorizar medidas de protección**, que se exporán nunha sección posterior.

4.2 Últimas alertas

Co obxectivo de proporcionar unha visión clara e accionable do estado das vulnerabilidades que afectan ás contornas industriais, este informe incorpora unha sección dedicada ás **alertas publicadas durante o último trimestre** por fontes oficiais. Dado que o boletín está concibido con periodicidade **trimestral**, este enfoque permite ofrecer un resumo manexable, actualizado e directamente aplicable para os equipos técnicos e responsables de seguridade.

Antes de presentar as alertas máis relevantes, resulta fundamental explicar brevemente **onde pode o lector consultar, monitorizar ou subscribirse a estas notificacións**, tanto para contornas **ICS/OT** como para infraestruturas **TI** que, debido á crecente converxencia tecnolóxica, poden ter un impacto indirecto ou directo sobre a operación industrial.

4.2.1 Fontes principais de avisos

Ademais dos avisos específicos de cada fabricante —que se incluirán de maneira estruturada nun anexo posterior ao final do informe— as seguintes plataformas constitúen os repositorios máis fiables e actualizados para o seguimento de vulnerabilidades significativas:

- **INCIBE-CERT – Avisos de Seguridade en Sistemas de Control Industrial** [43]: Fonte nacional de referencia para España en materia de ciberseguridade industrial. Publica vulnerabilidades relevantes de fabricantes ICS e fornece información técnica, CVSS, impacto e medidas de mitigación.
- **CCN-CERT – Alertas e vulnerabilidades** [44][45]: Aínda que orientado principalmente a administracións públicas, a súa utilidade é transversal. Inclúe boletíns de severidade alta que poden afectar a sistemas IT con impacto potencial en contornas OT interconectados.
- **CISA – ICS Advisories (ICSA)** [46]: É a base de datos máis recoñecida a nivel internacional para avisos de sistemas de control industrial. Inclúe información detallada, CVSS, produtos afectados, descrición técnica, escenarios de explotación e mitigacións.

Estas fontes constitúen a base mínima para un programa de vixilancia de vulnerabilidades en organizacións industriais, complementadas cos **avisos dos fabricantes cuxos equipos estean despregados en planta (ver anexo con algúns deles)**.

4.2.2 Consideracións clave para a interpretación de alertas

Ao revisar vulnerabilidades ICS é importante lembrar que:

- As **puntuacións CVSS non sempre reflicten o risco real en OT**, onde a dispoñibilidade e a seguridade física son factores críticos.

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

- As alertas de TI (por exemplo, servizos Windows ou middleware corporativo) **poden impactar OT** se se utilizan estacións de enxeñaría, servidores SCADA ou sistemas de mantemento remoto.
- Moitas vulnerabilidades de fabricantes ICS **non poden parchearse inmediatamente** debido a restricións operativas, polo que as mitigacións compensatorias adquiren un papel central.
- A maioría de advisories carecen de telemetría sobre explotación activa; por iso, fontes como **CISA KEV** [7] ou reportes de intelixencia industrial axudan a priorizar.

Esta sección servirá en cada informe como referencia práctica para equipos de seguridade, mantemento e operación, axudando a tomar decisións informadas sobre que vulnerabilidades aparecen novas e son destacables polo seu alto risco.

4.2.3 Alertas ICS de alta criticidade do trimestre

De entre os avisos publicados no período analizado, preséntanse a continuación as **vulnerabilidades de severidade alta ou crítica** que afectan directamente a **contornas ICS**, seguindo un formato sintético e orientado á acción. Cada ficha resume os elementos clave para facilitar unha rápida procura, pero sen excesivo detalle. Para iso convídase a consultar a fonte orixinal de INCIBE-CERT (que aglutina en formato estruturado os avisos de orixe internacional).

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DE SUNBIRD
URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-sunbird
Produtos afectados: Sunbird DCIM (varias versións).
Vector de ataque: Acceso remoto non autenticado / manipulación de parámetros / escalada.
Severidade: Alta–Crítica (segundo módulo afectado).
Impacto potencial en OT: Acceso non autorizado a sistemas de xestión de infraestruturas críticas; posibilidade de manipular datos de monitorización, alterar configuracións ou provocar perda de visibilidade.
Probabilidade de explotación: Moderada; funcións expostas a través da interface web e da API.
Mitigacións inmediatas: Parchear segundo a versión; restrinxir accesos web;

segmentar a rede de xestión; esixir autenticación robusta.
Prioridade: Moi alta.

MECANISMO DE RECUPERACIÓN DE CONTRASINAIS DÉBIL EN MAXHUB PIVOT

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/mecanismo-de-recuperacion-de-contrasenas-debiles-en-maxhub-pivot

Produtos afectados: MAXHUB Pivot – plataforma colaborativa.

Vector de ataque: Explotación dun mecanismo feble de recuperación de contrasinais.

Severidade: Alta.

Impacto potencial en OT: Compromiso de contas administrativas utilizadas en salas de control ou contornas híbridas OT/IT; risco de movemento lateral.

Probabilidade de explotación: Elevada se o servizo está exposto a Internet.

Mitigacións inmediatas: Actualizar o firmware; deshabilitar funcións expostas; aplicar MFA nos accesos administrativos.

Prioridade: Alta.

INXECCIÓN SQL EN IVIEW DE ADVANTECH

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/inyeccion-sql-en-iview-de-advantech-0

Produtos afectados: Advantech iView – plataforma de monitorización industrial.

Vector de ataque: Inxección SQL a través de peticións HTTP non saneadas.

Severidade: Crítica.

Impacto potencial en OT: Compromiso total do servidor de monitorización; posibilidade de alterar datos, credenciais ou parámetros de rede; risco de interrupción operacional.

Probabilidade de explotación: Alta; vectores sinxelos e documentados.

Mitigacións inmediatas: Parchear; segmentar; bloquear acceso externo; activar WAF; revisar credenciais.

Prioridade: Moi alta.

OMISIÓN DE AUTENTICACIÓN EN MONITORING PLATFORM DE SOLISCLOUD

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/omision-de-autenticacion-en-monitoring-platform-de-soliscloud

Produtos afectados: SolisCloud – plataforma de monitorización de inversores solares.

Vector de ataque: Omisión de autenticación na API web.
Severidade: Alta–crítica.
Impacto potencial en OT: Acceso directo a datos de produción enerxética; posibilidade de manipular parámetros de monitorización ou de xestión remota.
Probabilidade de explotación: Alta se o sistema está exposto.
Mitigacións inmediatas: Limitar accesos; implementar autenticación obrigatoria; segmentación estrita; actualizar á versión corrixida.
Prioridade: Moi alta.

VALIDACIÓN INADECUADA EN ISTAR DE JOHNSON CONTROLS
URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/validacion-inadecuada-en-istar-de-johnson-controls
Produtos afectados: Johnson Controls iSTAR – sistemas de control de accesos.
Vector de ataque: Validación insuficiente de parámetros.
Severidade: Alta.
Impacto potencial en OT: Risco de manipulación do control de accesos físicos; impacto directo na seguridade de instalacións industriais.
Probabilidade de explotación: Moderada.
Mitigacións inmediatas: Parcheo; endurecemento de rede; aplicar monitorización de integridade.
Prioridade: Alta.

MÚLTIPLES VULNERABILIDADES EN EC² NMIS/BIODOSE DE MIRION MEDICAL
URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-el-software-ec2-nmis-biodose-de-mirion-medical
Produtos afectados: Mirion EC² NMIS / Biodose – sistemas de medición e monitorización radiolóxica.
Vector de ataque: Varias vulnerabilidades (inclúe acceso non autenticado, exposición de datos e escalada).
Severidade: Alta–crítica.
Impacto potencial en OT: Risco para sistemas de seguridade radiolóxica; perda de integridade nas medicións; posible alteración de alarmas.
Probabilidade de explotación: Moderada–alta segundo o vector.
Mitigacións inmediatas: Parchear; limitar acceso á rede interna; segmentar sistemas

de seguridade.

Prioridade: Moi alta.

FALTA DE AUTENTICACIÓN EN PRODUTOS DE ISKRA

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/falta-de-autenticacion-en-productos-de-iskra

Produtos afectados: Equipos Iskra (medición/xestión enerxética).

Vector de ataque: Acceso non autenticado a interfaces de xestión.

Severidade: Crítica.

Impacto potencial en OT: Risco directo para redes de enerxía; alteración de medicións ou parámetros de control; interrupcións do servizo.

Probabilidade de explotación: Alta.

Mitigacións inmediatas: Aplicar autenticación forte; segmentar; revisar accesos remotos; parchear se procede.

Prioridade: Moi alta.

CONTROL INADECUADO DE XERACIÓN DE CÓDIGO EN LONGWATCH (VÍDEO INDUSTRIAL E CONTROL)

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/control-inadecuado-de-la-generacion-de-codigo-en-longwatch-de-industrial-video

Produtos afectados: Longwatch Video System – sistemas de vídeo industrial.

Vector de ataque: Inxección de código / xeración dinámica insegura.

Severidade: Alta.

Impacto potencial en OT: Manipulación de vídeo industrial; cegueira operativa; risco en operacións remotas.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Parchear; restrinxir interfaces web; aplicar segmentación.

Prioridade: Alta.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS CODESYS

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-codesys-1

Produtos afectados: CODESYS V2/V3 e compoñentes asociados.

Vector de ataque: Execución remota de código, desbordamentos, elusión da

autenticación.

Severidade: Crítica.

Impacto potencial en OT: Compromiso directo de PLCs e lóxica de control; risco máximo para a produción.

Probabilidade de explotación: Moi alta; CODESYS está amplamente utilizado en múltiples fabricantes.

Mitigacións inmediatas: Parchear; restrinxir portos; segmentar; aplicar firewalls industriais.

Prioridade: Crítica.

BORRADO INCORRECTO DE ENTRADAS EN EATON GALILEO

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/borrado-incorrecto-de-entradas-en-eaton-galileo-de-eaton

Produtos afectados: Eaton Galileo – software HMI.

Vector de ataque: Manexo incorrecto de entradas; posible corrupción de datos ou fallo inesperado.

Severidade: Alta.

I**mpacto potencial en OT:** Perda de integridade nas interfaces HMI; risco de erros en supervisión ou control.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Actualizar; illar redes HMI; validar entradas en capas superiores.

Prioridade: Alta.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DE MITSUBISHI

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-mitsubishi-0

Produtos afectados: Diversos produtos de Mitsubishi Electric para automatización industrial.

Vector de ataque: Múltiples vectores, incluíndo acceso non autenticado, desbordamentos e manipulación de parámetros.

Severidade: Alta–crítica.

Impacto potencial en OT: Risco directo sobre PLCs, interrupcións de procesos industriais, modificación da lóxica de control e perda de visibilidade.

Probabilidade de explotación: Elevada en contornas expostas ou sen segmentación adecuada.
Mitigacións inmediatas: Parchear segundo versións; segmentación; control estrito de accesos remotos; monitorización de integridade.
Prioridade: Moi alta.

FALTA DE AUTENTICACIÓN EN SMART ALERT SISA DE SIRCOM

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/falta-de-autenticacion-en-smart-alert-sisa-de-sircom
Produtos afectados: Sircom SMART Alert SISA.
Vector de ataque: Falta de autenticación en interface crítica.
Severidade: Crítica.
Impacto potencial en OT: Acceso non autorizado a sistemas de alarma; posible manipulación de eventos ou inhibición de alertas.
Probabilidade de explotación: Alta en sistemas accesibles desde redes non confiables.
Mitigacións inmediatas: Activar autenticación; segmentar alarmas críticas; revisar configuracións de exposición.
Prioridade: Crítica.

MÚLTIPLES VULNERABILIDADES EN TCIV+ DE ZENITEL

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-tciv-3-de-zenitel
Produtos afectados: Intercomunicadores industriais TCIV+ (Zenitel).
Vector de ataque: Execución remota de código, omisións de autenticación, desbordamentos.
Severidade: Alta–Crítica.
Impacto potencial en OT: Risco para comunicacións internas de planta; manipulación de audio/vídeo; pivote cara a outros sistemas.
Probabilidade de explotación: Moderada–Alta.
Mitigacións inmediatas: Actualizar firmware; segmentar rede AV/OT; restrinxir acceso web.
Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DE ASHLAR-VELLUM

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-ashlar-vellum-1

Produtos afectados: Software CAD/CAM industrial Ashlar-Vellum.

Vector de ataque: Xestión inadecuada da memoria; acceso non autorizado; corrupción de datos.

Severidade: Alta.

Impacto potencial en OT: Riscos sobre o deseño técnico, documentación de enxeñaría e continuidade da produción.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Aplicar actualizacións; illar estacións de enxeñaría; control de integridade.

Prioridade: Alta.

VALIDACIÓN INCORRECTA EN PRODUTOS DE JANITZA ELECTRONICS GMBH

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/validacion-incorrecta-en-productos-de-janitza-electronics-gmbh

Produtos afectados: Equipos de monitorización enerxética Janitza.

Vector de ataque: Validación insuficiente de entradas.

Severidade: Alta.

Impacto potencial en OT: Alteración de medicións enerxéticas; posibles efectos en cascada sobre o control de carga ou a calidade de subministración.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Actualizar o firmware; segmentación de sistemas de monitorización; regras de protección de rede.

Prioridade: Alta.

VALIDACIÓN INCORRECTA DE ENTRADA EN PRODUTOS DE FESTO

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/validacion-incorrecta-de-entrada-en-productos-de-festo

Produtos afectados: Módulos e controladores Festo.

Vector de ataque: Validación deficiente que permite a manipulación de parámetros.

Severidade: Alta.

Impacto potencial en OT: Risco sobre actuadores pneumáticos/eléctricos; afectación

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

directa a liñas automatizadas.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Parchear; restrinxir acceso á lóxica; supervisión de parámetros.

Prioridade: Alta.

OMISIÓN DE AUTENTICACIÓN EN EDGENIUS DE ABB

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/omision-de-autenticacion-en-edgenius-de-abb

Produtos afectados: ABB Edgenius – plataforma industrial edge.

Vector de ataque: Falta de autenticación en servizos expostos.

Severidade: Crítica.

Impacto potencial en OT: Control non autorizado sobre nodos edge; alterar fluxos de datos OT–IT; risco operativo significativo.

Probabilidade de explotación: Alta se os servizos están accesibles.

Mitigacións inmediatas: Aplicar autenticación estrita; segmentar edge; actualizar o software.

Prioridade: Crítica.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DE ICAM365

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-icam365

Produtos afectados: Cámaras industriais iCAM365.

Vector de ataque: Omisión de autenticación, exposición de credenciais, execución remota.

Severidade: Alta–crítica.

Impacto potencial en OT: Manipulación da videovixilancia; puntos cegos; pivote cara a outras redes.

Probabilidade de explotación: Alta.

Mitigacións inmediatas: Parchear; bloquear accesos externos; segmentación da rede de vídeo.

Prioridade: Moi alta.

DESBORDAMENTO DE BÚFER BASEADO EN PILA EN APPLETON (EMERSON)

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/desbordamiento-de-bufer-basado-en-pila-en-appleton-de-emerson

Produtos afectados: Controladores industriais Appleton de Emerson.

Vector de ataque: Desbordamento de búfer.

Severidade: Alta–crítica.

Impacto potencial en OT: Execución remota de código; interrupcións de servizo; corrupción de procesos.

Probabilidade de explotación: Moderada–alta.

Mitigacións inmediatas: Actualizar o firmware; segmentación estrita; limitar o acceso a servizos vulnerables.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES NO SERVIDOR PREMIUM DE AUTOMATED LOGIC / WEBCTRL

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-el-servidor-premium-de-automated-logic-webctrl

Produtos afectados: Automated Logic WebCTRL / Premium Server.

Vector de ataque: Varias vulnerabilidades, incluíndo execución remota e autenticación insuficiente.

Severidade: Alta–crítica.

Impacto potencial en OT: Compromiso do sistema de xestión de edificios (BMS); posibilidade de alteracións ambientais ou enerxéticas que afecten procesos industriais.

Probabilidade de explotación: Elevada.

Mitigacións inmediatas: Parchear; segmentar o BMS das redes OT; reforzar a autenticación.

Prioridade: Moi alta.

INXECCIÓN DE COMANDOS EN PRODUTOS DE OPTO-22

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/inyeccion-de-comandos-en-productos-de-opto-22

Produtos afectados: Controladores e módulos Opto-22.

Vector de ataque: Inxección de comandos mediante entradas non validadas.

Severidade: Alta.

Impacto potencial en OT: Execución remota de comandos; alteración de procesos; risco de perda de control operacional.

Probabilidade de explotación: Moderada–alta.

Mitigacións inmediatas: Parchear; segmentar; restrinxir acceso web/API; validar entradas.

Prioridade: Moi alta.

CONDICIÓN DE CARREIRA NO KERNEL DE WINDOWS EN PRODUTOS DE PHILIPS

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/condicion-de-carrera-en-el-kernel-de-windows-en-productos-de-philips

Produtos afectados: Equipos Philips dependentes de Windows (varios modelos).

Vector de ataque: Explotación de condición de carreira no núcleo.

Severidade: Alta.

Impacto potencial en OT: Interrupción de sistemas médicos industriais; denegación de servizo; perda de dispoñibilidade.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Aplicar parches de Microsoft; restrinxir privilexios; segmentar.

Prioridade: Alta.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DA FAMILIA MAP 5000 DE BOSCH

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-la-familia-map-5000-de-bosch

Produtos afectados: Sistemas Bosch MAP 5000.

Vector de ataque: Varias vulnerabilidades (inclúe autenticación débil, execución remota, manipulación de datos).

Severidade: Alta–crítica.

Impacto potencial en OT: Compromiso de sistemas de detección e alarma; risco para a seguridade física.

Probabilidade de explotación: Moderada–alta.

Mitigacións inmediatas: Actualizar o firmware; endurecer credenciais; segmentar sistemas de alarma.

Prioridade: Moi alta.

EXECUCIÓN DE CÓDIGO MALICIOSO EN MILCOS DE MITSUBISHI ELECTRIC

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/ejecucion-de-codigo-malicioso-en-milcos-de-mitsubishi-electric

Produtos afectados: Plataformas MILCoS de Mitsubishi.

Vector de ataque: Execución remota de código por validación insuficiente.

Severidade: Crítica.

Impacto potencial en OT: Compromiso total do sistema; manipulación da lóxica ou parámetros; interrupción de procesos.

Probabilidade de explotación: Alta.

Mitigacións inmediatas: Aplicar parches; segmentar; controlar accesos remotos; monitorizar.

Prioridade: Crítica.

MÚLTIPLES VULNERABILIDADES EN EWIO-2 DE METZ CONNECT

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-ewio-2-de-metz-conect

Produtos afectados: Dispositivos EWIO-2.

Vector de ataque: Autenticación débil, exposición de credenciais, execución remota.

Severidade: Alta–Crítica.

Impacto potencial en OT: Manipulación de datos enerxéticos; pivote cara a redes internas; risco operativo relevante.

Probabilidade de explotación: Alta.

Mitigacións inmediatas: Actualizar o firmware; aplicar contrasinais robustos; segmentación estrita.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DE ZENITEL

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-zenitel

Produtos afectados: Sistemas Zenitel (varios modelos).

Vector de ataque: Execución de código, falta de autenticación, desbordamentos.

Severidade: Alta–crítica.

Impacto potencial en OT: Risco nas comunicacións internas; posibilidade de

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

interceptar, manipular ou bloquear sinais.

Probabilidade de explotación: Moderada–alta.

Mitigacións inmediatas: Parchear; segmentar redes AV; restrinxir accesos.

Prioridade: Moi alta.

VULNERABILIDADE EN SAM LIGHT DE JUSTECH

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/vulnerabilidad-en-sam-light-de-justech

Produtos afectados: SAM Light – Justech.

Vector de ataque: Validación insuficiente; manipulación de parámetros.

Severidade: Alta.

Impacto potencial en OT: Risco de manipulación de sistemas de iluminación industrial; impacto na seguridade operativa.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Parchear; restrinxir accesos; segmentación.

Prioridade: Alta.

MÚLTIPLES VULNERABILIDADES EN XBT L1000 DE IDEC

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-xbt-l1000-de-idec

Produtos afectados: IDEC XBT L1000.

Vector de ataque: Desbordamentos, exposición de información, elusión da autenticación.

Severidade: Alta–Crítica.

Impacto potencial en OT: Manipulación de HMI; risco de perda de integridade operativa.

Probabilidade de explotación: Moderada–Alta.

Mitigacións inmediatas: Actualizar; segmentar; reforzar a autenticación.

Prioridade: Moi alta.

VULNERABILIDADE NA TARXETA MIR420 DE JOHNSON CONTROLS

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/vulnerabilidad-en-tarjeta-mir420-de-johnson-controls

Produtos afectados: Tarxeta MIR420.

Vector de ataque: Validación insuficiente; manipulación remota.

Severidade: Alta.

Impacto potencial en OT: Risco para o control de accesos ou integración en sistemas de seguridade.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Parchear; restrinxir acceso; segmentación.

Prioridade: Alta.

VULNERABILIDADE EN GG4 DE TECNOCONTROL ILUMINACIÓN

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/vulnerabilidad-en-gg4-de-tecnocontrol-iluminacion

Produtos afectados: Controladores GG4.

Vector de ataque: Exposición de servizos sen autenticación.

Severidade: Alta.

Impacto potencial en OT: Manipulación de iluminación crítica; impacto na seguridade e na visibilidade operativa.

Probabilidade de explotación: Moderada–alta.

Mitigacións inmediatas: Actualizar; implementar autenticación; segmentar.

Prioridade: Moi alta.

VULNERABILIDADE EN ROBOTSTUDIO DE ABB

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/vulnerabilidad-en-robotstudio-de-abb

Produtos afectados: ABB RobotStudio.

Vector de ataque: Entrada non validada; posible manipulación de parámetros.

Severidade: Alta.

Impacto potencial en OT: Risco na programación e control de robots; posibles fallos ou movementos indebidos.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Parchear; segmentar estacións de enxeñaría; reforzar autenticación.

Prioridade: Alta.

VULNERABILIDADE EN COBUILDERPRO DE NKG

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/vulnerabilidad-en-cobuilderpro-de-nkg

Produtos afectados: CoBuilderPro.

Vector de ataque: Exposición de servizos; validación insuficiente.

Severidade: Alta.

Impacto potencial en OT: Manipulación de datos industriais; risco de corrupción de configuracións.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Actualizar; segmentar; restrinxir accesos.

Prioridade: Alta.

AVISOS DE SEGURIDADE DE SIEMENS – NOVEMBRO 2025

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/avisos-de-seguridad-de-siemens-de-noviembre-2025

Produtos afectados: Múltiples produtos industriais de Siemens (PLC, HMI, redes e software de enxeñaría).

Vector de ataque: Diversos vectores (execución remota de código, elevación de privilexios, omisión de autenticación, desbordamentos).

Severidade: Alta–crítica segundo produto e CVE.

Impacto potencial en OT: Compromiso directo de equipos de automatización e monitorización; risco de interrupción de procesos, alteración da lóxica de control e perda de visibilidade.

Probabilidade de explotación: Moderada–alta, especialmente en sistemas expostos ou sen segmentación.

Mitigacións inmediatas: Aplicar os parches e mitigacións específicas de cada aviso; segmentar redes OT; restrinxir accesos remotos; reforzar autenticación e monitorización.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DE SCHNEIDER

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-schneider-4

Produtos afectados: Diversos dispositivos e software industriais de Schneider Electric.

Vector de ataque: Múltiples vectores (RCE, desbordamentos, exposición de información, autenticación débil).

Severidade: Alta–crítica.

Impacto potencial en OT: Compromiso de PLC, pasarelas ou ferramentas de enxeñaría; risco para a continuidade do proceso e a seguridade das instalacións.

Probabilidade de explotación: Alta en contornas con acceso de rede non controlado.

Mitigacións inmediatas: Parchear segundo as versións afectadas; segmentar; limitar acceso lóxico; reforzar credenciais e monitorización.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN AVEVA

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-aveva

Produtos afectados: Plataformas AVEVA de supervisión e control (SCADA/HMI e software asociado).

Vector de ataque: Inxección, RCE, exposición de información e outros vectores de aplicación.

Severidade: Alta–crítica.

Impacto potencial en OT: Manipulación de datos de proceso, pantallas HMI e lóxica de control; risco de paradas de planta ou funcionamento fóra de especificación.

Probabilidade de explotación: Moderada–alta, especialmente se as consolas están accesibles desde redes IT ou externas.

Mitigacións inmediatas: Actualizar a versións corrixidas; illar estacións de enxeñaría e SCADA; aplicar endurecemento e xestión de contas.

Prioridade: Moi alta.

PREDICIÓN DE CONTRASINAIS EN VARITRON DE JUMO

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/prediccion-de-contrasenas-en-varitron-de-jumo

Produtos afectados: Controladores JUMO VARITRON.

Vector de ataque: Predición de contrasinais por algoritmo débil ou patrón previsible.

Severidade: Alta.

Impacto potencial en OT: Acceso non autorizado á configuración do controlador; modificación de parámetros de proceso; risco de desviacións operativas.

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

Probabilidade de explotación: Alta se o equipo é accesible por rede ou interface remota.

Mitigacións inmediatas: Actualizar o firmware; cambiar credenciais por outras robustas e non predefinidas; segmentar o acceso aos controladores.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN DEVICEON/IEDGE DE ADVANTECH

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-deviceoniedge-de-advantech

Produtos afectados: Advantech DeviceOn/iEdge – plataformas de xestión e edge computing.

Vector de ataque: RCE, autenticación insuficiente, exposición de credenciais e manipulación de APIs.

Severidade: Alta–Crítica.

Impacto potencial en OT: Control non autorizado de nodos edge; alteración de telemetría e ordes cara a dispositivos de campo; posible pivote cara a redes internas.

Probabilidade de explotación: Alta, especialmente en despregues conectados a Internet ou redes IT.

Mitigacións inmediatas: Parchear; limitar a exposición de servizos; reforzar a autenticación (MFA cando sexa posible); segmentar a capa edge.

Prioridade: Moi alta.

CREDENCIAIS INSUFICIENTEMENTE PROTEXIDAS EN UBOX DE UBIA

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/credenciales-insuficientemente-protegidas-en-ubox-de-ubia

Produtos afectados: Dispositivos UBOX de UBIA.

Vector de ataque: Almacenamento ou transmisión insegura de credenciais.

Severidade: Alta.

Impacto potencial en OT: Compromiso de contas administrativas; acceso a servizos críticos de conectividade ou integración OT/IT.

Probabilidade de explotación: Moderada–alta se se ten acceso á rede ou ao dispositivo.

Mitigacións inmediatas: Actualizar o firmware; cambiar credenciais; habilitar cifrado e mecanismos de protección adicionais; limitar accesos administrativos.

Prioridade: Alta.

MÚLTIPLES VULNERABILIDADES EN SPRECON-E/C/E-P/E-T3 DE SPRECHER AUTOMATION

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-sprecon-e-c-e-p-e-t3-de-sprecher-automation

Produtos afectados: Dispositivos SPRECON-E, SPRECON-C, SPRECON-E-P, SPRECON-E-T3.

Vector de ataque: Diversos (RCE, elusión da autenticación, manipulación de comunicacións).

Severidade: Alta–crítica.

Impacto potencial en OT: Risco directo sobre sistemas de protección e control en redes eléctricas; potencial perda de estabilidade da rede ou interrupcións de subministración.

Probabilidade de explotación: Moderada–alta en contornas con acceso remoto ou mala segmentación.

Mitigacións inmediatas: Parchear; segmentar redes de protección; limitar interfaces remotas; reforzar monitorización de eventos.

Prioridade: Crítica.

DESBORDAMENTO DE BÚFER EN CNCSOFT-G2 DE DELTA ELECTRONICS

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/desbordamiento-de-bufer-en-cncsoft-g2-de-delta-electronics-0

Produtos afectados: Delta Electronics CNCSoft-G2 – software de configuración/programación.

Vector de ataque: Desbordamento de búfer mediante ficheiros ou entradas manipuladas.

Severidade: Alta–crítica.

Impacto potencial en OT: Execución de código en estacións de enxeñaría; posible modificación maliciosa de proxectos ou parámetros enviados a máquinas CNC.

Probabilidade de explotación: Moderada, normalmente require a interacción do usuario con ficheiros maliciosos.

Mitigacións inmediatas: Actualizar á versión corrixida; evitar abrir proxectos non confiables; segmentar estacións de enxeñaría.

Prioridade: Moi alta.

FALTA DE AUTENTICACIÓN EN LICENSE PLATE RECOGNITION (LPR) CAMERA DE SURVISION

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/falta-de-autenticacion-en-license-plate-recognition-lpr-camera-de-survision

Produtos afectados: Cámaras LPR de SurVision.

Vector de ataque: Acceso a servizos da cámara sen autenticación adecuada.

Severidade: Alta.

Impacto potencial en OT: Manipulación de sistemas de control de accesos baseados en matrículas; xeración de puntos cegos ou alteración de rexistros.

Probabilidade de explotación: Alta se as cámaras están expostas a redes non confiables.

Mitigacións inmediatas: Activar e reforzar a autenticación; segmentar a rede de videovixilancia; restrinxir o acceso remoto.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN VIZAIR DE RADIOMETRICS

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-vizair-de-radiometrics

Produtos afectados: Sistemas Radiometrics VizAir.

Vector de ataque: Varias vulnerabilidades en servizos e APIs (incluíndo posible RCE e exposición de información).

Severidade: Alta–Crítica.

Impacto potencial en OT: Manipulación de datos meteorolóxicos ou ambientais usados en operacións; risco de decisións operativas erróneas.

Probabilidade de explotación: Moderada–Alta segundo a exposición.

Mitigacións inmediatas: Parchear; limitar accesos; reforzar autenticación e cifrado das comunicacións.

Prioridade: Alta.

INXECCIÓN DE ARGUMENTOS EN ICM VIEWER DE IDIS

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/inyeccion-de-argumentos-en-icm-viewer-de-idis

Produtos afectados: IDIS ICM Viewer.

Vector de ataque: Inxección de argumentos na liña de comandos ou chamadas internas.

Severidade: Alta.

Impacto potencial en OT: Execución de comandos non autorizados desde estacións de visualización; manipulación de videovixilancia ou pivote cara a outros sistemas.

Probabilidade de explotación: Moderada.

Mitigacións inmediatas: Actualizar o software; evitar a apertura de ligazóns ou ficheiros non confiables; segmentar estacións cliente.

Prioridade: Alta.

MÚLTIPLES VULNERABILIDADES EN MONITOUCH V-SFT-6 DE FUJI ELECTRIC

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-monitouch-v-sft-6-de-fuji-electric

Produtos afectados: Software MONITOUCH V-SFT-6 de Fuji Electric.

Vector de ataque: Manexo inseguro de ficheiros de proxecto, desbordamentos e outras debilidades.

Severidade: Alta–crítica.

Impacto potencial en OT: Compromiso de estacións de enxeñaría; alteración de proxectos HMI descargados a paneis de operador.

Probabilidade de explotación: Moderada, require o uso de ficheiros manipulados.

Mitigacións inmediatas: Parchear; restrinxir o uso de proxectos de orixe descoñecida; segmentar estacións de enxeñaría.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN BRIGHTLAYER SOFTWARE SUITE (BLSS) DE EATON

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-brightlayer-software-suite-blss-de-eaton

Produtos afectados: Eaton Brightlayer Software Suite (BLSS).

Vector de ataque: RCE, xestión insegura da autenticación, exposición de datos e outros vectores en compoñentes web.

Severidade: Alta–Crítica.

Impacto potencial en OT: Manipulación de sistemas de xestión de enerxía e activos; alteración de configuracións eléctricas ou de monitorización.

Probabilidade de explotación: Alta se os servizos BLSS están expostos a redes amplas.

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

Mitigacións inmediatas: Actualizar; segmentar a plataforma de xestión; aplicar endurecemento de accesos e credenciais.

Prioridade: Moi alta.

MÚLTIPLES VULNERABILIDADES EN PRODUTOS DE WAGO

URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-wago-1

Produtos afectados: PLC e dispositivos industriais WAGO (varias gamas).

Vector de ataque: RCE, desbordamentos, autenticación débil e outros vectores sobre servizos de xestión e comunicación.

Severidade: Alta–crítica.

Impacto potencial en OT: Compromiso de controladores e módulos de E/S; risco alto para a continuidade e a seguridade do proceso industrial.

Probabilidade de explotación: Alta en contornas con exposición de servizos ou sen segmentación OT.

Mitigacións inmediatas: Parchear segundo a guía do fabricante; segmentar redes de control; limitar accesos de administración; reforzar monitorización en profundidade.

Prioridade: Crítica.

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

5 Recomendacións

Esta sección reúne **recomendacións prácticas para reforzar a ciberseguridade industrial seguindo un percorrido lóxico**: comezamos con principios xerais que orientan calquera programa de seguridade en contornas OT, avanzamos cara a prioridades tácticas propostas por distintas organizacións especializadas e terminamos con aspectos específicos da xestión de vulnerabilidades e de programas de parcheo, obxecto último deste informe teórico-práctico.

5.1 Principios xerais de ciberseguridade OT

O documento **Principles of Operational Technology Cybersecurity** [47] de 2024 é unha guía impulsada polo Australian Cyber Security Centre (ACSC), e elaborada de forma conxunta con axencias nacionais de ciberseguridade de oito países e expertos en sistemas de control industrial. O seu obxectivo é ofrecer un conxunto de principios sinxelos, compartidos e aplicables á maioría de sectores industriais, que complemente marcos como NIST ou IEC 62443 pero cun enfoque moi claro na realidade de planta.

Expoñen seis principios básicos:

1. **Seguridade física por riba de todo**

O documento insiste en que **a seguridade física e a integridade do proceso son a prioridade absoluta**. Calquera medida de ciberseguridade debe respectar o deseño de seguridade funcional, os encravamentos, os sistemas instrumentados de seguridade e os límites operativos. Isto implica evitar cambios apresurados, probas insuficientes ou solucións "de TI" que poidan provocar paradas non controladas ou comportamentos inesperados en campo.

2. **Deseñar para unha contorna hostil**

Os sistemas OT deben pensarse e operarse coma se estivesen permanentemente expostos a fallos, erros humanos e ataques. O principio convida a reducir a superficie de exposición, segmentar redes, limitar servizos e evitar a dependencia de accesos remotos innecesarios. A idea de fondo é que a resiliencia debe empezar no deseño, non só na resposta a incidentes.

3. **Previsibilidade e estabilidade operacional**

Outro dos principios vitais é garantir que, mesmo en condicións de tensións ou fallo parcial, o comportamento do sistema sexa estable e predicible. Isto implica **deseñar**

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

modos degradados seguros, redundancia axeitada e procedementos de operación manual para cando as capas dixitais de supervisión fallen. A ciberseguridade enténdese aquí como unha extensión natural do deseño robusto de procesos.

4. **Coñecemento continuo da contorna OT**

O documento subliña a **necesidade de contar con inventarios actualizados de activos, versións de firmware, configuracións e dependencias de rede.** Sen ese coñecemento é moi difícil priorizar vulnerabilidades, avaliar o impacto dun incidente ou planificar un parcheo. A visibilidade, tanto de activos como de comunicacións, considérase unha condición básica de calquera programa de seguridade.

5. **Preparación para incidentes e recuperación**

Aceptar que os incidentes ocorrerán leva de forma natural a reforzar a capacidade de detección, resposta e recuperación. O principio **anima a integrar a ciberseguridade OT nos plans de continuidade e recuperación da organización, incluíndo copias de seguridade específicas de sistemas de control, procedementos de restauración probados e tempos de recuperación aliñados co risco** de proceso.

6. **Xestión de riscos integrada co negocio**

Por último, insístese en que **os riscos OT son riscos de negocio e, en moitos casos, de seguridade das persoas. As decisións sobre que mitigar, que aceptar e que pospor deben tomarse de forma informada, documentada e con participación de operacións, seguridade e dirección.** O principio apunta a modelos de goberno nos que OT teña voz propia dentro da xestión corporativa do risco.

Estes seis principios constitúen o marco xeral do que en certo modo, pódese considerar que derivan as recomendacións máis concretas dos apartados seguintes.

5.2 Enfoque pragmático

O informe **Dragos OT/ICS Cybersecurity Year in Review 2025** [39] traduce estes principios en liñas de acción moi concretas, pensadas para organizacións que xa deron os primeiros pasos pero necesitan ordenar as súas prioridades.

Plan de resposta a incidentes ICS específico

Recoméndase **dispor dun plan de resposta a incidentes deseñado expresamente para sistemas de control industrial**. Este plan debe contemplar distintos escenarios (ransomware, perda de visibilidade HMI, manipulación de PLC, etc.) e, sobre todo,

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

involucrar a enxeñaría e operación tanto na súa redacción como nos exercicios e simulacros.

Arquitectura defendible

Outra prioridade é **evolucionar desde redes planas e moi interconectadas cara a arquitecturas "defendibles", con zonas e condutos ben definidos, DMZ industrial, minimización de servizos expostos e controis claros** nos puntos de converxencia IT/OT. O obxectivo é que un incidente ou unha intrusión nunha parte da rede non se traduza facilmente en perda de control do proceso.

Visibilidade e monitorización OT

O informe insiste en que **a visibilidade específica de OT (protocolos industriais, cambios en lóxicas de control, modificacións en configuracións) é fundamental**. Sen esa visibilidade, a detección de actividade anómala vólvese tardía ou directamente imposible, e pérdese a oportunidade de reaccionar antes de que o impacto sexa físico.

Acceso remoto seguro

Sitúase o acceso remoto como un dos vectores de risco máis críticos. Anímase a **revisar de forma sistemática VPN, accesos de terceiros, mantementos remotos e calquera mecanismo que permita entrar en OT desde fóra da planta**, reforzando autenticación, aplicando o principio de mínimo privilexio e asegurando a trazabilidade das sesións.

Xestión de vulnerabilidades baseada en risco (Now/Next/Never)

Por último, o informe expón que **a xestión de vulnerabilidades en ICS debe centrarse no risco real para o proceso, non unicamente na puntuación técnica das CVE. Esta visión enlaza coa filosofía Now / Next / Never**, que se desenvolve a continuación, e que ofrece unha forma práctica de decidir que merece parcheo inmediato, que pode esperar e que pode xestionarse con medidas compensatorias.

Unha vez contextualizada a contorna de ameazas, a pregunta práctica é como decidir que vulnerabilidades requiren acción inmediata, cales poden esperar e cales quizá non deban parchearse nunca en condicións normais. A filosofía **Now / Next / Never**, ofrece unha resposta operativa a esta cuestión.

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

Desde este punto de vista, **unha vulnerabilidade clasifícase en Now cando combina varios elementos**:

a) afecta a un activo crítico para o proceso ou a seguridade;
b) é explotable de forma remota ou cun esforzo razoable;
c) e non existe unha mitigación compensatoria eficaz xa implantada (segmentación, listas brancas, restricións de acceso, etc.).

Estas vulnerabilidades son as que poden permitir a un atacante tomar control directo de equipos crave ou provocar unha perda de visión inmediata, e polo tanto deben abordarse coa máxima prioridade. Na práctica, isto non sempre implica parchear de forma inmediata, pero si despregar medidas que reduzan de forma rápida a súa explotabilidade (cambios de configuración, regras en firewalls, illamento adicional) e planificar o parcheo na primeira xanela segura posible.

Na **categoría Next sitúanse vulnerabilidades que, a pesar de ser relevantes**:

a) requiren unha combinación de factores menos probable para causar un impacto grave,
b) ou ben contan con certo nivel de mitigación grazas á arquitectura existente.

Son candidatas a ser resoltas como parte de campañas de mellora planificadas, a miúdo combinando actuacións de reforzo da arquitectura (por exemplo, reducir exposición ou endurecer accesos) coa aplicación progresiva de parches cando as xanelas de mantemento permíteno.

Por último, **a categoría Never agrupa vulnerabilidades que, no contexto concreto da organización, dificilmente chegarán a materializarse nun risco significativo**. Pode tratarse de fallos que só afectan a funcionalidades non utilizadas, a configuracións moi específicas que non se dan en planta ou a equipos completamente illados e sen repercusión real sobre o proceso. Clasificar unha vulnerabilidade como Never non significa ignorala, senón documentar a decisión, xustificala en base a risco e manter unha monitorización suficiente como para reformulala se cambian as condicións (por exemplo, se un activo deixa de estar illado ou se lle engaden novas funcións).

Este enfoque axuda a que as decisións sobre parcheo se apoien no impacto operativo e non só na severidade técnica da vulnerabilidade, e conecta de forma natural cos programas de xestión de parches descritos no apartado seguinte.

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

5.3 Programa de parcheo en ICS: guía práctica de CISA

A guía **Recommended Practice for Patch Management of Control Systems** de CISA [30], converteuse nunha referencia para estruturar programas de parcheo realistas en contornas ICS. Non propón un calendario ríxido, senón unha forma de organizar o proceso para equilibrar seguridade e continuidade.

Un primeiro bloque do programa ten que ver coa **gobernanza e o alcance**. É necesario definir que sistemas entran no programa (PLC, RTU, HMI, servidores de historización, estacións de enxeñaría, pasarelas, sistemas de seguridade, etc.), quen é responsable de que (seguridade, enxeñaría, operación, mantemento, provedores) e como se van tomar as decisións de cambio. Integrar o parcheo nos procesos de xestión de cambios existentes axuda a evitar actuacións illadas e non coordinadas.

O segundo bloque céntrase no **inventario e a clasificación de activos**. Sen unha lista fiable de equipos, versións de firmware e roles no proceso, a xestión de parches convértese nun exercicio teórico. A guía recomenda clasificar activos por criticidade operacional, pola súa exposición (por exemplo, se están accesibles desde outras redes) e pola facilidade para intervir sobre eles (xanelas de parada, redundancias, etc.). Esta clasificación será a base da priorización posterior.

A partir de aí entra en xogo a **monitorización de vulnerabilidades e avisos**. O programa debe establecer como se reciben e procesan os avisos de fabricantes, boletíns de organismos oficiais ou novas CVE. O importante non é só recibir información, senón relacionala de forma sistemática co inventario: que modelos están afectados, que versións, en que plantas, e que papel xogan no proceso.

O seguinte paso é a **análise de impacto e a priorización**, onde encaixa a filosofía Now / Next / Never. Para cada vulnerabilidade relevante avalíanse cuestións como: se afecta a activos críticos, se require acceso local ou remoto, se xa existe algún control que reduza a súa explotabilidade, que impacto tería unha explotación exitosa en termos de seguridade física e continuidade de servizo, e que alternativas hai ao parche directo (cambios de configuración, segmentación adicional, restricións de acceso). Con estes elementos, decídese se unha vulnerabilidade considérase de tratamento inmediato, programable ou aceptable con mitigacións compensatorias (véxase o esquema de decisión proposto na figura da sección 3.2.2).

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

A **fase de probas e planificación** é especialmente importante en ICS. Sempre que sexa posible, recoméndase validar os parches en contornas de laboratorio ou preprodución que reproduzan de maneira razoable o comportamento dos sistemas reais. A partir dos resultados, planifícanse xanelas de mantemento coordinadas con operación, defínese a orde en que se actuará sobre os distintos compoñentes e documéntanse os posibles escenarios de rollback se algunha cousa non sae como se esperaba.

Na **execución do parcheo**, a guía suxire traballar con procedementos estandarizados e listas de comprobación: que servizos deter, que pasos seguir, que verificacións realizar antes e despois de aplicar cada parche. É igualmente importante rexistrar que se actualizou, en que momento e con que resultado, para poder reconstruír o estado do sistema en caso de problema.

Tras a execución, o programa contempla unha **fase de verificación e seguimento**. Non basta con comprobar que os sistemas arrincan: hai que asegurarse de que as comunicacións son estables, que as aplicacións de supervisión e control funcionan correctamente e que non se introduciron regresións sutís. Nalgúns casos, pode ser razoable establecer un período de observación reforzada tras campañas de parcheo importantes.

Por último, CISA destaca a necesidade de **documentar e aprender** de cada ciclo de parcheo: actualizar inventarios e diagramas, rexistrar incidencias e melloras detectadas no procedemento, e revisar periodicamente o equilibrio entre parches aplicados, parches diferidos e vulnerabilidades aceptadas con medidas compensatorias.

5.4 Alternativas

Un elemento transversal e que é importante admitir, é o feito de que **non sempre será posible aplicar parches,** ou non nos prazos desexables. Neses casos, o programa debe contemplar explicitamente as **medidas compensatorias**: segmentar e illar activos vulnerables, restrinxir ao máximo os accesos lóxicos, aplicar listas brancas de aplicacións, reforzar a monitorización sobre eses sistemas e revisar de forma periódica se as condicións cambiaron o suficiente como para reabrir a posibilidade de parchear.

A ciberseguridade OT esixe equilibrio entre seguridade e continuidade. Non todas as vulnerabilidades poden parchearse con rapidez, e algunhas non necesitan parchearse en absoluto. Pero todas requiren xestión. Cando o parcheo directo non é viable por restricións de operación, compatibilidade ou soporte, deben valorarse e implantarse

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

medidas compensatorias que reduzan o risco sen comprometer a seguridade física nin a estabilidade do proceso.

Así, **proponse un enfoque que combina principios xerais, prioridades tácticas e prácticas operativas para construír programas de seguridade industrial realistas, sostibles e adaptados** a contornas onde a fiabilidade é esencial.

6 Conclusións

O presente informe ofreceu unha **visión integral e estruturada do estado das vulnerabilidades e alertas que afectan aos sistemas de control industrial, incorporando tanto un marco conceptual como unha análise práctica orientado á acción**. A combinación de ambos os enfoques permite ao lector comprender non só que vulnerabilidades existen e como evolucionan, senón tamén que factores condicionan a súa explotación, a súa criticidade e as decisións de mitigación.

En primeiro lugar, **expuxéronse os fundamentos teóricos que permiten interpretar adecuadamente o risco asociado ás vulnerabilidades en contornas OT**, destacando aspectos como a definición e taxonomía de vulnerabilidades, e a criticidade asociada ao tempo de explotación, o tempo de remediación, a relación entre ambos e o impacto específico que estes factores adquiren cando a dispoñibilidade do proceso e a seguridade física son prioritarias. Expuxéronse as etapas da análise e xestión de vulnerabilidades, e mesmo un marco teórico de cálculo do retorno esperado de devanditas accións. Contextualizouse esta información con estudos contrastados de organismos como ENISA, CISA ou ISC².

En segundo lugar, **analizouse o panorama recente de alertas ICS con datos procedentes de fontes especializadas, sintetizando tendencias globais xerais, algunhas técnicas de ataque predominantes e sectores máis impactados**, así como se enlaza unha boa base de datos de ciberincidentes industriais reais. Posteriormente, **facilítanse numerosas fontes de CERTs nacionais e internacionais de avisos, vulnerabilidades e alertas accionables en contornas ICS/OT do último trimestre recopilados por INCIBE dos organismos citados**, así como un **anexo coas referencias dos avisos de seguridade dalgúns dos principais fabricantes** de compoñentes no mercado.

Proporcionáronse **recomendacións baseadas en boas prácticas internacionais**, **incluíndo principios xerais de ciberseguridade OT definidos de maneira colexiada entre os principais países do mundo**, **prioridades tácticas propostas por entidades como Dragos e SANS, e unha descrición detallada da filosofía Now / Next / Never** aplicada á priorización do tratamento de vulnerabilidades. Este enfoque contribúe a que as organizacións orienten os seus esforzos de mitigación cara a aquilo que reduce de maneira máis efectiva o risco operacional.

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

O eixo central das recomendacións nesta materia particular, constitúeo a **guía de CISA para a xestión de parches** en contornas ICS, que se desenvolveu **para ofrecer un conxunto de directrices prácticas sobre gobernanza, inventario, análise de impacto, validación de parches, execución, verificación e uso de medidas compensatorias cando o parcheo directo non é viable.**

Para reforzar a aplicabilidade do informe, incluíuse un **glosario de termos específicos** que facilita a lectura e comprensión do documento, así como un anexo con enlaces aos portais oficiais de advisories de fabricantes OT amplamente utilizados no ecosistema industrial galego.

O período analizado evidencia que **as vulnerabilidades en contornas OT seguen concentrándose en fallos recorrentes de deseño, configuracións por defecto e compoñentes legacy, afectando a un amplo rango de fabricantes** (incluído un aviso relevante de Siemens polo volume de dispositivos impactados). A diversidade e frecuencia destes avisos confirman que a superficie de exposición industrial continúa crecendo, e que os riscos asociados á cadea de subministración e ao ciclo de vida dos equipos seguen sendo determinantes para a seguridade das operacións.

En conxunto, **as alertas analizadas mostran un ecosistema OT onde os incidentes potenciais poden traducirse rapidamente en impactos operativos relevantes**. Para o tecido empresarial e as AAPP galegas, isto reforza a **necesidade de consolidar inventarios precisos, mellorar a hixiene de configuración e adoptar unha xestión de parches realista pero sistemática**, aliñada cos condicionantes de dispoñibilidade propios da contorna industrial.

É probable que **aumente a explotación automatizada de vulnerabilidades** recentemente publicadas, acurtando a marxe de reacción dispoñible para as organizacións. Tamén se prevé un maior foco dos atacantes en dispositivos amplamente despregados e en servizos inadvertidamente expostos, o que fará máis crítica a visibilidade continua da contorna.

Ademais, **a presión regulamentaria e operativa sobre fabricantes podería derivar en ciclos de actualización máis frecuentes**. **Para Galicia, isto implicará reforzar capacidades internas de análises de alertas, mellorar a coordinación con provedores e avanzar cara a modelos de reforzo continuo da seguridade OT, co fin de elevar a resiliencia global do ecosistema industrial rexional.**

En conxunto, o boletín achega valor ao tecido empresarial e ás administracións públicas galegas ao proporcionar un **marco conceptual sintetizado** que facilita a interpretación técnica do risco, xunto cun **resumo actualizado de alertas relevantes para sectores críticos**. Ademais, as **recomendacións operativas** incluídas permiten mellorar a resiliencia das contornas ICS mediante prácticas contrastadas e aplicables, mentres que os recursos e referencias ofrecidos contribúen a establecer unha **vixilancia continua e estruturada de vulnerabilidades**.

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

Bibliografía

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

[2] INCIBE (2024). *Balance de Ciberseguridade 2024.* Recuperado de https://www.incibe.es/sites/default/files/Comunicaci%C3%B3n_2025/Infograf%C3%ADa_BalanceCiberseguridad_INCIBE_2024_web.pdf

[3] Xunta de Galicia (2025). *Rede de Laboratorios e Centros Demostradores — Proxecto RETECH.* Recuperado de https://ciberseguridadegalicia.gal/es/proyecto-retech/red-de-laboratorios-y-centros-demostradores

[4] MITRE (2025). *CVE® List – Common Vulnerabilities and Exposures*. Recuperado de https://www.cve.org/

[5] FIRST (2023). *Common Vulnerability Scoring System v4.0 – Specification Document*. Recuperado de https://www.first.org/cvss/v4-0/specification-document

[6] CISA (2007). *Cybersecurity & Infrastructure Security Agency*. Recuperado de https://www.cisa.gov/

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

[8] OWASP Foundation (2001). *OWASP — Open Worldwide Application Security Project*. Recuperado de https://owasp.org/

[9] MITRE (1958). *MITRE Corporation*. Recuperado de https://www.mitre.org/

[10] OWASP (2003). *OWASP Top 10 — The Ten Most Critical Web Application Security Risks*. Recuperado de https://owasp.org/www-project-top-ten/

[11] MITRE (2025). *MITRE ATT&CK® — Adversarial Tactics, Techniques & Procedures*. Recuperado de https://attack.mitre.org/

[12] MITRE (2025). *MITRE ATT&CK® for ICS — Knowledge Base for Industrial Control System Threats*. Recuperado de https://attack.mitre.org/matrices/ics/

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

[14] MITRE (2007). *CAPEC — Common Attack Pattern Enumeration and Classification*. Recuperado de https://capec.mitre.org/

[15] NIST (2005). *NVD — National Vulnerability Database*. Recuperado de https://nvd.nist.gov/

[16] NIST (2025). *National Institute of Standards and Technology — Public Cybersecurity Resources*. Recuperado de https://www.nist.gov/publications

[17] European Union (2025). *EUVD — European Vulnerability Database*. Recuperado de https://euvd.enisa.europa.eu/

[18] MITRE (2009). *CWE Top 25 Most Dangerous Software Weaknesses*. Recuperado de https://cwe.mitre.org/top25/

[19] OASIS (2017). *CVRF — Common Vulnerability Reporting Framework*. Recuperado de https://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html

[20] OpenVAS (2005). *OpenVAS — Open Vulnerability Assessment Scanner*. Recuperado de https://www.openvas.org/

[21] Greenbone Networks (2008). *Greenbone Vulnerability Management*. Recuperado de https://www.greenbone.net/

[22] Tenable (1998). *Nessus — Vulnerability Assessment Platform*. Recuperado de https://www.tenable.com/products/nessus

[23] Qualys (1999). *Qualys Cloud Platform — Vulnerability Management*. Recuperado de https://www.qualys.com/

[24] Gartner (2025). *Critical Capabilities for CPS Protection Platforms.* Recuperado de https://www.gartner.com/en/documents/6186155

[25] Nozomi Networks (2013). *Nozomi Networks — OT & IoT Security Platform*. Recuperado de https://www.nozominetworks.com/

[26] Claroty (2015). *Claroty xDome / Claroty Platform — Cyber-Physical System Security*. Recuperado de https://www.claroty.com/

[27] Dragos (2016). *Dragos Platform — Industrial Cybersecurity for OT*. Recuperado de https://www.dragos.com/

[28] InprOTech (2020). *Guardian — Plataforma de Monitorización de ciberseguridade industrial*. Recuperado de https://inprotech.es/guardian/

[29] ENISA (2019). *Technical Reports on Cybersecurity Situational Awareness — Vulnerabilities*. Recuperado de https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities

[30] CISA (2008). *Recommended Practice: Patch Management for Control Systems*. Recuperado de https://www.cisa.gov/sites/default/files/2023-01/RP_Patch_Management_S508C.pdf

[31] Qualys (2025). *Survey of Top 10 Exploited Vulnerabilities in 2023*. Recuperado de https://blog.qualys.com/qualys-insights/2023/09/26/qualys-survey-of-top-10-exploited-vulnerabilities-in-2023

[32] ENISA (2012). *Introduction to Return on Security Investment (ROSI)*. Recuperado de https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment

[33] Stewart, J. M., Chapple, M., & Gibson, D. (2021). *CISSP Official (ISC)² Study Guide* (9th ed.). Sybex / Wiley.

[34] Soo Hoo, K. J. (2000). *How much is enough? A risk management approach to computer security*. Recuperado de https://cisac.fsi.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security

[35] Sonnenreich, W., Albanese, J., & Stout, B. (2005). *Return on Security Investment (ROSI): A Practical Quantitative Model*. Recuperado de https://www.scitepress.org/papers/2005/25802/25802.pdf

[36] Nozomi Networks (2025). *OT/IoT Cybersecurity Trends & Insights — July 2025 Review*. Recuperado de https://es.nozominetworks.com/ot-iot-cybersecurity-trends-insights-july-2025

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

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

[39] Dragos (2025). *OT Cybersecurity Year in Review — 2025 Edition*. Recuperado de https://www.dragos.com/ot-cybersecurity-year-in-review#download-the-report

[40] Kaspersky ICS CERT (2025). *Industrial Cybersecurity Statistics*. Recuperado de https://ics-cert.kaspersky.com/statistics/

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

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

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

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

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

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

[47] Australian Cyber Security Centre (2024). *Principles of Operational Technology Cyber Security*. Recuperado de https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/principles-of-operational-technology-cyber-security

Glosario

APT (Advanced Persistent Threat / Ameaza Persistente Avanzada)

Tipo de atacante ou campaña caracterizada polo seu alto grao de sofisticación, persistencia e orientación a obxectivos estratéxicos. Adoitan ser grupos patrocinados por Estados ou actores con grandes recursos.

BC/DR (Business Continuity / Disaster Recovery)

Conxunto de plans, procedementos e capacidades que permiten a unha organización continuar operando ou recuperarse tras un incidente grave. En OT, inclúe restauración de sistemas de control e de comunicacións industriais.

CAPEC (Common Attack Pattern Enumeration and Classification)

Catálogo de patróns de ataque recorrentes que describe como os atacantes explotan debilidades técnicas. Útil para entender tácticas e métodos de ataque en ICS.

CISA (Cybersecurity and Infrastructure Security Agency)

Axencia estadounidense responsable da ciberseguridade de infraestruturas críticas. Publica avisos ICS, o catálogo KEV e guías como a de xestión de parches en sistemas de control.

CERT (Computer Emergency Response Team)

Equipo especializado no manexo de incidentes de ciberseguridade. Publica avisos, coordinacións e recomendacións. Existen CERT nacionais, sectoriais e corporativos.

CCN-CERT (Centro Criptológico Nacional – CERT)

CERT español orientado principalmente a administracións públicas e organismos de interese estratéxico. Proporciona alertas, informes e guías técnicas.

CISA KEV (Known Exploited Vulnerabilities)

Catálogo mantido por CISA que recompila vulnerabilidades que están a ser explotadas activamente no mundo real. Son consideradas prioritarias para mitigación.

CMDB (Configuration Management Database)

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

Base de datos que recolle e xestiona a información de configuración de activos tecnolóxicos, incluídas versións, relacións e cambios.

CPS (Cyber-Physical Systems / Sistemas Ciberfísicos)

Sistemas onde compoñentes dixitais, comunicacións e procesos físicos interactúan estreitamente. OT é un exemplo de CPS.

CPS PP (Cyber-Physical Systems Protection Platforms)

Plataformas de seguridade específicas para contornas ciberfísicas, capaces de entre outros, descubrir activos OT, identificar vulnerabilidades e detectar anomalías.

CVE (Common Vulnerabilities and Exposures)

Sistema estandarizado de identificación de vulnerabilidades cun identificador único para cada fallo documentado.

CVSS (Common Vulnerability Scoring System)

Sistema de puntuación que clasifica a severidade técnica dunha vulnerabilidade segundo impacto e explotabilidade.

DCS (Distributed Control System / Sistema de Control Distribuído)

Arquitectura de control distribuído habitual en industrias de proceso continuo. Componse de múltiples controladores coordinados desde unha interface de supervisión.

DMZ industrial (Zona desmilitarizada industrial)

Zona de rede intermedia entre TI e OT deseñada para limitar a exposición entre ambas. Aloxa servizos que actúan como punto de intercambio controlado.

Fail-safe / Fail-secure

Conceptos que describen como debe comportarse un sistema de control ante un fallo: deixar o proceso nun estado seguro (fail-safe) ou manter protección mediante restricións estritas (fail-secure).

Hardening (Endurecemento)

Conxunto de prácticas para reducir a superficie de ataque dun sistema: deshabilitar servizos innecesarios, reforzar autenticación, limitar accesos e aplicar configuracións seguras.

HMI (Human–Machine Interface / interface Home–Máquina)

interface que permite aos operadores visualizar e controlar sistemas industriais, xestionar alarmas e supervisar procesos.

ICS (Industrial Control Systems / Sistemas de Control Industrial)

Familia de sistemas deseñados para supervisar e controlar procesos industriais. Inclúe SCADA, DCS, PLC, RTU e outros equipos.

ICS-CERT

Equipo de resposta a incidentes orientado a sistemas de control industrial. Historicamente parte do Departamento de Seguridade Nacional de EE. UU., agora integrado en CISA.

INCIBE (Instituto Nacional de Ciberseguridad)

Organización española que publica avisos, guías e recomendacións, incluíndo alertas específicas para sistemas industriais.

Inventario de activos (Asset Inventory)

Relación estruturada dos compoñentes presentes nunha contorna OT, incluíndo a súa función, versión, criticidade e localización na rede.

IoT / IIoT (Internet of Things / Industrial Internet of Things)

Conxunto de dispositivos conectados que recompilan datos e actúan na contorna. No ámbito industrial refírese a dispositivos IIoT, que se integran con sistemas de control.

KEV (Known Exploited Vulnerabilities)

Vulnerabilidades que se sabe están a ser explotadas no mundo real. Considéranse prioritarias para mitigación.

MITRE ATT&CK / MITRE ATT&CK for ICS

Marco que documenta tácticas e técnicas usadas por atacantes. A versión ICS recompila técnicas específicas aplicables a contornas industriais.

NIST NVD (National Vulnerability Database)

Base de datos mantida por NIST que amplía a información de CVE e proporciona métricas adicionais de severidade.

Now / Next / Never

Modelo de priorización de vulnerabilidades baseado en risco operativo real:

- *Now*: vulnerabilidades críticas que poden afectar de inmediato a control ou visibilidade do proceso.
- *Next*: vulnerabilidades relevantes pero cuxo risco depende de factores adicionais (exposición, arquitectura).
- *Never*: vulnerabilidades que, no contexto concreto, non supoñen risco significativo se existen controis axeitados.

OT (Operational Technology / Tecnoloxías de Operación)

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

PLC (Programmable Logic Controller / Autómata programable)

Dispositivo de control industrial que executa lóxicas e ordena a actuación sobre equipos físicos como válvulas e motores.

PSIRT (Product Security Incident Response Team)

Equipo de resposta dun fabricante encargado de vulnerabilidades e avisos de seguridade relacionados cos seus produtos.

Purdue Model / Modelo Purdue

Modelo de referencia que segmenta as contornas industriais en niveis (IT corporativo, DMZ, supervisión, control, campo) para estruturar a seguridade e as comunicacións.

Red Team / Purple Team

Actividades avanzadas de avaliación de seguridade: Red Team simula ataques reais, Purple Team combina Red e Blue Team para mellorar defensas.

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

Rollback

Proceso para reverter un parche ou cambio se produce efectos non desexados, restaurando a configuración anterior sen interromper o proceso.

RTU (Remote Terminal Unit / Unidade Terminal Remota)

Dispositivo que recompila datos de sensores ou equipos remotos e comunícaos a sistemas SCADA ou outras plataformas de control.

Safety vs. Security

Distinción entre seguridade funcional (protección de persoas e equipos fronte a fallos do proceso) e ciberseguridade (protección de sistemas fronte a ataques ou usos indebidos).

SCADA (Supervisory Control and Data Acquisition)

Sistema de supervisión e adquisición de datos que centraliza información procedente de equipos de campo e permite o control de procesos distribuídos.

Threat hunting OT

Actividade de procura proactiva de indicios de intrusión ou comportamento anómalo en redes e sistemas industriais.

TI (Tecnoloxías da Información)

Sistemas e servizos corporativos de xestión de información, comunicacións e aplicacións de negocio.

TTP (Tactics, Techniques and Procedures)

Descrición estruturada dos métodos utilizados por atacantes en campañas reais.

Xanela de mantemento

Período planificado durante o cal se permite intervir en sistemas de control ou equipos sen afectar a operación.

Zero-day

Vulnerabilidade descoñecida para o fabricante no momento en que é explotada, sen parche dispoñible inicialmente.

Anexo. Avisos de fabricantes OT

Coa fin de facilitar a consulta directa dos avisos de seguridade publicados polos principais fabricantes de tecnoloxía industrial, inclúese a continuación unha **relación dos portais oficiais onde cada provedor publica vulnerabilidades, parches, mitigacións e boas prácticas asociadas aos seus produtos**.

Este anexo serve como complemento natural á sección de alertas do boletín, permitindo ao lector acceder rapidamente á información primaria e manter un seguimento continuo das actualizacións de seguridade relevantes para a súa contorna.

Siemens

https://www.siemens.com/global/en/products/services/cert.html?SiemensSecurityAdvisories=

Schneider Electric

https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Rockwell Automation

https://www.rockwellautomation.com/en-gb/trust-center/security-advisories.html

ABB

https://global.abb/group/en/technology/cyber-security/alerts-and-notifications

B&R (Bernecker & Rainer Automation)

https://www.br-automation.com/en/service/cyber-security/cyber-security-advisories-and-notices/

Mitsubishi Electric

https://www.mitsubishielectric.com/psirt/vulnerability/index.html

Omron

https://automation.omron.com/en/us/about-omron-automation/cybersecurity

Beckhoff

https://infosys.beckhoff.com/english.php?content=../content/1033/ipc_security/976057355.html&id=

Festo

https://www.festo.com/us/en/e/support/get-support/report-security-risk-psirt-id_330543/

Esta relación non é exhaustiva, pero recolle a varios dos fabricantes máis presentes en contornas ICS/OT. Aconséllase ao lector buscar os recursos asociados aos seus fabricantes de referencia.

Consultar periodicamente estes portais ou subscribirse nos casos que o permita, axuda a anticipar riscos, validar configuracións, programar campañas de parcheo e, en xeral, manter un nivel de vixilancia acorde ao nivel de risco asumible, e aliñado co ciclo de vida dos sistemas industriais.

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial
Informe de ciberalertas – I

AMTEGA – Xunta de Galicia 2026

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