CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial

Informe de ciberalertas - II

Abril 2026

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_
XUNTA DE GALICIA
Xacobeo 2027

Edita: Xunta de Galicia

Axencia para a Modernización Tecnolóxica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Ano: 2026

Índice

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

1 Introdución

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

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

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

--

A crecente exposición das infraestruturas industriais a ameazas de ciberseguridade segue a consolidarse como un dos principais retos para a seguridade operativa, a continuidade do negocio e, en moitos casos, a seguridade física das persoas. A progresiva dixitalización dos procesos industriais, a incorporación de tecnoloxías de Internet das Cousas (IoT) e no borde (Edge), e a converxencia estrutural entre contornos IT e OT están a ampliar de forma sostida a superficie de ataque dos sistemas de control industrial (ICS), ao tempo que incrementan a complexidade da súa protección.

Se o **Informe de Ciberalertas OT – I** dende Observatorio da AMTEGA sentou as bases conceptuais da xestión de vulnerabilidades —definicións, clasificacións, tempos de explotación e remediación, e fundamentos económicos do risco—, este segundo informe céntrase nun problema eminentemente práctico: **como priorizar actuacións nun contexto no que o volume de vulnerabilidades publicadas é estruturalmente inmanexable para a maioría das organizacións industriais**.

A evidencia empírica amosa que cada ano se publican miles de novas vulnerabilidades ou CVEs, unha proporción moi elevada delas con severidade media ou alta segundo

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

CVSS. En contornos industriais, caracterizados por ciclos de vida longos, restricións operativas severas e dependencia de xanelas de mantemento planificadas, pretender manter unha infraestrutura "libre de vulnerabilidades" mediante parcheo sistemático resulta, na práctica, inviable. Esta realidade obriga a abandoar enfoques puramente reactivos ou baseados exclusivamente en métricas técnicas, e avanzar cara a **estratexias de priorización baseadas no risco real para o proceso e o negocio**.

Neste contexto, o presente informe introduce e desenvolve distintos enfoques complementarios orientados a apoiar a toma de decisións en contornos OT. Analízanse as limitacións prácticas do uso exclusivo de CVSS como criterio de urxencia, e explóranse alternativas máis accionables que incorporan información sobre explotación activa, probabilidade real de ataque e contexto operativo. Entre elas destacan o **catálogo de vulnerabilidades explotadas coñecidas (KEV) da CISA**, os modelos de clasificación operativa como **Now / Next / Never**, e métricas probabilísticas como **EPSS**, así como aproximacións máis avanzadas empregadas en solucións comerciais especializadas.

O obxectivo non é substituír un estándar por outro, senón **proporcionar un marco coherente que permita ás organizacións industriais decidir onde investir esforzos limitados para reducir de forma efectiva o risco**, mantendo o equilibrio entre seguridade, dispoñibilidade e estabilidade do proceso. Deste xeito, o informe mantén o enfoque didáctico e aplicado do Observatorio de Ciberseguridade Industrial, reforzando a súa utilidade como ferramenta de apoio para responsables de operación, enxeñaría, mantemento e seguridade no ecosistema industrial galego.

Adicionalmente, o informe complétase cunha recompilación de **boas prácticas internacionais en materia de xestión de vulnerabilidades**, a análise de **medidas compensatorias e estratexias de mitigación cando o parcheo non é viable**, e unha selección das **principais ciberalertas rexistradas durante o primeiro trimestre**, co obxectivo de ofrecer unha visión integral, práctica e actualizada da situación da ciberseguridade industrial e as súas ameazas en forma de vulnerabilidades técnicas.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

2 Resumo executivo

Este informe ten como obxectivo principal apoiar a toma de decisións en materia de **priorización de riscos de ciberseguridade en contornos industriais (OT/ICS).**

O contexto no que se encadra este documento ven marcado por un **incremento sostido da explotación de vulnerabilidades coñecidas**, unha crecente profesionalización do cibercrime e unha maior exposición dos sistemas industriais como consecuencia da converxencia IT/OT e da dependencia de servizos dixitais externos. A este escenario engádese un feito estrutural: **o volume anual de novas CVE publicadas, moitas delas clasificadas como de severidade media ou alta segundo CVSS, supera amplamente a capacidade real das organizacións industriais para aplicar parches de forma sistemática**. O universo total agregado é de mais de trescentas mil CVEs na actualidade.

En contornos OT/ICS, esta limitación non é só organizativa, senón tamén técnica e operativa. Os longos ciclos de vida dos equipos, as restricións de certificación por parte dos fabricantes, a dependencia de xanelas de mantemento planificadas e o risco de regresión funcional fan que **parchealo todo non sexa tecnicamente viable nin desexable dende o punto de vista da continuidade do negocio**. Esta realidade obriga a abandonar enfoques exhaustivos ou baseados exclusivamente en métricas técnicas, e avanzar cara a **estratexias de priorización baseadas no risco real, na explotación efectiva e no contexto operativo**.

Dende unha perspectiva de negocio, o informe pon o foco na **continuidade operativa, a seguridade das persoas e a protección dos procesos críticos**, aspectos especialmente sensibles en sectores industriais e de infraestruturas esenciais. As interrupcións derivadas de incidentes de ciberseguridade en OT non se traducen unicamente en perdas económicas directas, senón tamén en impactos reputacionais, incumprimentos regulatorios e, en casos extremos, riscos para a seguridade física.

Para dar resposta a este reto, o informe estrutúrase arredor de distintos **enfoques complementarios de priorización**:

- O **Catálogo de Vulnerabilidades Coñecidas Explotadas (KEV)** da CISA. O KEV permite identificar aquelas vulnerabilidades para as cales existe evidencia de explotación activa no mundo real, actuando como un primeiro filtro de urxencia fronte ao elevado volume de CVE dispoñibles.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

- Este enfoque complétase con outros modelos de priorización empregados no ámbito industrial, como **Now / Next / Never**, que facilita unha clasificación cualitativa das vulnerabilidades segundo a urxencia real de actuación;
- **EPSS (Exploit Prediction Scoring System)**, que introduce unha estimación probabilística da probabilidade de explotación;
- e **modelos máis avanzados empregados por solucións comerciais**, baseados na combinación de CVSS, intelixencia de ameazas, exposición e contexto operativo mediante algoritmos e intelixencia propia.

En conxunto, estes enfoques permiten pasar dunha lectura puramente técnica a unha **xestión baseada en risco e impacto no proceso**, especialmente axeitada para entornos OT, **para axudar aos responsables de planta e ciberseguridade, a decidir cal é a estratexia de xestión mais apropiada** no seu caso.

Xunto coa análise de vulnerabilidades e os mecanismos de priorización, o informe incorpora un conxunto de **boas prácticas internacionais de xestión de vulnerabilidades**, así como **medidas compensatorias e estratexias de mitigación orientadas a reducir o risco cando o parcheo non é inmediato ou viable**. Estas inclúen accións técnicas, organizativas e de arquitectura que permiten actuar sobre a probabilidade e o impacto dos incidentes, reforzando a resiliencia dos sistemas industriais a curto e medio prazo.

En síntese, preténdese trasladar unha mensaxe clara: a xestión da ciberseguridade en OT non pode basearse nun enfoque exhaustivo e reactivo, senón nun modelo **selectivo, pragmático e baseado en risco real**, que teña en conta as limitacións técnicas do parcheo, priorice as vulnerabilidades con explotación confirmada ou maior probabilidade de ataque, e combine métricas técnicas con contexto operativo.

O informe complétase coa nova **análise das ciberalertas de maior severidade rexistradas durante o trimestre (onde destacaríamos as que afectan a varias solucións de Siemens, Schneider ou Mitsubishi Electric)**, así como cun **anexo específico cos principais avisos de seguridade publicados por fabricantes de equipamento ICS/OT** (estendido con respecto á versión orixinal do Informe), proporcionando deste xeito unha visión integral, actualizada e accionable do estado da ameaza para responsables técnicos e de negocio.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027

3 Metodoloxía e fontes

O **Informe de Ciberalertas – II** elaborouse seguindo unha metodoloxía similar á empregada na primeira edición do informe, co obxectivo de manter coherencia entre entregables e facilitar a súa lectura comparada. Nesta segunda edición, a metodoloxía axústase ao foco específico do documento, centrado na **priorización de vulnerabilidades, a xestión do risco e as estratexias de mitigación en entornos OT/ICS**.

A redacción do informe baseouse nun proceso estruturado en varias fases, orientado á recompilación, selección e análise de información relevante para a ciberseguridade industrial:

- **Identificación e seguimento de fontes oficiais** de alertas, vulnerabilidades e ameazas, tanto a nivel nacional como internacional.
- **Revisión periódica de catálogos de vulnerabilidades**, prestando especial atención a aquelas con evidencia de explotación activa ou impacto potencial en entornos industriais.
- **Selección de contidos relevantes**, priorizando a súa aplicabilidade práctica en canto á priorización e mitigación de vulnerabilidades detectadas.
- **Análise contextual en clave OT**, tendo en conta as limitacións propias destes contornos en materia de parcheo, mantemento e xestión de cambios.

Este enfoque permite centrar o informe nas vulnerabilidades e alertas máis relevantes dende un punto de vista operativo, evitando unha simple enumeración de avisos.

As fontes de información utilizadas engaden algunhas novas ás xa empregadas polo Observatorio na edición previa:

- Os **marcos conceptuais e a análise baseada en risco** apóianse nos traballos do SANS Institute sobre xestión de vulnerabilidades baseada en risco, así como en estudos académicos e técnicos centrados na mellora das métricas de severidade e prioridade. Estas achegas xustifican a necesidade de ir máis aló do CVSS tradicional, especialmente en contornos OT.
- Para os **estándares e métricas de severidade**, empregouse principalmente a documentación oficial de CVSS v4.0 elaborada por FIRST, complementada con

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

referencias a MITRE e ao ecosistema CVE como base común para a identificación de vulnerabilidades.

- Os **catálogos e datos sobre vulnerabilidades e explotación** baséanse en fontes de NIST/NVD para a análise cuantitativa e a evolución histórica da severidade, así como no catálogo Known Exploited Vulnerabilities (KEV) de CISA, incluíndo a súa documentación técnica e feeds de datos, como referencia central para a explotación activa.
- O **marco regulatorio e as directrices operativas asociadas ao KEV** fundamentáronse nas directrices publicadas por CISA, xunto con material técnico de apoio de NIST e análises sectoriais que contextualizan a evolución e o alcance deste catálogo.
- As **métricas de probabilidade de explotación (EPSS)** introdúcense a partir de documentación de FIRST e contribucións académicas, permitindo complementar a severidade técnica con estimacións probabilísticas de explotación.
- Os **enfoques comerciais e modelos avanzados de priorización** ilústranse mediante documentación pública e white papers de fabricantes de solucións de xestión de vulnerabilidades como Qualys, Tenable ou Rapid7, como exemplo da integración de métricas, intelixencia de ameazas e contexto operativo.
- Para as **boas prácticas de xestión de vulnerabilidades e mitigación**, utilizáronse guías e recomendacións de organismos públicos e fabricantes tecnolóxicos, cubrindo aspectos como parcheo, medidas compensatorias e virtual patching.
- Finalmente, as **alertas operativas e avisos do trimestre** baséanse en información procedente de organismos nacionais de resposta a incidentes e nos avisos de seguridade industrial publicados por CISA e redifusionados por INCIBE.

Estas fontes empregáronse tanto para a identificación de alertas relevantes como para a elaboración das seccións de priorización e recomendacións.

Lémbrase que informe non pretende ser exhaustivo nin substituír os sistemas de vixilancia continua das organizacións. O seu obxectivo é **ofrecer unha visión sintética e práctica das alertas e vulnerabilidades máis relevantes do período analizado**, así

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

como proporcionar criterios e referencias que faciliten a toma de decisións en materia de ciberseguridade industrial.

A información presentada debe ser interpretada como apoio á xestión do risco, e complementada con análises específicas adaptadas ao contexto técnico e operativo de cada organización.

4 Priorización de vulnerabilidades

4.1 Contexto ICS/OT fronte a IT tradicional

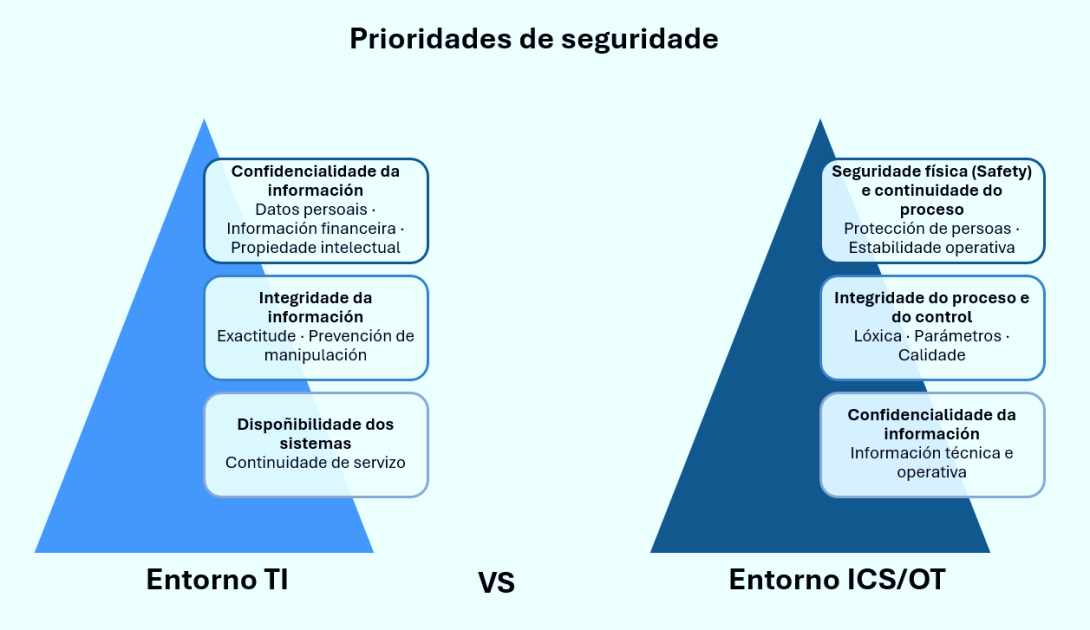
4.1.1 Dimensións de seguridade

A converxencia IT/OT e a dixitalización industrial poden levar a aplicar, por inercia, prácticas de seguridade deseñadas para entornos corporativos. Porén, os entornos **ICS/OT (Industrial Control Systems / Operational Technology)** presentan restricións técnicas, operativas e de seguridade funcional que fan que o seu modelo de operación e a súa ciberseguridade deban abordarse cun **enfoque diferenciado**.

De maneira sintética, en TI adoita primar a protección de datos e servizos de información, mentres que en OT o obxectivo último é garantir que o proceso físico se manteña **seguro, estable, dispoñible e dentro de especificación**, mesmo en condicións degradadas.

A tríade clásica **CIA (Confidencialidade, Integridade, Dispoñibilidade)** continúa sendo válida como marco xeral. Con todo, a orde de prioridade e a interpretación dos impactos difiren.

- En TI, a **confidencialidade** e a **integridade da información** adoitan ser determinantes (datos persoais, propiedade intelectual, información financeira), con impactos reputacionais e legais moi relevantes.
- En OT, a **dispoñibilidade do proceso** e a **seguridade física (safety)** adoitan ser críticas: unha intrusión pode traducirse en **paradas de planta**, **perda de control**, **danos en equipamento**, **degradación de calidade**, ou mesmo **risco para persoas**.



Prioridades de seguridade segundo a tipo de entorno. Fonte: elaboración propia (2026)

En consecuencia, unha vulnerabilidade con impacto "moderado" dende unha lectura puramente TI pode ser **crítica** se afecta á capacidade de controlar un PLC, unha HMI, unha pasarela industrial ou un SCADA que actúa sobre un proceso físico. E **un elemento crítico a resaltar, é que o risco en OT, inclúe efectos ciberfísicos**, non só dixitais.

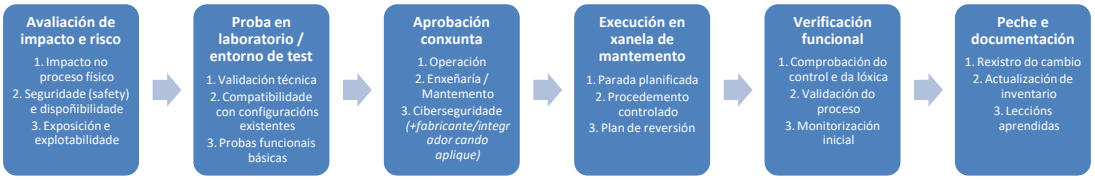
4.1.2 Contexto operativo

Neste eido, os entornos industriais están deseñadas para operar con **altos niveis de previsibilidade e estabilidade**, frecuentemente con requisitos de tempo real. Isto condiciona prácticas que en TI se consideran rutineiras:

- **Xanelas de mantemento limitadas**: moitos activos só se poden intervir durante paradas planificadas ou campañas anuais.
- **Alta sensibilidade a interrupcións**: escaneos agresivos, reinicios non coordinados ou cambios de configuración poden provocar indispoñibilidades ou estados non previstos.
- **Dependencias complexas**: cambios en firmware, drivers, librarías, ou no software de enxeñaría poden afectar a compatibilidade con versións de proxectos, comunicacións industriais ou módulos de E/S.

Así, mentres en TI o "cambio" (actualizacións frecuentes, hardening continuo) forma parte do ciclo normal, en OT o cambio require **xestión de cambios rigorosa**, probas e coordinación con operación e mantemento:

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027



Xestión de cambios en entornos OT (ICS/OT). Fonte: elaboración propia (2026)

4.1.3 Modelado de ameazas

No relativo á ciberseguridade, a superficie de ataque concéntrase principalmente ni usuario: endpoints, correo, identidade, SaaS e exposición a Internet en xeral. En OT, ademais deses factores (por converxencia), existen riscos específicos:

- **Protocolos industriais historicamente inseguros** (sen cifrado nin autenticación forte por deseño como Modbus), con alta prevalencia en entornos legados.
- **Acceso remoto de terceiros e mantementos** (integradores, fabricantes, soporte), a miúdo esencial para a continuidade do negocio.
- **Segmentación imperfecta e puntos de salto IT/OT**, onde unha intrusión en TI pode derivar en movemento lateral cara a OT.
- **Activos de longa vida útil** (10–25 anos), con obsolescencia, fin de soporte e limitacións para actualizar.

4.1.4 Gobernanza

Un **elemento clave para unha xestión eficaz da ciberseguridade** é a **gobernanza**. Mentres que en entornos TI as decisións sobre configuracións e parcheo adoitan centralizarse nos equipos de sistemas ou seguridade, nos entornos OT estas decisións teñen un carácter necesariamente **transversal**. A súa correcta adopción require a participación coordinada de operación, mantemento, enxeñaría e ciberseguridade, así como, en moitos casos, de provedores e integradores tecnolóxicos.

Por este motivo, resulta recomendable dispoñer dun **marco formal de gobernanza OT**, que inclúa procedementos estruturados de xestión de cambios, mecanismos claros para priorizar vulnerabilidades e un conxunto de criterios documentados que permitan decidir de maneira informada cando aceptar risco, pospoñer a aplicación de parches ou

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

aplicar medidas compensatorias. Este enfoque favorecerá decisións equilibradas entre seguridade, continuidade operativa e seguridade funcional.

Todas estas diferencias descritas entre entornos IT tradicionais e ICS/OT, explican a razón pola que, en entornos industriais:

- A prioridade non é "parchear todo canto antes", senón **xestionar o risco do proceso**. Disto falaremos na proxima sección.
- A información máis valiosa non é só a listaxe de CVEs e severidades asociadas, senón o **contexto operativo, o nivel de risco asumible** e as **capacidades de mitigación.** Aquí entran en xogo as estratexias de mitigación descritas posteriormente neste Informe, e que forman a parte nuclear do mesmo.
- E a toma de decisións require equilibrar **seguridade, continuidade e safety**.

4.2 Xestión basada en risco

A xestión da ciberseguridade en **entornos industriais ICS/OT** debe entenderse, de maneira prioritaria, como un exercicio de **xestión do risco**. Nun contexto no que os sistemas dixitais interactúan directamente con procesos físicos, persoas e instalacións, o obxectivo non pode ser a eliminación completa do risco —algo inasumible en sistemas complexos e operativos—, senón a súa **identificación, comprensión e tratamento ata niveis compatibles cos obxectivos de negocio**.

Dende unha perspectiva didáctica, o risco pode definirse como a **posibilidade de que un evento adverso se materialice e xere consecuencias negativas sobre a organización**. En entornos industriais, estas consecuencias non se limitan a perdas económicas ou reputacionais, senón que poden afectar á **continuidade da produción, á calidade do produto, ao cumprimento regulatorio e, de maneira especialmente crítica, á seguridade física das persoas e das instalacións (safety)**. Por este motivo, a xestión do risco constitúe un elemento central da gobernanza da seguridade industrial.

De forma clásica, o risco exprésase como unha combinación entre a probabilidade de ocorrencia dun evento e o impacto asociado á súa materialización, segundo a relación amplamente aceptada:

Risco = Probabilidade × Impacto

Aínda que esta formulación cuantitativa é deliberadamente sinxela, resulta moi útil para comprender que o risco non é un valor absoluto nin inherente a un elemento illado, senón o resultado dun **conxunto de factores que deben interpretarse no seu**

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

contexto real. En particular, tamén no ámbito da ciberseguridade industrial, isto implica recoñecer que unha vulnerabilidade técnica, por si soa, non define o risco.

En entornos ICS/OT, o denominado **risco técnico** depende da interacción de múltiples variables. A existencia dunha vulnerabilidade é só un dos compoñentes da ecuación. O risco real vén condicionado, entre outros aspectos:

- pola **factibilidade técnica do ataque**,
- pola **exposición do activo vulnerable dentro da arquitectura industrial**,
- polo seu **papel no proceso operativo** ,
- e polas **consecuencias reais que tería unha perda (de control, fuga de información ou unha indispoñibilidade).**

Deste xeito, **dúas vulnerabilidades cunha severidade técnica similar poden representar niveis de risco radicalmente distintos** en función do entorno no que estean despregadas.

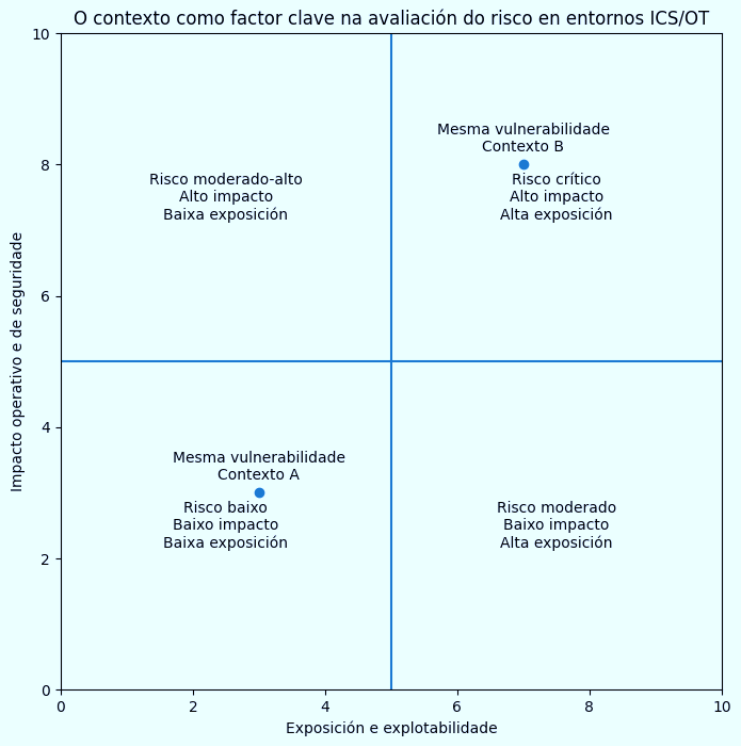
Esta visión contextual resulta especialmente relevante á hora de xestionar vulnerabilidades en sistemas industriais. A aplicación mecánica de métricas técnicas descontextualizadas pode conducir a decisións pouco realistas, como priorizar correccións de baixo impacto operativo mentres se relegan outras que, sen destacar tecnicamente, supoñen un risco significativo para o proceso. En resposta a esta problemática, nos últimos anos consolidouse o enfoque de **xestión de vulnerabilidades baseada en risco**.

Neste sentido, resulta particularmente ilustrativo e conciso o enfoque exposto polo SANS Institute [1] no artigo Risk-Based Vulnerability Management and Patching Industrial Systems [2], no que se aborda de maneira explícita a diferenza entre unha xestión de vulnerabilidades baseada unicamente en métricas técnicas e unha xestión realmente **baseada en risco** en entornos industriais.

O artigo pon o foco en que, en ICS/OT, a decisión de **cando e como mitigar unha vulnerabilidade** debe contrapesar dous eixes fundamentais: por unha banda, a **ameaza potencial** asociada á vulnerabilidade (incluíndo a súa explotabilidade e o impacto no proceso) e, pola outra, o **custo técnico e operativo da mitigación**, que pode incluír paradas de planta, riscos de regresión funcional, perda de estabilidade ou dependencia de terceiros. Dende esta perspectiva, parchear "todo canto antes" non só resulta inviable, senón que pode introducir novos riscos.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

SANS subliña que o **contexto é decisivo**: a mesma vulnerabilidade pode ser crítica ou asumible dependendo da súa exposición real, do rol do activo no proceso e das medidas compensatorias existentes.



Nivel de risco para unha mesma vulnerabilidades segundo o contexto. Fonte: elaboración propia (2026)

Por este motivo, o artigo **cuestiona o uso do indicador** para medir a severidade das vulnerabilidades **CVSS** (Common Vulnerability Scoring System Standard, de 0 a 10), [3] xa descrito no anterior Informe de ciberalertas - I dispoñible na web da AMTEGA [4], como único criterio de priorización; sinala que a magnitude dunha puntuación de severidade non reflicte por si soa a urxencia real de mitigación nun entorno industrial, se non se analiza xunto co contexto operativo e o risco global, que é diferente en cada organización.

Esta aproximación serve como base conceptual para a seguinte sección do informe, na que se revisará o papel do **CVSS**, e se introducirán **métricas e enfoques complementarios** orientados a medir non só a severidade técnica, senón tamén a **urxencia real de mitigación** dende unha perspectiva máis práctica e realista para entornos ICS/OT, tendo en conta que **a día de hoxe, existen máis de trescentas mil vulnerabilidades publicadas** e con etiqueta ou nomenclatura estándar para identificación da vulnerabilidade (CVE, Common Vulnerabilities and Exposures) asignada [5].

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

4.3 CVSS (Common Vulnerability Scoring System)

O **CVSS (Common Vulnerability Scoring System)** [3] é un estándar amplamente adoptado para **avaliar a gravidade das vulnerabilidades**, asignándolles unha puntuación numérica en función de diferentes parámetros técnicos. Entre eles inclúense aspectos como a facilidade de explotación, o impacto potencial sobre a confidencialidade, a integridade e a dispoñibilidade, ou a necesidade de interacción por parte do usuario afectado.

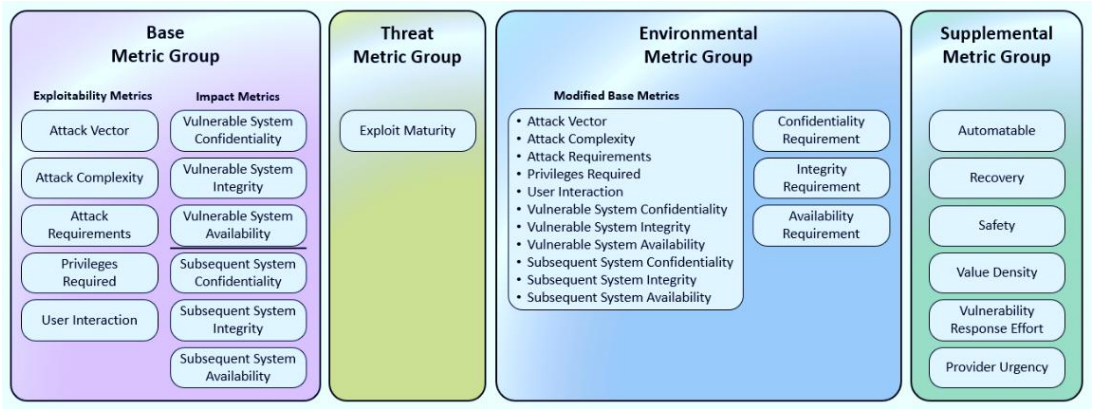
A versión **CVSS 4.0** representa a evolución máis recente deste estándar internacional e introduce un modelo máis **flexible, expresivo e preciso** ca versións anteriores. O seu propósito é ofrecer unha valoración que non só describa as características técnicas intrínsecas dunha vulnerabilidade, senón que tamén permita **aproximarse mellor ao seu impacto real e ao seu comportamento en función do contexto** no que se manifesta. Para iso, CVSS 4.0 estrutura a súa avaliación arredor de **catro grandes grupos de métricas**, que permiten caracterizar con maior detalle o risco asociado.

- O primeiro grupo corresponde ás **métricas Base**, que describen as propiedades inherentes da vulnerabilidade e non dependen nin do momento temporal nin do entorno concreto no que se atope o sistema afectado. Estas métricas subdivídense en dous bloques:
    - por unha banda, as métricas de **Explotabilidade**, que reflicten a dificultade técnica da explotación (vector de ataque, complexidade, privilexios necesarios ou interacción do usuario);
    - e, por outra, as métricas de **Impacto**, que avalían as consecuencias directas dunha explotación exitosa. Neste apartado considérase non só o efecto sobre o compoñente directamente afectado, senón tamén sobre sistemas relacionados, incorporando mesmo posibles repercusións sobre a seguridade física, unha dimensión que cobra especial relevancia en contornos industriais e ciberfísicos.
- O segundo grupo está constituído polas **métricas de Ameaza**, que introducen información sobre o estado real de explotación da vulnerabilidade. Dado que estes factores evolucionan co tempo, este conxunto permite axustar a valoración cando existen evidencias públicas de explotación, código dispoñible ou incidentes confirmados. Desta forma, dúas vulnerabilidades con impacto técnico

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

semellante poden recibir puntuacións diferentes en función da actividade observada por parte de actores maliciosos.

- O terceiro grupo, correspondente ás **métricas Ambientais**, permite adaptar a puntuación ao **contexto específico de cada organización**. Estas métricas teñen en conta elementos como a criticidade do activo afectado, a existencia de controis mitigadores ou a relevancia relativa de cada dimensión de seguridade. En entornos OT, CPS ou industriais, onde a dispoñibilidade do proceso e a seguridade física adoitan prevalecer fronte á confidencialidade, este axuste resulta especialmente relevante para reflectir con maior fidelidade a severidade operativa dunha vulnerabilidade.
- Finalmente, CVSS 4.0 incorpora un cuarto conxunto de **métricas Suplementarias**, deseñadas para achegar información adicional sobre características externas da vulnerabilidade, como posibles implicacións regulamentarias, aspectos relacionados coa seguridade humana ou a viabilidade da explotación automatizada. Estas métricas non inflúen no cálculo da puntuación final, pero proporcionan contexto adicional que pode ser empregado polas organizacións para enriquecer os seus propios modelos de priorización.



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

A escala de CVSS aínda na sua cuarta versión, continúa establecida entre 0 e 10, clasificando as vulnerabilidades en catro niveis de severidade:

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027

Nivel de severidade	Puntuación CVSS
Ningunha	0.0
Baixa	0.1 – 3.9
Media	4.0 – 6.9
Alta	7.0 – 8.9
Crítica	9.0 – 10.0

Categorías de severidade de CVSS 4.0. Fonte: elaboración propia (2026)

En conxunto, **CVSS 4.0 ofrece unha avaliación algo máis matizada da gravidade das vulnerabilidades**, pero aínda así, en moitos ámbitos non se considera suficiente.

4.3.1 Limitacións de CVSS

Aínda que **CVSS** constitúe unha referencia amplamente aceptada para describir a severidade técnica das vulnerabilidades, a súa aplicación directa e illada presenta **limitacións prácticas significativas en entornos OT e industriais**. Estas limitacións non derivan de deficiencias do estándar en si mesmo, senón do feito de que foi concibido como un **sistema de clasificación técnica**, non como un mecanismo completo de toma de decisións operativas.

- En primeiro lugar, CVSS **non incorpora de forma explícita o contexto operativo real** no que se atopa o activo vulnerable. En entornos ICS/OT, factores como a función do equipo no proceso, a existencia de redundancias, o impacto dunha parada non planificada ou a presenza de controis compensatorios poden ser determinantes á hora de avaliar o risco. Dúas vulnerabilidades cunha puntuación CVSS idéntica poden requirir respostas radicalmente distintas segundo o entorno industrial no que se manifesten.

- En segundo lugar, a puntuación CVSS **non reflicte necesariamente a ameaza real no tempo**. Unha vulnerabilidade cunha severidade técnica elevada pode non estar a ser explotada activamente, mentres que outra con puntuación inferior pode formar parte de campañas de ataque coñecidas. En entornos OT, onde o parcheo inmediato non sempre é viable, esta distinción resulta clave para priorizar actuacións de forma realista.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

- Adicionalmente, CVSS **non ten en conta o custo técnico e operativo da mitigación**, un aspecto especialmente relevante en sistemas industriais. A aplicación dun parche pode implicar paradas de planta, probas extensivas, riscos de regresión funcional ou dependencia de terceiros (explicado anteriormente no contexto operativo de entornos ICS/OT). Avaliar a urxencia dunha mitigación sen considerar estes custos pode conducir a decisións que, lonxe de reducir o risco global, o incrementen.

Por estes motivos, en calquera ámbito pero especialmente polas súas peculiaridades, no ámbito industrial resulta necesario complementar CVSS con **métricas e enfoques adicionais**, orientados a capturar mellor a realidade operativa e a ameaza efectiva.

Entre estas métricas complementarias destacan as que veremos a continuación en mais profundidade como alternativas a CVSS, como son:

- **KEV (Known Exploited Vulnerabilities)**, orientado a identificar vulnerabilidades con evidencia de explotación activa no mundo real.
- **Now / Next / Never**, enfoque cualitativo de priorización que permite clasificar as vulnerabilidades segundo a urxencia real de actuación en función do risco operativo.
- **EPSS (Exploit Prediction Scoring System)**, que introduce unha estimación probabilística da probabilidade de explotación.
- **Modelos avanzados empregados por solucións comerciais**, baseados na combinación de múltiples fontes (CVSS, intelixencia de ameazas, telemetría, exposición e contexto operativo) xunto con algoritmos e intelixencia propia, co obxectivo de ofrecer priorizacións máis precisas e accionables.

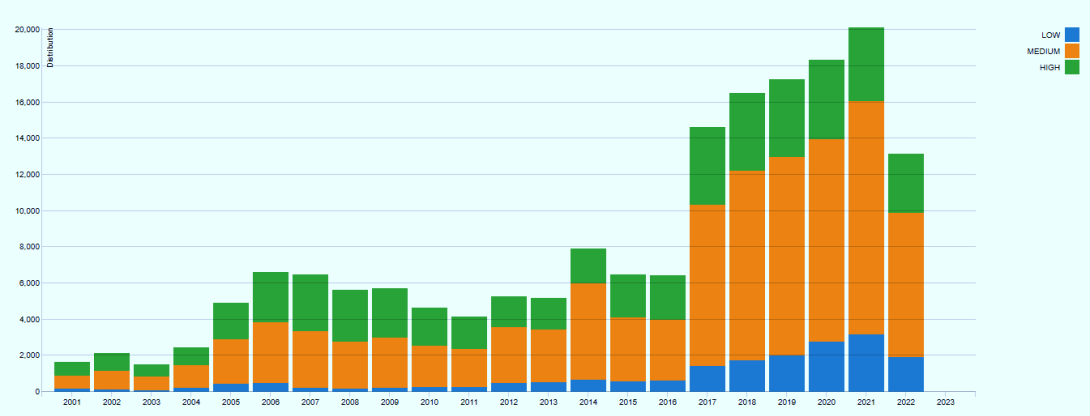
A combinación destes enfoques permite **evolucionar dende unha avaliación baseada exclusivamente na gravidade técnica cara a unha priorización baseada en risco,** máis coherente coa realidade dos entornos industriais.

Este enfoque non pretende substituír CVSS, senón situar a súa puntuación dentro dun marco máis amplo, no que a toma de decisións se apoia no contexto, na ameaza real e nos obxectivos de negocio.

4.4 Alternativas

Como punto de arranque desta subsección, resulta ilustrativo recorrer á **visualización histórica da distribución de severidade CVSS publicada pola NVD (National**

Vulnerability Database) do NIST (national Institute of Standards and Technology) americano, aínda que estea baseada en **CVSS v2**. Esta gráfica amosa de maneira clara unha tendencia sostida no tempo: **o volume total de CVE publicadas é moi elevado** e, dentro delas, unha porcentaxe significativa concéntrase en rangos de **severidade media e alta** [6][7].



Distribución de severidades CVSS no tempo. Fonte: NIST (2022)

Esta realidade ten implicacións prácticas directas para a xestión da ciberseguridade, especialmente en **entornos industriais ICS/OT**. Mesmo asumindo un programa de parcheo maduro, con recursos dedicados e procesos ben definidos, resulta **materialmente imposible** aplicar parches a todas as vulnerabilidades de severidade media ou alta segundo CVSS, mantendo ao mesmo tempo a estabilidade operativa, a seguridade funcional e a continuidade do proceso.

En entornos industriais, onde os ciclos de actualización son longos, as xanelas de mantemento limitadas e o custo dun cambio non planificado é elevado, pretender manter unha infraestrutura "libre de vulnerabilidades" dende unha lectura puramente cuantitativa de CVSS non é realista. A gráfica evidencia que o problema non é puntual nin circunstancial, senón **estrutural**: **o ritmo de aparición de vulnerabilidades supera amplamente a capacidade de remediación directa.**

Este feito obriga, necesariamente, a adoptar **estratexias de priorización**, nas que a severidade CVSS constitúe só un elemento máis do proceso de decisión. A xestión eficaz require incorporar criterios adicionais que permitan distinguir que vulnerabilidades representan un **risco real e inmediato** para o entorno industrial e cales poden ser tratadas de forma diferida, mitigadas mediante controis compensatorios ou mesmo aceptadas temporalmente.

A partir desta constatación, esta sección abordará enfoques que permiten ir máis aló de CVSS, incorporando información sobre explotación real, probabilidade, contexto

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027

operativo e impacto no proceso, co obxectivo de construír modelos de priorización máis realistas e accionables para entornos ICS/OT.

4.4.1 KEV (Known Exploited Vulnerabilities)

4.4.1.1 Introdución

O **KEV (Known Exploited Vulnerabilities)** [8] é un catálogo público que recolle vulnerabilidades para as cales existe **evidencia confirmada de explotación activa no mundo real**. A súa finalidade principal é axudar ás organizacións a **priorizar accións de mitigación** centrándose naquelas vulnerabilidades que xa están a ser empregadas por actores maliciosos, e que, polo tanto, representan un risco inmediato.

Este catálogo está **xestionado pola Cybersecurity and Infrastructure Security Agency (CISA)** [9], a axencia federal dos Estados Unidos responsable da protección das infraestruturas críticas e da coordinación nacional en materia de ciberseguridade. O KEV forma parte das iniciativas de CISA orientadas a mellorar a xestión do risco a escala sistémica, indo máis aló de métricas puramente teóricas ou técnicas.

Dende un punto de vista operativo, o KEV introduce un criterio fundamental que complementa CVSS: **a explotación real**. Mentres que CVSS describe a severidade potencial dunha vulnerabilidade, o KEV responde á pregunta de se esa vulnerabilidade **xa está a ser utilizada activamente en ataques**, independentemente da súa puntuación CVSS.

O catálogo KEV publícase e mantense de forma continua no sitio web oficial de CISA, onde se pode consultar a listaxe actualizada de vulnerabilidades incluídas. Adicionalmente, CISA integra o KEV no seu ecosistema máis amplo de información sobre vulnerabilidades e alertas, dispoñible no seu portal institucional.

A relevancia do KEV resulta especialmente notable en **entornos ICS/OT**, onde a capacidade de parcheo é limitada e onde resulta crítico identificar con rapidez aquelas vulnerabilidades que representan unha ameaza inmediata para a operación. Ao basearse en explotación confirmada, o KEV permite establecer un **primeiro filtro de urxencia**, reducindo o volume de vulnerabilidades a xestionar e facilitando unha toma de decisións máis pragmática e aliñada co risco real.

4.4.1.2 Formato

O **catálogo KEV** publícase cun **formato estruturado e estandarizado**, deseñado para facilitar a súa interpretación operativa e a súa integración en procesos de xestión de vulnerabilidades. Cada entrada do catálogo corresponde a unha vulnerabilidade

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

concreta para a cal existe evidencia confirmada de explotación activa, e inclúe un conxunto de campos orientados á toma de decisións.

De maneira xeral, cada rexistro do KEV preséntase cun **formato de tipo imprimible, CSV ou JSON** [10], pensado para o seu tratamento automatizado e a súa integración en ferramentas de xestión de vulnerabilidades. Así, ademais da consulta en liña, CISA pon á disposición unha **versión descargable e imprimible do catálogo KEV**, especialmente útil para o seu uso en entornos desconectados, revisións periódicas, comités de seguridade ou procedementos documentais.

Cada entrada ou rexistro do KEV, inclúe un conxunto de campos ben definidos:

Campo	Valor
cveID	Identificador CVE único da vulnerabilidade.
vendorProject	Fabricante ou proxecto responsable do produto afectado.
product	Produto ou compoñente concreto impactado pola vulnerabilidade.
vulnerabilityName	Denominación resumida da vulnerabilidade.
dateAdded	Data na que a vulnerabilidade foi incorporada ao catálogo KEV, indicando o momento a partir do cal existe evidencia de explotación activa.
shortDescription	Descrición concisa do problema e do seu impacto potencial.
requiredAction	Acción recomendada por CISA para mitigar o risco (aplicación de parches, mitigacións ou retirada do produto).
dueDate	Prazo límite recomendado para a mitigación, empregado como referencia de urxencia.
knownRansomwareCampaignUse	Indicador sobre o uso coñecido da vulnerabilidade en campañas de ransomware.
notes	Referencias adicionais a avisos do fabricante, análises técnicas ou fontes externas relevantes.
cwes	Lista de categorías CWE asociadas á vulnerabilidade.

Estrutura dos rexistros do KEV. Fonte: elaboración propia (2026)

Como se ve, permiten comprender non só a natureza técnica da vulnerabilidade, senón tamén a súa **relevancia operativa e temporal**, facilitando a súa utilización como criterio de priorización en programas de xestión baseados en risco.

Este formato facilita que o KEV poida empregarse como un **primeiro filtro de priorización**, especialmente útil en entornos industriais nos que resulta inviable abordar de forma simultánea todas as vulnerabilidades publicadas.

4.4.1.3 Subscripción a actualizacións e novidades

Dado que o catálogo KEV se **actualiza de maneira continua**, coa incorporación de novas vulnerabilidades segundo se detecta explotación activa, resulta especialmente recomendable manter un mecanismo de seguimento das novidades.

CISA ofrece a posibilidade de **subscribirse ás notificacións oficiais**, de forma que as organizacións poidan recibir alertas cando se producen actualizacións relevantes do catálogo. Esta subscrición permite anticipar accións de análise e priorización sen depender exclusivamente de revisións manuais [11].

4.4.1.4 Construcción do KEV

O **catálogo KEV (Known Exploited Vulnerabilities)** non é o resultado dun cálculo algorítmico nin dunha puntuación automática, senón dun **proceso de análise continua baseado en intelixencia de ameazas, evidencias de explotación real e coordinación interinstitucional**. A súa xeración responde a unha lóxica cualitativa e operativa, orientada a identificar vulnerabilidades que xa están a ser empregadas de maneira efectiva por actores maliciosos.

Dende o punto de vista conceptual, o KEV baséase nun principio fundamental: **unha vulnerabilidade só se incorpora ao catálogo cando existe evidencia fiable de explotación activa no mundo real**.

CISA xera e mantén o catálogo KEV a partir dunha combinación de **múltiples fontes de información**, entre as que se inclúen:

- **Intelixencia de ameazas gobernamental**, procedente de axencias federais, equipos de resposta a incidentes e organismos de seguridade.
- **Información compartida por provedores de tecnoloxía e fabricantes**, a través de procesos coordinados de divulgación de vulnerabilidades.
- **Datos de explotación observada**, recollidos en incidentes reais, campañas activas ou análises forenses.
- **Colaboración con socios internacionais e sectoriais**, especialmente no ámbito das infraestruturas críticas.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

- **Aportacións do ecosistema de ciberseguridade**, incluíndo investigacións públicas contrastadas e informes de alta confianza.

Este enfoque garante que a inclusión dunha vulnerabilidade no KEV responda a **evidencias verificadas**, evitando a dependencia exclusiva de predicións ou modelos probabilísticos.

A decisión de incorporar unha vulnerabilidade ao catálogo KEV segue un proceso de **avaliación humana especializada**, no que se analizan factores como:

- existencia de explotación confirmada,
- alcance e reproducibilidade da explotación,
- relevancia para infraestruturas críticas e servizos esenciais,
- impacto observado ou potencial en entornos reais.

Unha vez confirmada a explotación activa, a vulnerabilidade engádese ao catálogo xunto cun **prazo recomendado de mitigación** (obrigatorio para algunhas entidades por normativa, como veremos), que serve como referencia temporal para a priorización das accións defensivas.

O KEV é un catálogo **dinámico e vivo**, que se actualiza de maneira continua a medida que se detectan novas explotacións. Non existe unha cadencia fixa de publicación: as entradas incorpóranse en función da aparición de nova información relevante.

Esta natureza dinámica implica que o KEV non debe interpretarse como unha listaxe exhaustiva de vulnerabilidades perigosas, senón como un **conxunto priorizado das que representan unha ameaza inmediata** nun momento dado.

4.4.1.5 Uso e importancia

Segundo a propia axencia, o catálogo debe empregarse como unha **lista de referencia prioritaria** para identificar aquelas vulnerabilidades para as cales existe constancia de explotación activa en contornos reais, servindo como punto de partida mínimo para a acción correctiva [12].

CISA recomenda integrar o KEV de maneira sistemática nos procesos habituais de xestión de vulnerabilidades e riscos.

- En primeiro lugar, as organizacións deben **inventariar e identificar os activos** expostos ás vulnerabilidades incluídas no catálogo, determinando se os sistemas afectados forman parte do seu contorno operativo. A continuación, debe

realizarse unha **avaliación de exposición real**, tendo en conta o contexto técnico e operativo no que se atopan eses activos.

- Unha vez identificada a afectación, CISA indica que as vulnerabilidades listadas no KEV deben ser **priorizadas de forma inmediata**, independentemente doutras métricas como a puntuación CVSS. Para cada vulnerabilidade, débense executar as **accións recomendadas** polo propio catálogo, que poden incluír a aplicación de parches oficiais, a implantación de mitigacións compensatorias cando o parcheo non é viable, ou a retirada do produto vulnerable se non existe unha solución adecuada.
- Adicionalmente, CISA subliña a importancia de **respectar os prazos de remediación** asociados a cada entrada do KEV, empregándoos como referencia de urxencia na planificación das actuacións. O seguimento continuo do catálogo, que se actualiza de forma regular, resulta clave para incorporar novas vulnerabilidades explotadas e axustar as prioridades de resposta.
- Finalmente, o KEV debe empregarse como un **complemento aos modelos tradicionais de xestión do risco**, achegando un criterio baseado en intelixencia de ameazas e explotación confirmada. Deste xeito, o catálogo contribúe a focalizar recursos limitados nas ameazas máis relevantes e a reducir de forma efectiva a superficie de risco das organizacións.

No contexto dos Estados Unidos, o catálogo KEV adquiriu unha relevancia singular ao converterse nun **instrumento de obrigado cumprimento** para determinados organismos federais. A través da *Binding Operational Directive 22-01 (BOD 22-01)*, CISA estableceu a obrigatoriedade de mitigar as vulnerabilidades incluídas no KEV dentro de **prazos estritos e predefinidos**, en función do risco asociado a cada entrada [13].

Esta directiva é de aplicación ás axencias civís federais do poder executivo, que están **legalmente obrigadas a identificar os activos afectados polas vulnerabilidades KEV e a executar as accións correctivas requiridas antes da data límite indicada no catálogo**. O incumprimento destes prazos pode dar lugar a accións de supervisión e a requirimentos adicionais por parte das autoridades competentes.

A adopción do KEV como referencia regulatoria supón un **cambio de paradigma na xestión de vulnerabilidades**, ao introducir criterios baseados en explotación real e prazos de remediación obrigatorios. Aínda que esta obriga legal non é directamente aplicable fóra do ámbito regulado nos Estados Unidos, o modelo establecido por CISA

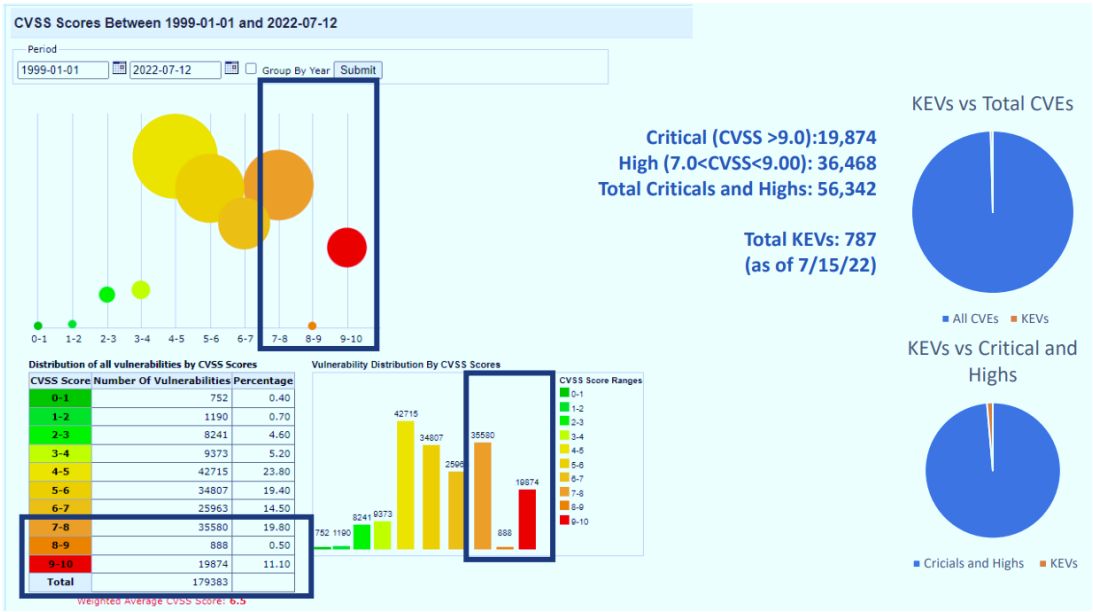
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

constitúe unha **boa práctica de referencia internacional**, especialmente para organizacións con sistemas críticos, industriais ou de alta exposición ao risco.

Neste sentido, o catálogo KEV non só actúa como unha ferramenta técnica, senón tamén como un **mecanismo de gobernanza do risco**, que aliña a intelixencia de ameazas, a xestión operativa e o cumprimento normativo baixo un enfoque claro de priorización e urxencia.

Un dos principais valores engadidos do KEV reside na súa capacidade para **reducir drasticamente o universo de vulnerabilidades sobre o que deben focalizarse os esforzos de remediación**. Segundo a análise presentada por CISA no marco da Binding Operational Directive 22-01 en 2022, o emprego do KEV permite pasar dun conxunto inicial de decenas de miles de vulnerabilidades potencialmente relevantes a un subconxunto moito máis reducido, baseado en evidencia real de explotación [14].

En concreto, no momento do estudo de referencia, o número total de vulnerabilidades clasificadas como **Críticas e Altas segundo CVSS** superaba as **56.000 entradas**. Porén, ao aplicar o filtro do KEV —é dicir, considerar unicamente aquelas vulnerabilidades para as cales existía constancia de explotación activa—, o universo reducíase a **787 vulnerabilidades coñecidas como explotadas**. Isto supón unha **redución do 98.6 %** do conxunto inicial de vulnerabilidades de severidade media e alta que, en teoría, poderían requirir atención.

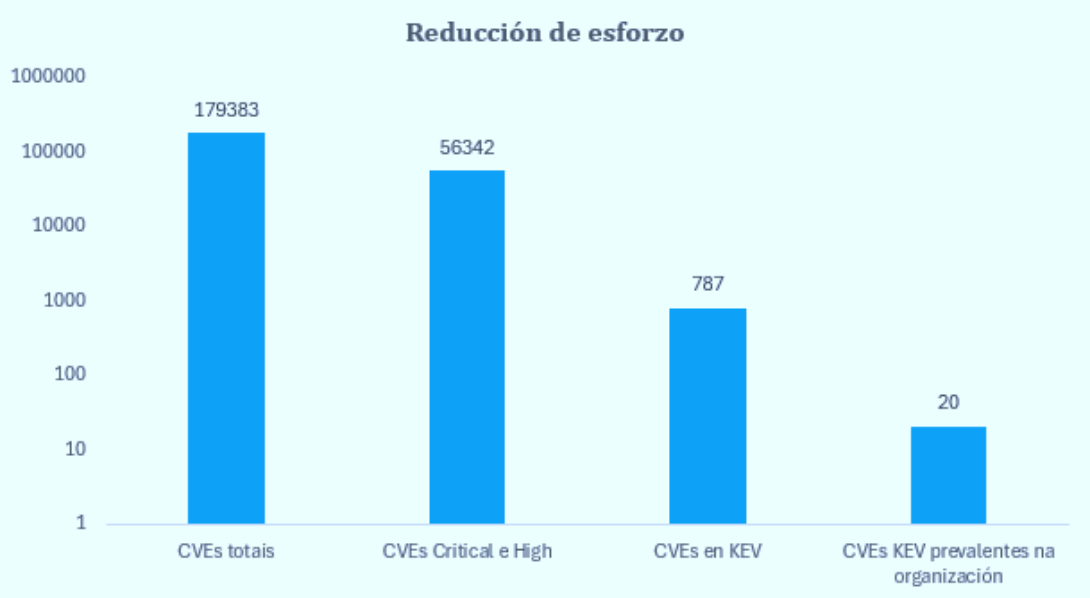


Redución drástica de CVEs de severidade alta e crítica no KEV. Fonte: CISA (2022)

Esta redución ten un impacto directo e moi significativo no nivel de esforzo operativo que deben asumir os equipos de seguridade. Ao limitar o foco a un

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027

subconxunto moito máis manexable, resulta posible asignar recursos de maneira máis eficiente, acurtar os tempos de resposta e priorizar accións con maior impacto real na redución do risco. Tal e como ilustra a gráfica, esta aproximación transforma un problema estruturalmente inabarcable nun conxunto de actuacións concretas e executables, mesmo en contornos empresariais complexos. **Pasamos dun universo total de mais de 179.000 CVEs publicados no momento do estudio, a ter que accionar a mitigación de únicamente uns 20** dentro da organización (dato estimado). O cambio é considerable, como se ve na figura de escala logarítmica.



Redución do número de CVEs a xestionar na organización co uso de KEV. Fonte: CISA (2022)

Pero non todo son boas noticias. Aínda que o KEV permite unha redución moi significativa do universo de vulnerabilidades prioritarias, o catálogo non é estático. A presión constante exercida polos ciberdelincuentes e a rápida explotación de novas vulnerabilidades fixeron que, en **2025**, o número de entradas do KEV experimentase un **incremento interanual próximo ao 20 %, con 245 novas vulnerabilidades**, o que supón unha tasa de crecemento aproximadamente un 30% superior ós dous anos precedentes [15].

Este crecemento parecería consecuencia directa da maior sofisticación dos actores maliciosos e da súa capacidade para explotar vulnerabilidades nunha fase cada vez máis temperá, quizais apoiados en sistemas semiautomáticos de intelixencia artificial. A pesar deste incremento, o KEV continúa representando un subconxunto moi reducido en comparación co total de vulnerabilidades publicadas anualmente, mantendo así o seu valor como mecanismo de priorización efectiva.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

Este contexto pon de manifesto dúas realidades complementarias: por unha banda, a **necesidade de empregar mecanismos como o KEV para conter a carga operativa**; por outra, a importancia de asumir que a xestión de vulnerabilidades é un proceso dinámico, que require seguimento continuo, actualización periódica e capacidade de adaptación fronte á evolución constante do panorama de ameazas.

Finalmente, cómpre salientar que **o enfoque promovido polo catálogo KEV non se limita ao ámbito regulatorio ou institucional**, senón que está xa **plenamente integrado en solucións comerciais de xestión de vulnerabilidades e risco**. Plataformas comerciais de xestión de vulnerabilidades como Tenable, incorporan explicitamente as **datas límite de remediación establecidas por CISA no marco da BOD 22-01** como criterio de priorización e agrupación de vulnerabilidades [16]. Isto evidencia que o prazo de mitigación imposto polo KEV constitúe un **factor operativo clave na avaliación do risco real**, xunto con métricas tradicionais como CVSS ou a exposición do activo. A adopción deste criterio por ferramentas profesionais, reforza a idea de que o KEV representa hoxe unha **referencia práctica e validada polo mercado** para orientar os esforzos de corrección cara ás vulnerabilidades cun impacto máis inmediato e probado en contornos reais.

4.4.2 Now/Next/Never

4.4.2.1 Introdución

A necesidade de dispoñer de **modelos de priorización claros, operativos e adaptados ao risco real** en contornos industriais levou, nos últimos anos, ao desenvolvemento de enfoques que van máis alá das métricas clásicas de severidade. Neste contexto insírese a estratexia **Now / Next / Never**, hoxe amplamente asociada ao fabricante Dragos como veremos, pero cuxa base conceptual procede de traballos previos no ámbito da ciberseguridade industrial e da xestión do risco.

Un dos traballos de referencia iniciais neste ámbito é o documento impulsado principalmente por **Allan Manion** no marco do Software Engineering Institute (SEI), no que se aborda a necesidade de **priorizar a remediación de vulnerabilidades en función do impacto operativo, o contexto do activo e a factibilidade da mitigación**, especialmente en sistemas ciberfísicos e industriais [17].

Este enfoque supón un afastamento explícito da priorización automática baseada unicamente en métricas técnicas, propoñendo criterios como:

- a función crítica do activo no proceso industrial,

- as consecuencias operativas dun fallo ou indispoñibilidade,
- a probabilidade real de explotación,
- e as restricións operativas para aplicar cambios ou parches.

Estes principios sentaron as bases conceptuais para modelos posteriores máis simplificados e orientados á toma de decisións operativas.

Sobre esta base, **Dragos** consolidou e popularizou o enfoque de **xestión de vulnerabilidades baseada en risco** especificamente adaptado a contornos **ICS/OT**. Nun artigo de referencia, a compañía expón **cinco razóns fundamentais polas que este enfoque resulta crítico en OT** [18], que poden resumirse do seguinte xeito:

1. **Priorización efectiva fronte a un volume inabarcable de vulnerabilidades.** Nun contexto de recursos limitados e listaxes de vulnerabilidades cada vez máis extensas, resulta esencial identificar cales son realmente críticas no contexto concreto dos equipos, procesos e operacións industriais, evitando unha aproximación indiscriminada.
2. **Continuidade operativa como requisito esencial.** Os métodos tradicionais de parcheo adoitan requirir paradas de sistema, algo que non sempre é viable en contornos OT. A diferenza dos sistemas IT, os sistemas ciberfísicos xestionan procesos físicos e resultados operativos, polo que non poden ser parcheados de forma frecuente nin sen unha planificación rigorosa.
3. **Necesidade de comprensión contextual do risco.** A avaliación do risco específica de OT permite unha análise máis precisa do impacto real das vulnerabilidades, tendo en conta o rol do activo, o proceso ao que dá soporte e as consecuencias operativas dunha posible explotación.
4. **Asignación eficiente de recursos de ciberseguridade.** Ao concentrar os esforzos nas vulnerabilidades de maior risco real, as organizacións poden optimizar o uso dos seus recursos técnicos e humanos, mellorando a eficacia global das accións de seguridade.
5. **Cumprimento normativo e esixencias regulatorias.** Moitos marcos reguladores esixen ás organizacións demostrar e reportar prácticas efectivas de xestión de vulnerabilidades (como vimos coas axencias federais americanas, ou en España con ENS ou NIS2), o que reforza a necesidade de enfoques estruturados, xustificables e baseados en risco.

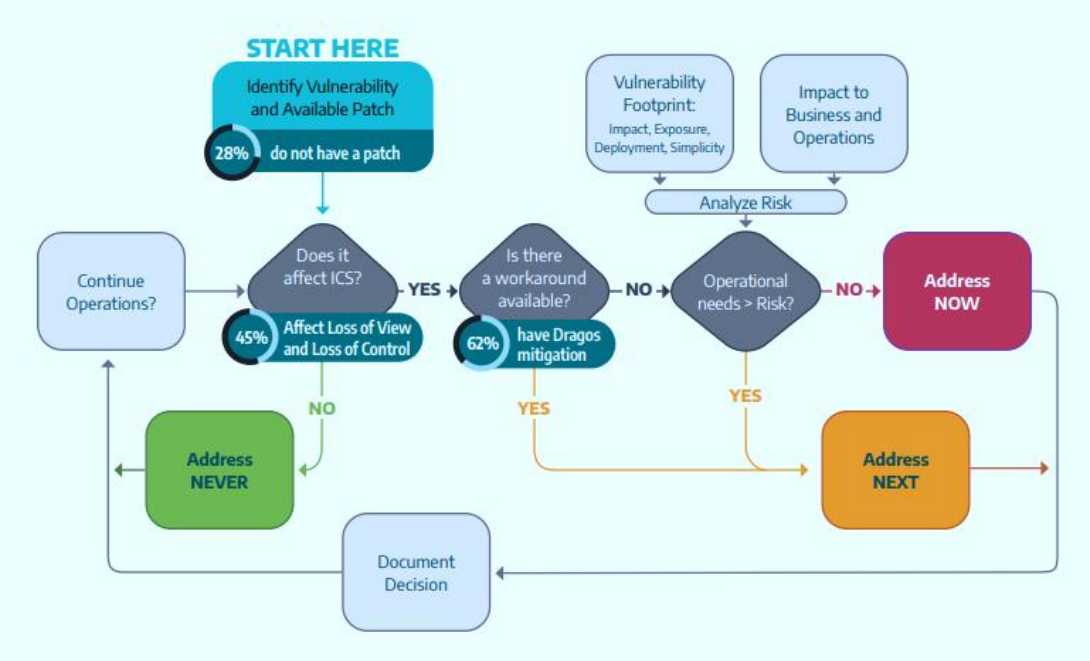
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

Este conxunto de argumentos reforza a necesidade de empregar modelos de priorización que integren risco operativo e contexto industrial, e non só métricas técnicas illadas.

4.4.2.2 Estratexia

Neste marco conceptual, Dragos introduce formalmente a estratexia **Now / Next / Never** no seu *whitepaper* sobre xestión de vulnerabilidades baseada en risco en contornos OT [17][18][19]. Este modelo propón unha **clasificación clara e accionable das vulnerabilidades** segundo a urxencia e a conveniencia da súa remediación.

A lóxica da estratexia inspírase no **árbore de decisión de parcheo urxente do Department of Homeland Security (DHS) americano**, empregado historicamente para determinar cando unha vulnerabilidade debe ser mitigada de forma inmediata, cando pode ser planificada ou cando resulta máis prudente aceptar o risco [20].



Árbore de decisión de parcheo urxente do DHS. Fonte: Dragos (2024)

Este modelo de referencia foi xa presentado no boletín anterior de ciberalertas (*Ciberalertas – I*) deste Observatorio da AMTEGA [4].

A estratexia Now / Next / Never traduce ese enfoque de decisión a un formato sinxelo, comprensible e operativo para equipos de seguridade e operacións industriais, facilitando a súa adopción en contornos reais.

- As vulnerabilidades clasificadas como **Now** son aquelas que afectan a activos críticos, resultan razoablemente explotables e non contan con mitigacións

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

compensatorias eficaces. Trátase de situacións que poden derivar nun control inmediato de sistemas clave ou nunha perda de visibilidade crítica, polo que requiren actuación prioritaria. Isto non implica necesariamente parchear de forma inmediata, senón **reducir canto antes a explotabilidade** mediante medidas técnicas e planificar o parcheo na primeira xanela segura dispoñible.

- Na categoría **Next** sitúanse vulnerabilidades relevantes, pero cunha menor probabilidade de causar impacto grave ou parcialmente mitigadas pola arquitectura existente. Estas vulnerabilidades deben xestionarse de forma planificada, integrándose en campañas de mellora progresiva que combinen reforzo da arquitectura, redución da exposición e parcheo cando as condicións operativas o permitan.
- Finalmente, a categoría **Never** agrupa vulnerabilidades que, no contexto específico da organización, non representan un risco significativo a curto nin medio prazo. Isto pode deberse a que afectan a funcionalidades non utilizadas, configuracións inexistentes ou activos efectivamente illados. Clasificalas como Never non supón ignoralas, senón **documentar e xustificar a decisión**, mantendo unha vixilancia suficiente para revisala se cambian as condicións operativas.

A continuación, sintetízanse os escenarios de priorización descritos.

Categoría	Criterios principais	Risco operativo	Resposta recomendada
Now	Activo crítico; explotabilidade razoable; ausencia de mitigacións compensatorias eficaces	Alto / inmediato	Actuar con máxima prioridade: reducir rapidamente a explotabilidade (configuracións, segmentación, regras de acceso) e planificar o parcheo na primeira xanela segura
Next	Impacto posible pero menos probable; mitigación parcial pola arquitectura existente	Medio	Xestión planificada: reforzo progresivo da arquitectura e aplicación de parches durante mantementos programados

Never	Impacto improbable no contexto actual; funcionalidades non usadas ou activos illados	Baixo	Non parchear en condicións normais; documentar a decisión, xustificala por risco e manter monitorización para reavaliación futura

Táboa resumo da estratexia Now/Next/Never. Fonte: elaboración propia (2026)

Este enfoque complementa de forma natural métricas como **CVSS** e mecanismos como o **catálogo KEV**, ao introducir o **impacto operativo e o contexto industrial** como factores determinantes na toma de decisións.

4.4.3 EPSS (Exploit Prediction Scoring System)

4.4.3.1 Introducción

A crecente dificultade para xestionar volumes moi elevados de vulnerabilidades levou á aparición de enfoques complementarios ás métricas clásicas de severidade. Entre eles destaca o **Exploit Prediction Scoring System (EPSS)**, un modelo estatístico deseñado para **estimar a probabilidade de que unha vulnerabilidade sexa explotada no mundo real**, achegando unha dimensión preditiva á xestión do risco.

EPSS proporciona, para cada vulnerabilidade identificada mediante un CVE, unha **magnitude numérica entre 0 e 1**, que representa a probabilidade diaria de que esa vulnerabilidade sexa explotada nun horizonte temporal de 30 días. A diferenza de CVSS, que mide a severidade técnica dun fallo, EPSS céntrase en **anticipar o comportamento dos atacantes**, permitindo priorizar aquelas vulnerabilidades máis propensas a ser utilizadas de forma activa.

Explicadas as súas xeneralidades na descrición realizada por INCIBE-CERT [21], EPSS constitúe unha evolución significativa na xestión de vulnerabilidades, ao permitir **ordenar listas extensas de CVEs en función da súa probabilidade de explotación**, reducindo o esforzo necesario para identificar cales requiren unha atención prioritaria. Destacar que nese artigo non se considera a versión máis recente do modelo, **EPSS v4**, que introduce melloras na capacidade preditiva e na estabilidade das estimacións.

O modelo EPSS ten a súa orixe nun traballo de investigación presentado na conferencia **Black Hat USA 2019**, no que se propuxo por primeira vez un sistema de puntuación preditiva baseado en técnicas estatísticas e aprendizaxe automática para estimar a explotación de vulnerabilidades. Este traballo sentou as bases conceptuais dun enfoque que se afastaba da avaliación puramente técnica e introducía variables relacionadas coa evidencia histórica, o contexto e o comportamento dos atacantes [22].

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

Dende aquela, o modelo foi evolucionando progresivamente ata converterse nun estándar de facto para a estimación probabilística da explotación de vulnerabilidades.

4.4.3.2 Gobernanza e mantemento do EPSS

Na actualidade, EPSS é **mantido e xestionado por FIRST (Forum of Incident Response and Security Teams)**, unha organización internacional sen ánimo de lucro que agrupa equipos de resposta a incidentes (CSIRTs, CERTs e outras entidades de referencia en ciberseguridade a nivel mundial). FIRST é tamén responsable doutros estándares amplamente adoptados, como CVSS.

FIRST publica de maneira aberta o **modelo EPSS**, **a súa metodoloxía e os conxuntos de datos empregados**, permitindo transparencia e revisión continua. A documentación oficial do modelo, dispoñible no portal de FIRST, describe en detalle os **factores empregados para a estimación da probabilidade**, así como as métricas de avaliación do rendemento do modelo, incluíndo parámetros de **cobertura (*recall*)** e **eficiencia (*precision*)**, que permiten avaliar o equilibrio entre detección de vulnerabilidades explotadas e redución de falsos positivos [23].

Hai que subliñar que **EPSS non está deseñado para substituír nin CVSS nin mecanismos como o catálogo KEV, senón para complementalos**. Mentres CVSS mide impacto potencial e KEV achega evidencia de explotación confirmada, EPSS sitúase nun punto intermedio, permitindo **anticipar que vulnerabilidades teñen maior probabilidade de ser explotadas no futuro próximo**.

Neste sentido, **EPSS resulta especialmente útil como ferramenta de filtrado inicial e priorización dinámica, servindo de apoio á toma de decisións cando os recursos son limitados e o volume de vulnerabilidades supera a capacidade de resposta** inmediata das organizacións.

4.4.3.3 Uso e priorización

A utilidade práctica de EPSS como estratexia de priorización baséase non só no modelo estatístico en si, senón tamén na **dispoñibilidade aberta e actualizada dos seus datos**, así como na existencia de guías de uso que orientan a súa integración con outras métricas e enfoques.

FIRST publica de maneira aberta os **datos EPSS recalculados de forma periódica**, accesibles a través dun ficheiro descargable que contén, para cada vulnerabilidade:

- a identificación mediante **o seu CVE**,
- a **probabilidade estimada de explotación** nunha xanela temporal de 30 días,

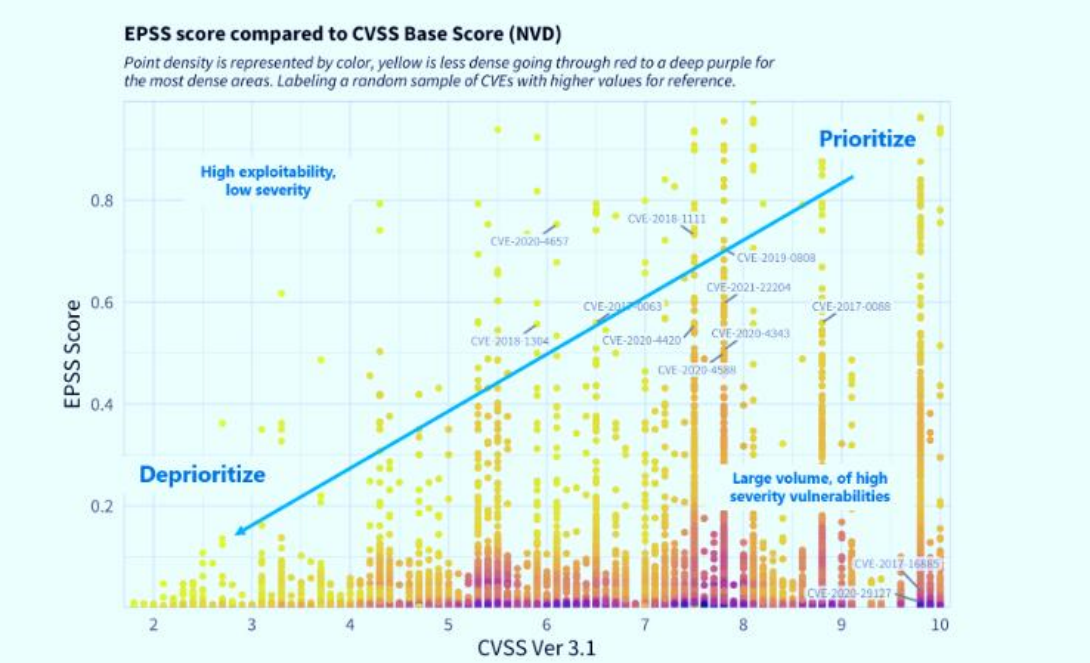
- e o **percentil de risco** no que se sitúa esa vulnerabilidade respecto do conxunto total.

Este conxunto de datos está dispoñible nun formato estruturado e facilmente integrable en procesos automatizados, permitindo ás organizacións incorporar EPSS nos seus fluxos de xestión de vulnerabilidades e nas súas ferramentas internas [24].

Adicionalmente, **FIRST ofrece acceso aos mesmos datos mediante unha API pública**, o que facilita a súa integración directa con plataformas de xestión de vulnerabilidades, SIEMs ou sistemas de análise propios, sen necesidade de descargar ficheiros completos de forma manual [25].

Este organismo publica tamén unha **guía de uso oficial de EPSS** na que se aborda como empregar este modelo de maneira eficaz, especialmente en combinación con CVSS [26]. A guía destaca novamente que EPSS non debe empregarse illadamente, senón como un **complemento que permite priorizar dentro de rangos de severidade similares**.

A aproximación recomendada consiste en empregar CVSS para **filtrar vulnerabilidades segundo o impacto potencial**, e aplicar posteriormente EPSS para **ordenar e priorizar aquelas cunha maior probabilidade de explotación**. Este enfoque permite reducir significativamente o número de vulnerabilidades que requiren atención inmediata, mellorando a eficiencia operativa.



Correlación entre puntuacións EPSS e CVSS. Fonte: First (2021)

Para rematar e ter unha visión de conxunto do visto ata o de agora, na súa documentación técnica FIRST reflexiona os **pros e contras de distintos enfoques de**

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027

priorización de vulnerabilidades, en función do enfoque, baseado en probabilidade, percentís ou clusterización [27]. Estes enfoques poden resumirse comparativamente do seguinte xeito:

Enfoque	Descrición	Vantaxes principais	Limitacións
Baseado en probabilidade (EPSS)	Prioriza segundo a probabilidade estimada de explotación nun horizonte temporal definido	Permite anticipar explotación real; alta granularidade; priorización dinámica	Pode resultar menos intuitivo; require interpretación estatística
Baseado en percentís (CVSS relativo)	Clasifica vulnerabilidades segundo a súa posición relativa en termos de severidade	Fácil de entender; amplamente adoptado	Non reflicte explotación real nin contexto operativo
Baseado en Clusterización (CVSS estándar, ~Now/Next/Never)	Agrupa vulnerabilidades en categorías de prioridade ~(alta/media/baixa)	Simplicidade operativa; facilita a toma de decisións	Perda de detalle; dependencia de criterios subxectivos

Distintos enfoques de xestión de vulnerabilidades. Fonte: elaboración propia (2026)

Este último enfoque de clusterización pode equipararse, dende unha perspectiva operativa, a modelos como **Now / Next / Never**, que traducen métricas técnicas e probabilísticas a decisións accionables para os equipos de seguridade e operacións.

En conxunto, a combinación destes enfoques permite ás organizacións adaptar a súa estratexia de priorización ao seu nivel de madurez, capacidade operativa e perfil de risco, mantendo un equilibrio entre precisión analítica e practicidade.

4.4.4 Enfoque de solucións comerciais

As **ferramentas comerciais de xestión de vulnerabilidades** incorporan hoxe modelos de priorización que van máis aló da simple enumeración de CVEs ou da súa severidade técnica. Solucións como as de Qualys, Tenable ou Rapid7 integran enfoques propios que combinan métricas tradicionais, intelixencia de ameazas, contexto do activo e criterios de risco operativo, co obxectivo de **axudar ás organizacións a decidir onde concentrar os seus esforzos de remediación**.

Esta sección ofrece unha visión sintética dalgúns destes enfoques (co grado de detalle que se puido obter tendo en conta que estas entidades lóxicamente tratan de preservar a sua propiedade intelectual e industrial), ilustrando como os fabricantes trasladan

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

conceptos como a priorización baseada en risco, a explotación activa ou o impacto no negocio a **mecanismos prácticos integrados nas súas plataformas**, facilitando a súa adopción en contornos reais e con recursos limitados.

4.4.4.1 VMDR (Vulnerabity Management Detection and Response)

Como se indicou, as solucións comerciais de xestión de vulnerabilidades evolucionaron cara a enfoques máis integrados e orientados ao risco. Neste contexto sitúase **VMDR (Vulnerability Management, Detection and Response)**, a plataforma de Qualys.

Esta combina capacidades clásicas de escaneo de vulnerabilidades con funcionalidades avanzadas de **detección continua, correlación de sinais de ameaza e resposta**, permitindo pasar dun modelo reactivo a un enfoque máis dinámico. A plataforma integra información procedente de múltiples fontes —activos, configuracións, intelixencia de ameazas e exposición— para ofrecer unha visión contextualizada do risco asociado a cada vulnerabilidade [28].

Un dos elementos clave de VMDR é que a priorización non se basea exclusivamente na severidade CVSS, senón que introduce unha **avaliación de risco orientada ao negocio**, na que se teñen en conta factores como a criticidade do activo, a súa exposición real, a existencia de exploits coñecidos e a relevancia da vulnerabilidade no contexto operativo da organización.

Emprega un modelo de priorización que busca responder á pregunta práctica e crucial de **que vulnerabilidades deben abordarse primeiro**. Para iso, Qualys introduce puntuacións e indicadores propios que combinan:

- severidade técnica da vulnerabilidade,
- intelixencia de ameazas e evidencia de explotación,
- contexto do activo afectado,
- e impacto potencial no negocio.

Este enfoque permite reducir o volume de vulnerabilidades consideradas críticas dende un punto de vista puramente técnico e focalizar os esforzos de remediación naquelas que **teñen maior probabilidade de materializarse nun risco real**, mellorando a eficiencia dos equipos de seguridade.

No seu whitepaper **"How to Shift from Managing Vulnerabilities to Business-Focused Risk Reduction"**, Qualys expón a necesidade de abandonar unha xestión

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

centrada no número de vulnerabilidades detectadas e evolucionar cara a un modelo orientado á **redución efectiva do risco para o negocio** [29].

Entre as principais ensinanzas deste documento destacan:

- a importancia de **priorizar en función do impacto no negocio**, e non só da severidade técnica;
- a necesidade de **contextualizar as vulnerabilidades** segundo o rol do activo e a súa exposición;
- a conveniencia de empregar **indicadores accionables**, comprensibles tamén para perfís non técnicos;
- e a integración da xestión de vulnerabilidades cos procesos de gobernanza, risco e cumprimento.

Nada inesperado para o lector que veña das seccións anteriores. Este enfoque encaixa de forma natural con outras estratexias de priorización baseadas en risco, como KEV, EPSS ou modelos de clasificación operativa tipo Now / Next / Never, reforzando a idea de que a xestión moderna de vulnerabilidades debe orientarse á toma de decisións informadas e á redución sostida do risco.

4.4.4.2 VPR (Vulnerability Priority Rating)

Novamente no ámbito das solucións comerciais de xestión de vulnerabilidades, **Tenable** desenvolveu o **Vulnerability Priority Rating (VPR)** como un mecanismo avanzado de priorización orientado a identificar aquelas vulnerabilidades que presentan un **maior risco real a curto prazo**. VPR forma parte central das capacidades de xestión de vulnerabilidades de Tenable e está deseñado para superar as limitacións dunha priorización baseada exclusivamente en CVSS.

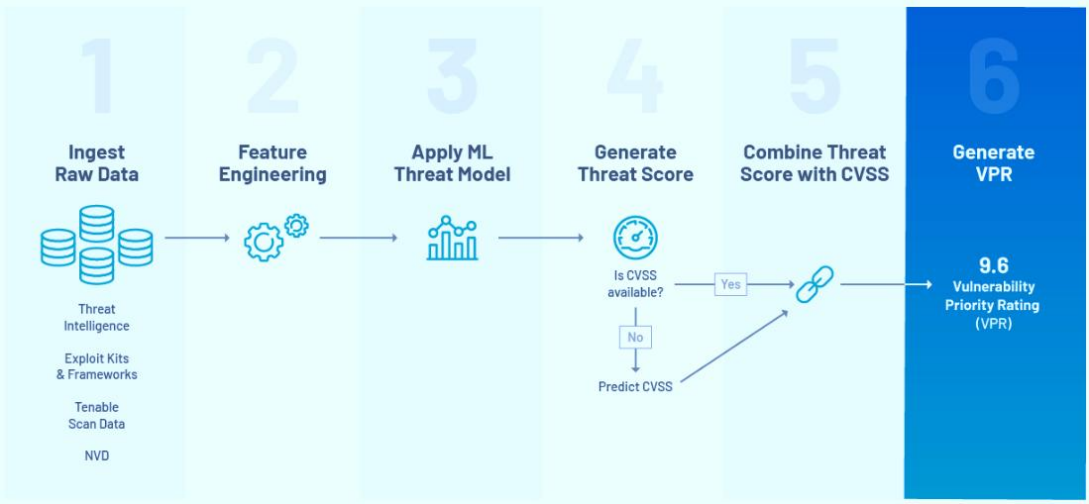
Segundo a documentación, VPR é unha **puntuación dinámica**, recalculada de forma continua, que estima a probabilidade de que unha vulnerabilidade sexa explotada e cause impacto nun horizonte temporal reducido [30].

A puntuación **VPR exprésase nunha escala de 0 a 10**, e constrúese a partir da combinación de múltiples sinais, entre eles:

- a severidade técnica da vulnerabilidade,
- a dispoñibilidade e madurez de exploits,
- a evidencia de explotación activa,

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

- a popularidade e exposición dos activos afectados,
- e a intelixencia de ameazas procedente de múltiples fontes.



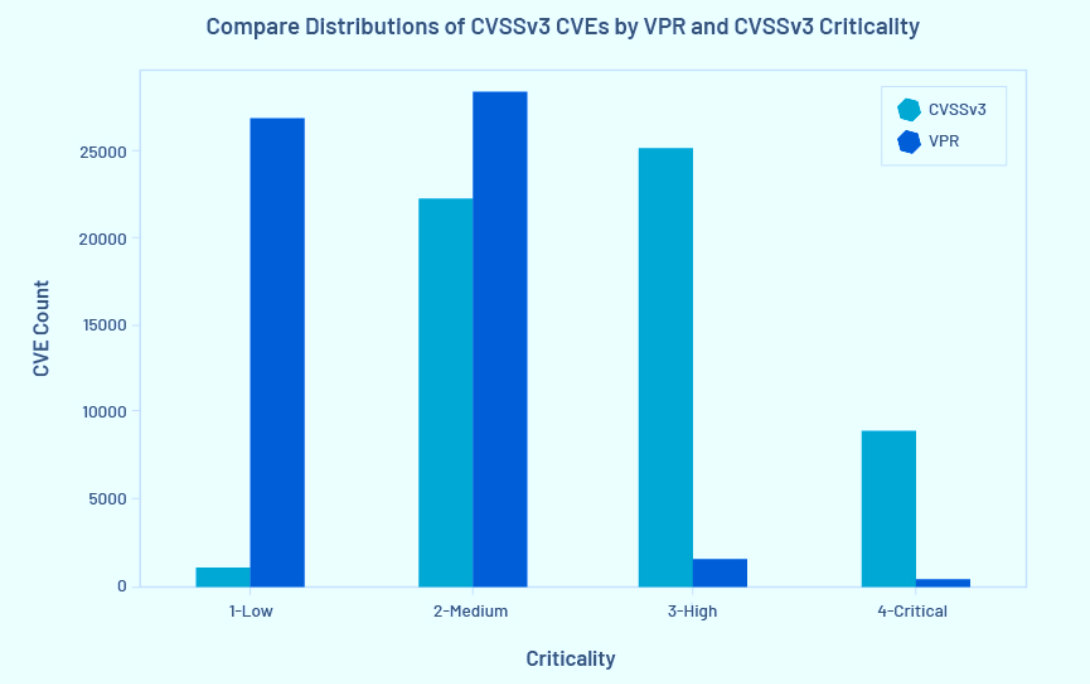
Pseudoproceso de cómputo do VPR. Fonte: Tenable (2020)

Este enfoque permite a Tenable ofrecer unha visión máis axustada ao risco real, priorizando vulnerabilidades que, aínda que non sempre presentan as puntuacións CVSS máis elevadas, teñen unha maior probabilidade de ser explotadas no curto prazo.

A entidade subliña que VPR non pretende substituír CVSS, senón **complementalo cunha dimensión temporal e preditiva**. Mentres CVSS proporciona unha medida estática do impacto potencial dunha vulnerabilidade, VPR introduce unha lóxica dinámica que responde á evolución do contexto de ameazas [31].

Un dos efectos máis relevantes desta diferenza é a **reducción significativa do universo de vulnerabilidades prioritarias**. Segundo datos achegados por Tenable, ao aplicar VPR como criterio principal, o foco de remediación pode reducirse a un **subconxunto moito máis pequeno de vulnerabilidades**, permitindo aos equipos concentrar os seus esforzos nas que presentan maior risco inmediato, fronte a longas listaxes de CVEs clasificadas como altas ou críticas por CVSS.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027



Distribución de CVEs por criticidade en CVSS fronte a VPR. Fonte: Tenable (2020)

Este mecanismo de filtrado resulta especialmente valioso en organizacións con grandes superficies de ataque, onde a capacidade de parcheo é limitada e resulta imprescindible tomar decisións baseadas en risco efectivo.

Nun whitepaper publicado en 2024, Tenable describe diversas **melloras introducidas no modelo VPR**, orientadas a incrementar a súa precisión e utilidade operativa [32]. Entre estas melloras inclúense:

- unha maior integración de sinais de explotación activa,
- o refinamento dos modelos estatísticos empregados,
- e unha mellor diferenciación entre vulnerabilidades con comportamento similar en termos de severidade técnica.

Estas melloras permiten unha priorización máis fina e adaptativa, reforzando o papel de VPR como ferramenta clave para a toma de decisións en xestión de vulnerabilidades.

En conxunto, VPR é outra mostra de como as solucións comerciais están a incorporar **modelos dinámicos e baseados en intelixencia de ameazas** para complementar métricas estándar como CVSS, aliñándose con enfoques máis amplos de xestión do risco e priorización efectiva.

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027

4.4.4.3 Active Risk (e variantes)

Rapid7 desenvolveu **Active Risk** como o seu enfoque avanzado de priorización de vulnerabilidades, orientado a ofrecer unha **avaliación continua e contextualizada do risco real** asociado aos activos dunha organización. Esta capacidade intégrase nas solucións de xestión de vulnerabilidades da compañía e representa unha evolución respecto a modelos anteriores baseados en puntuacións estáticas.

Segundo a documentación, Active Risk proporciona unha **puntuación de risco dinámica**, que combina información sobre vulnerabilidades, exposición do activo, intelixencia de ameazas e comportamento observado dos atacantes, co obxectivo de identificar aquelas situacións que requiren atención prioritaria [33].

Este enfoque pretende responder á necesidade de ir máis aló da severidade técnica, incorporando factores como:

- a probabilidade de explotación,
- a relevancia do activo no contexto do negocio,
- e a evidencia de actividade maliciosa asociada.

Deste xeito, Active Risk permite reducir o volume de vulnerabilidades consideradas críticas e concentrar os esforzos de remediación nos escenarios con maior impacto potencial.

Antes da introdución de Active Risk, Rapid7 empregou **diferentes enfoques de priorización de vulnerabilidades, que foron evolucionando progresivamente** a medida que aumentaba a complexidade dos contornos e das ameazas. Un *whitepaper* comparativo entre Tenable e Rapid7 describe e analiza estes modelos anteriores, permitindo entender a traxectoria de madurez da plataforma [34].

De forma resumida, estes enfoques previos inclúen:

1. **Priorización baseada en CVSS**: enfoque inicial centrado na severidade técnica das vulnerabilidades, con limitacións claras á hora de reflectir o risco real.
2. **Priorización baseada en exposición**: incorporación de factores como a accesibilidade do activo dende redes externas ou internas.
3. **Priorización baseada en intelixencia de ameazas**: consideración do tempo de vida da vulnerabilidade, da dispoñibilidade de exploits e da actividade maliciosa coñecida.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

4. **Priorización baseada en contexto do activo**: integración progresiva da criticidade do sistema e do seu rol no negocio.

Estes catro enfoques sentaron as bases conceptuais para o desenvolvemento de Active Risk, que os integra nun **modelo único, continuo e orientado á toma de decisións operativas**.

Active Risk consolida os enfoques anteriores nunha **visión holística do risco**, na que as puntuacións se recalculan de forma constante a medida que cambian as condicións de exposición, ameaza ou contexto.

Constitúe unha mostra mais de que a tendencia dos fabricantes diríxese cara a **modelos de priorización dinámicos e sempre baseados en risco**, aliñados cos principios xa subraiados polo DHS en 2008, e optimizados por Manion e os seus compañeiros de investigación en 2018 [20][17].

5 Recomendacións

Se o lector analizou previamente o anterior **Informe de Ciberalertas – I** [4], lembrará que existía unha **sección de recomendacións. Remitímolo alí para un tratamento máis detallado e contextualizado das fontes e dos marcos de referencia** empregados.

O propósito desta sección é **condensar as ideas clave e conectalas nun fío lóxico que vaia dende os principios xerais ata as prácticas operativas máis directamente relacionadas coa xestión de vulnerabilidades e o parcheo** en entornos industriais.

Como punto de partida, establecíanse uns **principios xerais de ciberseguridade OT** amplamente recoñecidos a nivel internacional, como os recollidos na **guía *Principles of Operational Technology Cybersecurity*, impulsada polo Australian Cyber Security Centre xunto con outras axencias nacionais**. Estes principios sitúan a seguridade física e a integridade do proceso como prioridade absoluta, promoven o deseño de sistemas resilientes para entornos hostís, subliñan a importancia da previsibilidade operativa e do coñecemento continuo da contorna OT, e integran a xestión dos riscos industriais dentro da xestión global do risco de negocio.

Sobre esta base, distintos **informes sectoriais de referencia no ámbito industrial, como os informes anuais de ciberseguridade OT/ICS elaborados por Dragos, propoñían un enfoque pragmático**, orientado a traducir eses principios en accións concretas: dispor de plans de resposta a incidentes específicos para ICS, evolucionar cara a arquitecturas defendibles con segmentación clara IT/OT, reforzar a visibilidade e a monitorización específicas de contornos industriais, asegurar o acceso remoto e adoptar unha xestión de vulnerabilidades baseada no risco real e non só na severidade técnica.

Neste contexto cobraba especial relevancia a filosofía **Now / Next / Never** que trouxemos de novo a colación, que proporciona un criterio operativo sinxelo para decidir que vulnerabilidades requiren actuación inmediata, cales poden abordarse de forma planificada e cales poden xestionarse mediante medidas compensatorias. Este enfoque permite aliñar as decisións de parcheo co impacto operativo, evitando tanto a inacción como as intervencións precipitadas. En cambio, no actual Informe propóñense outros modelos como o KEV, EPSS, ou solucións propietarias híbridas.

A nivel máis operativo, as boas prácticas internacionais en materia de parcheo en ICS, recollidas en guías prácticas publicadas por organismos como a Cybersecurity

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

and Infrastructure Security Agency (CISA), coinciden en que este debe concibirse como un proceso estruturado e cíclico, que inclúa gobernanza clara, inventarios fiables, análise de impacto, probas previas, execución controlada, verificación posterior e mellora continua. E **asumir que non sempre será posible parchear leva a incorporar de forma explícita medidas compensatorias** —como segmentación, illamento, restrición de accesos ou monitorización reforzada— como parte integral da xestión do risco.

En conxunto, esta combinación de principios xerais, prioridades tácticas e prácticas operativas permitía construír **programas de ciberseguridade OT realistas, sostibles e aliñados coa continuidade do negocio**, adaptados ás limitacións e á criticidade propias dos entornos industriais.

A continuación, veranse conceptos sobre **boas prácticas de xestión de vulnerabilidades, e medidas compensatorias** nos casos en que por causas técnicas ou coste/beneficio non sexa adecuada a mitigación primaria mediante parcheo.

5.1 Boas prácticas de xestión de vulnerabilidades

Esta sección compila **boas prácticas de referencia para xestionar vulnerabilidades e decidir medidas de mitigación** con criterios operativos, especialmente útiles en entornos industriais onde o parcheo pode ser complexo (xanelas de parada limitadas, dependencia de provedores, requisitos de seguridade funcional, etc.).

Para iso aportanse dúas fontes complementarias: por unha banda, un *paper* clásico de mitigacións en redes de control (INL/ISA, no contexto de programas de DHS) que pon o foco nas **medidas compensatorias e na arquitectura defendible**; e, por outra, a guía do NIST sobre **planificación de xestión de parches a nivel empresarial**, que estrutura un programa sistemático e repetible.

O documento **Mitigations for Security Vulnerabilities Found in Control System Networks [35] identifica patróns recorrentes observados en avaliacións en campo e formula medidas prácticas para reducir exposición e explotación en ICS/OT.** Un dos seus valores didácticos é que organiza a lóxica defensiva partindo do *modus operandi* do atacante: **(1) acceder á LAN de control, (2) comprender o proceso e (3) controlar o proceso**. A partir desta secuencia, propón un conxunto de mitigacións por capas, enfocadas a impedir ou dificultar cada etapa.

En relación co **perímetro e a separación IT/OT**, o *paper* insiste en que a segregación entre rede corporativa e rede de control é unha práctica xa habitual, xeralmente apoiada

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

en *firewalls*, e que serve tanto para reducir a exposición directa como para limitar a propagación de *malware* procedente do ámbito corporativo. Sobre esa base, propón ir máis alá da "fronteira única" e evolucionar cara a unha **segmentación interna por zonas de seguridade**, limitando as comunicacións entre segmentos a aquelas estritamente necesarias e baixo regras explícitas.

No que atinxe a **accesos e control de privilexios**, o documento enfatiza a necesidade de aplicar o principio de **mínimo privilexio** (en usuarios e aplicacións), eliminar servizos e aplicacións innecesarias e asegurar que as políticas de contrasinais e de resposta a incidentes estean definidas e operativas. O fío condutor é reducir superficie de ataque e limitar movemento lateral se se produce unha intrusión.

Unha recomendación especialmente relevante para ICS/OT é substituír, cando sexa posible, **protocolos en texto claro** por mecanismos que incorporen autenticación e cifrado. O *paper* ilustra o risco de credenciais capturadas en tránsito e como unha autenticación cifrada podería evitar ataques de interceptación. Ademais, vincula autenticación e integridade de comunicación co risco de **suplantación (spoofing)**, que podería derivar en perda de visión real do proceso por parte do persoal operador.

Finalmente, o documento dedica atención explícita á **xestión de parches**: recomenda aplicar parches de sistemas operativos e aplicacións "conforme están dispoñibles", pero subliña que en entornos de control isto debe facerse **tras probas previas para evitar impactos negativos na funcionalidade**. En paralelo, reforza a idea de que as melloras deben introducirse **en pequenos incrementos**, coordinadas co provedor do sistema de control e con procedementos de *rollback* que permitan reverter cambios se se detecta conflito coa operación. Esta aproximación incremental encaixa ben cunha estratexia de risco progresivo (priorizar o crítico, mitigar o inmediato e planificar actualizacións).

Por outra banda, **a publicación NIST SP 800-40r4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology [36], está orientada a establecer un enfoque de "mantemento preventivo" para tecnoloxía, convertendo a xestión de parches nun proceso de negocio repetible**: con gobernanza, planificación, execución controlada, medición e mellora continua. A guía non se limita ao acto de "aplicar parches", senón que enmarca a remediación de vulnerabilidades como un conxunto de opcións e decisións, onde o parche é unha delas. As principais ideas, recóllense a continuación.

a) Obxectivo e alcance do programa. O NIST parte da necesidade de que as organizacións definan un programa de xestión de parches como función transversal, con

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

roles e responsabilidades claros (propiedade de activos, seguridade, operacións/IT/OT, xestión de cambios) e unha aliñación explícita cos obxectivos do negocio. A intención é reducir a improvisación: o parcheo debe estar integrado na gobernanza e nos procesos formais de cambio.

b) Resposta ao risco: opcións cando aparece unha vulnerabilidade. A guía formula a resposta como decisión de tratamento do risco clásico.

En termos prácticos, cando se identifica unha vulnerabilidade, a organización pode:

- **evitar o risco** (retirando ou substituíndo a tecnoloxía),
- **mitigalo** (parche, reconfiguración, controis compensatorios),
- **transferilo/compartilo** (p.ex., mediante acordos/seguros cando aplica),
- **aceptalo** (cando o impacto esperado é asumible e queda documentado).

Este punto é clave porque formaliza o que en OT adoita ser inevitable: non todo se pode parchear, pero todo debe xestionarse.

c) Ciclo de vida da xestión de vulnerabilidades e parches. A SP 800-40r4 estrutura un fluxo continuo no que se diferencian etapas típicas:

- **Identificación e coñecemento do activo**: inventario, dependencia de software/firmware e coñecemento de exposición.
- **Obtención de información de vulnerabilidades e parches**: fontes de provedores, alertas, *feeds* e avaliación interna.
- **Avaliación do impacto e do risco**: análise de como a vulnerabilidade afecta ao activo e ao contexto (criticidade, exposición, compensacións existentes).
- **Priorización**: establecer orde e cadencia de remediación, diferenciando tratamento urxente vs. tratamento por mantemento programado.
- **Remediación**: aplicación do parche e/ou mitigacións alternativas (configuración, desactivación de servizos, segmentación, etc.).
- **Validación e verificación**: comprobar que a remediación foi efectiva e que non xerou efectos colaterais.
- **Rexistro e mellora continua**: documentación, métricas, revisión de procedementos e aprendizaxes.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Ciclo de vida da xestión de vulnerabilidades e parches segundo NIST SP 800-40r4. Fonte: NIST(2022)

Un tema interesante que plantexa a publicación, é a asignación dos activos a grupos. As organizacións deben **asignar cada activo a un grupo de mantemento** empregando inventarios de software, características técnicas e de negocio, e escenarios de resposta ao risco. Un **grupo de mantemento** reúne activos con **características semellantes e necesidades de mantemento de software similares** para cada escenario de risco.

O mantemento non inclúe só o **parcheado** (calendarios, probas, restricións de indispoñibilidade ou impacto dunha vulnerabilidade), senón tamén **outras medidas de mitigación e resposta ao risco**, incluídas mitigacións temporais cando non existen parches dispoñibles.

As organizacións deben **definir os grupos co nivel de detalle máis axeitado**, revisalos periodicamente e **axustalos cando sexa necesario**. Non se deben tratar certos activos como "excepcións": **todo activo ten necesidades de mantemento** e debe pertencer a un grupo, incluso se **non pode ou non debe ser parcheado**.

Exemplos simplificados de **grupos de mantemento**:

- **Portátiles da forza de traballo móbil**: impacto moderado, tolerantes a indispoñibilidade, con controis de seguridade nos dispositivos.
- **Centro de datos on-premises**: impacto alto, parches de firmware, SO e aplicacións, con ventás de mantemento programadas e fortes controis de rede.
- **Activos OT herdados**: sen posibilidade de parcheado, impacto alto, mitigados mediante illamento de rede e seguridade física.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

- **Smartphones corporativos**: impacto moderado, parcheado de SO e apps, tolerantes a indispoñibilidade.
- **Servidores on-premises para probas automatizadas**: impacto moderado, normalmente tolerantes a indispoñibilidade.
- **Contedores en nube pública con aplicacións orientadas a clientes**: impacto alto, moi tolerantes a indispoñibilidade, con controis de seguridade no sistema do contedor.

En síntese, o enfoque clave é **xestionar o mantemento e o risco por grupos de activos**, asegurando unha **resposta coherente, revisable e axeitada ao impacto de cada tipo de sistema**. Posteriormente como dicimos, a cada grupo asignaráselle una planificación de parcheado determinada.

d) Planificación: mantemento rutineiro e resposta de emerxencia. Unha das achegas máis prácticas do NIST é a distinción entre:

- **Parches rutineiros (mantemento programado)**: organización por "grupos de mantemento" (conxuntos de activos con requisitos e cadencias similares), definición de xanelas, probas, comunicación e execución repetible.
- **Parches de emerxencia**: cando a explotación é probable/inminente ou o impacto é alto, habilítanse procedementos acelerados, mantendo (na medida do posible) control de cambios, validación e mecanismos de reversión.

Esta separación permite que o "urxente" non destrúa o "importante": o programa segue funcionando sen caer nunha dinámica permanente de crise.

e) Dependencias, probas e control do cambio. A guía insiste en que a remediación debe considerar dependencias (aplicacións, librarías, configuracións) e require un enfoque de probas en entornos de non producción cando sexa posible. O obxectivo é minimizar interrupcións e regresións, incorporando procedementos de volta atrás e verificación post-implantación.

f) Medición e mellora (métricas). O NIST recomenda definir métricas que permitan avaliar a eficacia do programa (p.ex., cobertura de activos, tempo ata remediación, porcentaxe de excepcións, éxito/fracaso de implantacións, volume de vulnerabilidades abertas por criticidade, etc.). A finalidade non é "contar parches", senón demostrar redución de risco e capacidade operativa sostible. A continuación, un exemplo de cadro de mando asociado aos tempos de xestión de vulnerabilidades:

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Vulnerability Importance	Asset Importance		
	Low	Moderate	High
Low	By deadline: 64.7 % Average time: 80.4 days Median time: 75.2 days	By deadline: 72.4 % Average time: 34.7 days Median time: 33.7 days	By deadline: 85.0 % Average time: 14.6 days Median time: 8.1 days
Medium	By deadline: 66.5 % Average time: 75.1 days Median time: 70.7 days	By deadline: 68.7 % Average time: 33.2 days Median time: 31.6 days	By deadline: 71.4 % Average time: 12.9 days Median time: 10.5 days
High	By deadline: 68.6 % Average time: 62.1 days Median time: 58.0 days	By deadline: 78.8 % Average time: 26.8 days Median time: 22.1 days	By deadline: 85.5 % Average time: 8.8 days Median time: 8.1 days
Critical	By deadline: 81.4 % Average time: 44.4 days Median time: 41.3 days	By deadline: 92.3 % Average time: 21.2 days Median time: 23.9 days	By deadline: 95.2 % Average time: 5.2 days Median time: 5.1 days

Exemplo ficticio de indicadores de tempos de xestión de vulnerabilidades. Fonte: NIST (2022)

5.2 Mitigacións e medidas compensatorias

En contornos industriais, non sempre é posible reducir o risco unicamente mediante a aplicación de parches para correxir vulnerabilidades. **As restricións operativas, a dependencia de provedores, os ciclos longos de mantemento, os requisitos de seguridade funcional ou o custo, fan necesario complementar o parcheo con medidas compensatorias**, entendidas como controis técnicos, organizativos e procedementais que permiten **reducir a probabilidade de explotación e/ou o impacto dunha ameaza**, mesmo cando a vulnerabilidade subxacente segue presente.

As seguintes medidas recollen un **catálogo típico de mitigacións en OT**, extraído e sintetizado a partir das publicacións do Centro de Ciberseguridade Industrial (CCI) sobre a aplicación práctica da regulación en entornos industriais e medidas compensatorias [37][38]. Estas iniciativas non deben entenderse en modo algún como alternativas excluíntes, senón como elementos combinables dentro dunha estratexia de defensa en profundidade.

a) Segmentación de rede

A segmentación de rede consiste en dividir a infraestrutura OT en **zonas de seguridade con funcións e niveis de risco diferenciados**, limitando as comunicacións entre elas ao estritamente necesario. O seu principal beneficio é reducir a superficie de ataque e conter o movemento lateral dun adversario en caso de intrusión. Esta medida mitiga especialmente o risco de propagación de malware e de accesos non autorizados a sistemas críticos.

b) Industrial DMZ / Borde IT–OT

A implantación dunha **DMZ (zona desmilitarizada) industrial** no punto de converxencia entre IT e OT permite intermediar e controlar os fluxos de información

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

entre ambos dominios. Esta arquitectura reduce o risco de que incidentes procedentes do ámbito corporativo impacten directamente nos sistemas de control, ao tempo que facilita a aplicación de controis específicos (firewalls, proxies, pasarelas seguras) no perímetro máis sensible.

c) Monitorización pasiva e detección de anomalías

A monitorización pasiva de tráfico e comportamento en OT permite **detectar desviacións respecto do funcionamento normal** sen interferir no proceso. O seu valor reside en identificar actividades anómalas, cambios non autorizados ou patróns compatibles con intrusións, mitigando o risco de detección tardía e permitindo resposta temperá antes de que o impacto sexa físico.

d) Logging inmutable / rexistro inviolable

Rexistro centralizado e protexido de eventos e accións relevantes en OT proporciona trazabilidade e soporte á análise forense. O carácter inmutable dos rexistros reduce o risco de manipulación por parte dun atacante e contribúe tanto á detección de incidentes como ao cumprimento regulatorio e á aprendizaxe posterior.

e) Control de acceso robusto e separación de funcións

Control de acceso baseado en identidades, roles e privilexios mínimos, xunto coa separación de funcións críticas, limita o impacto potencial de credenciais comprometidas. Esta medida mitiga o risco de erros humanos, abuso interno e escalada de privilexios, especialmente en sistemas de enxeñaría e operación.

f) Acceso remoto seguro para mantemento

Dado que **o acceso remoto é un dos vectores de risco máis críticos en OT**, a súa protección **mediante autenticación forte, control de sesións, trazabilidade e acceso baixo demanda** reduce significativamente a probabilidade de intrusións externas e de uso indebido de contas de terceiros.

g) Xestión de parches e estratexias compensatorias

Cando o parcheo directo non é viable, poden aplicarse **medidas compensatorias técnicas (configuracións, regras de filtrado, desactivación de servizos) que reduzan a explotabilidade da vulnerabilidade**. Estas medidas permiten gañar tempo e reducir risco mentres se planifica unha actualización segura.

h) Copias de seguridade e recuperación orientadas a OT

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Os backups específicos de sistemas OT, incluíndo configuracións, lóxicas de control e datos de proceso, son esenciais para a recuperación tras incidentes. Esta medida mitiga o impacto de ataques destrutivos, erros de configuración e fallos de sistema, sempre que os procedementos de restauración sexan probados e coñecidos.

i) Bastionado de HMI e sistemas de enxeñaría

Reforzo da configuración de HMI, estacións de enxeñaría e servidores asociados reduce a superficie de ataque ao **eliminar servizos innecesarios, limitar aplicacións permitidas e aplicar configuracións** seguras. Trátase de activos de alto valor para un atacante, polo que o hardening oun endurecemento contribúe a diminuír tanto a probabilidade como o impacto dunha intrusión.

j) Xestión da cadea de subministración e firmware

A validación de provedores, firmware e actualizacións, así como o control da integridade dos compoñentes, reduce o risco de introducir vulnerabilidades ou código malicioso a través da cadea de subministración. Esta medida cobra especial relevancia en contornos OT con longos ciclos de vida dos equipos.

k) Resiliencia e seguridade funcional

A resiliencia do sistema e a seguridade funcional aseguran que, mesmo **en condicións anómalas ou de ataque, o proceso transite a estados seguros. A integración entre ciberseguridade e seguridade funcional mitiga riscos para as persoas, o medio e as instalacións**, máis aló da dimensión puramente dixital.

l) Procedementos operativos e formación

Os procedementos claros e a formación do persoal son unha medida compensatoria fundamental. **Un persoal formado é capaz de detectar anomalías, evitar erros críticos e responder de forma coordinada ante incidentes**, reducindo tanto a probabilidade como o impacto dos eventos de seguridade.

m) Parcheo virtual / Firewall de capa de aplicación

O **parcheo virtual** dedicámoslle algo máis de espacio pola sua relevancia e interese en OT, onde o equipamento adoita a ser máis delicado ou obsoleto. Consiste en empregar controis de seguridade —habitualmente *firewalls* de capa de aplicación, *firewalls* industriais ou sistemas de prevención de intrusións (IPS)— para **bloquear a explotación dunha vulnerabilidade sen modificar o sistema vulnerable**. Segundo a definición de Fortinet, esta técnica permite crear unha "capa de protección lóxica" fronte a exploits coñecidos, interceptando solicitudes maliciosas, patróns de ataque ou

comportamentos anómalos antes de que cheguen á aplicación ou dispositivo afectado [39]. Dende o punto de vista operativo, o parcheo virtual resulta especialmente útil en contornos OT cando:

- **non existe aínda un parche oficial** do fabricante,
- o equipo afectado é **legado ou está fóra de soporte,**
- ou **o parcheo directo implica un risco elevado** para a continuidade ou a seguridade funcional do proceso.

Entre os seus principais beneficios destacan a **redución inmediata da superficie de ataque**, a posibilidade de protección en tempo real sen intervención directa sobre o activo e a capacidade de gañar tempo para planificar unha actualización segura. Ademais, o parcheo virtual permite aplicar políticas coherentes a múltiples activos afectados por unha mesma vulnerabilidade, mellorando a eficiencia operativa.

Non obstante, hai que subliñar que o parcheo virtual **non elimina a vulnerabilidade subxacente**, polo que debe entenderse como unha medida compensatoria temporal ou complementaria, e non como substituto permanente do parcheo. O seu uso require unha correcta definición e mantemento das regras de protección, coñecemento profundo do tráfico e das aplicacións industriais, e unha supervisión continua para evitar impactos non desexados no proceso industrial.

A continuación, a modo de peche da sección, inclúese unha táboa resumo cos controis indicados.

Medida compensatoria	Definición sintética	Ameazas / riscos que mitiga
Segmentación de rede	División da rede OT en zonas de seguridade con comunicacións estritamente controladas	Movemento lateral, propagación de *malware*, accesos non autorizados a sistemas críticos
Industrial DMZ / Borde IT–OT	Zona intermedia entre IT e OT para controlar e filtrar intercambios de información	Intrusións dende IT, *malware* corporativo, exposición directa de OT
Monitorización pasiva e detección de anomalías	Observación continua do tráfico e comportamento OT sen interferir no proceso	Intrusións silenciosas, cambios non autorizados, detección tardía de ataques
Logging inmutable / rexistro inviolable	Rexistro centralizado e protexido de eventos e accións relevantes	Ocultación de actividades maliciosas, dificultade de análise

		forense, incumprimento regulatorio
Control de acceso robusto e separación de funcións	Xestión de identidades, roles e privilexios mínimos	Uso indebido de credenciais, erros humanos, escalada de privilexios
Acceso remoto seguro para mantemento	Accesos remotos controlados, autenticados e trazables	Intrusións externas, abuso de contas de terceiros, accesos persistentes
Xestión de parches e estratexias compensatorias	Aplicación planificada de parches ou medidas técnicas alternativas	Explotación de vulnerabilidades coñecidas, risco acumulado por parches diferidos
Copias de seguridade e recuperación orientadas a OT	*Backups* de configuracións, lóxicas e datos de proceso con procedementos probados	Impacto de ransomware, perda de control, indispoñibilidade prolongada
Bastionado de HMI e sistemas de enxeñaría	Reforzo de configuracións e eliminación de servizos innecesarios	Compromiso de activos críticos, control do proceso por atacantes
Xestión da cadea de subministración e firmware	Control da integridade de provedores, firmware e actualizacións	Introdución de código malicioso, vulnerabilidades de orixe
Resiliencia e seguridade funcional	Deseño de estados seguros e integración coa seguridade funcional	Impacto físico, riscos para persoas e instalacións
Procedementos operativos e formación	Definición de procedementos e capacitación do persoal	Erros humanos, resposta incorrecta a incidentes, detección tardía
Parcheo virtual / Firewall de capa de aplicación	Bloqueo de exploits mediante regras de seguridade sen modificar o activo vulnerable	Explotación de vulnerabilidades sen parche, risco en sistemas *legacy*

Táboa resumo de mitigacións e medidas compensatorias. Fonte: elaboración propia (2026)

5.3 Indicadores de seguimento

A **inclusión dun subapartado de métricas** é coherente coas guías oficiais recentes que enfatizan a **avaliación continua da efectividade das medidas de ciberseguridade** (non só a súa existencia formal).

O documento de xuño de 2025 de **ENISA** (guía técnica de implementación no contexto **NIS2 / medidas de xestión do risco**) dedica un capítulo específico ás "policies and procedures to assess the effectiveness…", indicando que a organización debe determinar **que medidas se monitorizan e miden, como, cando e quen é responsable de medir**

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

e avaliar os resultados [46]. Ademais, propón métodos concretos (auditoría, análise de vulnerabilidades —VA—, monitorización de rendemento, etc.) e recomenda definir **KPIs**, achegando unha listaxe non exhaustiva de exemplos.

Na práctica da **xestión de parches e vulnerabilidades**, o **NIST** recomenda evitar métricas simplistas e "non accionables" (por exemplo, "% total parcheado" sen contexto) e construír indicadores que crucen a **criticidade do activo** coa **criticidade e explotabilidade da vulnerabilidade**. Isto inclúe medidas de cumprimento por prazo, tempos medio e mediano de mitigación e segmentación por grupos de mantemento (especialmente relevante en OT debido ás restricións de ventá de mantemento e á presenza de activos *legacy*) [36].

Como referencia gobernamental directamente orientada a **KPIs de parcheo**, a guía federal canadense "Patch Management Guidance" explica que unha estratexia debe incluír indicadores de desempeño e ofrece exemplos concretos: métricas de **cobertura** (inventario cuberto), de **eficiencia/efectividade** (tempos mínimo/medio/máximo para parchear unha porcentaxe determinada, % parcheado en X días, % completamente parcheado, reconto de vulnerabilidades ou hosts sen parchear por criticidade, ratio automático vs manual, etc.), así como calendarios suxeridos de despregamento por prioridade (por exemplo, emerxencias en 48 horas; alta en dúas semanas) [47].

A nivel de **goberno corporativo**, o toolkit do **UK National Cyber Security Centre** para consellos de administración recomenda empregar cadros de mando con KPIs e menciona expresamente indicadores como o "tempo para implementar parches" ou os "días entre detección e remediación" como métricas esperables para apoiar a toma de decisións estratéxicas [48].

5.3.1.1 Catálogo proposto de KPIs/KRIs

Os seguintes indicadores están concibidos como **exemplos base** para seren adaptados á realidade OT (ventás de mantemento, activos legados, validación previa e controis compensatorios). En liña coas recomendacións do NIST, recoméndase segmentalos por **grupos de mantemento** e por **criticidade do activo**, co obxectivo de obter unha visión realista e accionable do risco e do desempeño do programa.

Indicador	Tipo	Definición operativa	Cálculo recomendado
Cobertura de inventario baixo xestión de parcheo	KPI	% de activos inventariados incluídos no proceso formal de parcheo	(# activos cubertos / # activos inventariados) × 100
Cobertura de telemetría para evidenciar estado de parcheo	KPI	% de activos cos que se pode verificar versión/firmware de forma fiable	(# activos con evidencias / # activos totais) × 100
% de activos "fully patched" (por familia tecnolóxica)	KPI	% de activos cos parches aplicables aplicados segundo baseline	(# fully patched / # operativos) × 100
Cumprimento de parcheo por SLA e criticidade	KPI	% de activos parcheados dentro do prazo definido por prioridade	(# parcheados en prazo / # obxectivo) × 100
Tempo medio de remediación (MTTR)	KPI	Media do tempo dende aprobación/dispoñibilidade ata instalación efectiva	Media (días)
Tempo mediano de remediación (Median TTR)	KPI	Mediana do tempo de remediación	Mediana (días)
% parcheado en ≤X días tras validación	KPI	Velocidade de despregue unha vez validado o parche	(# ≤X días / # obxectivo) × 100
Backlog de vulnerabilidades pendentes por criticidade	KRI	Volume de exposición acumulada por severidade e activo	Conteo por nivel (crit/alta/media/baixa)
Cumprimento en vulnerabilidades con explotación coñecida	KPI/KRI	% mitigadas no prazo para vulnerabilidades activas/explotadas	(# mitigadas en prazo / # detectadas) × 100
Taxa de éxito de despregue	KPI	% de instalacións exitosas por campaña	(# OK / # intentos) × 100
Ratio de despregue automático vs manual	KPI	% de parches despregados con automatización controlada	(# automáticos / # total) × 100
Cobertura de controis compensatorios en activos non parcheables	KRI	% de activos legacy/non parcheables con mitigación verificada	(# mitigados / # non parcheables) × 100
Tempo detección → contención	KPI	Tempo dende detección ata illamento/contención	Media (horas)
Tempo detección → recuperación operativa	KPI	Tempo total ata restablecer operación normal	Media (días)
% de sistemas críticos con MFA	KPI	% de sistemas e accesos críticos protexidos con MFA	(# con MFA / # críticos) × 100
% de accesos remotos revisados/auditados	KPI	% de conexións remotas sometidas a revisión periódica	(# auditadas / # total) × 100

Proposta de indicadores de seguimento relativos a vulnerabilidades. Fonte: elaboración propia (2026)

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

6 Alertas

6.1 Últimas alertas

Co obxectivo de **aportar un marco claro e operativo para avaliar a situación das vulnerabilidades nos sistemas industriais**, este informe incorpora un apartado específico centrado nas **alertas emitidas por organismos oficiais durante o trimestre máis recente**. Dado o carácter periódico da publicación, esta aproximación permite **concentrar a información máis relevante nun formato sintético e accionable**, pensado para facilitar a análise e a priorización por parte de equipos técnicos e responsables de seguridade.

Antes de entrar no detalle das alertas seleccionadas, resulta oportuno **ofrecer unha breve orientación sobre as principais canles dispoñibles para acceder, seguir ou recibir este tipo de avisos**, tanto no ámbito de **ICS/OT** como no de **infraestruturas TI** que, no contexto actual de converxencia tecnolóxica, **poden ter repercusión directa ou indirecta na continuidade da operación industrial**.

6.1.1 Fontes principais de avisos

Alén dos **avisos específicos emitidos polos propios fabricantes** —que se recollen de forma estruturada nun **anexo ao final do informe**— existen determinadas **plataformas de referencia** que actúan como **repositorios centrais, fiables e permanentemente actualizados** para o seguimento de **vulnerabilidades de especial relevancia** en contornos industriais.

Estas fontes proporcionan información clave para a **detección temperá**, a **avaliación do impacto** e a **toma de decisións informada** en materia de xestión de vulnerabilidades, tanto en **contornos ICS/OT** como en **infraestruturas TI** con posible repercusión sobre a operación industrial. O seu uso sistemático constitúe un **pilar fundamental dun programa de vixilancia de vulnerabilidades**, que debe completarse cos boletíns dos fabricantes cuxos equipos estean despregados en planta.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Fonte	Ámbito	Descrición	Valor achegado
INCIBE-CERT	Nacional (España) / ICS	Fonte nacional de referencia en **ciberseguridade industrial**. Publica avisos de vulnerabilidades que afectan a fabricantes e produtos ICS [40].	Información técnica detallada, **CVSS**, impacto operativo e **medidas de mitigación** adaptadas ao contexto industrial.
CCN-CERT	Nacional (España) / TI-OT	Orientado principalmente a administracións públicas, pero con **aplicabilidade transversal**. Publica alertas de alta criticidade [41][42].	Identificación de **vulnerabilidades severas en sistemas TI** con posible **impacto en contornos OT interconectadas**.
CISA – ICS Advisories (ICSA)	Internacional / ICS	Repositorio internacional máis recoñecido de avisos para **sistemas de control industrial** [43].	Descrición técnica completa, **CVSS**, produtos afectados, **escenarios de explotación** e **mitigacións recomendadas**.

Orixe principal dos avisos de vulnerabilidades. Fonte: elaboración propia (2026)

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

6.1.2 Consideracións clave para a interpretación de alertas

Ao analizar **vulnerabilidades en entornos ICS/OT**, resulta esencial ter en conta unha serie de consideracións específicas do ámbito industrial:

- As **puntuacións CVSS**, aínda que útiles como referencia inicial, **non sempre representan fielmente o risco real en OT**, onde a **dispoñibilidade do proceso** e a **seguridade física** teñen un peso determinante.
- As **alertas procedentes do ámbito TI** (por exemplo, servizos Windows, bases de datos ou middleware corporativo) poden ter un **impacto directo en OT** cando están presentes en **estacións de enxeñaría, servidores SCADA ou solucións de acceso remoto e mantemento**.
- Un número significativo de **vulnerabilidades en produtos ICS** non poden ser **corrixidas de forma inmediata** debido a **restricións operativas, de certificación ou de continuidade do servizo**, o que converte as **medidas compensatorias** nun elemento clave da estratexia de mitigación.
- A maioría dos **advisories técnicos** non inclúen información sobre **explotación activa en contornos reais**; por este motivo, fontes e enfoques complementarios

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

como os presentados neste Informe, resultan fundamentais para unha **priorización efectiva**.

Esta sección funcionará en cada edición do informe como unha **guía práctica de apoio** para os **equipos de seguridade, mantemento e operación**, facilitando a **identificación das novas vulnerabilidades relevantes** e a toma de **decisións fundamentadas** sobre aquelas que presentan un **maior nivel de risco (soamente teórico, á luz da información recompilada neste segundo Informe) para a operación industrial**.

6.1.3 Alertas ICS de alta criticidade do trimestre

De entre os avisos publicados no período analizado (**primeiro trimestre de 2026**), preséntanse a continuación nesta segunda entrega, unicamente **as vulnerabilidades de severidade crítica que afectan directamente a contornos ICS**, descritas de maneira sintética e orientada á acción.

Partimos da premisa de que o lector dispón dun programa propio de xestión de vulnerabilidades xa implantado e/ou realiza o seguimento habitual dos avisos dos fabricantes, polo que non se considerou oportuno dedicar un fragmento extenso do informe á descrición detallada de CVEs que poden non ser en absoluto do seu interese.

Pola contra, **a táboa resume os elementos esenciais para facilitar unha rápida identificación do risco, convidando en todo caso á consulta da fonte orixinal de INCIBE-CERT**, que recompila de forma estruturada os avisos de orixe internacional.

Nome	Data de publicación en INCIBE	Descrición	Recursos afectados	CVEs
Múltiples vulnerabilidades en produtos de Mitsubishi Electric	08/01/2026	Asher Davila e Malav Vyas reportaron 16 vulnerabilidades: 1 de severidade crítica, 11 altas, 3 medias e 1 baixa. No caso de que algunha destas vulnerabilidades fose explotada con éxito, podería permitir a un atacante acceder, divulgar ou manipular información confidencial, crear condicións de denegación de servizo (DoS), executar código remoto malicioso, así como eludir a autenticación.	MC Works64 : versión 4.04E e anteriores; GENESIS64, ICONICS Suite, GENESIS32, eMC Works64 tódalas versiones. BizViz versións anteriores a 9.7, incluida.	CVE-2022-33318, CVE-2022-29834,CVE-2022-33315, CVE-2022-33316, CVE-2022-33317, CVE-2022-33319, CVE-2022-33320, CVE-2024-1182, CVE-2024-1187, CVE-2024-8299, CVE-2024-8300, CVE-2024-9852
Avisos de seguridade de Siemens de xaneiro de 2026	12/01/2026	Siemens publicou no seu comunicado mensual varias actualizacións de seguridade nalgúns dos seus produtos.	Múltiples de Industrial Edge Services, TeleControl Server Basic, SIMATIC e RUGGEDCOM.	CVE-2025-40805, CVE-2025-40942, CVE-2025-40944, CVE-2025-40892, CVE-2025-40893, CVE-2025-40898

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Múltiples vulnerabilidades en produtos de AVEVA	14/01/2026	Christopher Wu, de Veracode, reportou 7 vulnerabilidades, 4 de severidade crítica e 3 de severidade alta. No caso de seren explotadas, poderían permitir a un atacante non autenticado executar código remoto e arbitrario, escalar privilexios e acceder ou filtrar datos confidenciais.	AVEVA Process Optimization (anterioremente denominado ROMeo) en versións anteriores á 2024.1, incluida.	CVE-2025-61937, CVE-2025-64691, CVE-2025-61943, CVE-2025-65118
Omisión de autenticación en produtos de ABB	19/01/2026	ABB reportou unha vulnerabilidade de severidade crítica que, no caso de ser explotada, podería permitir a un atacante omitir a autenticación dos sistemas afectados e apagalos, modificar as súas configuracións e instalar e executar código arbitrario.	Varios de ABB Ability OPTIMAX.	CVE-2025-14510
Múltiples vulnerabilidades en DIAView de Delta Electronics	19/01/2026	Delta Electronics, en colaboración con Tenable, reportou 2 vulnerabilidades de severidade crítica que, no caso de seren explotadas, poderían permitir a un atacante omitir a autenticación e acceder a datos confidenciais.	DIAView, versións anteriores a 4.3.1, incluida.	CVE-2025-62581, CVE-2025-62582
Múltiples vulnerabilidades en produtos de B&R	20/01/2026	B&R publicou 2 avisos de seguridade que resolven, en total, 1 vulnerabilidade de severidade crítica e 1 alta. A explotación exitosa destas vulnerabilidades podería permitir a un atacante facerse pasar por unha entidade de confianza ou bloquear o produto.	Varios de Automation Studio e Automation Runtime	CVE-2025-11043, CVE-2025-11044
Múltiples vulnerabilidades en MedDream PACS Premium	22/01/2026	Marcin "Icewall" Noga, de Cisco Talos, informou de 21 vulnerabilidades, 1 de severidade crítica que, no caso de ser explotada, podería permitir a un atacante ler ficheiros arbitrarios do servidor mediante unha solicitude HTTP manipulada.	MedDream PACS Premium, versión 7.3.6.870.	CVE-2025-53912
Omisión de autorización en hubs de Hubitat Elevation	23/01/2026	Aaron «theHastyOne» Hasty, de Ostrich Lab, informou dunha vulnerabilidade de severidade crítica que, no caso de ser explotada, podería permitir a un atacante non autenticado escalar privilexios e controlar os dispositivos máis alá do seu alcance permitido.	Varios de Elevation CX, versións de firmware anteriores á 2.4.2.157.	CVE-2026-1201
Asignación incorrecta de permisos en ibaPDA de iba Systems	29/01/2026	Siemens reportou unha vulnerabilidade de severidade crítica que, no caso de ser explotada, podería permitir a un atacante executar accións non autorizadas no sistema de ficheiros.	ibaPDA, versión 8.12.0.	CVE-2025-14988
Execución SQL remota en produtos de Johnson Controls	29/01/2026	Johnson Controls reportou 1 vulnerabilidade crítica que, no caso de ser explotada, podería permitir a un atacante executar comandos SQL de forma remota e, como consecuencia, alterar ou eliminar datos.	Varios de Metasys, SST, CCT.	CVE-2026-21654

Ausencia de autenticación na serie de codificadores de KiloView	30/01/2026	Muhammad Ammar (0xam225) informou sobre 1 vulnerabilidade de severidade crítica que, no caso de ser explotada, podería permitir a un atacante non autenticado ter control administrativo total.	Varias versións de hardware do codificador serie E1, E1-s, E2, G1, P1, P2, RE1.	CVE-2026-1453
Ausencia de autenticación en LAN 232 TRIO de Synectix	04/02/2026	Souvik Kandar, de MicroSec, informou sobre unha vulnerabilidade de severidade crítica que podería permitir que un atacante non autenticado modifique configuracións críticas do dispositivo ou restableza o dispositivo aos valores de fábrica.	Tódalas versións de Synectix LAN 232 TRIO.	CVE-2026-1633
Ausencia de autenticación en switches Ethernet de Moxa	04/02/2026	Moxa publicou un aviso para varios dos seus switches Ethernet no que informa sobre unha vulnerabilidade de severidade crítica que, no caso de ser explotada, podería comprometer a seguridade do dispositivo.	TN-A Series, en versión de firmware 4.1 e anteriores, e TN-G Series, en versión de firmware 5.5 e anteriores.	CVE-2024-12297
Ausencia de autenticación en Light Engine Pro de Avation	04/02/2026	Souvik Kandar informou sobre unha vulnerabilidade de severidade crítica que podería permitir a un atacante tomar o control total do dispositivo.	Tódalas versións de Avation Light Engine Pro.	CVE-2026-1341
Ausencia de autenticación en MOMA Seismic Station de RISS SRL	04/02/2026	A estación sísmica expón a súa interface de administración web sen requirir autenticación.	MOMA Seismic Station versións anteriores á v2.4.2520, incluida.	CVE-2026-1632
Múltiples vulnerabilidades en EVE X1 Server de Ilevia	06/02/2026	Gjoko Krstic, de Zero Science Lab, informou sobre 9 vulnerabilidades: 5 de severidade crítica, 3 altas e 1 media, que poderían permitir a un atacante executar comandos de shell arbitrarios e divulgar información confidencial do sistema.	EVE X1 versións anteriores á 4.7.18.0, incluida.	CVE-2025-34187, CVE-2025-34186, CVE-2025-34184, CVE-2025-34183, CVE-2025-34513, CVE-2025-34185, CVE-2025-34518, CVE-2025-34517
Múltiples vulnerabilidades en switches de xestión industrial de WAGO	09/02/2026	Diconio informou de 4 vulnerabilidades, 3 de severidade crítica e 1 alta que, no caso de seren explotadas, poderían permitir a atacantes remotos bloquear o servizo web, executar código arbitrario, eludir os controis de autenticación e obter credenciais de administrador en texto plano.	Modelos de switches de control industrial con firmware 2.64 ou inferior: 0852-1322, 0852-1328.	CVE-2026-22903, CVE-2026-22904, CVE-2026-22906, CVE-2026-22905
Múltiples vulnerabilidades en produtos de ZLAN Information Technology Co.	11/02/2026	Shorabh Karir e Deepak Singh, de KPMG, reportaron 2 vulnerabilidades de severidade crítica, cuxa explotación podería permitir a un atacante eludir a autenticación ou restablecer o contrasinal do dispositivo.	ZLAN5143D: versión v1.600.	CVE-2026-25084, CVE-2026-24789
Carga de ficheiros sen restrición en Airleader Master	13/02/2026	Angel Lomeli, de SySS GmbH, informou dunha vulnerabilidade de severidade crítica que, no caso de ser explotada, podería permitir a un atacante non autenticado executar código remotamente no servidor.	Airleader Master, versión 6.381 e anteriores.	CVE-2026-1358

Múltiples vulnerabilidades en produtos de Schneider Electric	11/02/2026	Pentest Limited e Robin Plugge, en colaboración con Schneider Electric, reportaron 3 vulnerabilidades, 1 delas crítica e 2 de severidade alta que, no caso de seren explotadas con éxito, poderían permitir a un atacante, entre outras accións, provocar unha denegación de servizo que daría lugar a interrupcións do servizo.	Varios productos da serie SCADAPacksupTM x70 RTU, das series EcoStruxureTM Building Operation e EcoStruxureTM Building Operation WebStation	CVE-2026-0667, CVE-2026-1227, CVE-2026-1226
Ausencia de autenticación en produtos de CCTV de Honeywell	18/02/2026	Souvik Kandar informou sobre 1 vulnerabilidade de severidade crítica que podería levar á apropiación de contas e ao acceso non autorizado ás transmisións da cámara; un atacante non autenticado pode cambiar o enderezo de correo electrónico de recuperación, o que podería levar a un maior compromiso da rede.	Varios produtos CCTV	CVE-2026-1670
Múltiples vulnerabilidades en USR-W610 de Jinan USR IOT Technology Limited	20/02/2026	Abhishek Pandey e Ranit Pradhan, de Payatu Security Consulting, informaron de 4 vulnerabilidades, 1 de severidade crítica, 2 altas e 1 media que, no caso de seren explotadas con éxito, poderían desactivar a autenticación, provocar unha condición de denegación de servizo ou o roubo de credenciais válidas, incluída a de administrador.	Jinan USR IOT Technology Limited (PUSR) USR-W610, versión 3.1.1.0 e anteriores.	CVE-2026-25715, CVE-2026-24455, CVE-2026-26048
Múltiples vulnerabilidades en MasterSCADA BUK-TS de InSAT	25/02/2026	Adem El Adeb informou sobre 2 vulnerabilidades de severidade crítica que poderían permitir a execución remota de código.	Tódalas versiones de InSAT MasterSCADA BUK-TS.	CVE-2026-21410, CVE-2026-22553
Múltiples vulnerabilidades en Frick Controls Quantum HD de Johnson Controls, Inc.	27/02/2026	Noam Moshe, do equipo de investigación 82 de Claroty, informou sobre 6 vulnerabilidades: 4 de severidade crítica, 1 alta e 1 media. A súa explotación podería levar á execución remota de código antes da autenticación, fuga de información ou denegación de servizo.	Frick Controls Quantum HD, versións anteriores á 10.22, incluída.	CVE-2026-21654, CVE-2026-21656, CVE-2026-21657, CVE-2026-21658
Múltiples vulnerabilidades en Copeland XWEB e XWEB Pro	27/02/2026	Amir Zaltzman e Noam Moshe, de Claroty Team82, informaron de 23 vulnerabilidades: 2 críticas, 19 altas, 1 media e 1 baixa. A explotación podería permitir evitar a autenticación, provocar denegación de servizo, crear corrupción de memoria e executar código arbitrario.	Copeland XWEB 300D PRO, 500D PRO, e XWEB 500B PRO: versión 1.12.1 e anteriores.	CVE-2026-21718, CVE-2026-24663
Múltiples vulnerabilidades en swtchenergy de SWITCH EV	27/02/2026	Khaled Sarieddine e Mohammad Ali Sayed informaron sobre 4 vulnerabilidades: 1 crítica, 2 altas e 1 media. Se fosen explotadas, poderían permitir o secuestro de sesións, a supresión ou desvío do tráfico lexítimo para causar denegación de servizo a gran escala e a manipulación dos datos enviados ao backend.	Todas as versións de swtchenergy.com.	CVE-2026-27767
Múltiples vulnerabilidades no sitio web de Chargemap	27/02/2026	Khaled Sarieddine e Mohammad Ali Sayed informaron sobre 4 vulnerabilidades: 1 crítica, 2 altas e 1 media. A explotación exitosa podería permitir obter control administrativo non autorizado sobre estacións de carga ou interromper os servizos de carga mediante denegacións de servizo.	Todas as versións do sitio web de Chargemap, chargemap.com.	CVE-2026-25851

Múltiples vulnerabilidades en OCPP Backends de Everon	04/03/2026	Khaled Sarieddine e Mohammad Ali Sayed informaron sobre 4 vulnerabilidades: 1 crítica, 2 altas e 1 media. En caso de seren explotadas, poderían permitir a un atacante obter control administrativo sobre estacións de carga vulnerables ou provocar ataques de denegación de servizo.	Todas as versións de OCPP Backends de Everon.	CVE-2026-26288
Execución remota de comandos en produtos Labkotec	04/03/2026	Souvik Kandar reportou unha vulnerabilidade de severidade crítica cuxa explotación podería permitir a un atacante obter control non autorizado sobre as operacións do sistema, interrompendo o funcionamento normal e xerando posibles riscos para a seguridade.	Labkotec LID-3300IP: todas as versións; Labkotec LID-3300IP Type 2: versións anteriores á V2.20.	CVE-2026-1775
Contrabando de solicitudes HTTP en LabX de Mettler-Toledo	05/03/2026	LabX presenta unha vulnerabilidade de severidade crítica que, de ser explotada, pode permitir a un atacante omitir a autenticación, afectando á confidencialidade e á integridade do produto.	LabX, versión 21.2.12; LabX Cloud, versión 1.2.12.	CVE-2025-55315
Múltiples vulnerabilidades en UMG 96RM-E de Janitza	10/03/2026	CERT@VDE, en coordinación con Janitza electronics GmbH, publicou 4 vulnerabilidades: 1 crítica e 3 medias. Un atacante remoto non autenticado podería obter acceso completo ao sistema e executar código remotamente.	UMG 96RM-E, versións anteriores á 3.13, incluída.	CVE-2025-41709
Avisos de seguridade de Siemens de marzo de 2026	10/03/2026	Siemens publicou no seu comunicado mensual varias actualizacións de seguridade en varios produtos, relacionadas cun total de 35 vulnerabilidades. No detalle do aviso indícase que emitiu 5 novos avisos de seguridade que recompilan 35 vulnerabilidades de distintas severidades.	Produtos Helio Flex 180 Kw Charging Station, SIDIS Prime, SICAM SIAPPSDK, RUGGEDCOM APE1808, e varios de SIMATIC.	CVE-2025-40943, CVE-2025-7783, CVE-2026-24858
Múltiples vulnerabilidades en ENERGY METER de Weidmueller	10/03/2026	CERT@VDE, en coordinación con Weidmueller, publicou 4 vulnerabilidades: 1 crítica e 3 medias. Un atacante remoto non autenticado podería obter acceso completo ao sistema e executar código remotamente.	ENERGY METER 750-230 e 750-24, versións de firmware 3.1 e anteriores.	CVE-2025-41709
Múltiples vulnerabilidades en Lantronix	11/03/2026	Francesco La Spina e Stanislav Dashevskyi, de Forescout Technologies, descubriron 8 vulnerabilidades, 2 de severidade crítica, 5 altas e 1 baixa. A súa explotación podería permitir evitar a autenticación e executar código con permisos de root.	EDS3000PS 3.1.0.0R2; EDS5000 2.1.0.0R1.	CVE-2025-67038, CVE-2025-67039
Falta de autenticación para unha función crítica para Honeywell	11/03/2026	Gjoko Krstic, de Zero Science, informou dunha vulnerabilidade de severidad crítica. O produto expón a súa interface HMI sen autenticación na configuración de fábrica, e isto podería permitir crear unha nova conta con permisos de administración de lectura e escritura.	Honeywell IQ4x BMS Controller nas seguintes versións: IQ4E, IQ412, IQ422, IQ4NC, IQ41x, IQ3 e IQECO, con firmware desde a v3.50_3.44 (incluída) ata a 4.36_build_4.3.7.9 (non incluída).	CVE-2026-3611
Múltiples vulnerabilidades en Ewon Flexy e Ewon Cosy de HMS	12/03/2026	Mr Nicolas SCHAFF e o equipo de VOC EDF informan sobre 4 vulnerabilidades: 2 críticas, 1 alta e 1 media que, en caso de seren explotadas, poderían permitir a un atacante executar código remoto, realizar ataques de forza bruta e causar denegacións de servicio ó sistema.	Todas as versións anteriores a: HMS Networks Ewon Flexy 15.0s2; HMS Networks Ewon Cosy+ 22.1s5; HMS Networks Ewon Cosy+, dende a versión 23.0s0 ata 23.0s2.	CVE-2026-25817, CVE-2026-25823
Desbordamento do búfer da pila en AC500 V3 de ABB	13/03/2026	ABB informou dunha vulnerabilidade crítica que podería permitir bloquear o dispositivo, provocar unha denegación de servizo ou executar código remotamente.	Todos os produtos AC500 V3 (PM5xxx) coa versión de firmware 3.9.0.	CVE-2025-15467

Múltiples vulnerabilidades en WebCTRL de Automated Logic	20/03/2026	Jonathan Lee, Thuy D. Nguyen e Neil C. Rowe informaron de 3 vulnerabilidades, 1 crítica e 2 altas, que poderían permitir ler, interceptar ou modificar as comunicacións.	Automated Logic WebCTRL Premium Server, versións anteriores á v8.5.	CVE-2026-24060
Compromiso total do sistema en produtos WAGO	23/03/2026	Un atacante remoto non autenticado pode explotar unha función oculta do prompt CLI para escapar da interface restrinxida, o que deriva nun compromiso absoluto do dispositivo.	Varios da serie 852-X, versións de firmware V1.2.0.S0 e anteriores, V1.1.9.S0 e anteriores, 1.2.1.S0 e anteriores, 1.2.3.S0 e anteriores, 1.2.8.S0 e anteriores, 1.0.6.S0 e anteriores.	CVE-2026-3587
Múltiples vulnerabilidades en produtos de Helmholz	24/03/2026	CERT@VDE, en colaboración con Helmholz GmbH & Co. KG, publicou dúas vulnerabilidades, unha crítica e outra alta, que poderían permitir executar código remoto ou realizar unha inxección SQL.	Helmholz myREX24V2 e myREX24V2.virtual, versións de firmware 2.19.3 e anteriores.	CVE-2026-32968
Múltiples vulnerabilidades en produtos de MB connect line	24/03/2026	CERT@VDE, en colaboración con MB connect line GmbH, publicou dúas vulnerabilidades, unha crítica e outra alta, que poderían permitir executar código remoto ou realizar unha inxección SQL.	MB connect line mbCONNECT24 e mymbCONNECT24, versións de firmware 2.19.3 e anteriores.	CVE-2026-32968
Múltiples vulnerabilidades Plant iT/Brewmaxx de Schneider Electric	25/03/2026	Schneider Electric reportou 4 vulnerabilidades: 1 crítica, 1 alta e 2 medias. A súa explotación podería implicar un risco de escalada de privilexios e execución remota de código.	Plant iT/Brewmaxx 9.60 e versións posteriores.	CVE-2025-49844
Execución remota de código en produtos de PTC	27/03/2026	Un investigador anónimo informou dunha vulnerabilidade crítica que podería permitir executar código remoto en Windchill PDMLink e FlexPLM mediante deserialización de datos non confiables.	Windchill PDMLink e FlexPLM, varias versións	CVE-2026-4681
Múltiples vulnerabilidades en produtos WAGO	30/03/2026	WAGO, en colaboración con CERTVDE, informou de 47 vulnerabilidades, 5 críticas, 21 altas e 21 medias, que poderían permitir evitar restricións de seguridade, escribir fóra dos límites do montículo e provocar a caída do dispositivo, entre outras accións.	Device Sphere, versións anteriores á 1.2.2; Solution Builder, versións anteriores á 2.4.2; Visualization And Control Hub, versións anteriores á 5.0.1.	CVE-2025-55315, CVE-2026-25983, CVE-2026-25897, CVE-2026-25987, CVE-2026-25898

Vulnerabilidades ICS críticas do primeiro trimestre de 2026. Fonte: elaboración propia (2026)

6.1.4 Exemplos reais de incidentes ICS

A evolución recente das ameazas en contornos industriais confirma unha tendencia consistente: unha parte crecente dos incidentes busca interromper operacións, non só roubar datos. Isto maniféstase tanto en ransomware e extorsión como en campañas de intrusión prolongada que explotan vulnerabilidades e credenciais válidas para acceder e moverse lateralmente entre sistemas [44][45].

En Europa, a explotación de vulnerabilidades mantense como vector de intrusión relevante e, na práctica, reduce a marxe de reacción das organizacións. No ámbito estatal e hacktivista, a presión xeopolítica incrementa a actividade contra sectores estratéxicos e infraestruturas críticas, incluídas organizacións do Estado español, polo que o risco non pode interpretarse como "alleo" ao contorno rexional.

Para o ecosistema industrial galego (auga, enerxía, alimentación, automoción, loxística…), o aspecto máis importante é que **moitos incidentes comezan en IT, pero acaban condicionando decisións operativas: paradas preventivas, operación degradada, recuperación escalonada e comunicación coa cadea de subministración**. Co fin de facer didáctico este bloque, descríbense tres incidentes recentes no Estado español do ano 2025 de xeito anonimizado, ofrecendo contexto sectorial e xeográfico, consecuencias observadas e mitigacións recomendables.

As descricións baséanse en información pública e en patróns recorrentes recollidos en informes sectoriais e repositorios de incidentes OT.

6.1.4.1 Incidente no sector augas

Nunha cidade mediana do nordeste peninsular, **un operador municipal de auga e saneamento sufriu un incidente no que varios sistemas corporativos quedaron cifrados, afectando a compoñentes administrativos e de atención ao público** (portais web, xestión interna e determinados servizos dixitais). A información dispoñible indica que o subministro e o saneamento se mantiveron, isto é, **non houbo impacto directo no proceso físico**. O escenario é representativo porque, mesmo cando OT non resulta comprometido, a perda de IT pode afectar operacións por dependencia funcional (xestión de incidencias, facturación, trazabilidade documental, coordinación con contratas).

Dende o punto de vista causal, este tipo de incidentes adoita encaixar en cadeas de ataque onde o acceso inicial se obtén por **servizos expostos, credenciais reutilizadas/comprometidas ou phishing**, e despois se produce movemento lateral e cifrado en dominios Windows. En contornos de servizos esenciais, a consecuencia máis habitual é a activación de protocolos de resposta e continxencia, con retorno temporal a procedementos manuais e coordinación con autoridades.

A aprendizaxe principal é arquitectónica e de gobernanza: cando existe **segmentación efectiva entre IT e OT**, control estrito de accesos remotos e unha práctica realista de continuidade, é posible conter o incidente no ámbito corporativo e manter a operación física.

Como **medidas preventivas e de mitigación** aplicables, recoméndanse: **endurecemento de acceso** (MFA e mínimos privilexios), **separación de dominios e rutas de administración**, **copias de seguridade** offline verificadas e **probas periódicas** de restauración, así como plans de continxencia que contemplen operación degradada e comunicación pública coordinada.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

6.1.4.2 Incidente na industria alimentaria

Nun polo industrial do sueste peninsular, **unha planta de produción alimentaria comunicou un ciberataque que obrigou a adoptar unha medida típica en contornos industriais: un apagado controlado** para conter a propagación e preservar a seguridade do proceso**. O efecto foi un impacto temporal na produción e na loxística asociada, con recuperación progresiva**. Este patrón é especialmente relevante para Galicia pola importancia do sector alimentario e pola súa dependencia de cadeas de frío, trazabilidade e prazos contractuais.

A literatura de referencia describe que, en incidentes de alto impacto, as organizacións poden escoller "parar con control" antes de arriscar unha parada caótica ou unha contaminación de dominios (por exemplo, propagación a servidores de planta, saltos a sistemas de supervisión ou bloqueo de estacións críticas). Este tipo de decisións non implica necesariamente compromiso OT, pero si evidencia a **interdependencia**: se as capacidades de monitorización, xestión de identidades ou certos servizos de planta dependen de IT, un incidente pode forzar unha parada por prudencia.

Didacticamente, cómpre salientar tres puntos.

- Primeiro, a rapidez: informes do sector sinalan que **unha parte significativa das intrusións modernas progresa a gran velocidade**, reducindo a ventá de detección e contención.
- Segundo, a gobernanza: **sen procedementos e responsabilidades claras** (quen decide parar, en que condicións, como se valida a volta á produción), **a resposta tende a ser improvisada.**
- Terceiro, a continuidade: **é imprescindible dispoñer de escenarios de operación degradada** e de recuperación por fases.

Como **medidas recomendables**, destacan: **reforzo de acceso remoto** (incluíndo rexistro e supervisión de sesións), **segmentación e listas de fluxo estritas entre IT/OT**, **endurecemento de endpoints** de usuarios e servidores de planta, e un **programa de xestión de vulnerabilidades** que priorice activos e exposición real, non só CVSS (tal e como se indica no presente informe técnico).

6.1.4.3 Incidente na industria pesada (metalurxia)

Nun entorno industrial do norte peninsular, **unha instalación de industria pesada comunicou un incidente que afectou a sistemas internos** e tivo como consecuencia unha **paralización significativa da actividade durante varios días, con recuperación escalonada e comunicación a clientes e provedores**. Este caso é útil

para ilustrar que **o impacto dun ciberataque non se mide só pola duración da parada, senón pola afectación á cadea de subministración** (pedidos, transporte, calidade, contratos) e polos custos de recuperación.

En contornos deste tipo, as causas recorrentes inclúen **explotación de vulnerabilidades** en compoñentes expostos (por exemplo, portais, VPNs, dispositivos perimetrais) **e deficiencias de segmentación** que permiten que un incidente IT degrade sistemas industriais por dependencia ou por accesos de administración compartidos.

Tamén se observa que **a recuperación require disciplina**: **inventario fiable**, restauración dende **backups verificadas, revalidación de integridade** e, moitas veces, **priorización de servizos mínimos** antes do retorno completo.

7 Conclusións

Este informe ofrece unha **lectura actualizada do panorama de vulnerabilidades que afecta aos contornos ICS/OT**, combinando unha **revisión conceptual dos principais modelos de avaliación do risco** asociado a vulnerabilidades cunha **análise práctica das alertas e tendencias observadas no período recente**. O enfoque seguido permite comprender non só a **crecente magnitude da problemática**, senón tamén as súas **implicacións reais sobre a operación industrial**, a continuidade do servizo e a seguridade das persoas e dos procesos.

Nun primeiro nivel, o documento aborda os **fundamentos que condicionan a xestión de vulnerabilidades en contornos industriais**, poñendo de manifesto as limitacións dos enfoques puramente técnicos ou baseados unicamente na severidade. Analízase o papel de métricas como CVSS, EPSS e KEV, así como os seus puntos fortes e carencias cando se aplican a sistemas onde a dispoñibilidade, o ciclo de vida prolongado dos activos e as restricións operativas son factores determinantes. Este marco permite interpretar o risco dende unha perspectiva máis próxima á realidade OT/ICS.

Nun segundo plano, preséntase unha **visión sintética das alertas e avisos máis relevantes do trimestre**, apoiada en fontes oficiais e especializadas. Esta revisión evidencia unha **tendencia á alza no volume de vulnerabilidades publicadas**, cun impacto transversal sobre fabricantes, tecnoloxías e sectores industriais.

O informe subliña que esta situación dificulta de forma notable a xa de por sí **complexa operativa da xestión de vulnerabilidades en ICS/OT**, facendo inviable un tratamento exhaustivo e homoxéneo de todos os avisos. Neste contexto, a priorización baseada no **risco efectivo** —e non só na severidade teórica— convértese nun elemento esencial para manter niveis aceptables de exposición sen comprometer a operación industrial.

A partir desta análise, expóñense **diversas alternativas e enfoques complementarios de mitigación**, dende modelos baseados en explotación coñecida ou probabilidade de ataque, ata estratexias apoiadas en segmentación, medidas compensatorias e gobernanza do parcheo.

Máis que propor unha solución única, o informe invita ao lector a **reflexionar críticamente sobre o seu propio contexto** e a **deseñar procedementos de xestión de vulnerabilidades adaptados**, combinando aquelas prácticas das descritas (ou

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

análogas) que mellor se aliñen co seu nivel de madurez, perfil de risco e capacidades operativas.

Reducir a complexidade mediante unha aproximación pragmática, estruturada e orientada ao impacto real, **é un dos principais retos actuais da ciberseguridade industrial en Galicia**, onde desgraciadamente o nivel de madurez neste eido todavía ten marxe de mellora. Se este boletín contribúe a que **algunha organización do ecosistema galego cuestione os seus modelos actuais, explore enfoques alternativos e avance cara a unha xestión máis eficaz e sostible do risco en OT, o obxectivo do Informe poderá darse por cumprido.**

En definitiva, o valor deste traballo reside en ofrecer **información accionable, criterios de análise e referencias prácticas** que axuden ás organizacións galegas a evolucionar cara a unha xestión máis madura das vulnerabilidades industriais, aliñada coa realidade operativa e coas mellores prácticas internacionais.

Isto posibilitará sen dúbida **fortalecer o ecosistema e o tecido produtivo do noso país para acadar un nivel de resiliencia acorde aos tempos que vivimos**, de tensión xeopolítica e automatización crecente da actividade cibercriminal.

Bibliografía

[1] SANS Institute (1989). *SANS Institute – Sitio oficial*. Recuperado de https://www.sans.org/

[2] SANS Institute (2024). *Risk-Based Vulnerability Management and Patching Industrial Systems*. Recuperado de https://www.sans.org/blog/risk-based-vulnerability-management-and-patching-industrial-systems

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

[4] Ciberseguridade Galicia – AMTEGA (2026). *Portal oficial de ciberseguridade de Galicia.* Recuperado de https://ciberseguridadegalicia.gal/gl

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

[6] National Institute of Standards and Technology (NIST) (1901). *National Institute of Standards and Technology – Sitio oficial*. Recuperado de https://www.nist.gov

[7] National Institute of Standards and Technology (NIST) (2025). *National Vulnerability Database (NVD) – Visualizacións da distribución de severidade CVSS ao longo do tempo*. Recuperado de https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

[8] Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Known Exploited Vulnerabilities Catalog (KEV)*. Recuperado de https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[9] Cybersecurity and Infrastructure Security Agency (CISA). (2018). *CISA – Sitio oficial*. Recuperado de https://www.cisa.gov/

[10] Cybersecurity and Infrastructure Security Agency (CISA). (2018). *Known Exploited Vulnerabilities Catalog – Feed en formato JSON*. Recuperado de https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

[11] Cybersecurity and Infrastructure Security Agency (CISA). (2018). *Servizo de subscrición a alertas e comunicacións de CISA*. Recuperado de https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?topic_id=USDHSCISA_136

[12] Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Reducing the Significant Risk of Known Exploited Vulnerabilities*. Recuperado de https://www.cisa.gov/known-exploited-vulnerabilities

[13] Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities*. Recuperado de https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

[14] National Institute of Standards and Technology (NIST). (2022). *DHS Binding Operational Directive 22-01 – Presentación técnica*. Recuperado de https://csrc.nist.gov/csrc/media/Presentations/2022/dhs-binding-operational-directive-bod-22-01/7-Bokan%20Day2%201130am%20DHS%20Binding%20Operational%20Directive%2022-01.pdf

[15] Cybersecurity News. (2025). *CISA expands KEV Catalog to include more actively exploited vulnerabilities*. Recuperado de https://cybersecuritynews.com/cisa-expands-kev-catalog/

[16] Tenable. (2024). *BOD 22-01: Key Exploitable Vulnerabilities Report*. Recuperado de https://www.tenable.com/tenable-io-reports/bod-22-01-key-exploitable-vulnerabilities-report

[17] Spring, J. M., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2018). *Towards Improving CVSS*. Recuperado de https://www.sei.cmu.edu/documents/574/2018_019_001_538372.pdf

[18] Dragos, Inc. (2024). *5 Reasons Why Risk-Based Vulnerability Management Matters in OT*. Recuperado de https://www.dragos.com/blog/5-reasons-why-risk-based-vulnerability-management-matters-in-ot

[19] Dragos, Inc. (2024). *Risk-Based Vulnerability Management for Operational Technology: A Framework for Prioritizing Risks to Industrial Control Systems*. Recuperado de https://hub.dragos.com/hubfs/116-Datasheets/Dragos_Risk-Based_Vulnerability_Management_OT_Cybersecurity.pdf?hsLang=en

[20] 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

[21] Instituto Nacional de Ciberseguridad (INCIBE). (2023). *EPSS: avanzando na predicción e xestión de vulnerabilidades*. Recuperado de https://www.incibe.es/incibe-cert/blog/epss-avanzando-en-la-prediccion-y-gestion-de-vulnerabilidades

[22] Jacobs, J., Romanosky, S., Edwards, B., Roytman, M., & Adjerid, I. (2019). *Predictive Vulnerability Scoring System (EPSS)*. Recuperado de https://i.blackhat.com/USA-19/Thursday/us-19-Roytman-Predictive-Vulnerability-Scoring-System-wp.pdf

[23] Forum of Incident Response and Security Teams (FIRST). (n.d.). *Exploit Prediction Scoring System (EPSS) Model*. Recuperado de https://www.first.org/epss/model

[24] Forum of Incident Response and Security Teams (FIRST). (n.d.). *EPSS Scores (CSV data)*. Recuperado de https://epss.empiricalsecurity.com/epss_scores-current.csv.gz

[25] Forum of Incident Response and Security Teams (FIRST). (n.d.). *EPSS API documentation*. Recuperado de https://www.first.org/epss/api

[26] Forum of Incident Response and Security Teams (FIRST). (n.d.). *EPSS User Guide*. Recuperado de https://www.first.org/epss/user-guide

[27] Forum of Incident Response and Security Teams (FIRST). (n.d.). *Probability, Percentiles, and Binning in EPSS scores*. Recuperado de https://www.first.org/epss/articles/prob_percentile_bins

[28] Qualys, Inc. (n.d.). *What is vulnerability management: detection and response*. Recuperado de https://www.qualys.com/fundamentals/what-is-vulnerability-management-detection-response

[29] Qualys, Inc. (2025). *How to shift from managing vulnerabilities to business-focused risk reduction* (white paper). Recuperado de https://cdn2.qualys.com/docs/mktg/whitepapers/how-to-shift-from-managing-vulnerabilities-to-business-focused-risk-reduction.pdf

[30] Tenable, Inc. (2025). *Solution overview: Tenable Vulnerability Priority Rating (VPR)*. Recuperado de https://dam.tenable.com/a4d872a3-0f2a-4dbd-99ff-b31c0109b502/solution-overview-tenable-vulnerability-priority-rating-vpr.pdf

[31] Tenable, Inc. (2020). *What is VPR and how is it different from CVSS*. Recuperado de https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss

[32] Tenable, Inc. (2024). *Enhancements to Tenable Vulnerability Priority Rating (VPR)* (white paper). Recuperado de https://dam.tenable.com/9cd34a71-a912-40c6-bf85-

b31c01120285/white-paper-enhancements-to-tenable-vulnerability-priority-rating-vpr.pdf

[33] Rapid7, Inc. (n.d.). *Prioritize vulnerabilities like an attacker with Active Risk.* Recuperado de https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/vulnerability-risk-score-sb.pdf

[34] Tenable, Inc. (n.d.). *A comparison of Tenable and Rapid7 approaches to vulnerability prioritization* (white paper). Recuperado de https://www.tenable.com/sites/default/files/uploads/documents/whitepapers/TEN_Rapid7PriorPaper_Final.pdf

[35] Cybersecurity and Infrastructure Security Agency (CISA). (2006). *Mitigations for Vulnerabilities in CSNets and Industrial Control Systems*. Recuperado de https://www.cisa.gov/sites/default/files/2023-01/MitigationsForVulnerabilitiesCSNetsISA_S508C.pdf

[36] National Institute of Standards and Technology (NIST). (2022). *NIST Special Publication 800-40 Revision 4: Guide to Enterprise Patch Management Technologies*. Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

[37] Centro de Ciberseguridad Industrial (CCI). (2025). *Levando o regulamento á realidade OT: medidas compensatorias en OT (Parte I)*. Recuperado de https://www.cci-es.org/activities/llevando-la-regulacion-a-la-realidad-ot-medidas-compensatorias-en-ot-parte-i/

[38] Centro de Ciberseguridad Industrial (CCI). (2025). *Levando o regulamento á realidade OT: medidas compensatorias en OT (Parte II)*. Recuperado de https://www.cci-es.org/activities/llevando-la-regulacion-a-la-realidad-ot-medidas-compensatorias-en-ot-parte-ii/

[39] Fortinet, Inc. (n.d.). *Virtual patching*. Recuperado de https://www.fortinet.com/lat/resources/cyberglossary/virtual-patching

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

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

[42] CCN-CERT (2025). *Vulnerabilidades — Seguridade ao Día*. Recuperado de https://www.ccn-cert.cni.es/es/seguridad-al-dia/vulnerabilidades.html

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

[44] Waterfall Security Solutions (2025). *2025 OT Cyber Security Threat Report*. Recuperado de https://waterfall-security.com/wp-content/uploads/2025/03/2025-OT-Cyber-Security-Threat-Report.pdf

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

[46] ENISA (2025). *Technical Implementation Guidance on Cybersecurity Risk Management Measures (Version 1.0)*. Recuperado de https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

[47] Government of Canada (2025). *Patch Management Guidance*. Recuperado de https://www.canada.ca/en/government/system/digital-government/online-security-privacy/cyber-security-guidance-policy/patch-management-guidance.html

[48] UK National Cyber Security Centre (NCSC) (n. d.). *Cyber Security Toolkit for Boards*. Recuperado de https://www.ncsc.gov.uk/files/NCSC-Cyber-Security-Toolkit-for-Boards.pdf

Glosario

Acceso remoto

Mecanismo que permite a conexión a sistemas industriais dende localizacións externas, frecuentemente empregado por fabricantes e integradores para tarefas de soporte e mantemento.

Activo crítico

Elemento de infraestrutura (hardware, software ou sistema) cuxa indispoñibilidade, compromiso ou mal funcionamento pode ter un impacto significativo na continuidade operativa, na seguridade das persoas ou no negocio.

Activos legados

Equipos ou sistemas industriais con longos ciclos de vida, a miúdo fóra de soporte do fabricante e con limitacións para aplicar actualizacións de seguridade.

Ameaza

Circunstancia ou evento potencial, intencionado ou accidental, capaz de explotar unha vulnerabilidade e causar un impacto negativo sobre un sistema, proceso ou organización.

Análise baseada en risco

Enfoque de xestión da ciberseguridade que prioriza decisións en función da probabilidade de explotación e do impacto real sobre o proceso, en lugar de empregar unicamente métricas técnicas.

Arquitectura defendible

Deseño de sistemas industriais que incorpora segmentación, control de accesos e mecanismos de detección para reducir a superficie de ataque e limitar o impacto dunha intrusión.

Binding Operational Directive (BOD)

Directiva operativa emitida por CISA de obrigado cumprimento para determinadas axencias federais. A do informe, orientada á mitigación de vulnerabilidades críticas.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Ciberalerta

Aviso emitido por un organismo, fabricante ou entidade especializada que informa da existencia dunha ameaza, vulnerabilidade ou campaña de ataque relevante.

Ciberfísico (sistema)

Sistema no que compoñentes dixitais interactúan directamente con procesos físicos, como ocorre nos entornos industriais e de infraestruturas críticas.

Ciberseguridade industrial

Conxunto de prácticas, tecnoloxías e procedementos orientados a protexer sistemas ICS/OT fronte a ameazas cibernéticas, preservando a seguridade, dispoñibilidade e estabilidade do proceso.

CIA (Confidencialidade, Integridade, Dispoñibilidade)

Tríade clásica da seguridade da información que define os tres obxectivos fundamentais de protección dos sistemas.

CISA (Cybersecurity and Infrastructure Security Agency)

Axencia federal dos Estados Unidos responsable da protección das infraestruturas críticas e da coordinación nacional en materia de ciberseguridade.

Contexto operativo

Conxunto de condicións técnicas, organizativas e funcionais que determinan como opera un sistema industrial e condicionan as decisións de seguridade.

Control compensatorio

Medida técnica ou organizativa que reduce o risco dunha vulnerabilidade cando a súa corrección directa (parcheo) non é viable.

Converxencia IT/OT

Integración progresiva de sistemas de tecnoloxía da información e tecnoloxía operacional, que incrementa a eficiencia pero tamén a superficie de ataque.

CVE (Common Vulnerabilities and Exposures)

Identificador estándar que permite referenciar de forma única unha vulnerabilidade coñecida.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

CVSS (Common Vulnerability Scoring System)

Sistema estándar de puntuación que avalía a severidade técnica das vulnerabilidades nunha escala de 0 a 10.

Detección continua

Capacidade de identificar eventos, anomalías ou ameazas de forma permanente mediante mecanismos de monitorización.

EPSS (Exploit Prediction Scoring System)

Modelo estatístico que estima a probabilidade de explotación dunha vulnerabilidade nun horizonte temporal determinado de 30 días, entre 0 e 1.

Explotabilidade

Facilidade técnica coa que unha vulnerabilidade pode ser explotada por un atacante.

Explotación activa

Uso confirmado dunha vulnerabilidade en ataques reais observados no mundo real.

Exposición

Grao no que un activo é accesible ou visible para posibles atacantes, tanto interna como externamente.

Gobernanza OT

Marco organizativo que define roles, responsabilidades e procedementos para a xestión da seguridade en entornos industriais.

Hardening

Proceso de reforzo da configuración dun sistema para reducir a súa superficie de ataque e minimizar riscos. Bastionado.

HMI (Human-Machine Interface)

Interface que permite aos operadores supervisar e interactuar cos procesos industriais.

ICS (Industrial Control Systems)

Conxunto de sistemas empregados para monitorizar e controlar procesos industriais.

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Impacto

Consecuencia potencial da materialización dunha ameaza sobre operacións, persoas, activos ou negocio.

Intelixencia de ameazas

Información analizada sobre actores, técnicas e campañas de ataque empregada para apoiar a toma de decisións de seguridade.

IT (Information Technology)

Tecnoloxías orientadas á xestión da información e dos sistemas corporativos.

KEV (Known Exploited Vulnerabilities)

Catálogo mantido por CISA que recolle vulnerabilidades con evidencia confirmada de explotación activa.

Mitigación

Acción destinada a reducir a probabilidade ou o impacto dunha vulnerabilidade ou ameaza.

Movemento lateral

Técnica empregada por atacantes para desprazarse entre sistemas dunha rede tras unha primeira intrusión.

Now / Next / Never

Modelo cualitativo de priorización de vulnerabilidades que clasifica as accións segundo a súa urxencia operativa.

NVD (National Vulnerability Database)

Base de datos pública do NIST que recompila información detallada sobre vulnerabilidades identificadas mediante CVE.

OT (Operational Technology)

Tecnoloxías empregadas para supervisar e controlar procesos físicos en entornos industriais.

Parada de planta

Interrupción planificada ou non planificada da produción industrial, con impacto operativo e económico.

Parcheo

Aplicación de actualizacións ou correccións para eliminar ou reducir vulnerabilidades nun sistema.

PLC (Programmable Logic Controller)

Dispositivo industrial programable empregado para controlar procesos e maquinaria.

Priorizar

Proceso de ordenar vulnerabilidades ou riscos segundo a súa relevancia e urxencia de tratamento.

Probabilidade

Estimación da posibilidade de que unha ameaza se materialice.

Proceso industrial

Conxunto de operacións físicas e lóxicas destinadas á produción de bens ou servizos.

Risco

Combinación da probabilidade de explotación dunha ameaza e do impacto asociado.

Risco técnico

Risco asociado exclusivamente ás características técnicas dunha vulnerabilidade, sen considerar o contexto operativo.

SCADA (Supervisory Control and Data Acquisition)

Sistema empregado para supervisar, controlar e adquirir datos de procesos industriais distribuídos.

Segmentación

Separación lóxica ou física de redes e sistemas para limitar movementos laterais e reducir a superficie de ataque.

Seguridade funcional (Safety)

Protección das persoas, instalacións e do proceso fronte a fallos que poidan causar danos físicos.

Superficie de ataque

Conxunto de puntos de entrada potencialmente explotables nun sistema ou infraestrutura.

Vulnerabilidade

Debilidade nun sistema, proceso ou configuración que pode ser explotada por unha ameaza.

Xanela de mantemento

Período temporal planificado no que se permiten intervencións técnicas en sistemas industriais.

Anexo. Avisos de fabricantes OT

Coa fin de facilitar a consulta directa dos avisos de seguridade publicados polos principais fabricantes de tecnoloxía industrial, inclúese a continuación unha **relación dos portais oficiais onde cada provedor publica vulnerabilidades, parches, mitigacións e boas prácticas asociadas aos seus produtos.** Tanto advisories de alertas, como PSIRT (Product Support Incident Response Team), ou soporte a incidencias de seguridade nos produtos.

Este anexo **serve como complemento natural á sección de alertas do trimestre**, permitindo ao lector acceder rapidamente á información primaria e manter un seguimento continuo das actualizacións de seguridade relevantes para o seu entorno.

Fabricante	URL dos advisories / PSIRT
ABB	https://global.abb/group/en/technology/cyber-security/alerts-and-notifications
Advantech	https://www.advantech.com/en-eu/security-advisory
Beckhoff	https://infosys.beckhoff.com/english.php?content=../content/1033/ipc_security/976057355.html&id=
Belden / Hirschmann	https://www.belden.com/support/security-assurance
Bosch (PSIRT)	https://psirt.bosch.com/security-advisories/
Bosch Rexroth	https://www.boschrexroth.com/en/dc/product-security/security-advisories/
B&R (Bernecker & Rainer Automation)	https://www.br-automation.com/en/service/cyber-security/cyber-security-advisories-and-notices/
Delta Electronics	https://www.deltaww.com/en-US/service-support/product-cybersecurity/advisory
Eaton	https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/security-notifications.html

Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ · XUNTA DE GALICIA · Xacobeo 2027

Emerson	https://www.emerson.com/en-us/support/security-notifications
Endress+Hauser	https://www.endress.com/en/pages/security
FANUC	https://www.fanuc.co.jp/en/product/vulnerability/
Festo	https://www.festo.com/us/en/e/support/get-support/report-security-risk-psirt-id_330543/
Honeywell	https://www.honeywell.com/us/en/product-security#security-notices
Johnson Controls	https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories
Mitsubishi Electric	https://www.mitsubishielectric.com/psirt/vulnerability/index.html
Moxa	https://www.moxa.com/en/support/product-support/security-advisory
Omron	https://automation.omron.com/en/us/about-omron-automation/cybersecurity
Phoenix Contact	https://www.phoenixcontact.com/en-pc/service-and-support/psirt
Pilz	https://www.pilz.com/en-INT/support/psirt
Rockwell Automation	https://www.rockwellautomation.com/en-gb/trust-center/security-advisories.html
Schneider Electric	https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp
SICK	https://www.sick.com/de/en/service-and-support/the-sick-product-security-incident-response-team-sick-psirt/w/psirt#advisories
Siemens	https://www.siemens.com/global/en/products/services/cert.html?SiemensSecurityAdvisories=
WAGO	https://www.wago.com/global/automation-technology/psirt
Yokogawa	https://www.yokogawa.com/es/library/resources/white-papers/yokogawa-security-advisory-report-list/

Táboa de advisories de fabricantes de ICS/OT. Fonte: elaboración propia (2026)

Esta relación non é exhaustiva, pero recolle a varios dos fabricantes máis presentes en entornos ICS/OT, de xeito ampliado con respecto á primeira edición do Informe. Aconséllase ao lector buscar os recursos asociados aos seus fabricantes de referencia.

A integración sistemática da información procedente destes portais nos procesos habituais de seguridade facilita unha xestión máis proactiva do risco, organizar de maneira máis eficiente as intervencións de mantemento e garantir unha supervisión continua acorde tanto co risco asumido como co ciclo de explotación dos sistemas industriais.

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridade Industrial
Informe de ciberalertas – II

AMTEGA – Xunta de Galicia 2026

Financiado pola Unión Europea NextGenerationEU
Plan de Recuperación, Transformación e Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
XUNTA DE GALICIA
Xacobeo 2027