CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Informe de ciberalertas - I

Enero 2026

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

Edita: Xunta de Galicia
Agencia para la Modernización Tecnológica de Galicia (AMTEGA)

Lugar: Santiago de Compostela
Año: 2026

Índice

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

1 Introducción

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

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

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

--

La progresiva digitalización del tejido industrial, junto con la consolidación de arquitecturas cada vez más interconectadas, **continúa ampliando de forma significativa la superficie de exposición de los sistemas OT**. Este fenómeno, observado desde hace varios años, se ha intensificado a medida que **la convergencia entre tecnologías de operación y tecnologías de la información se ha convertido en un elemento estructural** de sectores como la energía, el agua, la automoción, la alimentación o la logística. El crecimiento de esa interdependencia tecnológica ha generado un ecosistema operativo más eficiente, pero también **más vulnerable frente a actores maliciosos con capacidad técnica, motivación económica o interés estratégico**.

Los datos recogidos en el informe **ENISA Threat Landscape 2025** [1] muestran que la explotación de vulnerabilidades continúa siendo uno de los vectores de intrusión más relevantes en el panorama europeo, representando el **21,3 %** de los casos analizados. Destaca, además, que casi **el 70 % de los incidentes basados en vulnerabilidades derivan en una intrusión efectiva**, lo que evidencia la eficacia de este vector para los

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

actores maliciosos y la rapidez con la que se aprovechan errores recientemente publicados. Además, ENISA (Agencia de la Unión Europea para la Ciberseguridad) subraya la creciente capacidad de las campañas automatizadas para explotar vulnerabilidades en cuestión de días desde su divulgación pública, incrementando la presión sobre organizaciones que dependen de sistemas industriales y servicios críticos. De esta circunstancia y del contexto OT específico hablaremos en la sección siguiente.

De forma complementaria, el **Balance de Ciberseguridad 2024 del Instituto de Ciberseguridad de España (INCIBE)** [2] —el último disponible en la fecha de elaboración de este informe— indica que se han gestionado más de 97.000 incidentes en esa anualidad, con **más de 31.500 afectando directamente a empresas y más de 183.000 sistemas vulnerables identificados** en el territorio nacional. Estos datos subrayan la persistencia de defectos de seguridad y la necesidad de adoptar medidas preventivas robustas para mitigar riesgos que pueden traducirse en impactos operacionales severos.

En este contexto, el **presente informe adopta un doble enfoque** con el fin de reforzar su carácter didáctico y facilitar una comprensión progresiva de los elementos clave relacionados con la gestión de vulnerabilidades y alertas en entornos OT:

- Cada edición incluirá **un bloque conceptual orientado a clarificar aspectos teóricos de interés** —conceptos, modelos, prácticas de referencia y fundamentos metodológicos— que sirvan como base para interpretar adecuadamente los riesgos y las medidas asociadas.
- Se mantendrá un análisis estructurado y orientado a la acción, centrado **en las vulnerabilidades y alertas más relevantes del trimestre**, con el objetivo de proporcionar información práctica y directamente aplicable por parte de empresas y administraciones públicas.

En el primer informe, este bloque conceptual se centrará en **definir formalmente qué es una vulnerabilidad**, **analizar los tiempos de explotación** desde diversas perspectivas (incluyendo estudios de diferentes entidades y organismos) y examinar el retorno de la inversión asociado a su correcta gestión. En ediciones posteriores se abordarán otros aspectos esenciales del proceso de gestión de vulnerabilidades, entre los que podrían encontrarse:

- **Estrategias de priorización basadas en el riesgo** —considerando fuente como el catálogo KEV de CISA—;

- **La importancia de la visibilidad y del inventario OT** como base para la priorización y alineamiento con marcos como IEC 62443;
- **La aplicación de controles compensatorios cuando el parcheo no es viable**: segmentación, filtrado avanzado, *whitelisting y* otras técnicas de mitigación propias de entornos industriales.

De esta forma, el informe combina **orientación didáctica y utilidad operativa**, proporcionando tanto una base conceptual sólida como un análisis actualizado que permita **asentar la resiliencia del ecosistema industrial gallego frente a amenazas que evolucionan rápido y de complejidad creciente**.

Entre los avisos más relevantes del trimestre, destaca el emitido por Siemens, que afecta a un número especialmente elevado de productos y componentes ampliamente desplegados en sectores industriales y de infraestructuras críticas. Este hecho subraya la importancia de mantener una vigilancia continua sobre los fabricantes estratégicos y de reforzar los procesos internos de identificación y evaluación de impacto.

Además de este caso, se aprecia una intensificación de vulnerabilidades relacionadas con accesos remotos, errores de autenticación y exposiciones no intencionadas, junto a una dependencia creciente y anunciada entre redes IT y OT.

2 Metodología y fuentes

Este boletín se apoya en un conjunto amplio y contrastado de fuentes **oficiales, bases de datos de vulnerabilidades, informes especializados y avisos de fabricantes industriales**, con el fin de ofrecer una visión clara, actualizada y útil para empresas y administraciones públicas.

El enfoque adoptado combina dos elementos esenciales:

- **Consulta sistemática de fuentes fiables y reconocidas**, tanto nacionales como internacionales, que incluyen CERTs (Computer Emergency Response Teams, o Equipos de Respuesta ante Emergencias Informáticas), Agencias Europeas, bases de datos de vulnerabilidades, publicaciones de referencia, informes sectoriales y avisos oficiales de fabricantes OT/ICS.
- **Selección y organización de la información** para que resulte relevante y práctica, priorizando aquella relacionada con vulnerabilidades y alertas que afectan a tecnologías industriales empleadas en sectores estratégicos gallegos, como los representados en el Laboratorio de Ciberseguridad Industrial de AMTEGA [3].

Este boletín no pretende por ahora realizar análisis avanzados como la extracción de tendencias, la correlación entre fuentes o la evaluación comparada de criticidades. El propósito es garantizar una **visión clara, estructurada y fundamentada** en fuentes consolidadas, con alertas comprensibles y accionables por el ecosistema gallego para la protección de sus activos.

Las fuentes empleadas abarcan diferentes categorías relevantes para la construcción del informe. Entre ellas destacan:

- **CERT nacionales e internacionales**, como INCIBE-CERT, CCN-CERT (del Centro Criptológico Nacional), CISA (Agencia de Ciberseguridad y Seguridad de Infraestructuras estadounidense) o CERT@VDE (CERT alemán especializado en sistemas industriales y de control).
- **Agencias y organismos europeos e internacionales**, como ENISA o NIST (Instituto Nacional de Estándares y Tecnología estadounidense).
- **Bases de datos de vulnerabilidades ampliamente reconocidas**, como NVD, CVE.org o EUVD (norteamericanas y europea, respectivamente).

- **Informes y/o laboratorios de investigación en ciberseguridad industrial**, de orígenes como Nozomi Networks, Claroty Team82, Dragos, SANS, ICS STRIVE y Kaspersky ICS CERT.
- **Los paneles de avisos oficiales de seguridad publicados por fabricantes industriales**, como por ejemplo Siemens, Schneider Electric, Rockwell Automation, ABB, B&R, Mitsubishi Electric, Omron, Beckhoff y Festo.
- **Documentos y guías metodológicas** aplicables a la gestión de vulnerabilidades en entornos OT, como las publicadas por CISA.

En su conjunto, esta agrupación de fuentes proporciona una **base sólida, actualizada y orientada a la práctica**, que asegura que su contenido sea de utilidad para el tejido empresarial y las Administraciones Públicas ligadas al sector industrial.

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

3 Vulnerabilidades

3.1 Marco teórico

3.1.1 Definición

En el campo de la ciberseguridad, se entiende por **vulnerabilidad** cualquier **debilidad, error o deficiencia** presente en un sistema, red, aplicación, dispositivo o configuración, que **pudiera ser aprovechada por un atacante para comprometer la confidencialidad, integridad o disponibilidad** de la información o de los servicios que dicho activo proporciona. Esta definición, ampliamente aceptada en la literatura especializada, resulta igualmente aplicable tanto a entornos puramente TI como a infraestructuras OT e industriales.

Las vulnerabilidades pueden tener su origen en múltiples factores: **errores de diseño** (arquitecturas que no contemplan adecuadamente la seguridad), **errores de programación** (por ejemplo, ausencia de validación de entradas, desbordamientos de memoria o condiciones de carrera), **configuraciones incorrectas o inseguras** (servicios innecesarios expuestos, contraseñas por defecto, reglas de cortafuegos excesivamente permisivas), **software o firmware desactualizados** que no incorporan correcciones conocidas, o **procedimientos organizativos deficientes** que no establecen controles efectivos sobre cambios, accesos o gestión de parches.

Las consecuencias derivadas de la explotación de una **vulnerabilidad** pueden ser muy diversas, pero suelen materializarse en accesos no autorizados a sistemas o datos, **interrupciones del servicio**, alteración o destrucción de información, **escalada de privilegios** dentro de una red, instalación de malware o empleo de la infraestructura comprometida como punto de apoyo para lanzar ataques contra terceros. En entornos industriales, estas consecuencias pueden trasladarse incluso al plano físico: modificación de parámetros de proceso, parada de líneas de producción, daños en equipo o impacto sobre la seguridad de las personas físicas.

En el caso de los sistemas OT, una vulnerabilidad en un PLC, una HMI, una RTU, una pasarela de comunicaciones industrial o un servidor SCADA no afecta únicamente a un activo lógico, sino que puede comprometer la capacidad de controlar válvulas, motores, bombas, robots o sistemas de climatización industrial. De esta forma, una simple debilidad técnica puede convertirse en el origen de un incidente con repercusiones directas sobre la continuidad operativa, la calidad del producto o la seguridad 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 y su clasificación

Antes de abordar las distintas clasificaciones, resulta útil considerar los cinco **factores que permiten identificar una vulnerabilidad**:

1. **Exposición**: el activo vulnerable debe estar accesible para un atacante, ya sea de forma remota, local o física.
2. **Empleo de una técnica de ataque conocida**: la vulnerabilidad debe poder explotarse mediante un método documentado o comprendido.
3. **Impacto demostrable**: su explotación debe tener consecuencias medibles sobre el sistema, proceso o información.
4. **Condiciones de explotación**: deben existir los requisitos necesarios (privilegios, acceso, interacción del usuario, etc.).
5. **Existencia de un agente capaz de explotar**: un adversario con motivación, intención y medios.

Estos factores permiten juzgar entre una simple debilidad teórica y una **vulnerabilidad real y explotable**, lo que es esencial para su correcta priorización operativa.

Clasificaciones de vulnerabilidades

La literatura técnica y los marcos de referencia internacionales proponen distintas formas de **clasificar las vulnerabilidades**, en función de aspectos como el tipo de activo afectado, la causa raíz, la forma de explotación o el impacto potencial.

a) Según el tipo de activo afectado

- **Vulnerabilidades de software**: defectos presentes en el código de aplicaciones, sistemas operativos, servicios o firmware. Por ejemplo, un desbordamiento de búsqueda en el firmware de un PLC o un fallo de convalidación en una API de gestión de un SCADA.
- **Vulnerabilidades de hardware**: defectos en el diseño o implementación de componentes físicos que permiten comportamientos no previstos o inseguros. Aunque menos frecuentes pueden encontrarse en controladores específicos, tarjetas de comunicación o módulos criptográficos.
- **Vulnerabilidades de red y comunicaciones**: configuraciones inseguras en routers, switches, cortafuegos o dispositivos industriales de comunicación; uso

de protocolos sin cifrado ni autenticación (como Modbus/TCP o DNP3 en su versión clásica); servicios innecesarios expuestos a redes no confiables.

- **Vulnerabilidades en aplicaciones web**: debilidades en portales de administración, paneles de monitorización o interfaces web de ingeniería, que permiten ataques de inyección SQL, cross-site scripting (XSS) o eludir mecanismos de autenticación. En entornos OT, es habitual que la consola de gestión de un SCADA o de un historiador de datos se exponga mediante una interfaz web.
- **Vulnerabilidades en dispositivos IoT/IIoT**: firmware no actualizable, credenciales por defecto, servicios embebidos inseguros o falta de mecanismos de actualización, muy frecuentes en sensores, cámaras o dispositivos auxiliares conectados a redes industriales.
- **Vulnerabilidades específicas de sistemas OT**: afectan a PLC, HMI, sistemas SCADA, sistemas de control distribuido (DCS) o gateways industriales, e incluyen desde falta de autenticación en funciones críticas hasta ausencia de registros de auditoría o mecanismos débiles de integridad de firmware.

b) Según la causa raíz

- **Errores de programación**: fallos en el código que permiten ejecutar instrucciones no previstas, provocar condiciones de error explotables o manipular datos sin los controles adecuados.
- **Diseño inseguro del sistema**: arquitecturas que no contemplan segmentación de redes, separación de funciones o principios básicos de mínima exposición y mínimo privilegio.
- **Empleo de componentes obsoletos**: bibliotecas, sistemas operativos o firmware que dejaron de recibir soporte y acumulan vulnerabilidades conocidas.
- **Configuraciones defectuosas o por defecto**: servicios innecesarios activos, puertos abiertos sin justificación, credenciales predeterminadas o reglas de cortafuegos excesivamente permisivas.
- **Dependencias vulnerables**: inclusión de componentes de terceros (por ejemplo, bibliotecas en una aplicación industrial) que presentan vulnerabilidades ya documentadas.

c) Según su explotabilidad

Otro modo habitual de clasificar las vulnerabilidades es atendiendo a las condiciones necesarias para su explotación:

- **Explotables remotamente**: permiten a un atacante comprometer el sistema a través de la red, sin necesidad de acceso físico (por ejemplo, ejecución remota de código en un servidor SCADA expuesto).
- **Explotación local o con acceso físico**: requieren que el atacante tenga acceso directo al sistema o a la red interna (por ejemplo, conexión a un puerto serie de un PLC en planta).
- **Requieren autenticación previa**: sólo pueden explotarse tras obtener o eludir credenciales válidas.
- **Explotables de forma automatizada**: su explotación puede integrarse fácilmente en herramientas y kits, facilitando campañas de ataque a gran escala.

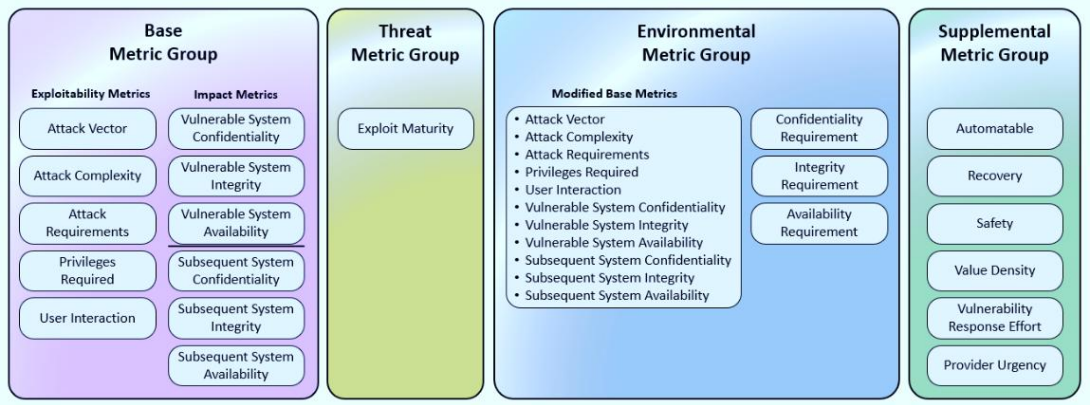
d) Según estándares y esquemas de referencia

En la práctica, la clasificación de vulnerabilidades adopta apoyarse en **estándares consolidados**:

- **CVE (Common Vulnerabilities and Exposures)** proporciona un identificador único para cada vulnerabilidad conocida, lo que facilita su seguimiento y referencia [4].
- **CVSS (Common Vulnerability Scoring System)** asigna una puntuación de criticidad (por general de 0 a 10) basada en factores como la facilidad de explotación, el impacto sobre confidencialidad, integridad y disponibilidad, o la necesidad de interacción del usuario [5].

  CVSS 4.0 constituye la versión más reciente del estándar internacional utilizado para medir la gravedad de una vulnerabilidad, aportando un modelo más preciso y flexible que sus predecesores. Su objetivo es ofrecer una valoración que refleje tanto la naturaleza intrínseca de la vulnerabilidad como su explotación real y su impacto en una entorno concreto. Establece su valoración de severidad a partir de cuatro grupos de métricas que permiten describir con precisión el riesgo asociado a una vulnerabilidad.

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. Fuente: first.org (2023)

El primer grupo, las **métricas Base**, representa las características intrínsecas de la vulnerabilidad que no dependen del tiempo ni del entorno donde se encuentre el sistema afectado. Estas métricas se dividen en dos subconjuntos: las de **Explotabilidad**, que describen la facilidad técnica con la que puede explotarse el fallo en el sistema vulnerable —como el vector de ataque, la complejidad, los privilegios requeridos o la interacción del usuario—, y las de **Impacto**, que evalúan las consecuencias directas de una explotación exitosa. Estas últimas consideran tanto el impacto sobre el propio sistema vulnerable como el impacto sobre sistemas subsiguientes, pudiendo incluir incluso implicaciones sobre la seguridad física, un aspecto incluido originariamente con CVSS v3 al ampliar el concepto de alcance (scope en inglés) más allá del componente técnico afectado.

El segundo grupo, las **métricas de Amenaza (Threat)**, incorpora información relativa al estado de explotación conocido de la vulnerabilidad. Dado que estas condiciones pueden variar en el tiempo, este grupo permite ajustar la severidad en función de si existen pruebas públicas de explotación, código disponible o incidentes confirmados. Así, una vulnerabilidad con alto impacto teórico, pero sin evidencia de explotación, puede recibir una valoración diferente respecto de otra activamente explotada por actores maliciosos.

El tercer grupo, las **métricas Ambientales (Environmental)**, adapta la puntuación al contexto específico de cada organización. Este ajuste tiene en cuenta la criticidad del sistema afectado, la existencia de controles que mitiguen los impactos o la importancia relativa de atributos como la confidencialidad, la integridad o la disponibilidad. En entornos OT o CPS, donde la disponibilidad y

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

la seguridad física pueden ser prioritarias, estas métricas permiten reflejar de forma más realista la severidad operativa de una vulnerabilidad.

Finalmente, CVSS 4.0 incorpora un cuarto grupo denominado **métricas Suplementarias (Supplemental),** que proporciona descriptores adicionales sobre características externas de la vulnerabilidad —como requisitos reglamentarios, aspectos relacionados con la seguridad humana o la posibilidad de explotación automatizada—. Estas métricas **no afectan al cálculo de la puntuación CVSS**, pero permiten a cada organización incorporar factores que resulten relevantes en su propio modelo de priorización, enriqueciendo la interpretación del riesgo sin modificar la puntuación estándar.

La escala continúa midiendo de 0 a 10. Las categorías de severidad son las siguientes: de 0,0 a 3,9 se declara baja, de 4,0 a 6,9 media, de 7,0 a 8,9 alta y de 9,0 a 10 crítica.

En su conjunto, CVSS 4.0 proporciona una visión más ajustada del riesgo, especialmente útil en contextos OT e industriales donde la explotación de una vulnerabilidad puede trascender el plano digital y afectar a la continuidad operativa o a la seguridad física.

- El **catálogo KEV (Known Exploited Vulnerabilities)** de la CISA [6][7] recoge vulnerabilidades que se sabe que están siendo **explotadas activamente**, constituyendo un subconjunto especialmente prioritario a la hora de planificar medidas de mitigación.

En entornos OT continuamente se encuentran vulnerabilidades asociadas al uso de protocolos sin cifrado ni autenticación robusta, lógicas de control expuestas sin controles de acceso, firmware desactualizado o paneles de administración accesibles desde redes no segmentadas. En estos casos, la correcta clasificación y comprensión del contexto operativo es crucial para determinar su verdadera criticidad.

3.1.3 Organismos y marcos de referencia

La gestión de vulnerabilidades se apoya en el trabajo de diversos **organismos y comunidades de referencia**, que proporcionan marcos conceptuales, listados de debilidades y modelos de ataque. Entre los más relevantes destacan **OWASP** [8] y **MITRE** [9].

3.1.3.1 OWASP

El **Open Worldwide Application Security Project (OWASP) es** una organización internacional sin ánimo de lucro dedicada a mejorar la seguridad del software. Se estructura como una comunidad abierta en la que participan profesionales de desarrollo, auditoría y operación de sistemas, que colaboran en la creación de guías, herramientas y buenas prácticas.

Su proyecto más conocido **es el OWASP Top 10** [10], un informe que se actualiza periódicamente y que recoge los diez riesgos más críticos en seguridad de aplicaciones web. Este documento se ha consolidado como un **estándar de concienciación** para desarrolladores y responsables de seguridad, al ofrecer una síntesis de las vulnerabilidades más frecuentes y de mayor impacto observadas en la práctica.

Aunque el foco original de OWASP se ubica en el ámbito de las aplicaciones web corporativas, muchos de los riesgos identificados son plenamente aplicables a **interfaces de gestión y supervisión industrial**. Por ejemplo:

- Consolas web utilizadas para administrar sistemas SCADA o historiadores de planta.
- Portales de mantenimiento remoto de equipos industriales.
- APIs (interfaces de programación de aplicaciones) expuestas que permiten interactuar con dispositivos OT o recopilar datos de proceso.

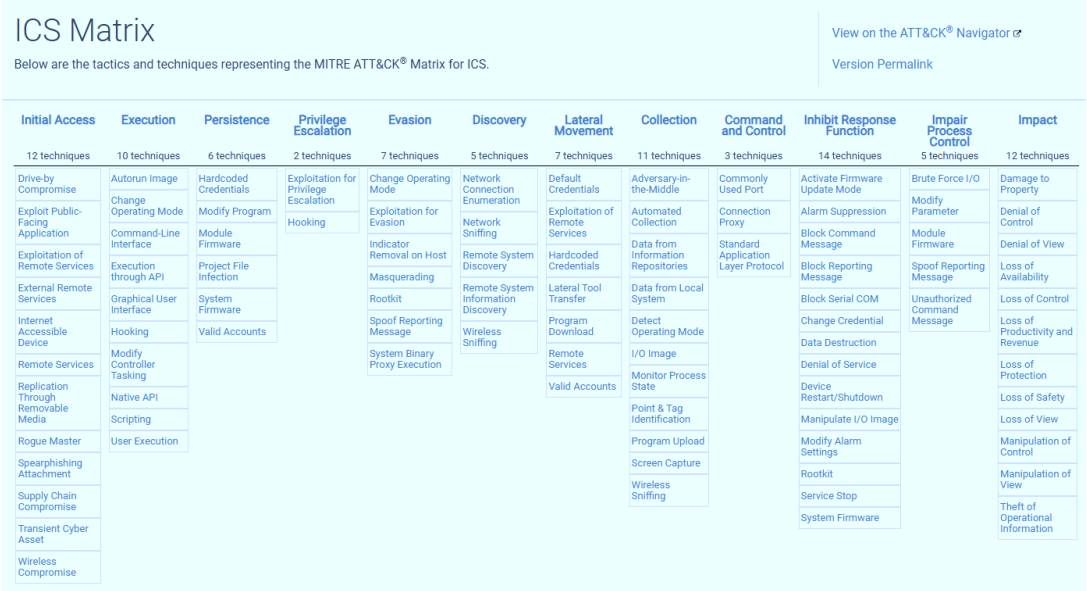
En todos estos casos, errores como **la inyección de código**, la **falta de control de acceso**, **la gestión deficiente de sesiones** o **la exposición de información sensible** pueden facilitar a un atacante el acceso a sistemas industriales que, en principio, no deberían ser alcanzables desde el exterior.

3.1.3.2 MITRE ATT&CK, CWE e CAPEC

La entidad **MITRE** es una organización estadounidense sin ánimo de lucro que provee ingeniería de sistemas, I+D y soporte sobre tecnologías de la información al gobierno de Estados Unidos de América, y mantiene varios catálogos de conocimiento esenciales para comprender y gestionar vulnerabilidades y ataques:

- **MITRE ATT&CK** es una matriz que documenta técnicas y procedimientos utilizados por atacantes reales, organizados por tácticas (objetivos) y fases de la intrusión. Ofrece una taxonomía práctica para entender cómo se encadenan distintas acciones maliciosas en campañas reales [11].

- **MITRE ATT&CK for ICS** amplía este modelo al ámbito industrial, recogiendo técnicas específicas utilizadas contra sistemas de control industrial (ICS), como la manipulación de lógicas de PLC, la inserción de comandos maliciosos en protocolos industriales o la modificación de parámetros de control [12].



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

- **CWE (Common Weakness Enumeration)** proporciona un catálogo estructurado **de debilidades de software**, es decir, patrones de errores que pueden dar lugar a vulnerabilidades (por ejemplo, "validación insuficiente de entradas" o "gestión insegura de recursos") [13].
- **CAPEC (Common Attack Pattern Enumeration and Classification)** clasifica patrones de ataque recurrentes, facilitando la comprensión de cómo se explotan en la práctica las debilidades recogidas en CWE [14].

En el contexto OT, estos marcos permiten relacionar **vulnerabilidades técnicas concretas** (por ejemplo, un fallo de autenticación en la interfaz web de un PLC) con **técnicas de ataque documentadas** (como el abuso de servicios remotos o la modificación de lógicas de control), proporcionando un lenguaje común para analistas, operadores y equipos de respuesta ante incidentes.

Además de OWASP y MITRE, existen otros marcos y estándares relevantes para la caracterización formal y el 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

La **NVD (National Vulnerability Database)** [15], mantenida por NIST [16], constituye la base de datos de referencia para la clasificación y consulta de vulnerabilidades. Amplía el registro CVE con:

- métricas CVSS oficiales,
- análisis de severidades,
- puntuaciones temporales y contextuales,
- enlaces a recursos adicionales.

En entornos OT, la NVD es particularmente útil para identificar firmware vulnerable, bibliotecas afectadas o componentes obsoletos incluidos en equipos industriales. Recientemente, por cuestiones de soberanía tecnológica en Europa se impulsó la creación de la **alternativa EUVD (EU Vulnerability Database)** [17].

3.1.3.4 MITRE Top 25

El **MITRE CWE Top 25 Most Dangerous Software Weaknesses** [18] identifica cada año las 25 debilidades más peligrosas en software, basadas en su prevalencia y severidad. Muchas de ellas están presentes también en dispositivos industriales, incluyendo:

- validación insuficiente de entradas (CWE-20)
- errores de gestión de memoria (CWE-119),
- exposición de información sensible (CWE-200),
- configuraciones inseguras (CWE-16).

Su utilidad radica en que permite prever qué errores son más probables en software industrial, especialmente en firmware de PLC o aplicaciones de ingeniería.

3.1.3.5 CVRF – Common Vulnerability Reporting Framework

El **CVRF (Common Vulnerability Reporting Framework)** [19] es un estándar de estructuración de informes de vulnerabilidades promovido por OASIS (un consorcio internacional de estándares tecnológicos). Permite a fabricantes y CERT publicar avisos de forma consistente, incluyendo:

- descripción técnica de la vulnerabilidad,

- impacto,
- productos afectados,
- enlaces CVE y métricas CVSS,
- recomendaciones de mitigación

Fabricantes industriales como Siemens, Schneider Electric o Rockwell Automation emplean formatos compatibles con CVRF para distribuir avisos de seguridad, lo que facilita su integración en herramientas automáticas de gestión de vulnerabilidades.

3.1.4 Herramientas de análisis de vulnerabilidades

Las herramientas de análisis de vulnerabilidades constituyen un elemento central del proceso, ya que permiten automatizar la detección de un gran número de debilidades conocidas. Sin embargo, su uso debe entenderse siempre como un complemento —y no como sustituto— de un análisis experto.

3.1.4.1 Escáneres tradicionales

Entre las herramientas más extendidas se encuentran:

- **OpenVAS / Greenbone**: OpenVAS [20] nació como un proyecto de software libre para el análisis de vulnerabilidades, que con el tiempo dio lugar a soluciones comerciales como las de Greenbone [21]. Aunque OpenVAS sigue siendo una herramienta útil con fines didácticos y en determinados escenarios, en entornos profesionales se considera preferible emplear versiones soportadas y con bases de firmas actualizadas regularmente.
- **Nessus (Tenable)** [22]: uno de los escáneres de vulnerabilidades más reconocidos. Dispone de una amplia base de datos de plugins mantenida por Tenable y ofrece capacidades avanzadas para detectar debilidades en sistemas, aplicaciones y redes. Adopta destacarse por su precisión en la detección y por la disponibilidad de documentación y soporte.
- **Qualys** [23]: plataforma basada en la nube que combina evaluación de vulnerabilidades con otras capacidades (análisis de configuración, cumplimiento normativo, monitorización continua). Su arquitectura distribuida y su orientación a grandes entornos la convierten en una opción adecuada para organizaciones con infraestructuras complejas y heterogéneas.

En todos los casos, estas herramientas permiten generar informes estructurados en los que las vulnerabilidades se clasifican por criticidad, lo que facilita su priorización.

3.1.4.2 Soluciones específicas para OT (CPS PP)

Gartner define las **plataformas de protección para sistemas ciberfísicos** (CPS PP, Cyber-Physical Systems Protection Platform [24], por sus siglas en inglés) como aquellas soluciones que utilizan el conocimiento de los protocolos industriales, el tráfico de red operacional o de producción, y el comportamiento de los activos físicos, con el fin de **descubrir, categorizar, mapear y proteger a los CPS en entornos de producción o críticos que quedan fuera del ámbito tradicional de TI**.

En el contexto de la **ciberseguridad industrial**, surgieron estas soluciones especializadas que, entre otras cosas, permiten **identificar vulnerabilidades y debilidades en sistemas OT sin interferir con su funcionamiento**. Estas herramientas, entre las que se incluyen plataformas como **Nozomi** [25], **Claroty** [26], **Dragos** [27] o la gallega **InprOTech Guardian** [28], se basan habitualmente en la monitorización activo-pasiva del tráfico de red industrial y en el análisis de la configuración de dispositivos.

Sus principales aportaciones en este ámbito son:

- Descubrimiento automático de **activos OT** (PLC, HMI, variadores, sensores, gateways, etc.).
- Identificación de **versiones de firmware** y correlación con bases de vulnerabilidades conocidas.
- Detección de **protocolos y servicios expuestos** que puedan suponer un riesgo.
- Análisis de **anomalías en el comportamiento de** la red o de los dispositivos, que puede revelar tanto vulnerabilidades como incidentes en curso.

Este enfoque resulta especialmente valioso en redes donde el uso de escáneres tradicionales podría ser demasiado intrusivo o suponer riesgos para la disponibilidad del proceso.

Es destacar que en el Laboratorio de Ciberseguridad Industrial de AMTEGA se disponen tanto de escáneres de vulnerabilidades como de plataformas CPS PP para analizar y evaluar por parte de cualquier entidad interesada en comprender los beneficios de estas tecnologías.

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

3.1.5 Limitaciones y retos del análisis de vulnerabilidades

A pesar de su importancia, el análisis de vulnerabilidades presenta diversas **limitaciones y retos** que se deben tener en cuenta a la hora de interpretar sus resultados.

Falsos positivos

En primer lugar, las herramientas automatizadas pueden generar tanto **falsos positivos** (vulnerabilidades inexistentes, o que en realidad no son explotables en el contexto concreto) como **falsos negativos** (debilidades que pasan inadvertidas). Eso implica que los resultados deben ser revisados críticamente y, en caso necesario, validados mediante análisis manual.

Necesidad de recursos

En segundo lugar, la implementación de un programa de análisis de vulnerabilidades eficaz requiere **recursos especializados** (tiempo, personal, herramientas), cosa que no siempre está al alcance de todas las organizaciones. Esta situación se acentúa en entornos industriales, donde la coordinación entre equipos de TI, equipos OT y proveedores externos añade complejidad.

Dinamismo das vulnerabilidades

Además, el propio dinamismo del panorama de amenazas hace que el conjunto de vulnerabilidades relevantes esté en constante evolución. Nuevas debilidades se descubren de forma continua, mientras que otras pasan a ser especialmente críticas cuando se constata su explotación activa en campañas reales.

Disponibilidad

En redes industriales, se suma un reto adicional: la **prioridad otorgada históricamente a la disponibilidad** frente a otros atributos de seguridad. Esta realidad hace que, en muchos casos, exista reticencia a introducir cambios —como actualizaciones de firmware o aplicación de parches— para no afectar al funcionamiento de los procesos.

Limitaciones del entorno

Asimismo, en determinados dispositivos IoT o IIoT empleados en entornos industriales, las vulnerabilidades detectadas no pueden corregirse de forma directa, bien por

limitaciones de hardware, bien por ausencia de mecanismos de actualización, lo que obliga a recurrir a controles compensatorios.

Volumen de defectos

Por último, el elevado volumen de información generado por los escaneos exige contar con criterios claros de **priorización**, de modo que los esfuerzos se concentren en aquellas vulnerabilidades cuyo tratamiento aporta un mayor beneficio en términos de reducción del riesgo. De esto se hablará con mayor profundidad en otros informes.

3.1.6 Pentesting vs análisis de vulnerabilidades

En el discurso habitual sobre ciberseguridad se emplean con frecuencia de manera indistinta los términos **análisis de vulnerabilidades** y **pruebas de penetración (pentesting)**, a pesar de que se trata de actividades con objetivos, alcances y metodologías claramente diferenciadas (aunque complementarias).

El **análisis de vulnerabilidades** se centra en **identificar y catalogar debilidades** mediante herramientas automatizadas y revisiones sistemáticas. Su alcance es amplio: se analiza un conjunto significativo de sistemas, servicios y dispositivos, generando un inventario de vulnerabilidades que se clasifican por criticidad. No se busca, en general, explotar esas debilidades, sino conocer su existencia y valorar su impacto potencial.

Las **pruebas de penetración**, por el contrario, consisten en la **simulación controlada de ataques reales**, llevada a cabo por profesionales especializados. Partiendo, en muchos casos, de la información obtenida en un análisis de vulnerabilidades, el objetivo del pentesting es **explotar de forma controlada las** debilidades detectadas para demostrar que podría lograr un atacante en un escenario real: acceder a datos sensibles, escalar privilegios, moverse lateralmente por la red o alterar el funcionamiento de un sistema.

En el contexto industrial, un ejemplo ilustrativo sería el siguiente: mientras que un análisis de vulnerabilidades podría revelar que la interfaz web de administración de un PLC usa credenciales por defecto y ejecuta una versión de firmware vulnerable, una prueba de penetración podría demostrar que, aprovechando estas debilidades, es posible modificar la lógica de control del PLC y alterar la secuencia de funcionamiento de una línea de producción.

Las diferencias entre ambos enfoques pueden sintetizarse de la siguiente manera:

- **Propósito**: el análisis de vulnerabilidades busca **detectar y clasificar**; el test de intrusión pretende **demostrar la explotabilidad e impacto real**.
- **Profundidad**: el análisis de vulnerabilidades es tipicamente **más amplia pero menos profunda**, mientras que el pentesting es **más focalizado y detallado**.
- **Metodología**: el análisis se apoya fuertemente en **herramientas automatizadas**; el test de intrusión combina herramientas y técnicas manuales, creatividad del analista y conocimiento específico del entorno.
- **Frecuencia**: el análisis de vulnerabilidades se plantea como una actividad periódica y recurrente, mientras que las pruebas de penetración adoptan realizarse de forma más puntual, asociadas a hitos (por ejemplo, puesta en producción de una nueva planta, cambios relevantes en la arquitectura o requisitos normativos).

Lejos de ser excluyentes, ambas actividades se **refuerzan mutuamente**. Un programa maduro de gestión de vulnerabilidades se beneficia de la capacidad de los escáneres y soluciones especializadas para identificar debilidades a gran escala, mientras que las pruebas de penetración aportan evidencia tangible del riesgo que éstas debilidades suponen, ayudando a priorizar esfuerzos y a sensibilizar a los responsables de negocio y operación sobre la necesidad de abordarlas de forma sistemática.

3.2 Gestión y explotación

3.2.1 Etapas del análisis de vulnerabilidades

El **análisis de vulnerabilidades** (también denominada evaluación o gestión de vulnerabilidades) es un proceso estructurado orientado a identificar, analizar, **priorizar y tratar** las debilidades presentes en los sistemas de una organización. Aunque existen variaciones según el marco metodológico adoptado, se pueden distinguir varias etapas comunes.

a) Identificación y clasificación de activos

El primer paso consiste en determinar **qué activos se van a proteger**. Esto implica elaborar y mantener un inventario actualizado de sistemas, aplicaciones y dispositivos, identificando aquellos que resultan más críticos para el negocio. En un entorno industrial, esto incluye no sólo servidores y equipos de red, sino también PLC, HMI, RTU, gateways, sensores, robots, variadores de frecuencia o sistemas de supervisión y adquisición de datos.

Una clasificación adecuada de los activos —por criticidad, función, dependencia de otros sistemas o impacto potencial en caso de fallo— permite orientar los esfuerzos de análisis hacia aquellos elementos cuya vulnerabilidad supondría un mayor riesgo.

b) Descubrimiento y escaneo de vulnerabilidades

Una vez definidos los activos, se ejecuta su análisis mediante **herramientas automatizadas de escaneo**, que comparan la configuración y el software instalado con bases de datos de vulnerabilidades conocidas. Estas herramientas permiten detectar, entre otros aspectos, versiones desactualizadas, servicios innecesarios, configuraciones débiles o parámetros inseguros.

En entornos puramente TI, el escaneo puede llevarse a cabo de forma relativamente intensiva. Sin embargo, en entornos OT debe actuarse con **especial cautela**, ya que algunos tipos de escaneo podrían afectar a dispositivos sensibles o a comunicaciones de control en tiempo real. Por este motivo, resulta habitual complementar o sustituir al escaneo activo por soluciones de monitorización pasiva específicas para ICS.

c) Análisis y priorización de resultados

Los aportes obtenidos en la fase de escaneo deben ser **analizados y priorizados**, teniendo en cuenta tanto la criticidad técnica de la vulnerabilidad como el contexto operacional en el que se encuentra. Aunque la puntuación CVSS proporciona una referencia útil, en entornos industriales es necesario considerar factores adicionales, como el impacto sobre la seguridad de las personas, disponibilidad de la instalación o potencial efecto en la calidad del producto.

En esta etapa, resulta especialmente útil disponer de información sobre si una vulnerabilidad está siendo **explotada activamente** (por ejemplo, a través del catálogo KEV de CISA mencionado [7]) o si forma parte de incidentes reales en el ámbito industrial, lo que refuerza la necesidad de priorizar su tratamiento.

d) Mitigación, remediación y verificación

Una vez priorizadas las vulnerabilidades, se definen e implementan **acciones de mitigación o remediación**. Idealmente, ello implica la aplicación de parches de seguridad o la actualización de firmware y configuraciones. No obstante, en entornos OT con restricciones operativas o tecnológicas, no siempre es posible aplicar parches de forma inmediata.

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

En estos casos, se recurre a **controles compensatorios**, tales como la segmentación de redes, la aplicación de reglas específicas en cortafuegos industriales, el refuerzo de mecanismos de autenticación o la limitación de accesos remotos. Tras la implementación de estas medidas, se realiza una **verificación** —mediante nuevos escaneos o revisiones— para confirmar que la vulnerabilidad fue corregida o que su riesgo se ha reducido a un nivel aceptable.

e) Documentación y mejora continua

El proceso concluye con **la documentación de los resultados**, decisiones adoptadas y las medidas implementadas. Esta documentación no sólo permite dejar constancia del trabajo realizado, sino que facilita la mejora de políticas y procedimientos, contribuyendo a consolidar un enfoque de **mejora continua** en la gestión de vulnerabilidades.

3.2.2 Gestión de las vulnerabilidades

La gestión de vulnerabilidades constituye un proceso esencial dentro de cualquier programa de ciberseguridad y, como se decía, es un reto por la gran cantidad de defectos que aparecen en una entorno. El nivel de riesgo no depende únicamente de la presencia de la vulnerabilidad, sino del **tiempo que permanece sin mitigar**, del **momento del ciclo de vida en** el que se encuentra y de la **capacidad real de explotación** por parte de un adversario. En entornos industriales y de operación (OT), donde la disponibilidad y la seguridad física son aspectos críticos, la falta de mitigación puede traducirse no sólo en incidentes digitales, sino en disrupciones de proceso, daños sobre equipo o consecuencias para la seguridad física de las personas (safety en inglés).

En este marco conceptual resulta imprescindible comprender dos parámetros fundamentales: el tiempo **de explotación** y **el tiempo de remediación**.

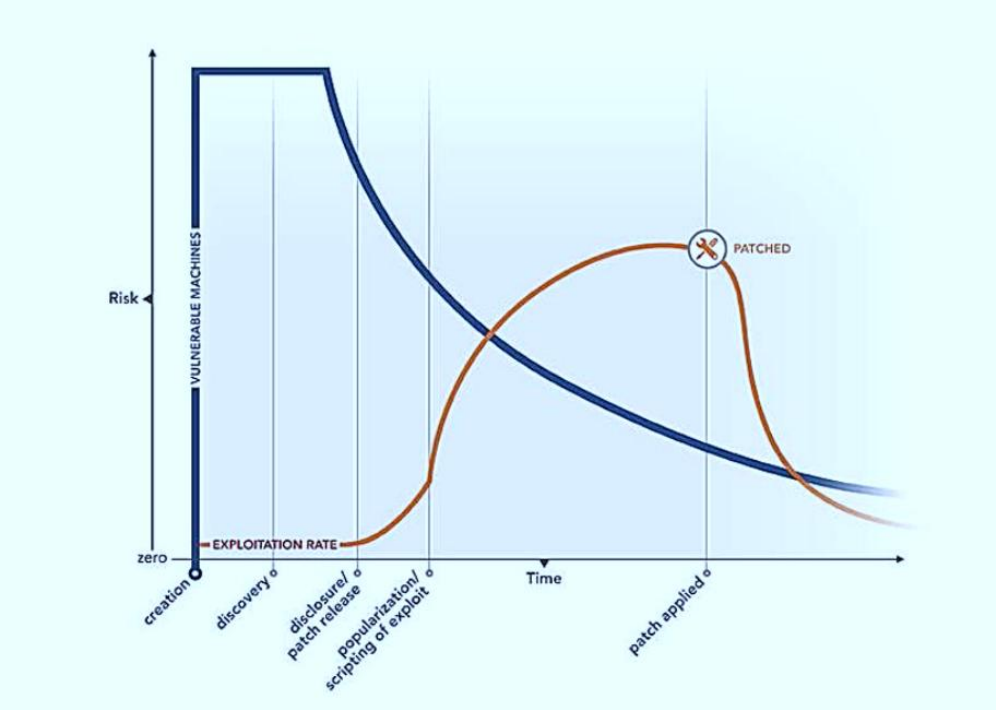
El **tiempo de explotación** (time-to-exploit en inglés) describe la rapidez con la que un adversario consigue explotar una vulnerabilidad desde su divulgación inicial. Las investigaciones del informe **ENISA State of Cybersecurity Vulnerabilities 2018–2019** [29] (el único especializado en este campo localizado), revelan que este intervalo se ha reducido de forma significativa en los últimos años, llegando a observarse casos en los que la explotación se produce en **cuestión de horas o días**.

Los ataques dirigidos mediante APT (Advanced Persistent Threat, técnicas avanzadas), patrocinados en muchos casos por estados nación por motivos geopolíticos o estratégicos, caerían dentro de la categoría de los no parcheables, pues ni siquiera

habrían sido divulgadas las vulnerabilidades (concepto conocido como vulnerabilidades de día cero, o zero-day).

Por su parte, el tiempo **de remediación** (time-to-remediate en inglés) mide cuánto tarda una organización en aplicar la medida correctiva recomendada. En entornos OT, este tiempo acostumbra ser considerablemente mayor que en el ámbito TI debido a la necesidad de planificar ventanas de mantenimiento, convalidar los parches en sistemas críticos o cumplir con restricciones de certificación de equipos industriales.

Cuando el tiempo de explotación es menor que el tiempo de remediación, la vulnerabilidad transita por una fase especialmente delicada en la que el riesgo se amplifica. Ese riesgo asociado a una vulnerabilidad puede entenderse como el resultado de la interacción entre **probabilidad de explotación** e **impacto potencial**. Y el riesgo no es constante, sino que evoluciona con el tiempo, como se puede ver en la siguiente figura.

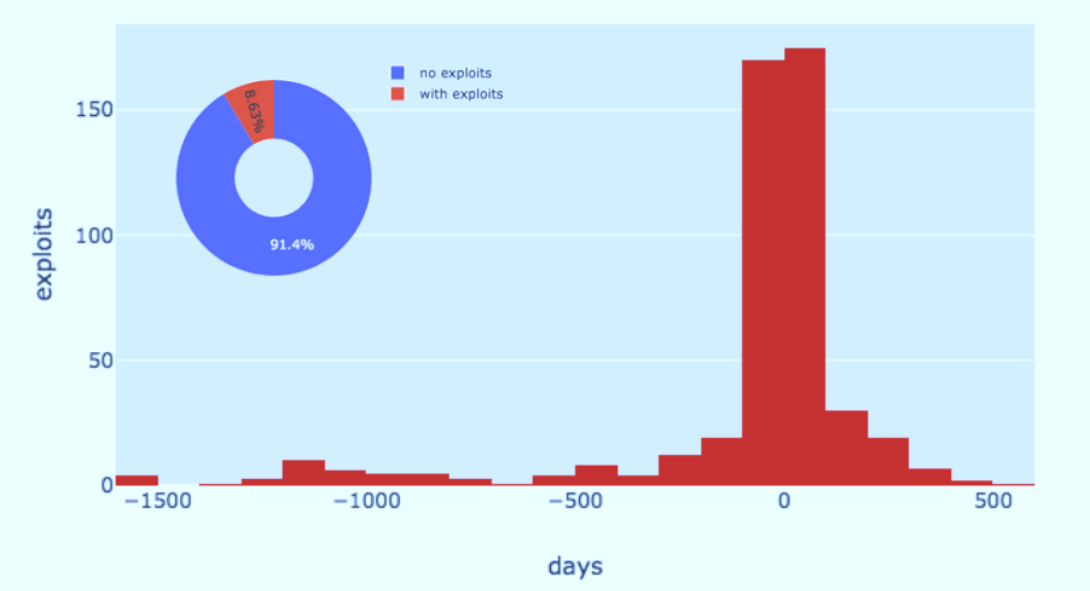


Riesgo de una vulnerabilidad frente al tiempo. Fuente: Alert Logic (2014)

A medida que avanza el ciclo de vida de la vulnerabilidad —desde su descubrimiento hasta su explotación activa en campañas reales— las condiciones cambian tanto para atacantes como para defensores. Por el lado ofensivo, la disponibilidad de información técnica, pruebas de concepto o exploits automatizados reduce el esfuerzo necesario para comprometer un sistema. Por el lado defensivo, cada día que pasa sin aplicar un parche, una actualización de firmware o una mitigación alternativa amplifica el riesgo de la

exposición, especialmente cuando la vulnerabilidad es ampliamente conocida o figura en catálogos como el KEV de CISA [7].

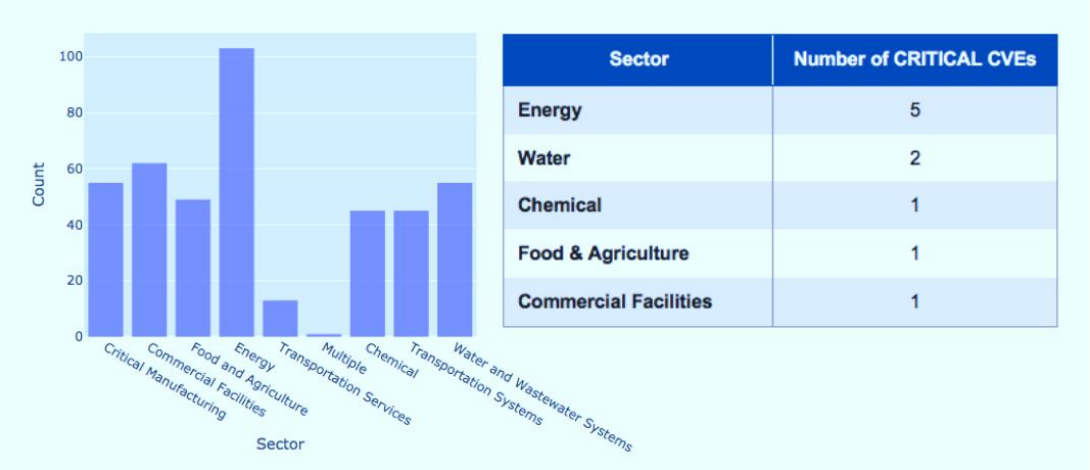
Los estudios especializados que analizan la evolución del riesgo refuerzan esta idea. El informe de ENISA State of Cybersecurity Vulnerabilities 2018–2019 [29] muestra como el tiempo desempeña un papel determinante en la probabilidad de explotación: **al menos el 8,65 % de todas las vulnerabilidades analizadas eran explotables en el momento del estudio**, y las vulnerabilidades **CRÍTICAS presentaban un tiempo medio de aparición del exploit de solo 24,83 días** respecto de su fecha de publicación, significativamente menor que en vulnerabilidades de otras categorías.



Tiempo de aparición del exploit desde la publicación de la vulnerabilidad (t=0). Fuente: ENISA (2019)

Como se ve, las vulnerabilidades en algunos casos comienzan a explotarse incluso varios años antes de la publicación de las mismas.

A continuación, se muestran los datos del informe de ENISA en cuanto a vulnerabilidades detectadas por sector de actividad:



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

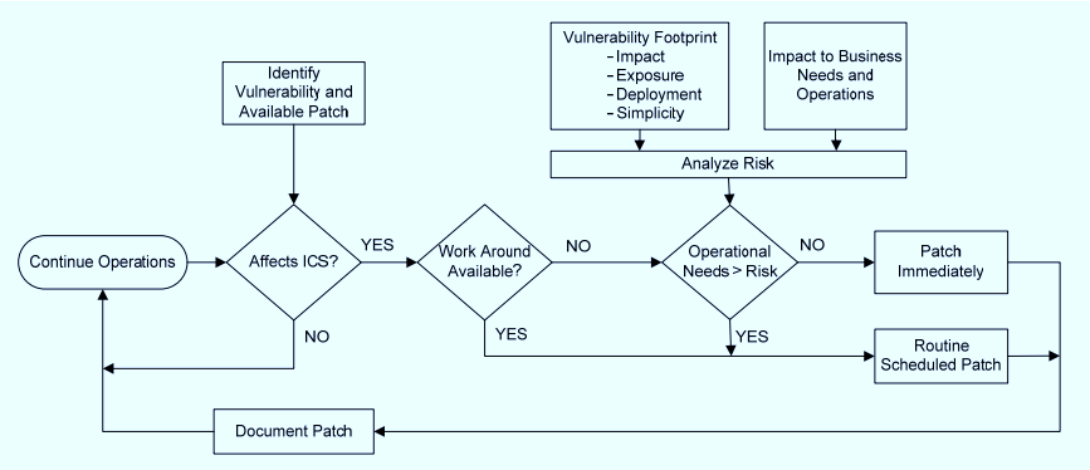
Vulnerabilidades por sector. Fuente: ENISA (2019)

La investigación revela además que, en numerosas ocasiones, los atacantes desarrollan comprobaciones automatizadas para detectar activos vulnerables poco después de la divulgación de una vulnerabilidad, acelerando el proceso de explotación.

Muchas vulnerabilidades alcanzan su punto crítico semanas o meses después de hacerse públicas, cuando los exploits maduraron y se incorporan a herramientas automatizadas y kits de ataque. Este comportamiento explica por qué vulnerabilidades antiguas continúan siendo explotadas durante años cuando no se aplican medidas correctivas.

Una dinámica semejante se deduce de las guías operativas de CISA para gestión de parches en entornos ICS [30], que describen la **ventana de remediación** como el período más crítico del ciclo de vida de la vulnerabilidad. Tras la publicación de un parche o mitigación oficial, los atacantes pueden analizar los cambios introducidos para comprender el fallo subyacente y generar exploits funcionales. CISA señala que los sistemas que no aplican parches se convierten en objetivos preferentes, y subraya que la **mayoría de los ataques exitosos se apoyan en vulnerabilidades conocidas para las que ya existía parche**. En este entorno, cada día de retraso incrementa la probabilidad de explotación, especialmente cuando la vulnerabilidad ha pasado a formar parte del catálogo KEV [7] o dispone de un exploit totalmente funcional.

Para facilitar la priorización por parte de los gestores de redes OT, CISA propone un árbol de decisión de urgencia de parcheo:



Árbol de decisión de urgencia de parcheo. Fuente: CISA (2008)

Por último, el análisis de Qualys sobre las vulnerabilidades más explotadas en 2023 [31] muestra que **varias de las diez vulnerabilidades más explotadas contaban con más de cinco años desde su divulgación**, y aun así continuaban registrando actividad maliciosa significativa. Además, el estudio destaca, alineado con ENISA, que **las vulnerabilidades con exploits disponibles tardan una media de menos de 30 días en ser explotadas activamente**, consolidando la idea de que la disponibilidad de código público acelera la explotación a escala industrial.

Por lo tanto, la gestión eficaz de vulnerabilidades no se limita a identificar debilidades en los sistemas, sino que exige una comprensión profunda de cómo evoluciona el riesgo a lo largo del tiempo y de cómo estos factores se combinan para crear oportunidades de ataque. En entornos OT, donde la seguridad está estrechamente vinculada a la disponibilidad y a la integridad del proceso productivo, adoptar esta visión resulta esencial para reducir la exposición efectiva frente a adversarios cada vez más rápidos en aprovechar vulnerabilidades conocidas.

3.3 ROI (Retorno de la Inversión)

Para comprender plenamente el impacto económico de la gestión de vulnerabilidades, resulta útil complementar la explicación conceptual con un **método estructurado de cálculo del ROI** (Return of Investment en inglés), ampliamente utilizado en análisis de riesgos y basado en un enfoque cuantitativo [32][33][34][35]. Esto permite no sólo estimar las pérdidas esperadas, sino también cuantificar los beneficios económicos derivados de aplicar medidas correctivas o mitigadoras.

A continuación se presenta el procedimiento teórico, seguido de un ejemplo práctico aplicado a una entorno industrial.

1. Identificación de activos y su valor económico (Asset Value, AV)

El primer paso consiste **en determinar qué activos están en riesgo y cuál es su valor**. En un entorno industrial, un activo puede ser un PLC, un sistema SCADA, una línea de producción, un robot o incluso un servidor de ingeniería. El valor del activo (AV) incluye no sólo su coste de sustitución, sino también los costes de indisponibilidad, pérdida de producción y efectos colaterales derivados de su fallo.

2. Identificación de amenazas relevantes (pares activo–amenaza)

A cada activo se le asignan amenazas plausibles: explotación remota de una vulnerabilidad del PLC, manipulación de parámetros en una HMI, caída del servidor SCADA por ransomware, etc. Cada par activo–amenaza permite cuantificar el riesgo de manera aislada.

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

El EF expresa **el porcentaje de pérdida que sufriría el activo si la amenaza se materializa**. Por ejemplo, una parada de línea causada por el compromiso de un PLC podría representar un EF del 25%, mientras que la corrupción total de un sistema SCADA podría alcanzar un EF del 80%.

4. Cálculo de la pérdida por evento (Single Loss Expectancy, SLE)

Se obtiene mediante la fórmula siguiente, **y expresa la pérdida asociada a un evento individual**:

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

Si el activo tiene un valor de 200.000 € y el EF es del 40%, entonces:

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

5. Probabilidad anual de materialización (Annual Prote of Occurrence, ARO)

El ARO **expresa cuantas veces al año se espera que se materialice la amenaza.** Puede estimarse mediante estadísticas históricas, información del sector, análisis experto o inteligencia de amenazas. Un ARO de 0,5 indica que el incidente podría producirse aproximadamente una vez cada dos años.

6. Cálculo de la pérdida anual esperada (Annual Loss Expectancy, ALE)

Se calcula como:

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

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

Siguiendo el ejemplo anterior:

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

7. Evaluación de contramedidas y de su impacto

Se analizan controles técnicos u organizativos: segmentación de red, actualización de firmware, despliegue de cortafuegos industriales, hardening del PLC, monitorización OT, etc. Cada contramedida puede reducir el EF (menor impacto), el ARO (menor probabilidad) o ambos.

Supongamos que la aplicación de parches y la segmentación reducen:

- el EF del 40% al **10%,**
- el ARO de 0,5 a **0,1.**

Los nuevos valores serían:

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

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

8. Cálculo del ROI de las contramedidas

Si el coste de aplicar las medidas es de 15.000 €, el ROI sería:

$$\mathbf{ROI = (ALE_1 - ALE_2 - coste\ de\ las\ medidas)}$$

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

Un ROI positivo indicaría que la inversión compensa económicamente, además de reducir de forma significativa el riesgo operacional.

3.3.1 Ejemplo práctico aplicado a un entorno OT

Para ilustrar el valor del ROI en entornos industriales, consideremos ahora un activo de alto valor económico: un **sistema SCADA central** que supervisa varios procesos críticos dentro de una instalación industrial. Su valor operativo (AV), considerando pérdidas de producción, penalizaciones contractuales, riesgos de calidad y potencial impacto físico, se estima en **5.000.000 €**.

El fabricante publica una vulnerabilidad crítica que permite ejecución remota de código. Basándonos en estudios de ENISA y CISA, sabemos que vulnerabilidades críticas pueden disponer de un exploit funcional en **menos de 25 días**, y que las vulnerabilidades conocidas sin parche aplicado figuran entre los vectores más explotados a escala global.

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

Si estimamos un EF del **40%** (impacto severo sobre la operación) y un ARO de **0,35**, la pérdida anual esperada antes de mitigación sería:

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

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

Aplicar segmentación avanzada, parcheo de vulnerabilidades del SCADA, endurecimiento de accesos remotos y monitorización OT reduce el EF al **10%** y el ARO a **0,1**:

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

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

Si el coste conjunto de estas medidas asciende a **150.000 €**, entonces:

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

Este resultado demuestra que, para activos industriales de alto valor, la mitigación de vulnerabilidades ofrece un retorno económico muy elevado y constituye un elemento clave para garantizar la continuidad operativa y reducir el riesgo global.

4 Alertas

4.1 Panorama de ataques

El panorama de amenazas contra sistemas de control industrial (ICS) y tecnologías de operación (OT) muestra, en los últimos años, un **crecimiento sostenido en el volumen de ataques, en su sofisticación técnica y en la amplitud de sectores afectados**. La información disponible procede en gran medida de informes de inteligencia de fabricantes especializados, encuestas sectoriales y repositorios de incidentes, por lo que debe interpretarse siempre teniendo en cuenta una limitación clave: **los datos disponibles representan sólo una fracción de los incidentes reales**, ya que muchas organizaciones optan por no hacerlos públicos por motivos de confidencialidad, impacto reputacional o ausencia de obligaciones reglamentarias de notificación.

En este apartado se sintetizan algunas de las fuentes más relevantes —SANS Institute, Dragos, Nozomi, Kaspersky ICSCERT o ICSStrive— con el objetivo de ofrecer una visión integrada de:

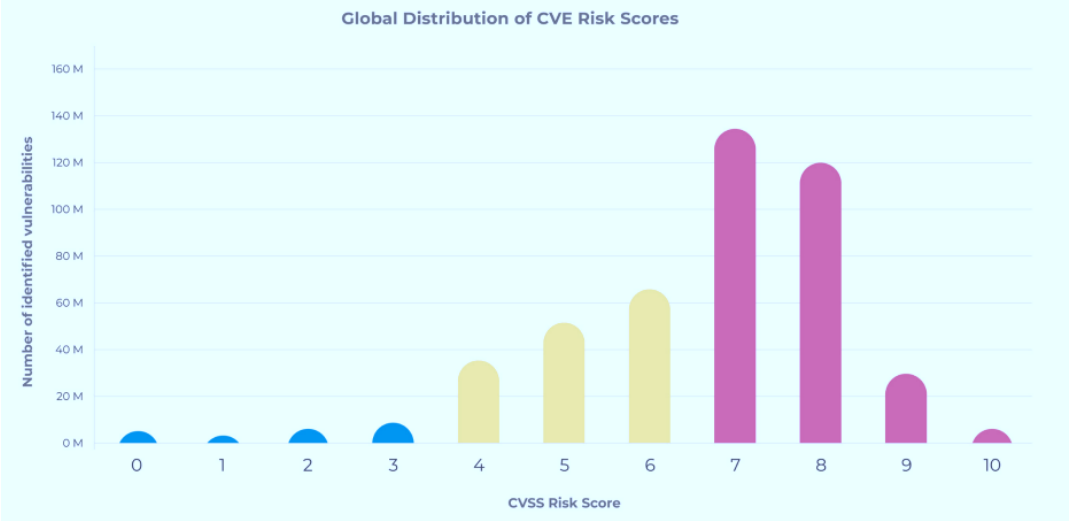
- **Tendencias generales de amenazas y ataques.**
- **Evolución cuantitativa** (volumen de incidentes y sistemas afectados).
- **Técnicas predominantes** empleadas por los atacantes.
- **Sectores y regiones más impactados**, con referencias específicas a Europa y, cuando es posible, a datos que afectan indirectamente al contexto español.

Algunos de estos aspectos se tratarán con más profundidad en futuros entregables del Observatorio de Ciberseguridad Industrial, como el Informe de Inteligencia de Amenazas.

4.1.1 Tendencias generales

Los informes de Nozomi Networks Labs **Trends e Insights 2025** [36] revelan un crecimiento continuo en la cantidad y gravedad de las vulnerabilidades ICS. Su último análisis **contempla 241 nuevos avisos de CISA** aplicables a entornos industriales y **619 vulnerabilidades ICS divulgadas**, afectando a unos **70 fabricantes distintos**. De particular relevancia es que **la mayoría presenta puntuaciones CVSS ≥ 7**, lo que confirma un riesgo elevado de explotación.

Asimismo, Nozomi identifica cuatro **vulnerabilidades catalogadas como KEV** (Known Exploited Vulnerabilities) por CISA, y **unas veinte con un EPSS superior al 1 %**, lo que implicaba una probabilidad realista de explotación a corto plazo (EPSS o Exploit Prediction Scoring System es un sistema de ciberseguridad que usa aprendizaje automático para predecir qué vulnerabilidades o CVEs, tienen mayor probabilidad de ser explotadas en los próximos 30 días). La distribución sectorial muestra mayor concentración en **Manufactura Crítica y Energía**, seguida de Comunicaciones, sectores todos ellos con fuerte presencia en Galicia.



Distribución de CVE por severidad. Fuente: Nozomi Networks (2025)

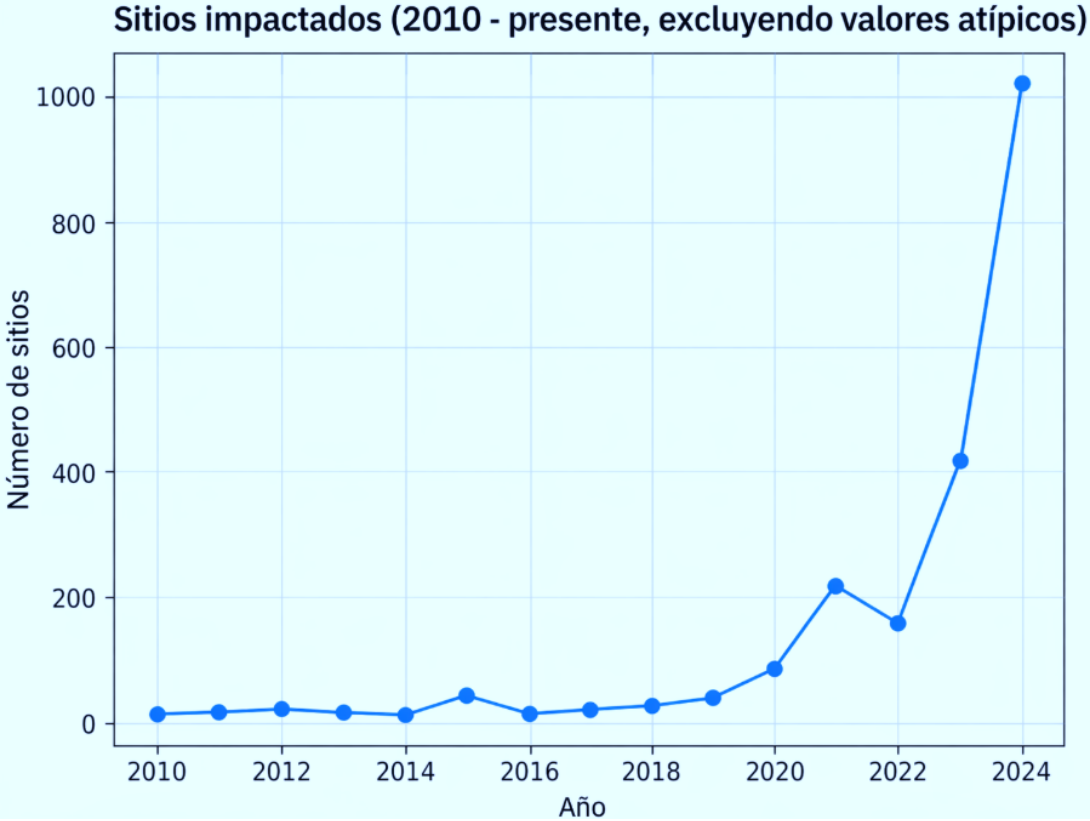
Distribution of CVEs by Exploitability and Severity

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%

Explotabilidad de las vulnerabilidades frente a la severidad. Fuente: Nozomi Networks (2025)

Por su parte, el informe **2025 OT Cyber Threat Report** de **ICSStrive** [37] refleja una intensificación sustancial de los ataques que generan **impacto físico en procesos industriales** (indisponibilidad de producción). El análisis longitudinal de su base de datos muestra un **incremento acumulado del 146 % en los ataques con repercusión física directa** en sedes operativas desde el año anterior. Este patrón indica una escalada progresiva en la agresividad y consecuencias de las intrusiones en OT, observándose

casos en los que una brecha inicial permite comprometer múltiples plantas o centros de producción.



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

Es destacable que la base de datos de ICSStrive, activa desde 2017, contiene **cientos de incidentes documentados**, incluidos ataques que derivaron en paradas de planta, daños a equipos, alteraciones en la calidad del producto o interrupciones graves de procesos críticos. Se puede consultar el detalle agregado en el propio informe enlazado.

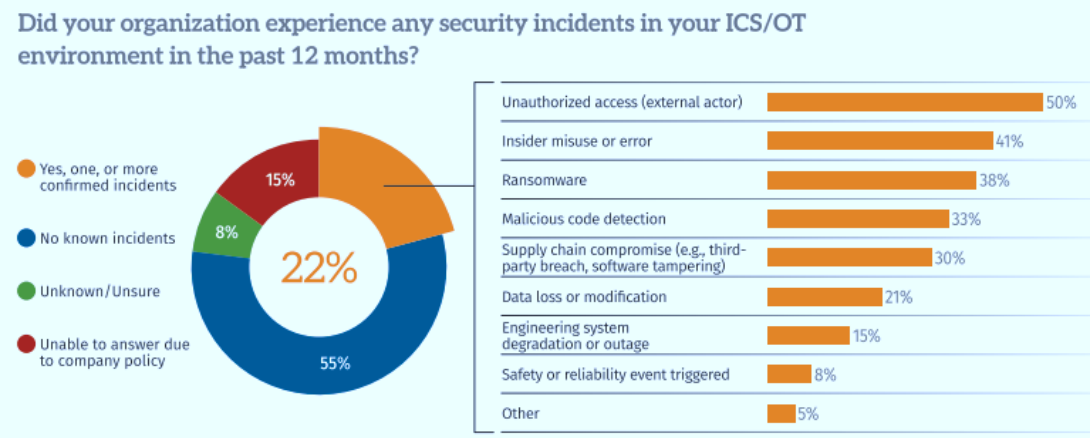
4.1.2 Detalles

4.1.2.1 Ransomware, accesos remotos y velocidad de ejecución

Los datos agregados de **SANS State of ICS/OT Security 2025** [38] confirman que los entornos ICS/OT siguen enfrentándose a amenazas de alto impacto. Según su encuesta internacional, el **22 % de las organizaciones experimentó al menos un incidente ICS/OT en los últimos 12 meses**. Los principales vectores fueron:

- **Acceso externo no autorizado (50 %)**
- **Ransomware (38 %)**

Además, cerca del **40 % de los incidentes han provocado interrupciones operativas** y alrededor del 20 % implicaron pérdidas financieras, exposición de datos o riesgos para la seguridad física.



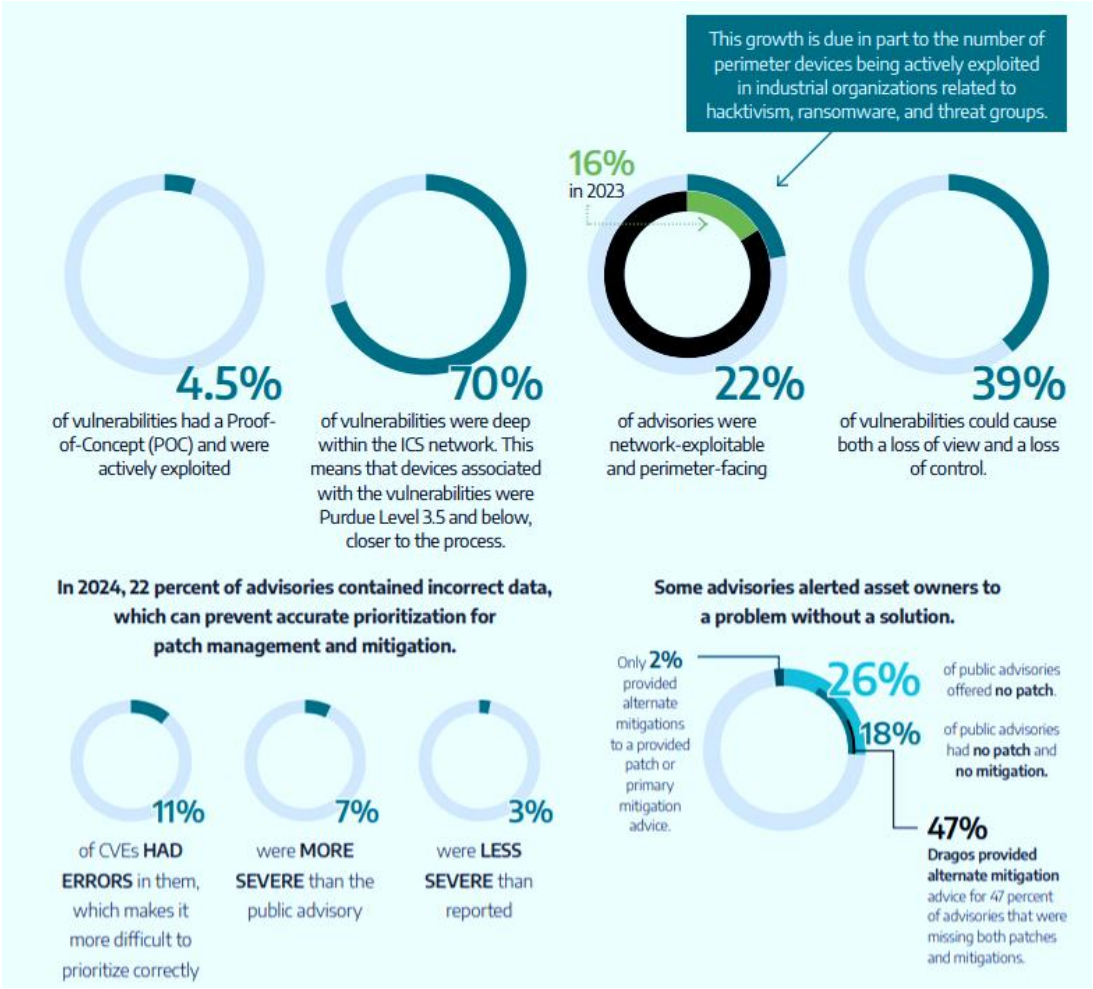
Encuesta de incidentes en entornos ICS/OT. Fuente: SANS (2025)

El informe de ICSStrive complementa estos datos con la observación de que, en incidentes de ransomware contra organizaciones industriales, el **tiempo medio entre la intrusión y la activación del cifrado es de unas 16 horas**, siendo en muchos casos considerablemente más rápido. Esta ventana de acción tan reducida incrementa la necesidad de capacidades de **detección temprana, vigilancia 24x7 y respuesta automatizada en OT**.

4.1.2.2 Vulnerabilidades analizadas

El informe **Dragos – Year in Review 2025** [39] señala que, en la comunicación pública de las vulnerabilidades, el CVSS por sí solo no refleja bien el riesgo real en entornos OT. Además, en 2024 un 22 % de los advisories incluían datos incorrectos y un 26 % no ofrecían parche, por lo que la priorización debe complementarse con contexto operativo y 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. Fuente: Dragos (2025)

4.1.2.3 Sectores y regiones más afectados

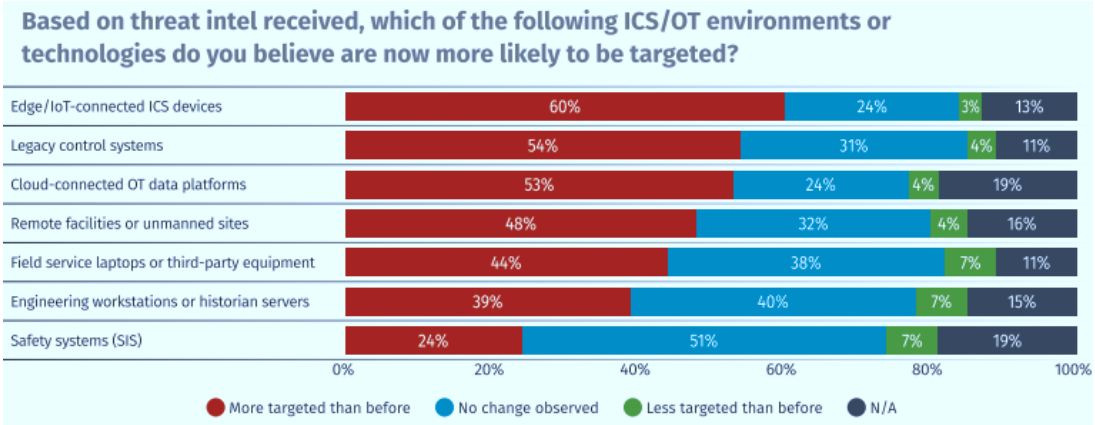
Los sectores más impactados de forma consistente en las distintas fuentes incluyen **energía, manufactura, agua, alimentación y logística**, todos ellos con fuerte peso en Galicia.

Según **Kaspersky ICS CERT** [40][41][42], aproximadamente **uno de cada cinco equipos ICS bloqueó objetos maliciosos** durante el segundo trimestre de 2025. La proporción global se situó en torno al **21,32%** con incrementos notorios en regiones como **Australia/Nueva Zelanda y Europa del Norte**.

En lo referente a **vectores de ataque**, destaca un aumento continuado de las amenazas procedentes del **correo electrónico**, con **picos próximos al 7% de equipos ICS afectados en Europa del Sur**, región que incluye España. Este dato pone de manifiesto la relevancia de reforzar políticas de filtrado y segmentación para evitar que accesos IT deriven en compromisos OT.

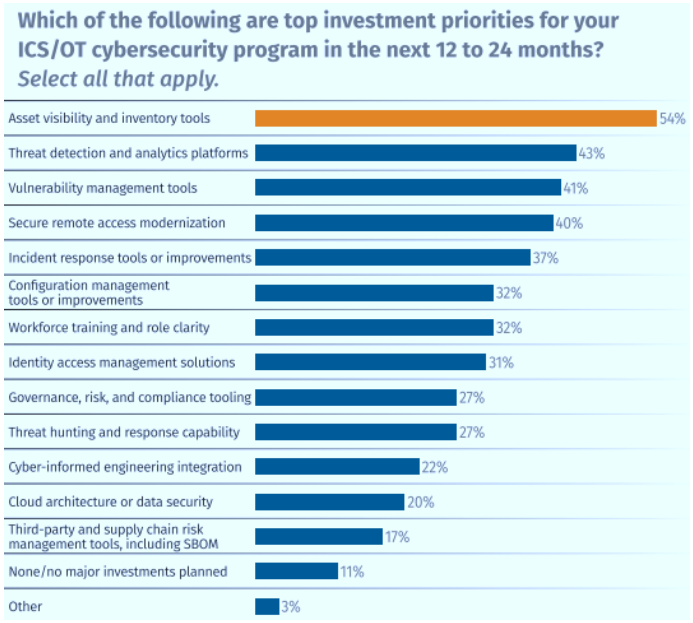
El informe regional **Kaspersky – Threat landscape foron automation systems (Europe, Q2 2025)** sitúa **Europa del Sur y del Este** entre las áreas europeas con **mayor riesgo de ataques dirigidos**, debido a la combinación de campañas de phishing, spyware y otros tipos de malware orientados a entornos industriales.

En cuanto a la percepción del riesgo y prioridades de inversión, **SANS** señala en [38] que más del **50 % de las organizaciones** considera que los sistemas **legacy, en el Edge/IoT y conectados a la nube** se volvieron los más atractivos para los atacantes:



Probabilidad de sufrir un ataque por tipo de activo según los encuestados. Fuente: SANS (2025)

Al mismo tiempo, las prioridades de inversión para los próximos 12–24 meses se centran en **visibilidad de activos, detección de amenazas y gestión de vulnerabilidades**, reflejando una maduración progresiva en la estrategia defensiva industrial.



Prioridad de inversión en ciberseguridad OT según los encuestados. Fuente: 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 Limitaciones de los datos y relevancia para Galicia

A pesar del valor que aportan los informes analizados, es necesario interpretar sus conclusiones con cautela.

El **subregistro de incidentes** sigue siendo un factor determinante, ya que muchas organizaciones optan por no hacer públicos los ataques que sufren, bien por miedo al impacto reputacional, bien por la ausencia de obligaciones reglamentarias que les exijan notificar esos incidentes. A ello se suma un **sesgo regional significativo**: las regiones con marcos normativos más estrictos o con mayor cultura de reporte tienden a mostrar cifras más completas, mientras que otras áreas permanecen infrarrepresentadas. También es de considerar **la dependencia de telemetría** propia de fabricantes como Nozomi o Kaspersky, cuyos análisis se basan en datos procedentes de organizaciones que emplean sus soluciones, lo que deja fuera sectores o geografías que no disponen de estas tecnologías.

Estas limitaciones no restan relevancia a las tendencias observadas, especialmente en el caso de Galicia. La comunidad cuenta con una **elevada concentración de sectores intensivos en OT**, como energía, agua, automoción, naval, alimentación o logística, todos ellos ampliamente mencionados como objetivos recurrentes en los informes internacionales. Además, España forma parte de **Europa del Sur**, una región que Kaspersky identifica de manera sistemática como una de las más expuestas a amenazas dirigidas contra sistemas industriales. La combinación de **ransomware, accesos remotos inseguros, vulnerabilidades ICS de alta severidad y la creciente superficie IoT** encaja de manera precisa con la estructura tecnológica de buena parte del tejido industrial gallego.

En su conjunto, este panorama constituye un insumo para **priorizar medidas de protección**, que se expondrán en una sección posterior.

4.2 Últimas alertas

Con el objetivo de proporcionar una visión clara y accionable del estado de las vulnerabilidades que afectan a los entornos industriales, este informe incorpora una sección dedicada a las **alertas publicadas durante el último trimestre** por fuentes profesionales. Dado que el boletín está concebido con periodicidad **trimestral**, este enfoque permite ofrecer un resumen manejable, actualizado y directamente aplicable para los equipos técnicos y responsables de seguridad.

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

Antes de presentar las alertas más relevantes, resulta fundamental explicar brevemente **dónde puede el lector consultar, monitorizar o suscribirse a estas notificaciones**, tanto para entornos **ICS/OT** como para infraestructuras **TI** que, debido a la creciente convergencia tecnológica, pueden tener un impacto indirecto o directo sobre la operación industrial.

4.2.1 Fuentes principales de avisos

Además de los avisos específicos de cada fabricante —que se incluirán de manera estructurada en un anexo posterior al final del informe— las siguientes plataformas constituyen los repositorios más fiables y actualizados para el seguimiento de vulnerabilidades significativas:

- **INCIBE-CERT – Avisos de Seguridad en Sistemas de Control Industrial** [43]: Fuente nacional de referencia para España en materia de ciberseguridad industrial. Publica vulnerabilidades relevantes de fabricantes ICS y proporciona información técnica, CVSS, impacto y medidas de mitigación.
- **CCN-CERT – Alertas y vulnerabilidades** [44][45]: Aunque orientado principalmente administraciones públicas, su utilidad es transversal. Incluye boletines de severidad alta que pueden afectar a sistemas IT con impacto potencial en entornos OT interconectados.
- **CISA – ICS Advisories (ICSA)** [46]: Es la base de datos más reconocida a nivel internacional para avisos de sistemas de control industrial. Incluye información detallada, CVSS, productos afectados, descripción técnica, escenarios de explotación y mitigaciones.

Estas fuentes constituyen la base mínima para un programa de vigilancia de vulnerabilidades en organizaciones industriales, complementadas con los **avisos de los fabricantes cuyos equipos estén desplegados en planta (ver anexo con algunos de ellos)**.

4.2.2 Consideraciones clave para la interpretación de alertas

Al revisar vulnerabilidades ICS es importante recordar que:

- Las **puntuaciones CVSS no siempre reflejan el riesgo real en OT**, donde la disponibilidad y la seguridad 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

- Las alertas de TI (por ejemplo, servicios Windows o Middleware corporativo) **pueden impactar OT** si se utilizan estaciones de ingeniería, servidores SCADA o sistemas de mantenimiento remoto.
- Muchas vulnerabilidades de fabricantes ICS **no pueden parchearse inmediatamente** debido a restricciones operativas, por lo que las mitigaciones compensatorias adquieren un papel central.
- La mayoría de advisories carecen de telemetría sobre explotación activa; por ello, fuentes como **CISA KEV** [7] o reportes de inteligencia industrial ayudan a priorizar.

Esta sección servirá en cada informe como referencia práctica para equipos de seguridad, mantenimiento y operación, ayudando a tomar decisiones informadas sobre que vulnerabilidades aparecen nuevas y son destacables por su alto riesgo.

4.2.3 Alertas ICS de alta criticidade do trimestre

De entre los avisos publicados en el período analizado, se distinguen a continuación las **vulnerabilidades de severidad alta o crítica** que afectan directamente a **entornos ICS**, siguiendo un formato sintético y orientado a la acción. Cada ficha resume los elementos clave para facilitar un filtrado rápido, pero sin excesivo detalle. Para ello se convierte a consultar la fuente original de INCIBE-CERT (que aglutina en formato estructurado los avisos de origen internacional).

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS DE SUNBIRD
URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-sunbird
Productos afectados: Sunbird DCIM (varias versiones).
Vector de ataque: Acceso remoto no autenticado / manipulación de parámetros / escalada.
Severidad: Alta–Crítica (según módulo afectado).
Impacto potencial en OT: Acceso no autorizado a sistemas de gestión de infraestructuras críticas; posibilidad de manipular datos de monitorización, alterar configuraciones o provocar pérdida de visibilidad.
Probabilidad de explotación: Moderada; funciones expuestas a través de la interfaz web y de la API.
Mitigaciones inmediatas: Parchear según la versión; restringir accesos web;

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

segmentar la red de gestión; exigir autenticación robusta.
Prioridad: Muy alta.

MECANISMO DE RECUPERACIÓN DE CONTRASEÑAS DÉBIL EN MAXHUB PIVOT
URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/mecanismo-de-recuperacion-de-contrasenas-debiles-en-maxhub-pivot
Productos afectados: MAXHUB Pivot – plataforma colaborativa.
Vector de ataque: Explotación de un mecanismo débil de recuperación de contraseñas.
Severidad: Alta.
Impacto potencial en OT: Compromiso de cuentas administrativas utilizadas en salas de control o entornos híbridas OT/IT; riesgo de movimiento lateral.
Probabilidad de explotación: Elevada si el servicio está expuesto a Internet.
Mitigaciones inmediatas: Actualizar el firmware; deshabilitar funciones expuestas; aplicar MFA en los accesos administrativos.
Prioridad: Alta.

INYECCIÓN SQL EN IVIEW DE ADVANTECH
URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/inyeccion-sql-en-iview-de-advantech-0
Productos afectados: Advantech iView – plataforma de monitorización industrial.
Vector de ataque: Inyección SQL a través de peticiones HTTP no saneadas.
Severidad: Crítica.
Impacto potencial en OT: Compromiso total del servidor de monitorización; posibilidad de alterar datos, credenciales o parámetros de red; riesgo de interrupción operacional.
Probabilidad de explotación: Alta; vectores sencillos y documentados.
Mitigaciones inmediatas: Parchear; segmentar; bloquear acceso externo; activar WAF; revisar credenciales.
Prioridad: Muy 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 en la API web.
Severidad: Alta–crítica.
Impacto potencial en OT: Acceso directo a datos de producción energética; posibilidad de manipular parámetros de monitorización o de gestión remota.
Probabilidad de explotación: Alta si el sistema está expuesto.
Mitigaciones inmediatas: Limitar accesos; implementar autenticación obligatoria; segmentación estricta; actualizar a la versión corregida.
Prioridad: Muy alta.

CONVALIDACIÓN INADECUADA EN ISTAR DE JOHNSON CONTROLES

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/validacion-inadecuada-en-istar-de-johnson-controls

Productos afectados: Johnson Controls iSTAR – sistemas de control de accesos.
Vector de ataque: Validación insuficiente de parámetros.
Severidad: Alta.
Impacto potencial en OT: Riesgo de manipulación del control de accesos físicos; impacto directo en la seguridad de instalaciones industriales.
Probabilidad de explotación: Moderada.
Mitigaciones inmediatas: Parcheo; endurecimiento de red; aplicar monitorización de integridad.
Prioridad: 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

Productos afectados: Mirion EC² NMIS / Biodose – sistemas de medición y monitorización radiológica.
Vector de ataque: Varias vulnerabilidades (incluye acceso no autenticado, exposición de datos y escalada).
Severidad: Alta–crítica.
Impacto potencial en OT: Riesgo para sistemas de seguridad radiológica; pérdida de integridad en las mediciones; posible alteración de alarmas.
Probabilidad de explotación: Moderada–alta según el vector.

Mitigaciones inmediatas: Parchear; limitar acceso a la red interna; segmentar sistemas de seguridad.
Prioridad: Muy alta.

FALTA DE AUTENTICACIÓN EN PRODUCTOS DE ISKRA

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/falta-de-autenticacion-en-productos-de-iskra
Productos afectados: Equipos Iskra (medición/gestión energética).
Vector de ataque: Acceso no autenticado a interfaces de gestión.
Severidad: Crítica.
Impacto potencial en OT: Riesgo directo para redes de energía; alteración de mediciones o parámetros de control; interrupciones del servicio.
Probabilidad de explotación: Alta.
Mitigaciones inmediatas: Aplicar autenticación fuerte; segmentar; revisar accesos remotos; parchear si procede.
Prioridad: Muy alta.

CONTROL INADECUADO DE GENERACIÓN DE CÓDIGO EN LONGWATCH (VÍDEO INDUSTRIAL Y CONTROL)

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/control-inadecuado-de-la-generacion-de-codigo-en-longwatch-de-industrial-video
Productos afectados: Longwatch Video System – sistemas de vídeo industrial.
Vector de ataque: Inyección de código / generación dinámica insegura.
Severidad: Alta.
Impacto potencial en OT: Manipulación de vídeo industrial; ceguera operativa; riesgo en operaciones remotas.
Probabilidad de explotación: Moderada.
Mitigaciones inmediatas: Parchear; restringir interfaces web; aplicar segmentación.
Prioridad: Alta.

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS CODESYS

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-codesys-1
Productos afectados: CODESYS V2/V3 y componentes asociados.

Vector de ataque: Ejecución remota de código, desbordamientos, elusión de la autenticación.
Severidad: Crítica.
Impacto potencial en OT: Compromiso directo de PLCs y lógica de control; riesgo máximo para la producción.
Probabilidad de explotación: Muy alta; CODESYS está ampliamente utilizado en múltiples fabricantes.
Mitigaciones inmediatas: Parchear; restringir puertos; segmentar; aplicar firewalls industriales.
Prioridad: 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
Productos afectados: Eaton Galileo – software HMI.
Vector de ataque: Manejo incorrecto de entradas; posible corrupción de datos o fallo inesperado.
Severidad: Alta
Impacto potencial en OT: Pérdida de integridad en las interfaces HMI; riesgo de errores en supervisión o control.
Probabilidad de explotación: Moderada.
Mitigaciones inmediatas: Actualizar; aislar redes HMI; convalidar entradas en capas superiores.
Prioridad: Alta.

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS DE MITSUBISHI

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-mitsubishi-0
Productos afectados: Diversos productos de Mitsubishi Electric para automatización industrial.
Vector de ataque: Múltiples vectores, incluyendo acceso no autenticado, desbordamientos y manipulación de parámetros.
Severidad: Alta–crítica.
Impacto potencial en OT: Riesgo directo sobre PLCs, interrupciones de procesos

industriales, modificación de la lógica de control y pérdida de visibilidad.
Probabilidad de explotación: Elevada en entornos expuestos o sin segmentación adecuada.
Mitigaciones inmediatas: Parchear según versiones; segmentación; control estricto de accesos remotos; monitorización de integridad.
Prioridad: Muy 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
Productos afectados: Sircom SMART Alert SISA.
Vector de ataque: Falta de autenticación en interfaz crítica.
Severidad: Crítica.
Impacto potencial en OT: Acceso no autorizado a sistemas de alarma; posible manipulación de eventos o inhibición de alertas.
Probabilidad de explotación: Alta en sistemas accesibles desde redes no confiables.
Mitigaciones inmediatas: Activar autenticación; segmentar alarmas críticas; revisar configuraciones de exposición.
Prioridad: 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
Productos afectados: Intercomunicadores industriales TCIV+ (Zenitel).
Vector de ataque: Ejecución remota de código, omisiones de autenticación, desbordamientos.
Severidad: Alta–Crítica.
Impacto potencial en OT: Riesgo para comunicaciones internas de planta; manipulación de audio/vídeo; pivote hacia otros sistemas.
Probabilidad de explotación: Moderada–Alta.
Mitigaciones inmediatas: Actualizar firmware; segmentar red AV/OT; restringir acceso web.
Prioridad: Muy 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

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

Vector de ataque: Gestión inadecuada de la memoria; acceso no autorizado; corrupción de datos.

Severidad: Alta.

Impacto potencial en OT: Riesgos sobre el diseño técnico, documentación de ingeniería y continuidad de la producción.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Aplicar actualizaciones; aislar estaciones de ingeniería; control de integridad.

Prioridad: Alta.

VALIDACIÓN INCORRECTA EN PRODUCTOS DE JANITZA ELECTRONICS GMBH

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

Productos afectados: Equipos de monitorización energética Janitza.

Vector de ataque: validación insuficiente de entradas.

Severidad: Alta.

Impacto potencial en OT: Alteración de mediciones energéticas; posibles efectos en cascada sobre el control de carga o la calidad de suministro.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Actualizar el firmware; segmentación de sistemas de monitorización; reglas de protección de red.

Prioridad: Alta.

CONVALIDACIÓN INCORRECTA DE ENTRADA EN PRODUCTOS DE FESTO

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

Productos afectados: Módulos y controladores Festo.

Vector de ataque: Convalidación deficiente que permite la manipulación de parámetros.

Severidad: Alta.

Impacto potencial en OT: Riesgo sobre actuadores neumáticos/eléctricos; afectación directa a líneas automatizadas.
Probabilidad de explotación: Moderada.
Mitigaciones inmediatas: Parchear; restringir acceso a la lógica; supervisión de parámetros.
Prioridad: 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
Productos afectados: ABB Edgenius – plataforma industrial edge.
Vector de ataque: Falta de autenticación en servicios expuestos.
Severidad: Crítica.
Impacto potencial en OT: Control no autorizado sobre nodos edge; alterar flujos de datos OT–IT; riesgo operativo significativo.
Probabilidad de explotación: Alta si los servicios están accesibles.
Mitigaciones inmediatas: Aplicar autenticación estricta; segmentar edge; actualizar el software.
Prioridad: Crítica.

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS DE ICAM365

URL: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-en-productos-de-icam365
Productos afectados: Cámaras industriales iCAM365.
Vector de ataque: Omisión de autenticación, exposición de credenciales, ejecución remota.
Severidad: Alta–crítica.
Impacto potencial en OT: Manipulación de la videovigilancia; puntos ciegos; pivote hacia otras redes.
Probabilidad de explotación: Alta.
Mitigaciones inmediatas: Parchear; bloquear accesos externos; segmentación de la red de vídeo.
Prioridad: Muy alta.

DESBORDAMIENTO DE BÚSQUEDA BASADO 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

Productos afectados: Controladores industriales Appleton de Emerson.

Vector de ataque: Desbordamiento de búsqueda.

Severidad: Alta–crítica.

Impacto potencial en OT: Ejecución remota de código; interrupciones de servicio; corrupción de procesos.

Probabilidad de explotación: Moderada–alta.

Mitigaciones inmediatas: Actualizar el firmware; segmentación estricta; limitar el acceso a servicios vulnerables.

Prioridad: Muy alta.

MÚLTIPLES VULNERABILIDADES EN 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, incluyendo ejecución remota y autenticación insuficiente.

Severidad: Alta–crítica.

Impacto potencial en OT: Compromiso del sistema de gestión de edificios (BMS); posibilidad de alteraciones ambientales o energéticas que afecten a procesos industriales.

Probabilidad de explotación: Elevada.

Mitigaciones inmediatas: Parchear; segmentar el BMS de las redes OT; reforzar la autenticación.

Prioridad: Muy alta.

INYECCIÓN DE COMANDOS EN PRODUCTOS DE OPTO-22

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

Productos afectados: Controladores y módulos Opto-22.

Vector de ataque: Inyección de comandos mediante entradas no validadas.

Severidad: Alta.

Impacto potencial en OT: Ejecución remota de comandos; alteración de procesos; riesgo de pérdida de control operacional.

Probabilidad de explotación: Moderada–alta.

Mitigaciones inmediatas: Parchear; segmentar; restringir acceso web/API; validar entradas.

Prioridad: Muy alta.

CONDICIÓN DE CARRERA EN EL KERNEL DE WINDOWS EN PRODUCTOS 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

Productos afectados: Equipos Philips dependientes de Windows (varios modelos).

Vector de ataque: Explotación de condición de carrera en el núcleo.

Severidad: Alta.

Impacto potencial en OT: Interrupción de sistemas médicos industriales; denegación de servicio; pérdida de disponibilidad.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Aplicar parches de Microsoft; restringir privilegios; segmentar.

Prioridad: Alta.

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS DE LA 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

Productos afectados: Sistemas Bosch MAP 5000.

Vector de ataque: Varias vulnerabilidades (incluye autenticación débil, ejecución remota, manipulación de datos).

Severidad: Alta–crítica.

Impacto potencial en OT: Compromiso de sistemas de detección y alarma; riesgo para la seguridad física.

Probabilidad de explotación: Moderada–alta.

Mitigaciones inmediatas: Actualizar el firmware; endurecer credenciales; segmentar sistemas de alarma.

Prioridad: Muy 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

Productos afectados: Plataformas MILCoS de Mitsubishi.

Vector de ataque: Ejecución remota de código por convalidación insuficiente.

Severidad: Crítica.

Impacto potencial en OT: Compromiso total del sistema; manipulación de la lógica o parámetros; interrupción de procesos.

Probabilidad de explotación: Alta.

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

Prioridad: 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

Productos afectados: Dispositivos EWIO-2.

Vector de ataque: Autenticación débil, exposición de credenciales, ejecución remota.

Severidad: Alta–Crítica.

Impacto potencial en OT: Manipulación de datos energéticos; pivote hacia redes internas; riesgo operativo relevante.

Probabilidad de explotación: Alta.

Mitigaciones inmediatas: Actualizar el firmware; aplicar contraseñas robustas; segmentación estricta.

Prioridad: Muy alta.

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS DE ZENITEL

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

Productos afectados: Sistemas Zenitel (varios modelos).

Vector de ataque: Ejecución de código, falta de autenticación, desbordamientos.

Severidad: Alta–crítica.

Impacto potencial en OT: Riesgo en las comunicaciones internas; posibilidad de interceptar, manipular o bloquear señales.

Probabilidad de explotación: Moderada–alta.

Mitigaciones inmediatas: Parchear; segmentar redes AV; restringir accesos.

Prioridad: Muy alta.

VULNERABILIDAD EN SAM LIGHT DE JUSTECH

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

Productos afectados: SAM Light – Justech.

Vector de ataque: Validación insuficiente; manipulación de parámetros.

Severidad: Alta.

Impacto potencial en OT: Riesgo de manipulación de sistemas de alumbrado industrial; impacto en la seguridad operativa.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Parchear; restringir accesos; segmentación.

Prioridad: 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

Productos afectados: IDEC XBT L1000.

Vector de ataque: Desbordamientos, exposición de información, elusión de la autenticación.

Severidad: Alta–Crítica.

Impacto potencial en OT: Manipulación de HMI; riesgo de pérdida de integridad operativa.

Probabilidad de explotación: Moderada–Alta.

Mitigaciones inmediatas: Actualizar; segmentar; reforzar la autenticación.

Prioridad: Muy alta.

VULNERABILIDAD EN LA TARJETA MIR420 DE JOHNSON CONTROLES

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

Productos afectados: Tarjeta MIR420.

Vector de ataque: Validación insuficiente; manipulación remota.

Severidad: Alta.

Impacto potencial en OT: Riesgo para el control de accesos o integración en sistemas de seguridad.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Parchear; restringir acceso; segmentación.

Prioridad: Alta.

VULNERABILIDAD EN GG4 DE TECNOCONTROL ILUMINACIÓN

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

Productos afectados: Controladores GG4.

Vector de ataque: Exposición de servicios sin autenticación.

Severidad: Alta.

Impacto potencial en OT: Manipulación de alumbrado crítica; impacto en la seguridad y en la visibilidad operativa.

Probabilidad de explotación: Moderada–alta.

Mitigaciones inmediatas: Actualizar; implementar autenticación; segmentar.

Prioridad: Muy alta.

VULNERABILIDAD EN ROBOTSTUDIO DE ABB

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

Productos afectados: ABB RobotStudio.

Vector de ataque: Entrada no validada; posible manipulación de parámetros.

Severidad: Alta.

Impacto potencial en OT: Riesgo en la programación y control de robots; posibles fallos o movimientos indebidos.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Parchear; segmentar estaciones de ingeniería; reforzar autenticación.

Prioridad: Alta.

VULNERABILIDAD EN COBUILDERPRO DE NKG

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

Productos afectados: CoBuilderPro.

Vector de ataque: Exposición de servicios; validación insuficiente.

Severidad: Alta.

Impacto potencial en OT: Manipulación de datos industriales; riesgo de corrupción de configuraciones.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Actualizar; segmentar; restringir accesos.

Prioridad: Alta.

AVISOS DE SEGURIDAD DE SIEMENS – NOVEMBRE 2025

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

Productos afectados: Múltiples productos industriales de Siemens (PLC, HMI, redes y software de ingeniería).

Vector de ataque: Diversos vectores (ejecución remota de código, elevación de privilegios, omisión de autenticación, desbordamientos).

Severidad: Alta–crítica según producto y CVE.

Impacto potencial en OT: Compromiso directo de equipos de automatización y monitorización; riesgo de interrupción de procesos, alteración de la lógica de control y pérdida de visibilidad.

Probabilidad de explotación: Moderada–alta, especialmente en sistemas expuestos o sin segmentación.

Mitigaciones inmediatas: Aplicar los parches y mitigaciones específicas de cada aviso; segmentar redes OT; restringir accesos remotos; reforzar autenticación y monitorización.

Prioridad: Muy alta.

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS DE SCHNEIDER

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

Productos afectados: Diversos dispositivos y software industriales de Schneider Electric.

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

Severidad: Alta–crítica.

Impacto potencial en OT: Compromiso de PLC, pasarelas o herramientas de ingeniería; riesgo para la continuidad del proceso y la seguridad de las instalaciones.

Probabilidad de explotación: Alta en entornos con acceso de red no controlado.

Mitigaciones inmediatas: Parchear según las versiones afectadas; segmentar; limitar acceso lógico; reforzar credenciales y monitorización.

Prioridad: Muy alta.

MÚLTIPLES VULNERABILIDADES EN AVEVA

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

Productos afectados: Plataformas AVEVA de supervisión y control (SCADA/HMI y software asociado).

Vector de ataque: Inyección, RCE, exposición de información y otros vectores de aplicación.

Severidad: Alta–crítica.

Impacto potencial en OT: Manipulación de datos de proceso, pantallas HMI y lógica de control; riesgo de paradas de planta o funcionamiento fuera de especificación.

Probabilidad de explotación: Moderada–alta, especialmente si las consolas están accesibles desde redes IT o externas.

Mitigaciones inmediatas: Actualizar a versiones corregidas; aislar estaciones de ingeniería y SCADA; aplicar endurecimiento y gestión de cuentas.

Prioridad: Muy alta.

PREDICIÓN DE CONTRASEÑAS EN VARITRON DE JUMO

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

Productos afectados: Controladores JUMO VARITRON.

Vector de ataque: Predicción de contraseñas por algoritmo débil o patrón previsible.
Severidad: Alta.
Impacto potencial en OT: Acceso no autorizado a la configuración del controlador; modificación de parámetros de proceso; riesgo de desviaciones operativas.
Probabilidad de explotación: Alta si el equipo es accesible por red o interfaz remota.
Mitigaciones inmediatas: Actualizar el firmware; cambiar credenciales por otras robustas y no predefinidas; segmentar el acceso a los controladores.
Prioridad: Muy 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
Productos afectados: Advantech DeviceOn/iEdge – plataformas de gestión y edge computing.
Vector de ataque: RCE, autenticación insuficiente, exposición de credenciales y manipulación de APIs.
Severidad: Alta–Crítica.
Impacto potencial en OT: Control no autorizado de nodos edge; alteración de telemetría y órdenes hacia dispositivos de campo; posible pivote hacia redes internas.
Probabilidad de explotación: Alta, especialmente en despliegues conectados a Internet o redes IT.
Mitigaciones inmediatas: Parchear; limitar la exposición de servicios; reforzar la autenticación (MFA cuando sea posible); segmentar la capa edge.
Prioridad: Muy alta.

CREDENCIALES INSUFICIENTEMENTE PROTEGIDAS EN UBOX DE UBIA
URL: https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci/credenciales-insuficientemente-protegidas-en-ubox-de-ubia
Productos afectados: Dispositivos UBOX de UBIA.
Vector de ataque: Almacenamiento o transmisión insegura de credenciales.
Severidad: Alta.
Impacto potencial en OT: Compromiso de cuentas administrativas; acceso a servicios críticos de conectividad o integración OT/IT.
Probabilidad de explotación: Moderada–alta si se tiene acceso a la red o al dispositivo.

Mitigaciones inmediatas: Actualizar el firmware; cambiar credenciales; habilitar cifrado y mecanismos de protección adicionales; limitar accesos administrativos.
Prioridad: 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
Productos afectados: Dispositivos SPRECON-E, SPRECON-C, SPRECON-E-P, SPRECON-E-T3.
Vector de ataque: Diversos (RCE, elusión de la autenticación, manipulación de comunicaciones).
Severidad: Alta–crítica.
Impacto potencial en OT: Riesgo directo sobre sistemas de protección y control en redes eléctricas; potencial pérdida de estabilidad de la red o interrupciones de suministro.
Probabilidad de explotación: Moderada–alta en entornos con acceso remoto o mala segmentación.
Mitigaciones inmediatas: Parchear; segmentar redes de protección; limitar interfaces remotas; reforzar monitorización de eventos.
Prioridad: 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
Productos afectados: Delta Electronics CNCSoft-G2 – software de configuración/programación.
Vector de ataque: Desbordamiento de búsqueda de ficheros o entradas manipuladas.
Severidad: Alta–crítica.
Impacto potencial en OT: Ejecución de código en estaciones de ingeniería; posible modificación maliciosa de proyectos o parámetros enviados a máquinas CNC.
Probabilidad de explotación: Moderada, normalmente requiere la interacción del usuario con ficheros maliciosos.
Mitigaciones inmediatas: Actualizar a la versión corregida; evitar abrir proyectos no confiables; segmentar estaciones de ingeniería.

Prioridad: Muy 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

Productos afectados: Cámaras LPR de SurVision.

Vector de ataque: Acceso a servicios de la cámara sin autenticación adecuada.

Severidad: Alta.

Impacto potencial en OT: Manipulación de sistemas de control de accesos basados en matrículas; generación de puntos ciegos o alteración de registros.

Probabilidad de explotación: Alta si las cámaras están expuestas a redes no confiables.

Mitigaciones inmediatas: Activar y reforzar la autenticación; segmentar la red de videovigilancia; restringir el acceso remoto.

Prioridad: Muy 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

Productos afectados: Sistemas Radiometrics VizAir.

Vector de ataque: Varias vulnerabilidades en servicios y APIs (incluyendo posible RCE y exposición de información).

Severidad: Alta–Crítica.

Impacto potencial en OT: Manipulación de datos meteorológicos o ambientales usados en operaciones; riesgo de decisiones operativas erróneas.

Probabilidad de explotación: Moderada–Alta según la exposición.

Mitigaciones inmediatas: Parchear; limitar accesos; reforzar autenticación y cifrado de las comunicaciones.

Prioridad: Alta.

INYECCIÓN 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

Productos afectados: IDIS ICM Viewer.

Vector de ataque: Inyección de argumentos en la línea de comandos o llamadas internas.

Severidad: Alta.

Impacto potencial en OT: Ejecución de comandos no autorizados desde estaciones de visualización; manipulación de videovigilancia o pivote hacia otros sistemas.

Probabilidad de explotación: Moderada.

Mitigaciones inmediatas: Actualizar el software; evitar la apertura de enlaces o ficheros no confiables; segmentar estaciones cliente.

Prioridad: 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

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

Vector de ataque: Manejo inseguro de ficheros de proyecto, desbordamientos y otras debilidades.

Severidad: Alta–crítica.

Impacto potencial en OT: Compromiso de estaciones de ingeniería; alteración de proyectos HMI descargados a paneles de operador.

Probabilidad de explotación: Moderada, requiere el uso de ficheros manipulados.

Mitigaciones inmediatas: Parchear; restringir el uso de proyectos de origen desconocido; segmentar estaciones de ingeniería.

Prioridad: Muy 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

Productos afectados: Eaton Brightlayer Software Suite (BLSS).

Vector de ataque: RCE, gestión insegura de la autenticación, exposición de datos y otros vectores en componentes web.

Severidad: Alta–Crítica.

Impacto potencial en OT: Manipulación de sistemas de gestión de energía y activos; alteración de configuraciones eléctricas o de monitorización.

Probabilidad de explotación: Alta si los servicios BLSS están expuestos a redes amplias.

Mitigaciones inmediatas: Actualizar; segmentar la plataforma de gestión; aplicar endurecimiento de accesos y credenciales.

Prioridad: Muy alta.

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS DE WAGO

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

Productos afectados: PLC y dispositivos industriales WAGO (varias gamas).

Vector de ataque: RCE, desbordamientos, autenticación débil y otros vectores sobre servicios de gestión y comunicación.

Severidad: Alta–crítica.

Impacto potencial en OT: Compromiso de controladores y módulos de E/S; riesgo alto para la continuidad y la seguridad del proceso industrial.

Probabilidad de explotación: Alta en entornos con exposición de servicios o sin segmentación OT.

Mitigaciones inmediatas: Parchear según la guía del fabricante; segmentar redes de control; limitar accesos de administración; reforzar monitorización en profundidad.

Prioridad: Crítica.

5 Recomendaciones

Esta sección reúne **recomendaciones prácticas para reforzar la ciberseguridad industrial siguiendo un recorrido lógico**: comenzamos con principios generales que orientan cualquier programa de seguridad en entornos OT, avanzamos hacia prioridades tácticas propuestas por distintas organizaciones especializadas y terminamos con aspectos específicos de la gestión de vulnerabilidades y de programas de parcheo, objeto último de este informe teórico-práctico.

5.1 Principios generales de ciberseguridad OT

El documento **Principal of Operational Technology Cybersecurity** [47] de 2024 es una guía impulsada por el Australian Cyber Security Centre (ACSC), y elaborada de forma conjunta con agencias nacionales de ciberseguridad de ocho países y expertos en sistemas de control industrial. Su objetivo es ofrecer un conjunto de principios sencillos, compartidos y aplicables a la mayoría de sectores industriales, que complemente marcos como NIST o IEC 62443 pero con un enfoque muy claro en la realidad de planta. Exponen seis principios básicos:

1. **Seguridad física por encima de todo**

El documento insiste en que **la seguridad física y la integridad del proceso son la prioridad absoluta**. Cualquier medida de ciberseguridad debe respetar el diseño de seguridad funcional, los enclavamientos, los sistemas instrumentados de seguridad y los límites operativos. Esto implica evitar cambios apresurados, pruebas insuficientes o soluciones "de TI" que puedan provocar paradas no controladas o comportamientos inesperados en campo.

2. **Diseñar para un entorno hostil**

Los sistemas OT deben pensarse y operarse como si estuvieran permanentemente expuestos a fallos, errores humanos y ataques. El principio invita a reducir la superficie de exposición, segmentar redes, limitar servicios y evitar la dependencia de accesos remotos innecesarios. La idea de fondo es que la resiliencia debe empezar en el diseño, no sólo en la respuesta a incidentes.

3. **Previsibilidad y estabilidad operacional**

Otro de los principios vitales es garantizar que, en condiciones de tensiones o fallo parcial, el comportamiento del sistema sea estable y predecible. Ello implica **diseñar modos degradados seguros, redundancia adecuada y procedimientos de**

operación manual para cuando las capas digitales de supervisión fallen. La ciberseguridad se entiende aquí como una extensión natural del diseño robusto de procesos.

4. **Conocimiento continuo del entorno OT**

El documento subraya **la necesidad de contar con inventarios actualizados de activos, versiones de firmware, configuraciones y dependencias de red.** Sin ese conocimiento es muy difícil priorizar vulnerabilidades, evaluar el impacto de un incidente o planificar un parcheo. La visibilidad, tanto de activos como de comunicaciones, se declara una condición básica de cualquier programa de seguridad.

5. **Preparación para incidentes y recuperación**

Aceptar que los incidentes ocurrirán lleva de forma natural a reforzar la capacidad de detección, respuesta y recuperación. El principio **anima a integrar la ciberseguridad OT en los planes de continuidad y recuperación de la organización, incluyendo copias de seguridad específicas de sistemas de control, procedimientos de restauración probados y tiempos de recuperación alineados con el riesgo** de proceso.

6. **Gestión de riesgos integrada con el negocio**

Por último, se insiste en que **los riesgos OT son riesgos de negocio y, en muchos casos, de seguridad de las personas. Las decisiones sobre qué mitigar, qué aceptar y qué posponer deben tomarse de forma informada, documentada y con participación de operaciones, seguridad y Dirección.** El principio apunta a modelos de gobierno en los que OT tenga voz propia dentro de la gestión corporativa del riesgo.

Estos seis principios constituyen el marco general del que en cierto modo, se puede considerar que derivan las recomendaciones más concretas de los apartados siguientes.

5.2 Enfoque pragmático

El informe **Dragones OT/ICS Cybersecurity Year in Review 2025** [39] traduce estos principios en líneas de acción muy concretas, pensadas para organizaciones que ya dieron los primeros pasos pero necesitan ordenar sus prioridades.

Plan de respuesta a incidentes ICS específico

Se recomienda **disponer de un plan de respuesta a incidentes diseñado expresamente para sistemas de control industrial**. Este plan debe contemplar distintos escenarios (ransomware, pérdida de visibilidad HMI, manipulación de PLC,

etc.) y, sobre todo, involucrar la ingeniería y operación tanto en su redacción como en los ejercicios y simulacros.

Arquitectura defendible

Otra prioridad **es evolucionar desde redes planas y muy interconectadas hacia arquitecturas "defendibles", con zonas y conductos bien definidos, DMZ industrial, minimización de servicios expuestos y controles claros** en los puntos de convergencia IT/OT. El objetivo es que un incidente o una intrusión en una parte de la red no se traduzca fácilmente en pérdida de control del proceso.

Visibilidad y monitorización OT

El informe insiste en que la **visibilidad específica de OT (protocolos industriales, cambios en lógicas de control, modificaciones en configuraciones) es fundamental**. Sin esa visibilidad, la detección de actividad anómala se vuelve tardía o directamente imposible, perdiendo la oportunidad de reaccionar antes de que el impacto sea físico.

Acceso remoto seguro

Se sitúa el acceso remoto como uno de los vectores de riesgo más críticos. Se anima a **revisar de forma sistemática VPN, accesos de terceros, mantenimientos remotos y cualquier mecanismo que permita entrar en OT desde fuera de la planta**, reforzando autenticación, aplicando el principio de mínimo privilegio y asegurando la trazabilidad de las sesiones.

Gestión de vulnerabilidades basada en riesgo (Now/Next/Never)

Por último, el informe expone que **la gestión de vulnerabilidades en ICS debe centrarse en el riesgo real para el proceso, no únicamente en la puntuación técnica de las CVE. Esta visión enlaza con la filosofía Now / Next / Never**, que se desarrolla a continuación, y que ofrece una forma práctica de decidir qué merece parcheo inmediato, qué puede esperar y qué puede gestionarse con medidas compensatorias.

Una vez contextualizado el entorno de amenazas, la pregunta práctica es cómo decidir que vulnerabilidades requieren acción inmediata, cuáles pueden esperar y cuáles quizá no deban parchearse nunca en condiciones normales. La filosofía **Now / Next / Never**, ofrece una respuesta operativa a esta cuestión.

Desde este punto de vista, **una vulnerabilidad se clasifica en Now cuando combina varios elementos**:

a) afecta a un activo crítico para el proceso o la seguridad;
b) es explotable de forma remota o con un esfuerzo razonable;
c) y no existe una mitigación compensatoria eficaz ya implantada (segmentación, listas blancas, restricciones de acceso, etc.).

Estas vulnerabilidades son las que pueden permitir a un atacante tomar control directo de equipos clave o provocar una pérdida de visión inminente, y por lo tanto deben abordarse con la máxima prioridad. En la práctica, esto no siempre implica parchear de forma inmediata, pero sí desplegar medidas que reduzcan de forma rápida su explotabilidad (cambios de configuración, reglas en firewalls, aislamiento adicional, etc.) y planificar el parcheo en la primera ventana segura posible.

En la **categoría Next se sitúan vulnerabilidades que, a pesar de ser relevantes**:

a) requieren una combinación de factores menos probable para causar un impacto grave,
b) o bien cuentan con cierto nivel de mitigación gracias a la arquitectura existente.

Son candidatas a ser resueltas como parte de campañas de mejora planificadas, a menudo combinando actuaciones de refuerzo de la arquitectura (por ejemplo, reducir exposición o endurecer accesos) con la aplicación progresiva de parches cuando las ventanas de mantenimiento lo permiten.

Por último, **la categoría Never agrupa vulnerabilidades que, en el contexto concreto de la organización, difícilmente llegarán a materializarse en un riesgo significativo**. Puede tratarse de fallos que sólo afectan a funcionalidades no utilizadas, a configuraciones muy específicas que no se dan en planta o a equipos completamente aislados y sin repercusión real sobre el proceso. Clasificar una vulnerabilidad como Never no significa ignorarla, sino documentar la decisión, justificarla en base a riesgo y mantener una monitorización suficiente como para reformularla si cambian las condiciones (por ejemplo, si un activo deja de estar aislado o se le añaden nuevas funciones).

Este enfoque ayuda a que las decisiones sobre parcheo se apoyen en el impacto operativo y no sólo en la severidad técnica de la vulnerabilidad, y conecta de forma natural con los programas de gestión de parches descritos en el apartado siguiente.

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

La guía **Recommended Practice for Patch Management of Control Systems** de CISA [30], se ha convertido en una referencia para estructurar programas de parcheo realistas en entornos ICS. No propone un calendario rígido, sino una forma de organizar el proceso para equilibrar seguridad y continuidad.

Un primer bloque del programa tiene que ver con la **gobernanza y el alcance**. Es necesario definir qué sistemas entran en el programa (PLC, RTU, HMI, servidores de historización, estaciones de ingeniería, pasarelas, sistemas de seguridad, etc.), quién es responsable de qué (seguridad, ingeniería, operación, mantenimiento, proveedores) y cómo se van a tomar las decisiones de cambio. Integrar el parcheo en los procesos de gestión de cambios existentes ayuda a evitar actuaciones aisladas y no coordinadas.

El segundo bloque se centra en el **inventario y la clasificación de activos**. Sin una lista fiable de equipos, versiones de firmware y roles en el proceso, la gestión de parches se convierte en un ejercicio teórico. La guía recomienda clasificar activos por criticidad operacional, por su exposición (por ejemplo, si están accesibles desde otras redes) y por la facilidad para intervenir sobre ellos (ventanas de parada, redundancias, etc.). Esta clasificación será la base de la priorización posterior.

A partir de ahí entra en juego la **monitorización de vulnerabilidades y avisos**. El programa debe establecer cómo se reciben y procesan los preavisos de fabricantes, boletines de organismos profesionales o nuevos CVE. Lo importante no es sólo recibir información, sino relacionarla de forma sistemática con el inventario: qué modelos están afectados, qué versiones, en qué plantas, y qué papel juegan en el proceso.

El siguiente paso es el **análisis de impacto y la priorización**, donde encaja la filosofía Now / Next / Never. Para cada vulnerabilidad relevante se evalúan cuestiones como: si afecta a activos críticos, si requiere acceso local o remoto, si ya existe algún control que reduzca su explotabilidad, qué impacto tendría una explotación exitosa en términos de seguridad física y continuidad de servicio, y qué alternativas hay al parcheo directo (cambios de configuración, segmentación adicional, restricciones de acceso). Con estos elementos, se declara si una vulnerabilidad se declara de tratamiento inmediato, programable o aceptable con mitigaciones compensatorias (véase el esquema de decisión propuesto en la figura de la sección 3.2.2).

La **fase de pruebas y planificación es** especialmente importante en ICS. Siempre que sea posible, se recomienda convalidar los parches en entornos de laboratorio o preproducción que reproduzcan de manera razonable el comportamiento de los sistemas reales. A partir de los resultados, se planifican ventanas de mantenimiento coordinadas con operación, se define el orden en el que se actuará sobre los distintos componentes y se documentan los posibles escenarios de rollback si algo no sale como se esperaba.

En **la ejecución del parcheo**, la guía sugiere trabajar con procedimientos estandarizados y listas de comprobación: qué servicios detener, qué pasos seguir, qué verificaciones realizar antes y después de aplicar cada parche. Es igualmente importante registrar qué se ha actualizado, en qué momento y con qué resultado, para poder reconstruir el estado del sistema en caso de problema.

Tras la ejecución, el programa contempla una **fase de verificación y seguimiento**. No basta con comprobar que los sistemas arrancan: hay que asegurarse de que las comunicaciones son estables, que las aplicaciones de supervisión y control funcionan correctamente y que no se han introducido regresiones sutiles. En algunos casos, puede ser razonable establecer un período de observación reforzada tras campañas de parcheo importantes.

Por último, CISA destaca la necesidad de **documentar y aprender** de cada ciclo de parcheo: actualizar inventarios y diagramas, registrar incidencias y mejoras detectadas en el procedimiento, y revisar periódicamente el equilibrio entre parches aplicados, parches diferidos y vulnerabilidades aceptadas con medidas compensatorias.

5.4 Alternativas

Un elemento transversal y que es importante admitir, es el hecho de que **no siempre será posible aplicar parches,** o no en los plazos deseables. En esos casos, el programa debe contemplar explícitamente las medidas **compensatorias**: segmentar e aislar activos vulnerables, restringir al máximo los accesos lógicos, aplicar listas blancas de aplicaciones, reforzar la monitorización sobre esos sistemas y revisar de forma periódica si las condiciones han cambiado lo suficiente como para reabrir la posibilidad de parchear.

La ciberseguridad OT exige equilibrio entre seguridad y continuidad. No todas las vulnerabilidades pueden parchearse con rapidez, y algunas no necesitan parchearse en

absoluto. Pero todas requieren gestión. Cuando el parcheo directo no es viable por restricciones de operación, compatibilidad o soporte, deben valorarse e implantarse medidas compensatorias que reduzcan el riesgo sin comprometer la seguridad física ni la estabilidad del proceso.

Así, **se propone un enfoque que combina principios generales, prioridades tácticas y prácticas operativas para construir programas de seguridad industrial realistas, sostenibles y adaptados** a entornos donde la fiabilidad es esencial.

6 Conclusiones

El presente informe ofrece una **visión integral y estructurada del estado de las vulnerabilidades y alertas que afectan a los sistemas de control industrial, incorporando tanto un marco conceptual como un análisis práctico orientado a la acción**. La combinación de ambos enfoques permite al lector comprender no sólo qué vulnerabilidades existen y cómo evolucionan, sino también que factores condicionan su explotación, su criticidad y las decisiones de mitigación.

En primer lugar, se **expusieron los fundamentos teóricos que permiten interpretar adecuadamente el riesgo asociado a las vulnerabilidades en entornos OT**, destacando aspectos como la definición y taxonomía de vulnerabilidades, y la criticidad asociada al tiempo de explotación, el tiempo de remediación, la relación entre ambos y el impacto específico que estos factores adquieren cuando la disponibilidad del proceso y la seguridad física son prioritarias. Se expusieron las etapas del análisis y gestión de vulnerabilidades, e incluso un marco teórico de cálculo del retorno esperado de dichas acciones. Se ha contextualizado esta información con estudios contrastados de organismos como ENISA, CISA o ISC2.

En segundo lugar, se **analizó el panorama reciente de alertas ICS con datos procedentes de fuentes especializadas, sintetizando tendencias globales generales, algunas técnicas de ataque predominantes y sectores más impactados**, así como se enlaza una buena base de datos de ciberincidentes industriales reales. Posteriormente, **se facilitan numerosas fuentes de CERTs nacionales e internacionales de avisos, vulnerabilidades y alertas accionables en entornos ICS/OT del último trimestre recopilados por INCIBE de los organismos citados**, así como un **anexo con las referencias de los preavisos de seguridad de algunos de los principales fabricantes** de componentes en el mercado.

Se han proporcionado **recomendaciones basadas en buenas prácticas internacionales**, **incluyendo principios generales de ciberseguridad OT definidos de manera colegiada entre los principales países del mundo**, **prioridades tácticas propuestas por entidades como Dragones y SANS, y una descripción detallada de la filosofía Now / Next / Never** aplicada a la priorización del tratamiento de vulnerabilidades. Este enfoque contribuye a que las organizaciones orienten sus esfuerzos de mitigación hacia aquello que reduce de manera más efectiva el riesgo operacional.

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

El eje central de las recomendaciones en esta materia particular, lo constituye la **guía de CISA para la gestión de parches** en entornos ICS, que se ha desarrollado **para ofrecer un conjunto de directrices prácticas sobre gobernanza, inventario, análisis de impacto, convalidación de parches, ejecución, verificación y uso de medidas compensatorias cuando el parcheo directo no es viable.**

Para reforzar la aplicabilidad del informe, se ha incluido un **glosario de términos específicos** que facilita la lectura y comprensión del documento, así como un anexo con enlaces a los portales oficiales de advisories de fabricantes OT ampliamente utilizados en el ecosistema industrial gallego.

El período analizado evidencia que **las vulnerabilidades en entornos OT siguen concentrándose en fallos recurrentes de diseño, configuraciones por defecto y componentes legacy, afectando a un amplio rango de fabricantes** (incluido un aviso relevante de Siemens por el volumen de dispositivos impactados). La diversidad y frecuencia de estos avisos confirman que la superficie de exposición industrial continúa creciendo, y que los riesgos asociados a la cadena de suministro y al ciclo de vida de los equipos siguen siendo determinantes para la seguridad de las operaciones.

En conjunto, **las alertas analizadas muestran un ecosistema OT donde los incidentes potenciales pueden traducirse rápidamente en impactos operativos relevantes**. Para el tejido empresarial y las Administraciones Públicas gallegas, esto refuerza **la necesidad de consolidar inventarios precisos, mejorar la higiene de configuración y adoptar una gestión de parches realista pero sistemática**, alineada con los condicionantes de disponibilidad propios de la entorno industrial.

Es probable que **aumente la explotación automatizada de vulnerabilidades** recientemente publicadas, acortando el margen de reacción disponible para las organizaciones. También se prevé un mayor foco de los atacantes en dispositivos ampliamente desplegados y en servicios inadvertidamente expuestos, lo que hará más crítica la visibilidad continua del entorno.

Además, la **presión regulatoria y operativa sobre fabricantes podría derivar en ciclos de actualización más frecuentes**. **Para Galicia, esto implicará reforzar capacidades internas de análisis de alertas, mejorar la coordinación con proveedores y avanzar hacia modelos de refuerzo continuo de la seguridad OT, a fin de elevar la resiliencia global del ecosistema industrial regional.**

En conjunto, el boletín aporta valor al tejido empresarial y a las administraciones públicas gallegas al proporcionar un **marco conceptual sintetizado** que facilita la interpretación técnica del riesgo, junto con un **resumen actualizado de alertas relevantes para sectores críticos**. Además, las **recomendaciones operativas** incluidas permiten mejorar la resiliencia de los entornos ICS mediante prácticas contrastadas y aplicables, mientras que los recursos y referencias ofrecidos contribuyen a establecer una **vigilancia continua y estructurada de vulnerabilidades**.

Todo ello **ayuda a las organizaciones de Galicia a avanzar hacia una gestión más madura del riesgo en OT**, apoyándose en información accionable y en alineación con estándares y recomendaciones de las principales fuentes a nivel global.

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 Ciberseguridad 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). *Red de Laboratorios y Centros Demostradores — Proyecto 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 ciberseguridad 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 Seguridad en Sistemas de Control Industrial (SCI) — Alerta Temprana*. Recuperado de https://www.incibe.es/index.php/incibe-cert/alerta-temprana/avisos-sci

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

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

Tipo de atacante o campaña caracterizada por su alto grado de sofisticación, persistencia y orientación a objetivos estratégicos. Acostumbran ser grupos patrocinados por Estados o actores con grandes recursos.

BC/DR (Business Continuity / Disaster Recovery)

Conjunto de planes, procedimientos y capacidades que permiten a una organización continuar operando o recuperarse tras un incidente grave. En OT, incluye restauración de sistemas de control y de comunicaciones industriales.

CAPEC (Common Attack Pattern Enumeration and Classification)

Catálogo de patrones de ataque recurrentes que describe cómo los atacantes explotan debilidades técnicas. Útil para entender tácticas y métodos de ataque en ICS.

CISA (Cybersecurity and Infrastructure Security Agency)

Agencia estadounidense responsable de la ciberseguridad de infraestructuras críticas. Publica avisos ICS, el catálogo KEV y guías como la de gestión de parches en sistemas de control.

CERT (Computer Emergency Response Team)

Equipo especializado en el manejo de incidentes de ciberseguridad. Publica avisos, coordinaciones y recomendaciones. Existen CERT nacionales, sectoriales y corporativos.

CCN-CERT (Centro Criptológico Nacional – CERT)

CERT español orientado principalmente a administraciones públicas y organismos de interés estratégico. Proporciona alertas, informes y guías técnicas.

CISA KEV (Known Exploited Vulnerabilities)

Catálogo mantenido por CISA que recopila vulnerabilidades que están siendo explotadas activamente en el mundo real. Son consideradas prioritarias para mitigación.

CMDB (Configuration Management Database)

Base de datos que recoge y gestiona la información de configuración de activos tecnológicos, incluidas versiones, relaciones y cambios.

CPS (Cyber-Physical Systems / Sistemas Ciberfísicos)

Sistemas donde componentes digitales, comunicaciones y procesos físicos interactúan estrechamente. OT es un ejemplo de CPS.

CPS PP (Cyber-Physical Systems Protection Platforms)

Plataformas de seguridad específicas para entornos ciberfísicos, capaces de entre otras funciones, descubrir activos OT, identificar vulnerabilidades y detectar anomalías.

CVE (Common Vulnerabilities and Exposures)

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

CVSS (Common Vulnerability Scoring System)

Sistema de puntuación que clasifica la severidad técnica de una vulnerabilidad según impacto y explotabilidad.

DCS (Distributed Control System / Sistema de Control Distribuido)

Arquitectura de control distribuido habitual en industrias de proceso continuo. Se compone de múltiples controladores coordinados desde una interfaz de supervisión.

DMZ industrial (Zona desmilitarizada industrial)

Zona de red intermedia entre TI y OT diseñada para limitar la exposición entre ambas. Aloja servicios que actúan como punto de intercambio controlado.

Fail-safe / Fail-secure

Conceptos que describen como debe comportarse un sistema de control ante un fallo: dejar el proceso en un estado seguro (fail-safe) o mantener protección mediante restricciones estrictas (fail-secure).

Hardening (Endurecimiento)

Conjunto de prácticas para reducir la superficie de ataque de un sistema: deshabilitar servicios innecesarios, reforzar autenticación, limitar accesos y aplicar configuraciones seguras.

HMI (Human–Machine Interface / interfaz Hombree–Máquina)

Interfaz que permite a los operadores visualizar y controlar sistemas industriales, gestionar alarmas y supervisar procesos.

ICS (Industrial Control Systems / Sistemas de Control Industrial)

Familia de sistemas diseñados para supervisar y controlar procesos industriales. Incluye SCADA, DCS, PLC, RTU y otros equipos.

ICS-CERT

Equipo de respuesta a incidentes orientado a sistemas de control industrial. Históricamente parte del Departamento de Seguridad Nacional de EE. UU., ahora integrado en CISA.

INCIBE (Instituto Nacional de Ciberseguridad)

Organización española que publica avisos, guías y recomendaciones, incluyendo alertas específicas para sistemas industriales.

Inventario de activos (Asset Inventory)

Relación estructurada de los componentes presentes en un entorno OT, incluyendo su función, versión, criticidad y localización en la red.

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

Conjunto de dispositivos conectados que recopilan datos y actúan en el entorno. En el ámbito industrial se refiere a dispositivos IIoT, que se integran con sistemas de control.

KEV (Known Exploited Vulnerabilities)

Vulnerabilidades que se sabe están siendo explotadas en el mundo real. Se presentan prioritarias para mitigación.

MITRE ATT&CK / MITRE ATT&CK for ICS

Marco que documenta tácticas y técnicas usadas por atacantes. La versión ICS recopila técnicas específicas aplicables a entornos industriales.

NIST NVD (National Vulnerability Database)

Base de datos mantenida por NIST que amplía la información de CVE y proporciona métricas adicionales de severidad.

Now / Next / Never

Modelo de priorización de vulnerabilidades basado en riesgo operativo real:

- *Now*: vulnerabilidades críticas que pueden afectar de inmediato a control o visibilidad del proceso.
- *Next*: vulnerabilidades relevantes pero cuyo riesgo depende de factores adicionales (exposición, arquitectura).
- *Never*: vulnerabilidades que, en el contexto concreto, no suponen riesgo significativo si existen controles adecuados.

OT (Operational Technology / Tecnologías de Operación)

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

PLC (Programmable Logic Controller / Autómata programable)

Dispositivo de control industrial que ejecuta lógicas y ordena la actuación sobre equipos físicos como válvulas y motores.

PSIRT (Product Security Incident Response Team)

Equipo de respuesta de un fabricante encargado de vulnerabilidades y avisos de seguridad relacionados con sus productos.

Purdue Model / Modelo Purdue

Modelo de referencia que segmenta los entornos industriales en niveles (IT corporativo, DMZ, supervisión, control, campo) para estructurar la seguridad y las comunicaciones.

Red Team / Purple Team

Actividades avanzadas de evaluación de seguridad: Red Team simula ataques reales, Purple Team combina Red y Blue Team para mejorar defensas.

Rollback

Proceso para revertir un parche o cambio si produce efectos no deseados, restaurando la configuración anterior sin interrumpir el proceso.

RTU (Remote Terminal Unit / Unidade Terminal Remota)

Dispositivo que recopila datos de sensores o equipos remotos y los comunica a sistemas SCADA u otras plataformas de control.

Safety vs. Security

Distinción entre seguridad funcional (protección de personas y equipos frente a fallos del proceso) y ciberseguridad (protección de sistemas frente a ataques o usos indebidos).

SCADA (Supervisory Control and Data Acquisition)

Sistema de supervisión y adquisición de datos que centraliza información procedente de equipos de campo y permite el control de procesos distribuidos.

Threat hunting OT

Actividad de búsqueda proactiva de indicios de intrusión o comportamiento anómalo en redes y sistemas industriales.

TI (Tecnologías de la Información)

Sistemas y servicios corporativos de gestión de información, comunicaciones y aplicaciones de negocio.

TTP (Tactics, Techniques and Procedures)

Descripción estructurada de los métodos utilizados por atacantes en campañas reales, y que se recogen en las matrices MITRE.

Ventana de mantenimiento

Período planificado durante el cual se permite intervenir en sistemas de control o equipos sin afectar a la operación.

Zero-day

Vulnerabilidad desconocida para el fabricante en el momento en que es explotada, sin parche disponible inicialmente.

Anexo. Avisos de fabricantes OT

Con el fin de facilitar la consulta directa de los avisos de seguridad publicados por los principales fabricantes de tecnología industrial, se incluye a continuación una **relación de los portales oficiales donde cada proveedor publica vulnerabilidades, parches, mitigaciones y buenas prácticas asociadas a sus productos**.

Este anexo sirve como complemento natural a la sección de alertas del boletín, permitiendo al lector acceder rápidamente a la información primaria y mantener un seguimiento continuo de las actualizaciones de seguridad relevantes para su entorno.

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 no es exhaustiva, pero recoge a varios de los fabricantes más presentes en entornos ICS/OT. Se aconseja al lector buscar los recursos asociados a sus fabricantes de referencia.

Consultar periódicamente estos portales o suscribirse en los casos que lo permita, ayuda a anticipar riesgos, validar configuraciones, programar campañas de parcheo y, en general, mantener un nivel de vigilancia acorde al nivel de riesgo asumible, y alineado con el ciclo de vida de los sistemas industriales.

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial
Informe de ciberalertas – I

Financiado pola Unión Europea NextGenerationEU

Plan de Recuperación, Transformación e Resiliencia

incibe_

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Xacobeo 2027