CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad Industrial

Informe de ciberalertas - II

Abril 2026

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

Edita: Xunta de Galicia

Agencia para la Modernización Tecnológica de Galicia (AMTEGA)

Lugar: Santiago de Compostela

Año: 2026

Índice

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

1 Introducción

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

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

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

--

La creciente exposición de las infraestructuras industriales a amenazas de ciberseguridad sigue consolidándose como uno de los principales retos para la seguridad operativa, la continuidad del negocio y, en muchos casos, la seguridad física de las personas. La progresiva digitalización de los procesos industriales, la incorporación de tecnologías de Internet de las Cosas (IoT) y en el borde (Edge), y la convergencia estructural entre entornos IT y OT están a ampliar de forma sostenida la superficie de ataque de los sistemas de control industrial (ICS), al tiempo que incrementan la complejidad de su protección.

Si el **Informe de Ciberalertas OT – I** desde Observatorio de la AMTEGA sentó las bases conceptuales de la gestión de vulnerabilidades —definiciones, clasificaciones, tiempos de explotación y remediación, y fundamentos económicos del riesgo—, este segundo informe se centra en un problema eminentemente práctico: **como priorizar actuaciones en un contexto en el que el volumen de vulnerabilidades publicadas es estructuralmente inmanejable para la mayoría de las organizaciones industriales**.

La evidencia empírica muestra que cada año se publican miles de nuevas vulnerabilidades o CVEs, una proporción muy elevada de las mismas con severidad media o alta según CVSS. En entornos industriales, caracterizados por ciclos de vida largos, restricciones operativas severas y dependencia ventanas de mantenimiento planificadas, pretender mantener una infraestructura "libre de vulnerabilidades" mediante parcheo sistemático resulta, en la práctica, inviable. Esta realidad obliga a abandonar enfoques puramente reactivos o basados exclusivamente en métricas técnicas, y avanzar hacia **estrategias de priorización basadas en el riesgo real para el proceso y el negocio**.

En este contexto, el presente informe introduce y desarrolla distintos enfoques complementarios orientados a apoyar la toma de decisiones en entornos OT. Se analizan las limitaciones prácticas del uso exclusivo de CVSS como criterio de urgencia, y se exploran alternativas más accionables que incorporan información sobre explotación activa, probabilidad real de ataque y contexto operativo. Entre ellas destacan el **catálogo de vulnerabilidades explotadas conocidas (KEV) de la CISA**, los modelos de clasificación operativa como **Now / Next / Never**, y métricas probabilísticas como **EPSS**, así como aproximaciones más avanzadas empleadas en soluciones comerciales especializadas.

El objetivo no es sustituir un estándar por otro, sino **proporcionar un marco coherente que permita a las organizaciones industriales decidir donde invertir esfuerzos limitados para reducir de forma efectiva** el riesgo, manteniendo el equilibrio entre seguridad, disponibilidad y estabilidad del proceso. De esta forma, el informe mantiene el enfoque didáctico y aplicado del Observatorio de Ciberseguridad Industrial, reforzando su utilidad como herramienta de apoyo para responsables de operación, ingeniería, mantenimiento y seguridad en el ecosistema industrial gallego.

Adicionalmente, el informe se completa con una recopilación de **buenas prácticas internacionales en materia de gestión de vulnerabilidades**, el análisis de **medidas compensatorias y estrategias de mitigación cuando el parcheo no es viable**, y una selección de las **principales ciberaleralertas registradas durante el primer trimestre**, con el objetivo de ofrecer una visión integral, práctica y actualizada de la situación de la ciberseguridad industrial y sus amenazas 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 Resumen ejecutivo

Este informe tiene como objetivo principal apoyar la toma de decisiones en materia de **priorización de riesgos de ciberseguridad en entornos industriales (OT/ICS).**

El contexto en el que se encuadra este documento viene marcado por un **incremento sostenido de la explotación de vulnerabilidades conocidas**, una creciente profesionalización del cibercrimen y una mayor exposición de los sistemas industriales como consecuencia de la convergencia IT/OT y de la dependencia de servicios digitales externos. A este escenario se añade un hecho estructural: **el volumen anual de nuevas CVE publicadas, muchas de ellas clasificadas como de severidad media o alta según CVSS, supera ampliamente la capacidad real de las organizaciones industriales para aplicar parches de forma sistemática**. El universo total agregado es de más de trescientas mil CVEs en la actualidad.

En entornos OT/ICS, esta limitación no es sólo organizativa, sino también técnica y operativa. Los largos ciclos de vida de los equipos, las restricciones de certificación por parte de los fabricantes, la dependencia de energías de mantenimiento planificadas y el riesgo de regresión funcional hacen que **parchearlo todo no sea técnicamente viable ni deseable desde el punto de vista de la continuidad del negocio**. Esta realidad obliga a abandonar enfoques exhaustivos o basados exclusivamente en métricas técnicas, y avanzar hacia **estrategias de priorización basadas en el riesgo real, en la explotación efectiva y en el contexto operativo**.

Desde una perspectiva de negocio, el informe pone el foco en la **continuidad operativa, la seguridad de las personas y la protección de los procesos críticos**, aspectos especialmente sensibles en sectores industriales y de infraestructuras esenciales. Las interrupciones derivadas de incidentes de ciberseguridad en OT no se traducen únicamente en pérdidas económicas directas, sino también en impactos reputacionales, incumplimientos regulatorios y, en casos extremos, riesgos para la seguridad física.

Para dar respuesta a este reto, el informe se estructura alrededor de distintos **enfoques complementarios de priorización**:

- El **Catálogo de Vulnerabilidades Conocidas Explotadas (KEV)** de la CISA. El KEV permite identificar aquellas vulnerabilidades para las que existe evidencia de explotación activa en el mundo real, actuando como un primer filtro de urgencia frente al elevado volumen de CVE disponibles.

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

- Este enfoque se completa con otros modelos de priorización empleados en el ámbito industrial, como **Now / Next / Never**, que facilita una clasificación cualitativa de las vulnerabilidades según la urgencia real de actuación;
- **EPSS (Exploit Prediction Scoring System)**, que introduce una estimación probabilística de la probabilidad de explotación;
- y **modelos más avanzados empleados por soluciones comerciales**, basados en la combinación de CVSS, inteligencia de amenazas, exposición y contexto operativo mediante algoritmos e inteligencia propia.

En conjunto, estos enfoques permiten pasar de una lectura puramente técnica a una **gestión basada en riesgo e impacto** en el proceso, especialmente adecuada para entornos OT, **para ayudar a los responsables de planta y ciberseguridad, a decidir cuál es la estrategia de gestión más apropiada en su** caso.

Junto con el análisis de vulnerabilidades y los mecanismos de priorización, el informe incorpora un conjunto de **buenas prácticas internacionales de gestión de vulnerabilidades**, así como **medidas compensatorias y estrategias de mitigación orientadas a reducir el riesgo cuando el parcheo no es inmediato o viable**. Estas incluyen acciones técnicas, organizativas y de arquitectura que permiten actuar sobre la probabilidad y el impacto de los incidentes, reforzando la resiliencia de los sistemas industriales a corto y medio plazo.

En síntesis, se pretende trasladar un mensaje claro: la gestión de la ciberseguridad en OT no puede basarse en un enfoque exhaustivo y reactivo, sino en un modelo **selectivo, pragmático y basado en riesgo real**, que tenga en cuenta las limitaciones técnicas del parcheo, priorice las vulnerabilidades con explotación confirmada o mayor probabilidad de ataque, y combine métricas técnicas con contexto operativo.

El informe se completa con el **nuevo análisis de las ciberalertas de mayor severidad registradas durante el trimestre (donde destacaríamos las que afectan a varias soluciones de Siemens, Schneider o Mitsubishi Electric)**, así como con un **anexo específico con los principales avisos de seguridad publicados por fabricantes de equipamiento ICS/OT** (extendido con respecto a la versión original del Informe), proporcionando de este modo una visión integral, actualizada y accionable del estado de la amenaza para responsables técnicos y de negocio.

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

3 Metodología y fuentes

El **Informe de Ciberalertas – II** se ha elaborado siguiendo una metodología similar a la empleada en la primera edición del informe, con el objetivo de mantener coherencia entre entregables y facilitar su lectura comparada. En esta segunda edición, la metodología se ajusta al foco específico del documento, centrado en **la priorización de vulnerabilidades, la gestión del riesgo y las estrategias de mitigación en entornos OT/ICS**.

La redacción del informe se ha basado en un proceso estructurado en varias fases, orientado a la recopilación, selección y análisis de información relevante para ciberseguridad industrial:

- **Identificación y seguimiento de fuentes oficiales** de alertas, vulnerabilidades y amenazas, tanto a nivel nacional como internacional.
- **Revisión periódica de catálogos de vulnerabilidades**, prestando especial atención a aquellas con evidencia de explotación activa o impacto potencial en entornos industriales.
- **Selección de contenidos relevantes**, priorizando su aplicabilidad práctica en cuanto a la priorización y mitigación de vulnerabilidades detectadas.
- **Análisis contextual en clave OT**, teniendo en cuenta las limitaciones propias de estos entornos en materia de parcheo, mantenimiento y gestión de cambios.

Este enfoque permite centrar el informe en las vulnerabilidades y alertas más relevantes desde un punto de vista operativo, evitando una simple enumeración de avisos.

Las fuentes de información utilizadas añaden algunas nuevas a las ya empleadas por el Observatorio en la edición previa:

- Los **marcos conceptuales y el análisis basado en riesgo** se apoyan en los trabajos del SANS Institute sobre gestión de Vulnerabilidades basada en riesgo, así como en estudios académicos y técnicos centrados en la mejora de las métricas de severidad y prioridad. Estas aportaciones justifican la necesidad de ir más allá del CVSS tradicional, especialmente en entornos OT.
- Para los **estándares y métricas de severidad,** se ha empleado principalmente la 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 y al ecosistema CVE como base común para la identificación de vulnerabilidades.

- Los **catálogos y datos sobre vulnerabilidades y explotación** se basan en fuentes de NIST/NVD para el análisis cuantitativo y la evolución histórica de la severidad, así como en el catálogo Known Exploited Vulnerabilities (KEV) de CISA, incluyendo su documentación técnica y feeds de datos, como referencia central para la explotación activa.
- El **marco regulatorio y las directrices operativas asociadas al KEV** se han fundamentado en las directrices publicadas por CISA, junto con material técnico de apoyo de NIST y análisis sectoriales que contextualizan la evolución y el alcance de este catálogo.
- Las **métricas de probabilidad de explotación (EPSS)** se introducen a partir de documentación de FIRST y contribuciones académicas, permitiendo complementar la severidad técnica con estimaciones probabilísticas de explotación.
- Los **enfoques comerciales y modelos avanzados de priorización** se ilustran mediante documentación pública y white papers de fabricantes de soluciones de gestión de vulnerabilidades como Qualys, Tenable o Rapid7, como ejemplo de la integración de métricas, inteligencia de amenazas y contexto operativo.
- Para las **buenas prácticas de gestión de vulnerabilidades y mitigación**, se han utilizado guías y recomendaciones de organismos públicos y fabricantes tecnológicos, cubriendo aspectos como parcheo, medidas compensatorias y virtual patching.
- Finalmente, **las alertas operativas y avisos del trimestre** se basan en información procedente de organismos nacionales de respuesta a incidentes y en los avisos de seguridad industrial publicados por CISA y redifusionados por INCIBE.

Estas fuentes se han empleado tanto para la identificación de alertas relevantes como para la elaboración de las secciones de priorización y recomendaciones.

Se recuerda que el informe no pretende ser exhaustivo ni sustituir a los sistemas de vigilancia continua de las organizaciones. Su objetivo **es ofrecer una visión sintética y práctica de las alertas y vulnerabilidades más relevantes del período analizado**,

así como proporcionar criterios y referencias que faciliten la toma de decisiones en materia de ciberseguridad industrial.

La información presentada debe ser interpretada como apoyo a la gestión del riesgo, y complementada con análisis específicos adaptados al contexto técnico y operativo de cada organización.

4 Priorización de vulnerabilidades

4.1 Contexto ICS/OT frente a IT tradicional

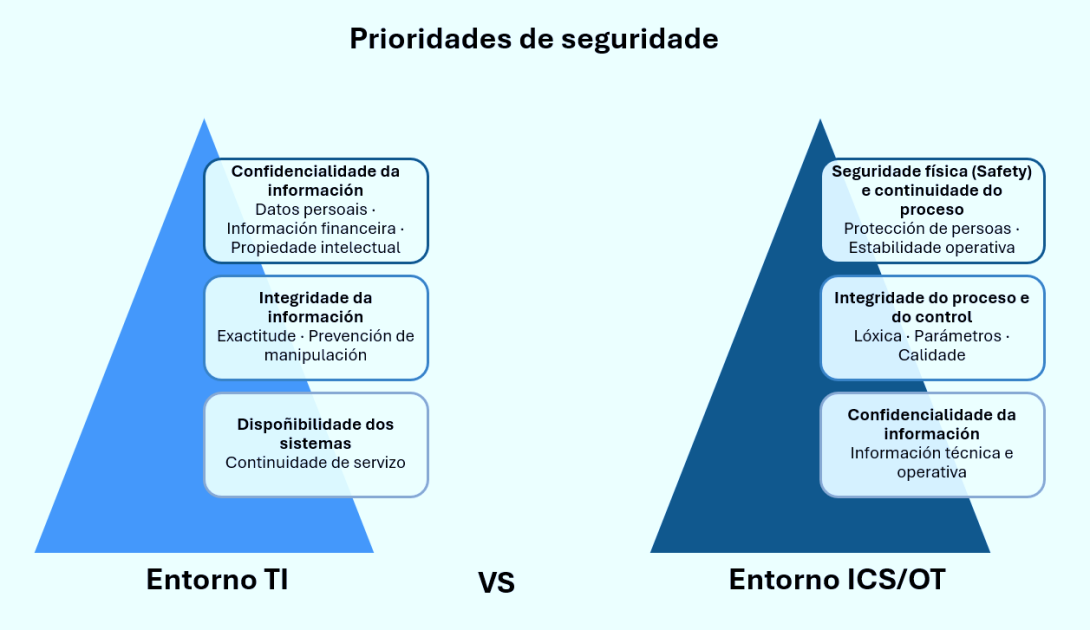
4.1.1 Dimensiones de seguridad

La convergencia IT/OT y la digitalización industrial pueden llevar a aplicar, por inercia, prácticas de seguridad diseñadas para entornos corporativos. Sin embargo, los entornos **ICS/OT (Industrial Control Systems / Operational Technology)** presentan restricciones técnicas, operativas y de seguridad funcional que hagan que su modelo de operación y su ciberseguridad deban abordarse con un **enfoque diferenciado**.

De manera sintética, en TI adopta primar la protección de datos y servicios de información, mientras que en OT el objetivo último es garantizar que el proceso físico se mantenga **seguro, estable, disponible y dentro de especificación**, incluso en condiciones degradadas.

La tría clásica **CIA (Confidencialidad, Integridad, Disponibilidad)** continúa siendo válida como marco general. Con todo, el orden de prioridad y la interpretación de los impactos difieren.

- En TI, **la confidencialidad** e **integridad de la información** acostumbran a ser determinantes (datos personales, propiedad intelectual, información financiera), con impactos reputacionales y legales muy relevantes.
- En OT, la **disponibilidad del proceso y la seguridad física (safety)** adoptan ser críticas: una intrusión puede traducirse en **paradas de planta**, **pérdida de control**, **daños en equipamiento**, **degradación de calidad**, o incluso **riesgo para personas**.



Prioridades de seguridad según el tipo de entorno. Fuente: elaboración propia (2026)

En consecuencia, una vulnerabilidad con impacto "moderado" desde una lectura puramente TI puede ser **crítica** si afecta a la capacidad de controlar un PLC, una HMI, una pasarela industrial o un SCADA que actúa sobre un proceso físico. Y **un elemento crítico a resaltar, es que el riesgo en OT incluye efectos ciberfísicos**, no sólo digitales.

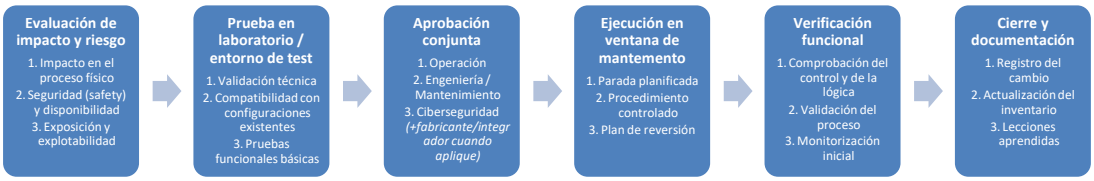
4.1.2 Contexto operativo

En este campo, los entornos industriales están diseñados para operar con **altos niveles de previsibilidad y estabilidad**, frecuentemente con requisitos de tiempo real. Esto condiciona prácticas que en TI se consideran rutinarias:

- **Ventanas de mantenimiento limitadas**: muchos activos sólo pueden intervenir durante paradas planificadas o campañas anuales.
- **Alta sensibilidad a interrupciones**: escaneos agresivos, reinicios no coordinados o cambios de configuración pueden provocar indisponibilidades o estados no previstos.
- **Dependencias complejas**: cambios en firmware, drivers, librerías, o en el software de ingeniería pueden afectar a la compatibilidad con versiones de proyectos, comunicaciones industriales o módulos de E/S.

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

Así, mientras en TI el "cambio" (actualizaciones frecuentes, hardening continuo) forma parte del ciclo normal, en OT el cambio requiere **gestión de cambios rigurosa**, pruebas y coordinación con operación y mantenimiento:



Gestión de cambios en entornos OT (ICS/OT). Fuente: elaboración propia (2026)

4.1.3 Modelado de amenazas

En lo relativo a la ciberseguridad, la superficie de ataque se concentra principalmente en el usuario: endpoints, correo, identidad, SaaS y exposición a Internet. En OT, además de esos factores (por convergencia), existen riesgos específicos:

- **Protocolos industriales históricamente inseguros** (sin cifrado ni autenticación fuerte por diseño como Modbus), con alta prevalencia en entornos legados.
- **Acceso remoto de terceros y mantenimientos** (integradores, fabricantes, soporte), a menudo esencial para la continuidad del negocio.
- **Segmentación imperfecta y puntos de salto IT/OT**, donde una intrusión en TI puede derivar en movimiento lateral hacia OT.
- **Activos de larga vida útil** (10–25 años), con obsolescencia, fin de soporte y limitaciones para actualizar.

4.1.4 Gobernanza

Un **elemento clave para una gestión eficaz de la ciberseguridad** es la **gobernanza**. Mientras que en entornos TI las decisiones sobre configuraciones y parcheo adoptan centralizarse en los equipos de sistemas o seguridad, en los entornos OT estas decisiones tienen un carácter necesariamente **transversal**. Su correcta adopción requiere la participación coordinada de operación, mantenimiento, ingeniería y ciberseguridad, así como, en muchos casos, de proveedores e integradores tecnológicos.

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

Por este motivo, resulta recomendable disponer **de un marco formal de gobernanza OT**, que incluya procedimientos estructurados de gestión de cambios, mecanismos claros para priorizar vulnerabilidades y un conjunto de criterios documentados que permitan decidir de manera informada cuando aceptar riesgo, posponer la aplicación de parches o aplicar medidas compensatorias. Este enfoque favorecerá decisiones equilibradas entre seguridad, continuidad operativa y seguridad funcional.

Todas estas diferencias descritas entre entornos IT tradicionales e ICS/OT, explican la razón por la que, en entornos industriales:

- La prioridad no es "parchear todo cuanto antes", sino **gestionar el riesgo del proceso**. De esto hablaremos en la próxima sección.
- La información más valiosa no es sólo el listado de CVEs y severidades asociadas, sino el **contexto operativo, el nivel de riesgo asumible y las capacidades de mitigación.** Aquí entran en juego las estrategias de mitigación descritas posteriormente en este Informe, y que forman la parte nuclear del mismo.
- Y la toma de decisiones requiere equilibrar **seguridad, continuidad y Safety**.

4.2 Gestión basada en riesgo

La gestión de la ciberseguridad en **entornos industriales ICS/OT** debe entenderse, de manera prioritaria, como un ejercicio de **gestión del riesgo**. En un contexto en el que los sistemas digitales interactúan directamente con procesos físicos, personas e instalaciones, el objetivo no puede ser la eliminación completa del riesgo —algo inasumible en sistemas complejos y operativos—, sino su **identificación, comprensión y tratamiento hasta niveles compatibles con los objetivos de negocio**.

Desde una perspectiva didáctica, el riesgo puede definirse como la **posibilidad de que un evento adverso se materialice y genere consecuencias negativas sobre la organización**. En entornos industriales, estas consecuencias no se limitan a pérdidas económicas o reputacionales, sino que pueden afectar a la **continuidad de la producción, calidad del producto, cumplimiento regulatorio y, de manera especialmente crítica, la seguridad física de las personas e instalaciones (safety)**. Por este motivo, la gestión del riesgo constituye un elemento central de la gobernanza de la seguridad industrial.

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

De forma clásica, el riesgo se expresa como una combinación entre la probabilidad de ocurrencia de un evento y el impacto asociado a su materialización, según la relación ampliamente aceptada:

Riesgo = Probabilidad × Impacto

Aunque esta formulación cuantitativa es deliberadamente sencilla, resulta muy útil para comprender que el riesgo no es un valor absoluto ni inherente a un elemento aislado, sino el resultado de un **conjunto de factores que deben interpretarse en su contexto real**. En particular, también en el ámbito de la ciberseguridad industrial, esto implica reconocer que una vulnerabilidad técnica, por sí sola, no define el riesgo.

En entornos ICS/OT, el denominado **riesgo técnico** depende de la interacción de múltiples variables. La existencia de una vulnerabilidad es sólo uno de los componentes de la ecuación. El riesgo real viene condicionado, entre otros aspectos:

- por la **factibilidad técnica del ataque**,
- por la **exposición del activo vulnerable dentro de la arquitectura industrial**,
- por su **papel en el proceso operativo,**
- y por las **consecuencias reales que tendría una pérdida (de control, fuga de información o una indisponibilidad).**

De esta forma, dos **vulnerabilidades con una severidad técnica similar pueden representar niveles de riesgo radicalmente distintos** en función del entorno en el que estén desplegadas.

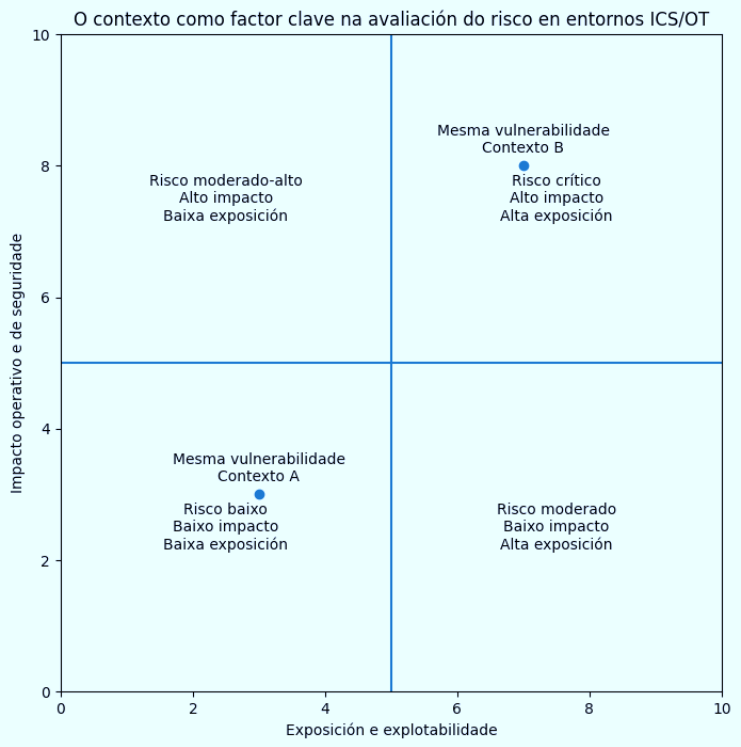
Esta visión contextual resulta especialmente relevante a la hora de gestionar vulnerabilidades en sistemas industriales. La aplicación mecánica de métricas técnicas descontextualizadas puede conducir a decisiones poco realistas, como priorizar correcciones de bajo impacto operativo mientras se relegan otras que, sin destacar técnicamente, suponen un riesgo significativo para el proceso. En respuesta a esta problemática, en los últimos años se ha consolidado el enfoque de **gestión de vulnerabilidades basada en riesgo**.

En este sentido, resulta particularmente ilustrativo y conciso el enfoque expuesto por el SANS Institute [1] en el artículo Risk-Bad Vulnerability Management and Patching Industrial Systems [2], en lo que se aborda de manera explícita la diferencia entre una gestión de vulnerabilidades basada únicamente en métricas técnicas y una gestión realmente basada en riesgo en entornos industriales.

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

El artículo pone el foco en que, en ICS/OT, la decisión de **cuándo y cómo mitigar una vulnerabilidad** debe contrapesar dos ejes fundamentales: por una parte, la **amenaza potencial** asociada a la vulnerabilidad (incluyendo su explotabilidad y el impacto en el proceso) y, por la otra, el **coste técnico y operativo de la mitigación**, que puede incluir paradas de planta, riesgos de regresión funcional, pérdida de estabilidad o dependencia de terceros. Desde esta perspectiva, parchear "todo cuanto antes" no sólo resulta inviable, sino que puede introducir nuevos riesgos.

SANOS subraya que el **contexto es decisivo**: la misma vulnerabilidad puede ser crítica o asumible dependiendo de su exposición real, del rol del activo en el proceso y de las medidas compensatorias existentes.



Nivel de riesgo para una misma vulnerabilidad según el contexto. Fuente: elaboración propia (2026)

Por este motivo, el articulo **cuestiona el uso del indicador** para medir la severidad de las vulnerabilidades **CVSS** (Common Vulnerability Scoring System Standard, de 0 a 10), [3] ya descrito en el anterior Informe de Ciberalertas - I disponible en la web de la AMTEGA [4], como único criterio de priorización; señala que la magnitud de una puntuación de severidad no refleja por sí sola la urgencia real de mitigación en un entorno industrial, si no se analiza junto con el contexto operativo y el riesgo global, que es diferente en cada organización.

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

Esta aproximación sirve como base conceptual para la siguiente sección del informe, en la que se revisará el papel del **CVSS**, y se introducirán **métricas y enfoques complementarios** orientados a medir no sólo la severidad técnica, sino también la **urgencia real de mitigación** desde una perspectiva más práctica y realista para entornos ICS/OT, teniendo en cuenta que **a día de hoy, existen más de trescientas mil vulnerabilidades publicadas y** con etiqueta o nomenclatura estándar para identificación de la vulnerabilidad (CVE, Common Vulnerabilities and Exposures) asignada [5].

4.3 CVSS (Sistema Común de Puntuación de Vulnerabilidades)

El **CVSS (Common Vulnerability Scoring System)** [3] es un estándar ampliamente adoptado para **evaluar la gravedad de las vulnerabilidades**, asignándoles una puntuación numérica en función de diferentes parámetros técnicos. Entre ellos se incluyen aspectos como la facilidad de explotación, el impacto potencial sobre la confidencialidad, la integridad y la disponibilidad, o la necesidad de interacción por parte del usuario afectado.

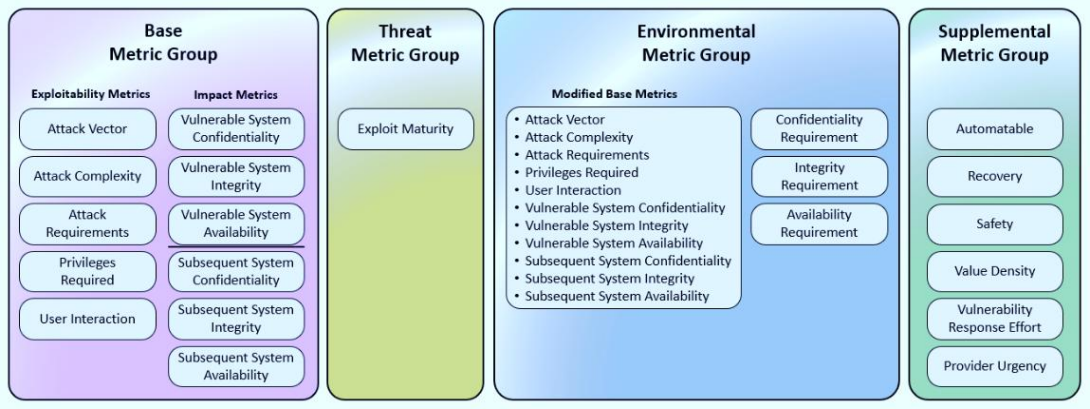
La versión **CVSS 4.0** representa la evolución más reciente de este estándar internacional e introduce un modelo más **flexible, expresivo y preciso** que versiones anteriores. Su propósito es ofrecer una valoración que no sólo describa las características técnicas intrínsecas de una vulnerabilidad, sino que también permita **aproximarse mejor a su impacto real y a su comportamiento en función del contexto en** el que se manifiesta. Para ello, CVSS 4.0 estructura su evaluación en torno a cuatro **grandes grupos de métricas**, que permiten caracterizar con mayor detalle el riesgo asociado.

- El primer grupo corresponde a las **métricas Base**, que describen las propiedades inherentes de la vulnerabilidad y no dependen ni del momento temporal ni del entorno concreto en el que se encuentre el sistema afectado. Estas métricas se subdividen en dos bloques:
    - por una banda, las métricas de **Explotabilidad**, que reflejan la dificultad técnica de la explotación (vector de ataque, complejidad, privilegios necesarios o interacción del usuario);
    - y, por otra, las métricas de **Impacto**, que evalúan las consecuencias directas de una explotación exitosa. En este apartado se considera no sólo el efecto sobre el componente directamente afectado, sino también sobre sistemas relacionados, incorporando incluso posibles

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

repercusiones sobre la seguridad física, una dimensión que cobra especial relevancia en entornos industriales y ciberfísicos.

- El segundo grupo está constituido por las **métricas de Amenaza**, que introducen información sobre el estado real de explotación de la vulnerabilidad. Dado que estos factores evolucionan con el tiempo, este conjunto permite ajustar la valoración cuando existen evidencias públicas de explotación, código disponible o incidentes confirmados. De esta forma, dos vulnerabilidades con impacto técnico semejante pueden recibir puntuaciones diferentes en función de la actividad observada por parte de actores maliciosos.
- El tercer grupo, correspondiente a las **métricas Ambientales**, permite adaptar la puntuación al **contexto específico de cada organización**. Estas métricas tienen en cuenta elementos como la criticidad del activo afectado, la existencia de controles mitigadores o la relevancia relativa de cada dimensión de seguridad. En entornos OT, CPS o industriales, donde la disponibilidad del proceso y la seguridad física adoptan prevalecer frente a la confidencialidad, este ajuste resulta especialmente relevante para reflejar con mayor fidelidad la severidad operativa de una vulnerabilidad.
- Finalmente, CVSS 4.0 incorpora un cuarto conjunto de **métricas Suplementarias**, diseñadas para aportar información adicional sobre características externas de la vulnerabilidad, como posibles implicaciones reglamentarias, aspectos relacionados con la seguridad humana o la viabilidad de la explotación automatizada. Estas métricas no influyen en el cálculo de la puntuación final, pero proporcionan contexto adicional que puede ser empleado por las organizaciones para enriquecer sus propios modelos de priorización.



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

La escala de CVSS aún en su cuarta versión, continúa establecida entre 0 y 10, clasificando las vulnerabilidades en cuatro niveles de severidad:

Nivel de gravedad	Puntuación CVSS
Ninguna	0.0
Baja	0.1 – 3.9
Media	4.0 – 6.9
Alta	7.0 – 8.9
Crítica	9.0 – 10.0

Categorías de severidad de CVSS 4.0. Fuente: elaboración propia (2026)

En conjunto, **CVSS 4.0 ofrece una evaluación algo más matizada de la hermana de las vulnerabilidades,** pero, aun así, en muchos ámbitos no se considera suficiente.

4.3.1 Limitaciones de CVSS

Aunque **CVSS** constituye una referencia ampliamente aceptada para describir la severidad técnica de las vulnerabilidades, su aplicación directa y aislada presenta **limitaciones prácticas significativas en entornos OT e industriales**. Estas limitaciones no derivan de deficiencias del estándar en sí mismo, sino del hecho de que fue concebido como un **sistema de clasificación técnica**, no como un mecanismo completo de toma de decisiones operativas.

- En primer lugar, CVSS **no incorpora de forma explícita el contexto operativo real** en el que se encuentra el activo vulnerable. En entornos ICS/OT, factores como la función del equipo en el proceso, la existencia de redundancias, el impacto de una parada no planificada o la presencia de controles compensatorios pueden ser determinantes a la hora de evaluar el riesgo. Dos vulnerabilidades con una puntuación CVSS idéntica pueden requerir respuestas radicalmente distintas según el entorno industrial en el que se manifiesten.
- En segundo lugar, la puntuación CVSS **no refleja necesariamente la amenaza real en el tiempo**. Una vulnerabilidad con una severidad técnica elevada puede no estar a ser explotada activamente, mientras que otra con puntuación inferior puede formar parte de campañas de ataque conocidas. En entornos OT, donde el

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

parcheo inmediato no siempre es viable, esta distinción resulta clave para priorizar actuaciones de forma realista.

- Adicionalmente, CVSS **no tiene en cuenta el coste técnico y operativo de la mitigación**, un aspecto especialmente relevante en sistemas industriales. La aplicación de un parche puede implicar paradas de planta, pruebas extensivas, riesgos de regresión funcional o dependencia de terceros (explicado anteriormente en el contexto operativo de entornos ICS/OT). Evaluar la urgencia de una mitigación sin considerar estos costes puede conducir a decisiones que, lejos de reducir el riesgo global, lo incrementen.

Por estos motivos, en cualquier ámbito, pero especialmente por sus peculiaridades, en el ámbito industrial resulta necesario complementar CVSS con **métricas y enfoques adicionales**, orientados a capturar mejor la realidad operativa y la amenaza efectiva.

Entre estas métricas complementarias destacan las que veremos a continuación en más profundidad como alternativas a CVSS, como son:

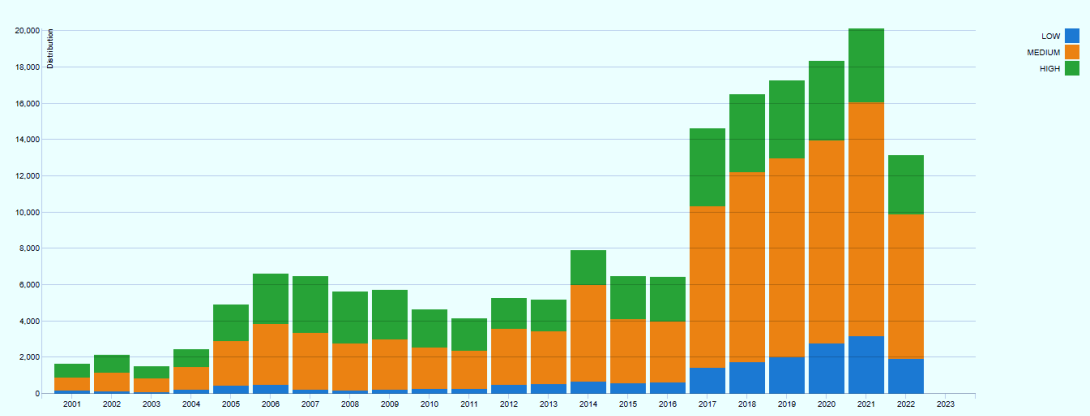
- **KEV (Known Exploited Vulnerabilities)**, orientado a identificar vulnerabilidades con evidencia de explotación activa en el mundo real.
- **Now / Next / Never**, enfoque cualitativo de priorización que permite clasificar las vulnerabilidades según la urgencia real de actuación en función del risco operativo.
- **EPSS (Exploit Prediction Scoring System)**, que introduce una estimación probabilística de la probabilidad de explotación.
- **Modelos avanzados empleados por soluciones comerciales**, basados en la combinación de múltiples fuentes (CVSS, inteligencia de amenazas, telemetría, exposición y contexto operativo) junto con algoritmos e inteligencia propia, con el objetivo de ofrecer priorizaciones más precisas y accionables.

La combinación de estos enfoques permite **evolucionar desde una evaluación basada exclusivamente en la gravedad técnica hacia una priorización basada en riesgo,** más coherente con la realidad de los entornos industriales.

Este enfoque no pretende sustituir CVSS, sino situar su puntuación dentro de un marco más amplio, en el que la toma de decisiones se apoya en el contexto, en la amenaza real y en los objetivos de negocio.

4.4 Alternativas

Como punto de arranque de esta subsección, resulta ilustrativo recurrir a la **visualización histórica de la distribución de severidad CVSS publicada por la NVD (National Vulnerability Database) del NIST (national Institute of Standards and Tecnology) americano,** aunque esté basada en **CVSS v2**. Esta gráfica muestra de manera clara una tendencia sostenida en el tiempo: **el volumen total de CVE publicadas es muy elevado** y, dentro de ellas, un porcentaje significativo se concentra en rangos de **severidad media y alta** [6][7].



Distribución de severidades CVSS en el tiempo. Fuente: NIST (2022)

Esta realidad tiene implicaciones prácticas directas para la gestión de la ciberseguridad, especialmente en **entornos industriales ICS/OT**. Incluso asumiendo un programa de parcheo maduro, con recursos dedicados y procesos bien definidos, resulta **materialmente imposible** aplicar parches a todas las vulnerabilidades de severidad media o alta según CVSS, manteniendo al mismo tiempo la estabilidad operativa, la seguridad funcional y la continuidad del proceso.

En entornos industriales, donde los ciclos de actualización son largos, las energías de mantenimiento limitadas y el coste de un cambio no planificado es elevado, pretender mantener una infraestructura "libre de vulnerabilidades" desde una lectura puramente cuantitativa de CVSS no es realista. La gráfica evidencia que el problema no es puntual ni circunstancial, sino **estructural**: **el ritmo de aparición de vulnerabilidades supera ampliamente la capacidad de remediación directa.**

Este hecho obliga, necesariamente, a adoptar **estrategias de priorización**, en las que la severidad CVSS constituye sólo un elemento más del proceso de decisión. La gestión eficaz requiere incorporar criterios adicionales que permitan distinguir que vulnerabilidades representan un riesgo **real e inmediato** para el entorno industrial y

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

cuáles pueden ser tratadas de forma diferida, mitigadas mediante controles compensatorios o incluso aceptadas temporalmente.

A partir de esta constatación, esta sección abordará enfoques que permiten ir más allá de CVSS, incorporando información sobre explotación real, probabilidad, contexto operativo e impacto en el proceso, con el objetivo de construir modelos de priorización más realistas y accionables para entornos ICS/OT.

4.4.1 KEV (Vulnerabilidades Explotadas Conocidas)

4.4.1.1 Introducción

El **KEV (Known Exploited Vulnerabilities)** [8] es un catálogo público que contempla vulnerabilidades para las cuales existe **evidencia confirmada de explotación activa en el mundo real**. Su finalidad principal es ayudar a las organizaciones a **priorizar acciones de mitigación** centrándose en aquellas vulnerabilidades que ya están siendo empleadas por actores maliciosos, y que, por lo tanto, representan un riesgo inmediato.

Este catálogo está **gestionado por la Cybersecurity and Infrastructure Security Agency (CISA)** [9], la agencia federal de los Estados Unidos responsable de la protección de las infraestructuras críticas y de la coordinación nacional en materia de ciberseguridad. El KEV forma parte de las iniciativas de CISA orientadas a mejorar la gestión del riesgo a escala sistémica, yendo más allá de métricas puramente teóricas o técnicas.

Desde un punto de vista operativo, el KEV introduce un criterio fundamental que complementa CVSS: **la explotación real**. Mientras que CVSS describe la severidad potencial de una vulnerabilidad, el KEV responde a la pregunta de esa vulnerabilidad **ya está siendo utilizada activamente en ataques**, independientemente de su puntuación CVSS.

El catálogo KEV se publica y se mantiene de forma continua en el sitio web oficial de CISA, donde se puede consultar el listado actualizado de vulnerabilidades incluidas. Adicionalmente, CISA integra el KEV en su ecosistema más amplio de información sobre vulnerabilidades y alertas, disponible en su portal institucional.

La relevancia del KEV resulta especialmente notable en **entornos ICS/OT**, donde la capacidad de parcheo es limitada y donde resulta crítico identificar con rapidez aquellas vulnerabilidades que representan una amenaza inmediata para la operación. Al basarse en explotación confirmada, el KEV permite establecer un **primer filtro de urgencia**,

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

reduciendo el volumen de vulnerabilidades a gestionar y facilitando una toma de decisiones más pragmática y alineada con el riesgo real.

4.4.1.2 Formato

El **catálogo KEV** se publica con un **formato estructurado y estandarizado**, diseñado para facilitar su interpretación operativa y su integración en procesos de gestión de vulnerabilidades. Cada entrada del catálogo corresponde a una vulnerabilidad concreta para la cual existe evidencia confirmada de explotación activa, e incluye un conjunto de campos orientados a la toma de decisiones.

De manera general, cada registro del KEV se cuenta con un **formato de tipo imprimible, CSV o JSON** [10], pensado para su tratamiento automatizado y su integración en herramientas de gestión de vulnerabilidades. Así, además de la consulta en línea, CISA pone a disposición una **versión descargable e imprimible del catálogo KEV**, especialmente útil para su uso en entornos desconectados, revisiones periódicas, comités de seguridad o procedimientos documentales.

Cada entrada o registro del KEV, incluye un conjunto de campos bien definidos:

Campo	Valor
cveID	Identificador único de CVE de la vulnerabilidad.
vendorProject	Fabricante o proyecto responsable del producto afectado.
product	Producto o componente concreto impactado por la vulnerabilidad.
vulnerabilityName	Denominación resumida de la vulnerabilidad.
dateAdded	Fecha en la que la vulnerabilidad fue incorporada al catálogo KEV, indicando el momento a partir del cual existe evidencia de explotación activa.
shortDescription	Descripción concisa del problema y de su impacto potencial.
requiredAction	Acción recomendada por CISA para mitigar el riesgo (aplicación de parches, mitigaciones o retirada del producto).
dueDate	Plazo límite recomendado para la mitigación, empleado como referencia de urgencia.
knownRansomwareCampaignUse	Indicador sobre el uso conocido de la vulnerabilidad en campañas de ransomware.
notes	Referencias adicionales a advertencias del fabricante, análisis técnicos o fuentes externas relevantes.

cwes	Lista de categorías CWE asociadas a la vulnerabilidad.

Estructura de los registros del KEV. Fuente: elaboración propia (2026)

Como se ve, permiten comprender no sólo la naturaleza técnica de la vulnerabilidad, sino también su **relevancia operativa y temporal**, facilitando su utilización como criterio de priorización en programas de gestión basados en riesgo.

Este formato facilita que el KEV pueda emplearse como un **primer filtro de priorización**, especialmente útil en entornos industriales en los que resulta inviable abordar de forma simultánea todas las vulnerabilidades publicadas.

4.4.1.3 Suscripción a actualizaciones y novedades

Dado que el catálogo KEV se **actualiza de manera continua,** con la incorporación de nuevas vulnerabilidades según se detecta explotación activa, resulta especialmente recomendable mantener un mecanismo de seguimiento de las novedades.

CISA ofrece la posibilidad de **suscribirse a las notificaciones especiales**, de forma que las organizaciones puedan recibir alertas cuando se producen actualizaciones relevantes del catálogo. Esta suscripción permite anticipar acciones de análisis y priorización sin depender exclusivamente de revisiones manuales [11].

4.4.1.4 Construcción del KEV

El **catálogo KEV (Known Exploited Vulnerabilities)** no es el resultado de un cálculo algorítmico ni de una puntuación automática, sino de un **proceso de análisis continúa basado en inteligencia de amenazas, evidencias de explotación real y coordinación interinstitucional**. Su generación responde a una lógica cualitativa y operativa, orientada a identificar vulnerabilidades que ya están siendo empleadas de manera efectiva por actores maliciosos.

Desde el punto de vista conceptual, el KEV se basa en un principio fundamental: **una vulnerabilidad sólo se incorpora al catálogo cuando existe evidencia fiable de explotación activa en el mundo real**.

CISA genera y mantiene el catálogo KEV a partir de una combinación de **múltiples fuentes de información**, entre las que se incluyen:

- **Inteligencia de amenazas gubernamental**, procedente de agencias federales, equipos de respuesta a incidentes y organismos de seguridad.
- **Información compartida por proveedores de tecnología y fabricantes**, a través de procesos coordinados de divulgación de vulnerabilidades.

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

- **Datos de explotación observada**, recogidos en incidentes reales, campañas activas o análisis forenses.
- **Colaboración con socios internacionales y sectoriales**, especialmente en el ámbito de las infraestructuras críticas.
- **Aportaciones del ecosistema de ciberseguridad**, incluyendo investigaciones públicas contrastadas e informes de alta confianza.

Este enfoque garantiza que la inclusión de una vulnerabilidad en el KEV responda a **evidencias verificadas**, evitando la dependencia exclusiva de predicciones o modelos probabilísticos.

La decisión de incorporar una vulnerabilidad al catálogo KEV sigue un proceso de **evaluación humana especializada**, en el que se analizan factores como:

- existencia de explotación confirmada,
- alcance y reproducibilidad de la explotación,
- relevancia para infraestructuras críticas y servicios esenciales,
- Impacto observado o potencial en entornos reales.

Una vez confirmada la explotación activa, la vulnerabilidad se añade al catálogo junto con un **plazo recomendado de mitigación** (obligatorio para algunas entidades por normativa, como veremos), que sirve como referencia temporal para la priorización de las acciones defensivas.

El KEV es un catálogo **dinámico y vivo**, que se actualiza de manera continua a medida que se detectan nuevas explotaciones. No existe una cadencia fija de publicación: las entradas se incorporan en función de la aparición de nueva información relevante.

Esta naturaleza dinámica implica que el KEV no debe interpretarse como un listado exhaustivo de vulnerabilidades peligrosas, sino como un **conjunto priorizado de las que representan una amenaza inmediata** en un momento dado.

4.4.1.5 Uso e importancia

Según la propia agencia, el catálogo debe emplearse como una **lista de referencia prioritaria** para identificar aquellas vulnerabilidades para las que existe constancia de explotación activa en entornos reales, sirviendo como punto de partida mínimo para la acción correctiva [12].

CISA recomienda integrar el KEV de manera sistemática en los procesos habituales de gestión de vulnerabilidades y riscos.

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

- En primer lugar, las organizaciones deben **inventariar e identificar los activos** expuestos a las vulnerabilidades incluidas en el Catálogo, determinando si los sistemas afectados forman parte de su entorno operativo. A continuación, debe realizarse una **evaluación de exposición real**, teniendo en cuenta el contexto técnico y operativo en el que se encuentran esos activos.
- Una vez identificada la afectación, CISA indica que las vulnerabilidades listadas en el KEV deben ser **priorizadas de forma inmediata**, independientemente de otras métricas como la puntuación CVSS. Para cada vulnerabilidad, deben ejecutar las **acciones recomendadas** por el propio catálogo, que pueden incluir la aplicación de parches oficiales, la implantación de mitigaciones compensatorias cuando el parcheo no es viable, o retirada del producto vulnerable si no existe una solución adecuada.
- Adicionalmente, CISA subraya la importancia de **respetar los plazos de remediación** asociados a cada entrada del KEV, empleándolos como referencia de urgencia en la planificación de las actuaciones. El seguimiento continuo del catálogo, que se actualiza de forma regular, resulta clave para incorporar nuevas vulnerabilidades explotadas y ajustar las prioridades de respuesta.
- Finalmente, el KEV debe emplearse como un **complemento a los modelos tradicionales de gestión del riesgo**, aportando un criterio basado en inteligencia de amenazas y explotación confirmada. De esta forma, el catálogo contribuye a focalizar recursos limitados en las amenazas más relevantes y a reducir de forma efectiva la superficie de riesgo de las organizaciones.

En el contexto de los Estados Unidos, el catálogo KEV adquirió una relevancia singular al convertirse en un **instrumento de obligado cumplimiento** para determinados organismos federales. A través de la *Binding Operational Directive 22-01 (BOD 22-01)*, CISA estableció la obligatoriedad de mitigar las vulnerabilidades incluidas en el KEV dentro de **plazos estrictos y predefinidos**, en función del riesgo asociado a cada entrada [13].

Esta directiva se aplica a las agencias civiles federales del poder ejecutivo, que están **legalmente obligadas a identificar los activos afectados por las vulnerabilidades KEV y a ejecutar las acciones correctivas requeridas antes de la fecha límite indicada en el catálogo**. El incumplimiento de estos plazos puede dar lugar a acciones de supervisión y a requerimientos adicionales por parte de las autoridades competentes.

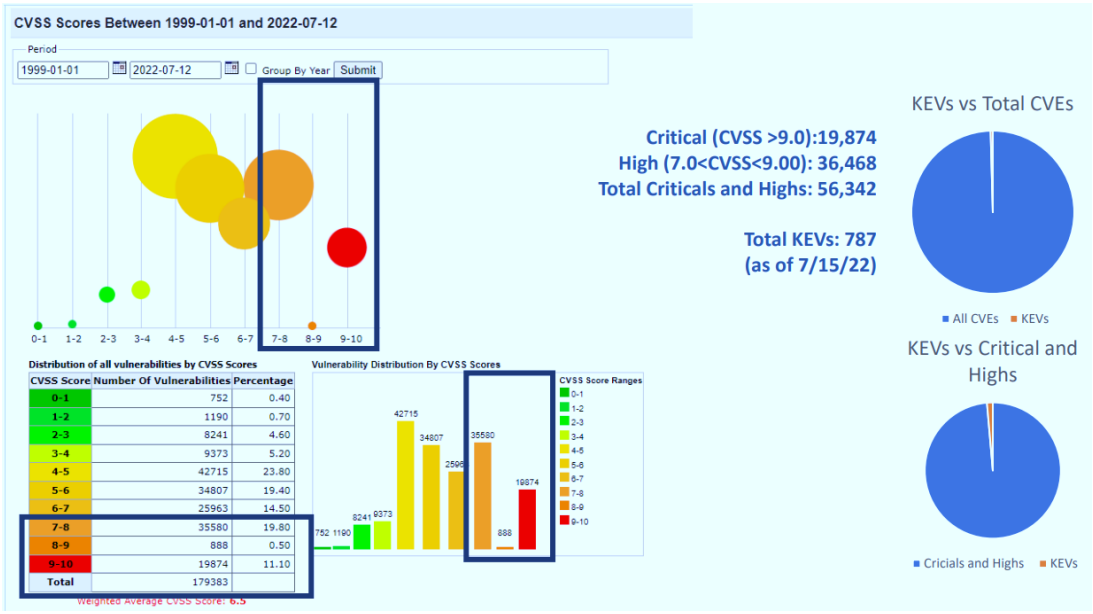
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

La adopción del KEV como referencia regulatoria supone un **cambio de paradigma en la gestión de vulnerabilidades**, al introducir criterios basados en explotación real y plazos de remediación obligatorios. Aunque esta obligación legal no es directamente aplicable fuera del ámbito regulado en los Estados Unidos, el modelo establecido por CISA constituye una **buena práctica de referencia internacional**, especialmente para organizaciones con sistemas críticos, industriales o de alta exposición al riesgo.

En este sentido, el catálogo KEV no sólo actúa como una herramienta técnica, sino también como un **mecanismo de gobernanza del riesgo**, que alinea la inteligencia de amenazas, la gestión operativa y el cumplimiento normativo bajo un enfoque claro de priorización y urgencia.

Uno de los principales valores añadidos del KEV reside en su capacidad para **reducir drásticamente el universo de vulnerabilidades sobre el que deben focalizarse los esfuerzos de remediación**. Según el análisis presentado por CISA en el marco de la Binding Operational Directive 22-01 en 2022, el empleo del KEV permite pasar de un conjunto inicial de decenas de miles de vulnerabilidades potencialmente relevantes a un subconjunto mucho más reducido, basado en evidencia real de explotación [14].

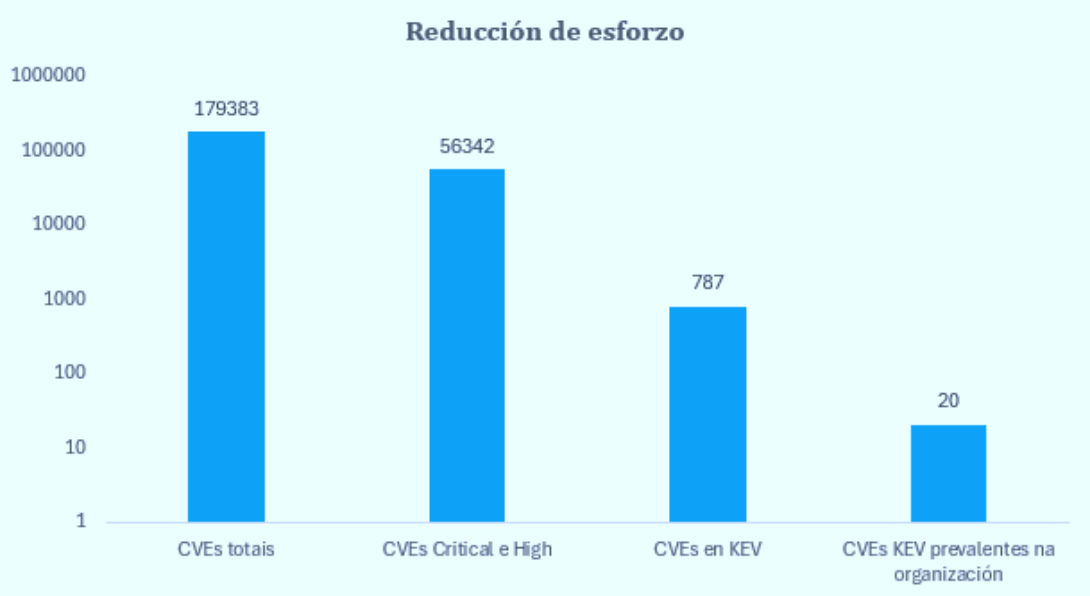
En concreto, en el momento del estudio de referencia, el número total de vulnerabilidades clasificadas como **Críticas y Altas según CVSS** superaba las **56.000 entradas**. Sin embargo, al aplicar el filtro del KEV —es decir, considerar únicamente aquellas vulnerabilidades para las cuales existía constancia de explotación activa—, el universo se reducía a **787 vulnerabilidades conocidas como explotadas**. Esto supone una **reducción del 98.6 %** del conjunto inicial de vulnerabilidades de severidad media y alta que, en teoría, podrían requerir atención.



Reducción drástica de CVEs de severidad alta y crítica en el KEV. Fuente: CISA (2022)

Esta reducción tiene un impacto directo y muy significativo en el nivel de esfuerzo operativo que deben asumir los equipos de seguridad. Al limitar el foco a un subconjunto mucho más manejable, resulta posible asignar recursos de manera más eficiente, acortar los tiempos de respuesta y priorizar acciones con mayor impacto real en la reducción del riesgo. Tal y como ilustra la gráfica, esta aproximación transforma un problema estructuralmente inabarcable en un conjunto de actuaciones concretas y ejecutables, incluso en entornos empresariales complejos. **Pasamos de un universo total de más de 179.000 CVEs publicados en el momento del estudio, a tener que accionar la mitigación de únicamente unos 20** dentro de la organización (dato estimado). El cambio es considerable, como se ve en la figura de escala logarítmica.

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



Reducción del número de CVEs a gestionar en la organización con el uso de KEV. Fuente: CISA (2022)

Pero no todo son buenas noticias. Aunque el KEV permite una reducción muy significativa del universo de vulnerabilidades prioritarias, el catálogo no es estático. La presión constante ejercida por los ciberdelincuentes y la rápida explotación de nuevas vulnerabilidades hicieron que, en **2025**, el número de entradas del KEV se experimenta un **incremento interanual cercano al 20 %, con 245 nuevas vulnerabilidades**, lo que supone una tasa de crecimiento aproximadamente un 30% superior a los dos años precedentes [15].

Este crecimiento parecería consecuencia directa de la mayor sofisticación de los actores maliciosos y de su capacidad para explotar vulnerabilidades en una fase cada vez más temprano, quizás apoyados en sistemas semiautomáticos de inteligencia artificial. A pesar de este incremento, el KEV continúa representando un subconjunto muy reducido en comparación con el total de vulnerabilidades publicadas anualmente, manteniendo así su valor como mecanismo de priorización efectiva.

Este contexto pone de manifiesto dos realidades complementarias: por una banda, la **necesidad de emplear mecanismos como el KEV para contener la carga operativa**; por otra, la importancia de asumir que la gestión de vulnerabilidades es un proceso dinámico, que requiere seguimiento continuo, actualización periódica y capacidad de adaptación frente a la evolución constante del panorama de amenazas.

Finalmente, cabe destacar que **el enfoque promovido por el catálogo KEV no se limita al ámbito regulatorio o institucional, sino** que está ya **plenamente integrado en soluciones comerciales de gestión de vulnerabilidades y riesgo**. Plataformas comerciales de gestión de vulnerabilidades como Tenable, incorporan explícitamente

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

las fechas límite de remediación establecidas por CISA en el marco de la BOD 22-01 como criterio de priorización y agrupación de vulnerabilidades [16]. Esto evidencia que el plazo de mitigación impuesto por el KEV constituye un **factor operativo clave en la evaluación del riesgo real**, junto con métricas tradicionales como CVSS o la exposición del activo. La adopción de este criterio por herramientas profesionales refuerza la idea de que el KEV representa hoy una **referencia práctica y validada por el mercado** para orientar los esfuerzos de corrección hacia las vulnerabilidades con un impacto más inmediato y probado en entornos reales.

4.4.2 Ahora/Siguiente/Nunca

4.4.2.1 Introducción

La necesidad de disponer de **modelos de priorización claros, operativos y adaptados al riesgo real** en entornos industriales ha llevado, en los últimos años, al desarrollo de enfoques que van más allá de las métricas clásicas de severidad. En este contexto se inserta la estrategia **Now / Next / Never**, hoy ampliamente asociada al fabricante Dragones como veremos, pero cuya base conceptual procede de trabajos previos en el ámbito de la ciberseguridad industrial y de la gestión del riesgo.

Uno de los trabajos de referencia iniciales en este ámbito es el documento impulsado principalmente por **Allan Manion** en el marco del Software Engineering Institute (SEI), en lo que se aborda la necesidad de **priorizar la remediación de vulnerabilidades en función del impacto operativo, el contexto del activo y la factibilidad de la mitigación**, especialmente en sistemas ciberfísicos e industriales [17].

Este enfoque supone un alejamiento explícito de la priorización automática basada únicamente en métricas técnicas, proponiendo criterios como:

- la función crítica del activo en el proceso industrial,
- las consecuencias operativas de un fallo o indisponibilidad,
- la probabilidad real de explotación,
- y las restricciones operativas para aplicar cambios o parches.

Estos principios sentaron las bases conceptuales para modelos posteriores más simplificados y orientados a la toma de decisiones operativas.

Sobre esta base, **Dragones** consolidó y popularizó el enfoque de **gestión de vulnerabilidades basada en riesgo** específicamente adaptado a entornos **ICS/OT**. En un artículo de referencia, la compañía expone **cinco razones fundamentales por las**

que este enfoque resulta crítico en OT [18], que pueden resumirse de la siguiente manera:

1. **Priorización efectiva frente a un volumen inabarcable de vulnerabilidades.** En un contexto de recursos limitados y listados de vulnerabilidades cada vez más extensas, resulta esencial identificar cuáles son realmente críticas en el contexto concreto de los equipos, procesos y operaciones industriales, evitando una aproximación indiscriminada.

2. **Continuidad operativa como requisito esencial.** Los métodos tradicionales de parcheo adoptan requerir paradas de sistema, algo que no siempre es viable en entornos OT. La diferencia de los sistemas IT, los sistemas ciberfísicos gestionan procesos físicos y resultados operativos, por lo que no pueden ser partidos de forma frecuente ni sin una planificación rigurosa.

3. **Necesidad de comprensión contextual del riesgo.** La evaluación del riesgo específico de OT permite un análisis más precisa del impacto real de las vulnerabilidades, teniendo en cuenta el rol del activo, el proceso al que da soporte y las consecuencias operativas de una posible explotación.

4. **Asignación eficiente de recursos de ciberseguridad.** Al concentrar los esfuerzos en las vulnerabilidades de mayor riesgo real, las organizaciones pueden optimizar el uso de sus recursos técnicos y humanos, mejorando la eficacia global de las acciones de seguridad.

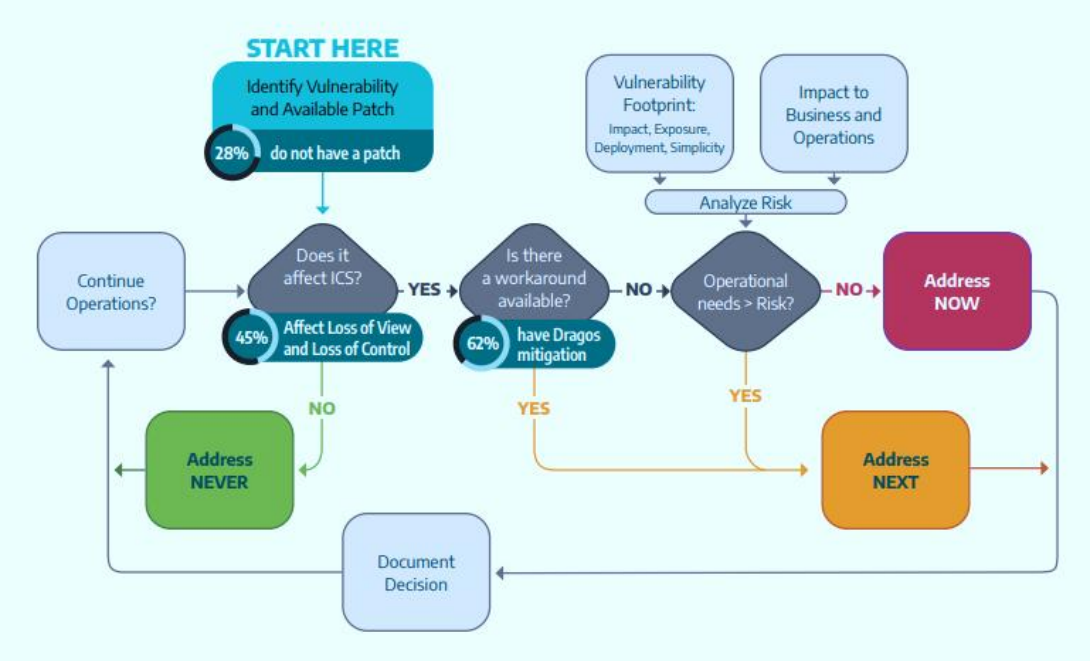
5. **Cumplimiento normativo y exigencias regulatorias.** Muchos marcos reguladores exigen a las organizaciones demostrar y reportar prácticas efectivas de gestión de vulnerabilidades (como vimos con las agencias federales americanas, o en España con ENS o NIS2), lo que refuerza la necesidad de enfoques estructurados, justificables y basados en riesgo.

Este conjunto de argumentos refuerza la necesidad de emplear modelos de priorización que integren riesgo operativo y contexto industrial, y no sólo métricas técnicas aisladas.

4.4.2.2 Estrategia

En este marco conceptual, Dragos introduce formalmente la estrategia **Now / Next / Never** en su *whitepaper* sobre gestión de vulnerabilidades basada en riesgo en entornos OT [17][18][19]. Este modelo propone una **clasificación clara y accionable de las vulnerabilidades** según la urgencia y la conveniencia de su remediación.

La lógica de la estrategia se inspira en el **árbol de decisión de parcheo urgente del Department of Homeland Security (DHS) americano**, empleado históricamente para determinar cuándo una vulnerabilidad debe ser mitigada de forma inmediata, cuando puede ser planificada o cuando resulta más prudente aceptar el riesgo [20].



Árbol de decisiones de parcheo urgente del DHS. Fuente: Dragos (2024)

Este modelo de referencia fue ya presentado en el boletín de ciberaleralertas (*Ciberalertas – I*) de este Observatorio de la AMTEGA [4].

La estrategia Now / Next / Never traduce ese enfoque de decisión a un formato sencillo, comprensible y operativo para equipos de seguridad y operaciones industriales, facilitando su adopción en entornos reales.

- Las vulnerabilidades clasificadas como **Now** son aquellas que afectan a activos críticos, resultan razonablemente explotables y no cuentan con mitigaciones compensatorias eficaces. Se trata de situaciones que pueden derivar en un control inmediato de sistemas clave o en una pérdida de visibilidad crítica, por lo que requieren actuación prioritaria. Esto no implica necesariamente parchear de forma inmediata, **sino reducir cuanto antes la explotabilidad** mediante medidas técnicas y planificar el parcheo en la primera energía segura disponible.
- En la categoría **Next** se sitúan vulnerabilidades relevantes, pero con una menor probabilidad de causar impacto grave o parcialmente mitigadas por la arquitectura existente. Estas vulnerabilidades deben gestionarse de forma planificada, integrándose en campañas de mejora progresiva que combinen

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

refuerzo de la arquitectura, reducción de la exposición y parcheo cuando las condiciones operativas lo permitan.

- Finalmente, la categoría **Never** agrupa vulnerabilidades que, en el contexto específico de la organización, no representan un riesgo significativo a corto ni medio plazo. Esto puede deberse a que afectan a funcionalidades no utilizadas, configuraciones inexistentes o activos efectivamente aislados. Clasificarlas como Never no supone ignorarlas, sino **documentar y justificar la decisión**, manteniendo una vigilancia suficiente para revisarla si cambian las condiciones operativas.

A continuación, se sintetizan los escenarios de priorización descritos.

Categoría	Criterios principales	Riesgo operativo	Respuesta recomendada
Now	Activo crítico; explotabilidad razonable; ausencia de mitigaciones compensatorias eficaces	Alto / inmediato	Actuar con máxima prioridad: reducir rápidamente la explotabilidad (configuraciones, segmentación, reglas de acceso) y planificar el parcheo en la primera energía segura
Next	Impacto posible pero menos probable; mitigación parcial pola arquitectura existente	Medio	Gestión planificada: refuerzo progresivo de la arquitectura y aplicación de parches durante mantenimientos programados
Never	Impacto improbable en el contexto actual; funcionalidades no usadas o activos aislados	Bajo	No parchear en condiciones normales; documentar la decisión, justificarla por riesgo y mantener monitorización para reevaluación futura

Tabla resumen de la estrategia Now/Next/Never. Fuente: elaboración propia (2026)

Este enfoque complementa de forma natural métricas como **CVSS** y mecanismos como **el catálogo KEV**, al introducir el **impacto operativo y el contexto industrial** como factores determinantes en la toma de decisiones.

4.4.3 EPSS (Sistema de Puntuación de Predicción de Exploits)

4.4.3.1 Introducción

La creciente dificultad para gestionar volúmenes muy elevados de vulnerabilidades llevó a la aparición de enfoques complementarios a las métricas clásicas de severidad. Entre ellos destaca el **Exploit Prediction Scoring System (EPSS)**, un modelo estadístico diseñado para **estimar la probabilidad de que una vulnerabilidad sea explotada en el mundo real**, aportando una dimensión predictiva a la gestión del riesgo.

EPSS proporciona, para cada vulnerabilidad identificada mediante un CVE, una **magnitud numérica entre 0 y 1**, que representa la probabilidad diaria de que esa vulnerabilidad sea explotada en un horizonte temporal de 30 días. La diferencia de CVSS, que mide la severidad técnica de un fallo, EPSS se celebra en **anticipar el comportamiento de los atacantes**, permitiendo priorizar aquellas vulnerabilidades más propensas a ser utilizadas de forma activa.

Explicadas sus generalidades en la descripción realizada por INCIBE-CERT [21], EPSS constituye una evolución significativa en la gestión de vulnerabilidades, al permitir **ordenar listas extensas de CVEs en función de su probabilidad de explotación**, reduciendo el esfuerzo necesario para identificar cuáles requieren una atención prioritaria. Destacar que en ese artículo no se considera la versión más reciente del modelo, **EPSS v4**, que introduce mejoras en la capacidad predictiva y en la estabilidad de las estimaciones.

El modelo EPSS tiene su origen en un trabajo de investigación presentado en la conferencia **Black Hat USA 2019**, en el que se propuso por primera vez un sistema de puntuación predictiva basado en técnicas estadísticas y aprendizaje automática para estimar la explotación de vulnerabilidades. Este trabajo sentó las bases conceptuales de un enfoque que se alejaba de la evaluación puramente técnica e introducía variables relacionadas con la evidencia histórica, el contexto y el comportamiento de los atacantes [22].

Desde aquella, el modelo ha ido evolucionando progresivamente hasta convertirse en un estándar de facto para la estimación probabilística de la explotación de vulnerabilidades.

4.4.3.2 Gobernanza y mantenimiento del EPSS

En la actualidad, EPSS **es mantenido y gestionado por FIRST (Forum of Incident Response and Security Teams)**, una organización internacional sin ánimo de lucro que agrupa equipos de respuesta a incidentes (CSIRTs, CERTs y otras entidades de referencia en ciberseguridad a nivel mundial). FIRST es también responsable de otros estándares ampliamente adoptados, como CVSS.

FIRST publica de manera abierta el **modelo EPSS**, **su metodología y los conjuntos de datos empleados**, permitiendo transparencia y revisión continua. La documentación oficial del modelo, disponible en el portal de FIRST, describe en detalle los **factores empleados para la estimación de la probabilidad**, así como las métricas de evaluación del rendimiento del modelo, incluyendo parámetros de **cobertura (*recall*)** y **eficiencia (*precision*)**, que permiten evaluar el equilibrio entre detección de vulnerabilidades explotadas y reducción de falsos positivos [23].

Hay que subrayar que **EPSS no está diseñado para sustituir ni CVSS ni mecanismos como el catálogo KEV, sino para complementarlos**. Mientras CVSS mide impacto potencial y KEV aporta evidencia de explotación confirmada, EPSS se sitúa en un punto intermedio, permitiendo **anticipar que vulnerabilidades tienen mayor probabilidad de ser explotadas en el futuro próximo**.

En este sentido, **EPSS resulta especialmente útil como herramienta de filtrado inicial y priorización dinámica, sirviendo de apoyo a la toma de decisiones cuando los recursos son limitados y el volumen de vulnerabilidades supera la capacidad de respuesta** inmediata de las organizaciones.

4.4.3.3 Uso e priorización

La utilidad práctica de EPSS como estrategia de priorización se basa no sólo en el modelo estadístico en sí, sino también **en la disponibilidad abierta y actualizada de sus datos**, así como en la existencia de guías de uso que orientan su integración con otras métricas y enfoques.

FIRST publica de manera abierta los **datos EPSS recalcados de forma periódica**, accesibles a través de un fichero descargable que contiene, para cada vulnerabilidad:

- la identificación mediante **su CVE**,
- la **probabilidad estimada de explotación** en una energía temporal de 30 días,
- y el **percentil de riesgo** en el que se ubica esa vulnerabilidad respecto del conjunto total.

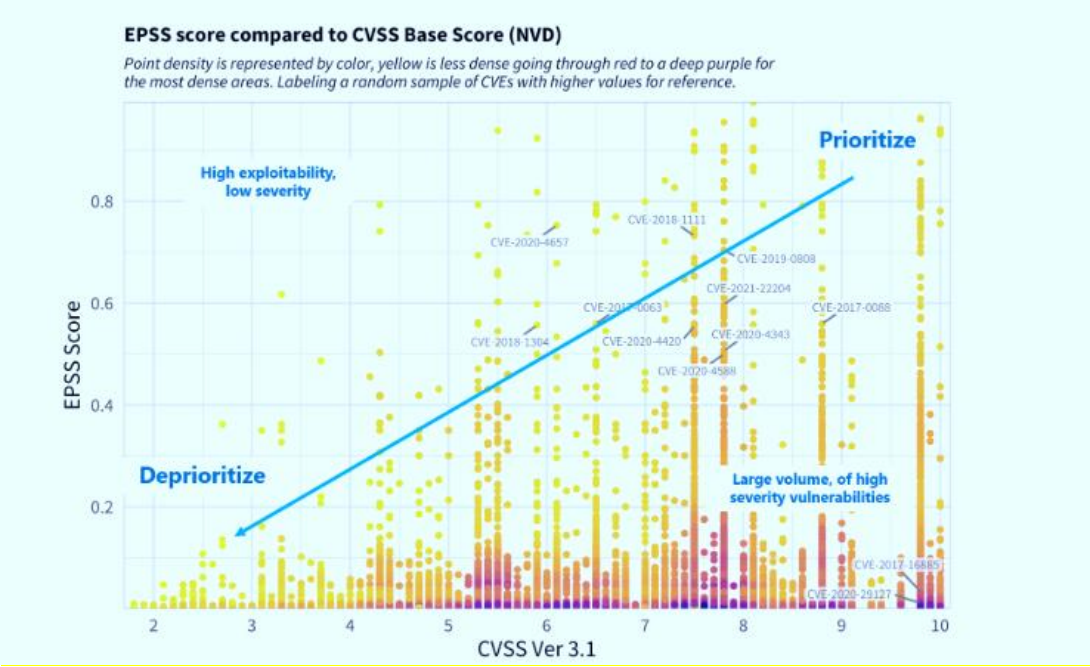
Financiado pola Unión Europea NextGenerationEU · Plan de Recuperación, Transformación e Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · XUNTA DE GALICIA · Xacobeo 2027

Este conjunto de datos está disponible en un formato estructurado y fácilmente integrable en procesos automatizados, permitiendo a las organizaciones incorporar EPSS en sus flujos de gestión de vulnerabilidades y en sus herramientas internas [24].

Adicionalmente, **FIRST ofrece acceso a los mismos datos mediante una API pública**, lo que facilita su integración directa con plataformas de gestión de vulnerabilidades, SIEMs o sistemas de análisis propios, sin necesidad de descargar ficheros completos de forma manual [25].

Este organismo publica también una **guía de uso oficial de EPSS** en la que se aborda como emplear este modelo de manera eficaz, especialmente en combinación con CVSS [26]. La guía destaca nuevamente que EPSS no debe emplearse aisladamente, sino como un **plus que permite priorizar dentro de rangos de severidad similares**.

La aproximación recomendada consiste en emplear CVSS para **filtrar vulnerabilidades según el impacto potencial**, y aplicar posteriormente EPSS para **ordenar y priorizar aquellas con una mayor probabilidad de explotación**. Este enfoque permite reducir significativamente el número de vulnerabilidades que requieren atención inmediata, mejorando la eficiencia operativa.



Correlación entre puntuaciones EPSS y CVSS. Fuente: First (2021)

Para acabar y tener una visión de conjunto del visto hasta ahora, en su documentación técnica FIRST reflexiona los **pros y contras de distintos enfoques de priorización de vulnerabilidades**, en función del enfoque, basado en probabilidad, percentiles o

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

clusterización [27]. Estos enfoques pueden resumirse comparativamente de la siguiente manera:

Enfoque	Descripción	Principales Vantajas	Limitaciones
Basado en la probabilidad (EPSS)	Prioriza según la probabilidad estimada de explotación en un horizonte temporal definido	Permite anticipar explotación real; alta granularidad; priorización dinámica	Puede ser menos intuitivo; requiere interpretación estadística
Basado en porcentajes (CVSS relativos)	Clasifica vulnerabilidades según su posición relativa en términos de severidad	Fácil de entender; ampliamente adoptado	No refleja explotación real ni contexto operativo
Basado en Clusterización (CVSS estándar, ~Now/Next/Never)	Agrupa vulnerabilidades en categorías de prioridad ~(alta/media/baja)	Simplicidad operativa; facilita la toma de decisiones	Pérdida de detalle; dependencia de criterios subjetivos

Distintos enfoques de gestión de vulnerabilidades. Fuente: elaboración propia (2026)

Este último enfoque de clusterización puede equipararse, desde una perspectiva operativa, a modelos como **Now / Next / Never**, que traducen métricas técnicas y probabilísticas a decisiones accionables para los equipos de seguridad y operaciones.

En conjunto, la combinación de estos enfoques permite a las organizaciones adaptar su estrategia de priorización a su nivel de madurez, capacidad operativa y perfil de riesgo, manteniendo un equilibrio entre precisión analítica y practicidad.

4.4.4 Enfoque de soluciones comerciales

Las **herramientas comerciales de gestión de vulnerabilidades** incorporan hoy modelos de priorización que van más allá de la simple enumeración de CVEs o de su severidad técnica. Soluciones como las de Qualys, Tenable o Rapidán integran enfoques propios que combinan métricas tradicionales, inteligencia de amenazas, contexto del activo y criterios de riesgo operativo, con el objetivo de **ayudar a las organizaciones a decidir donde concentrar sus esfuerzos de remediación**.

Esta sección ofrece una visión sintética de algunos de estos enfoques (con el grado de detalle que se ha podido obtener teniendo en cuenta que estas entidades lógicamente tratan de preservar su propiedad intelectual e industrial), ilustrando como los fabricantes trasladan conceptos como la priorización basada en riesgo, la explotación

activa o el impacto en el negocio a **mecanismos prácticos integrados en sus plataformas**, facilitando su adopción en entornos reales y con recursos limitados.

4.4.4.1 VMDR (Detección y Respuesta en la Gestión de Vulnerabilidades)

Como se indicó, las soluciones comerciales de gestión de vulnerabilidades han evolucionado hacia enfoques más integrados y orientados al riesgo. En este contexto se sitúa **VMDR (Vulnerability Management, Detection and Response)**, a la plataforma de Qualys.

Esta combina capacidades clásicas de escaneo de vulnerabilidades con funcionalidades avanzadas de **detección continua, correlación de señales de amenaza y respuesta**, permitiendo pasar de un modelo reactivo a un enfoque más dinámico. La plataforma integra información procedente de múltiples fuerzas —activos, configuraciones, inteligencia de amenazas y exposición— para ofrecer una visión contextualizada del riesgo asociado a cada vulnerabilidad [28].

Uno de los elementos clave de VMDR es que la priorización no se basa exclusivamente en la severidad CVSS, sino que introduce una **evaluación de riesgo orientada al negocio**, en la que se tienen en cuenta factores como la criticidad del activo, su exposición real, la existencia de exploits conocidos y la relevancia de la vulnerabilidad en el contexto operativo de la organización.

Emplea un modelo de priorización que busca responder a la pregunta práctica y crucial de **que vulnerabilidades deben abordarse primero**. Para ello, Qualys introduce puntuaciones e indicadores propios que combinan:

- gravedad técnica de la vulnerabilidad,
- inteligencia de amenazas y evidencia de explotación,
- contexto do activo afectado,
- e impacto potencial no negocio.

Este enfoque permite reducir el volumen de vulnerabilidades consideradas críticas desde un punto de vista puramente técnico y focalizar los esfuerzos de remediación en aquellas que **tienen mayor probabilidad de materializarse en un riesgo real**, mejorando la eficiencia de los equipos de seguridad.

En su whitepaper **"How to Shift from Managing Vulnerabilities to Business-Focused Risk Reduction"**, Qualys expone la necesidad de abandonar una gestión centrada en el

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

número de vulnerabilidades detectadas y evolucionar hacia un modelo orientado a la **reducción efectiva del riesgo para el negocio** [29].

Entre las enseñanzas principales de este documento destaco:

- la importancia de **priorizar en función del impacto en el negocio, y** no sólo de la severidad técnica;
- la necesidad de **contextualizar las vulnerabilidades** según el rol del activo y su exposición;
- la conveniencia de emplear **indicadores accionables**, comprensibles también para perfiles no técnicos;
- y la integración de la gestión de vulnerabilidades con los procesos de gobernanza, riesgo y cumplimiento.

Nada inesperado para el lector que venga de las secciones anteriores. Este enfoque encaja de forma natural con otras estrategias de priorización basadas en riesgo, como KEV, EPSS o modelos de clasificación operativa tipo Now / Next / Never, reforzando la idea de que la gestión moderna de vulnerabilidades debe orientarse a la toma de decisiones informadas y a la reducción sostenida del riesgo.

4.4.4.2 VPR (Valoración de Prioridad de Vulnerabilidades)

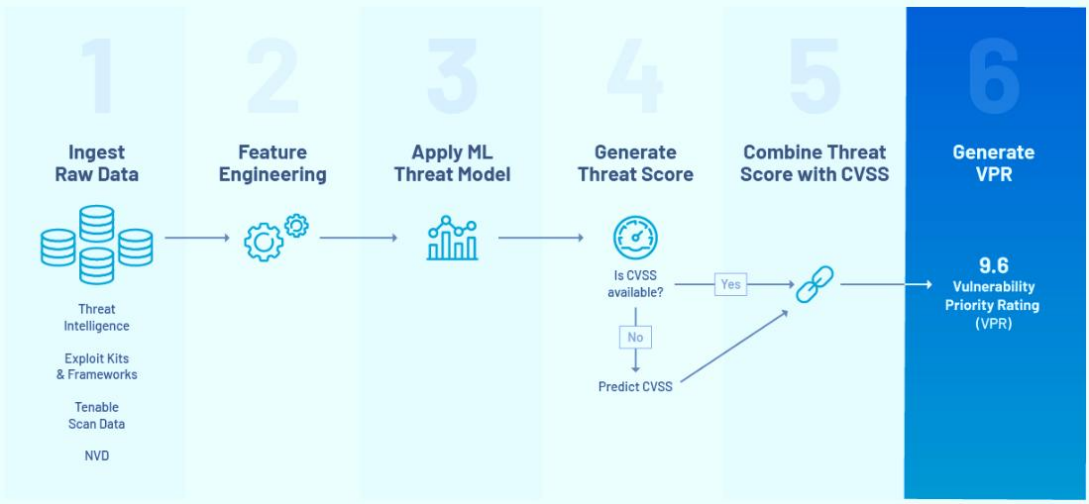
Nuevamente en el ámbito de las soluciones comerciales de gestión de vulnerabilidades, **Tenable** ha desarrollado **el Vulnerability Priority Rating (VPR)** como un mecanismo avanzado de priorización orientado a identificar aquellas vulnerabilidades que presentan un **mayor riesgo real a corto plazo**. VPR forma parte central de las capacidades de gestión de vulnerabilidades de Tenable y está diseñado para superar las limitaciones de una priorización basada exclusivamente en CVSS.

Según la documentación, VPR es una **puntuación dinámica**, recalculada de forma continua, que estima la probabilidad de que una vulnerabilidad sea explotada y cause impacto en un horizonte temporal reducido [30].

La puntuación **VPR se expresa en una escala de 0 a 10**, y se construye a partir de la combinación de múltiples señales, entre ellos:

- la gravedad técnica de la vulnerabilidad,
- la disponibilidad y madurez de exploits,
- a evidencia de explotación activa,

- la popularidad y exposición de los activos afectados,
- y la inteligencia de amenazas procedente de múltiples fuentes.

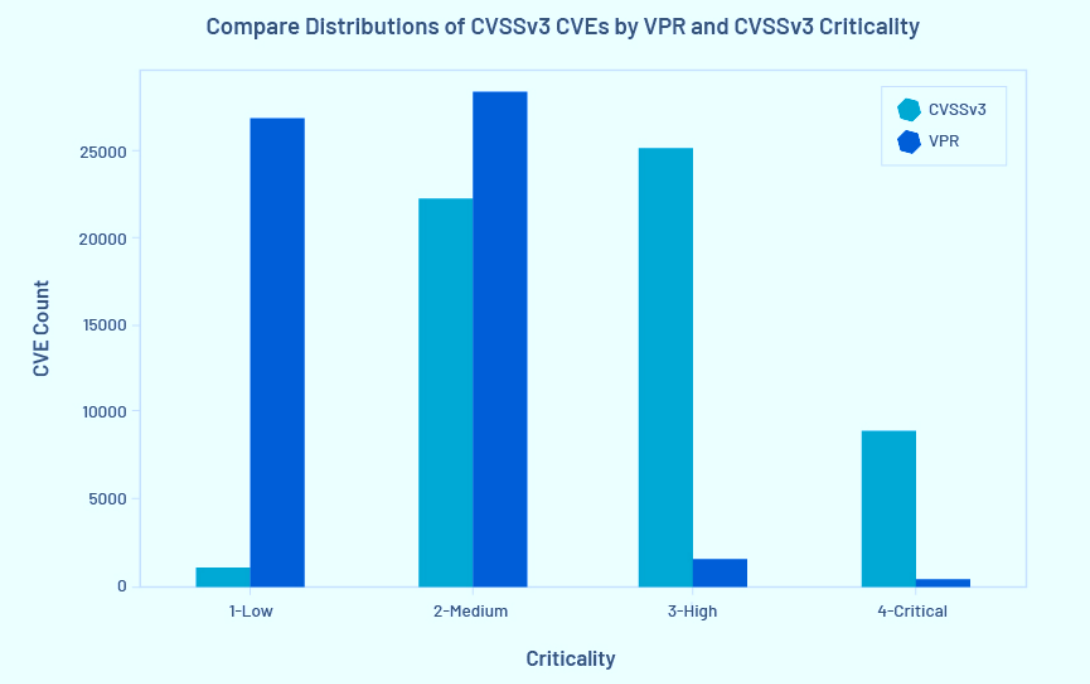


Pseudoproceso de cómputo del VPR. Fuente: Tenable (2020)

Este enfoque permite a Tenable ofrecer una visión más ajustada al riesgo real, priorizando vulnerabilidades que, aunque no siempre presentan las puntuaciones CVSS más elevadas, tienen una mayor probabilidad de ser explotadas en el corto plazo.

La entidad subraya que VPR no pretende sustituir CVSS, **sino complementarlo con una dimensión temporal y predictiva**. Mientras CVSS proporciona una medida estática del impacto potencial de una vulnerabilidad, VPR introduce una lógica dinámica que responde a la evolución del contexto de amenazas [31].

Uno de los efectos más relevantes de esta diferencia es la **reducción significativa del universo de vulnerabilidades prioritarias**. Segundos datos aportados por Tenable, al aplicar VPR como criterio principal, el foco de remediación puede reducirse a un **subconjunto mucho más pequeño de vulnerabilidades**, permitiendo a los equipos concentrar sus esfuerzos en las que presentan mayor riesgo inmediato, frente a largas listas de CVEs clasificadas como altas o críticas por CVSS.



Distribución de CVEs por criticidad en CVSS frente a VPR. Fuente: Tenable (2020)

Este mecanismo de filtrado resulta especialmente valioso en organizaciones con grandes superficies de ataque, donde la capacidad de parcheo es limitada y resulta imprescindible tomar decisiones basadas en riesgo efectivo.

En un whitepaper publicado en 2024, Tenable describe diversas **mejoras introducidas en el modelo VPR**, orientadas a incrementar su precisión y utilidad operativa [32]. Entre estas mejoras se incluyen:

- una mayor integración de señales de explotación activa,
- el refinamiento de los modelos estadísticos empleados,
- y una mejor diferenciación entre vulnerabilidades con comportamiento similar en términos de severidad técnica.

Estas mejoras permiten una priorización más fina y adaptativa, reforzando el papel de VPR como herramienta clave para la toma de decisiones en gestión de vulnerabilidades.

En conjunto, VPR es otra muestra de cómo las soluciones comerciales están incorporando **modelos dinámicos y basados en inteligencia de amenazas** para complementar métricas estándar como CVSS, alineándose con enfoques más amplios de gestión del riesgo y 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 Riesgo activo (y variantes)

Rapid7 desarrolló **Active Risk** como su enfoque avanzado de priorización de vulnerabilidades, orientado a ofrecer una **evaluación continua y contextualizada del riesgo real** asociado a los activos de una organización. Esta capacidad se regula en las soluciones de gestión de vulnerabilidades de la compañía y representa una evolución respecto a modelos anteriores basados en puntuaciones estáticas.

Según la documentación, Active Risk proporciona una **puntuación de riesgo dinámica**, que combina información sobre vulnerabilidades, exposición del activo, inteligencia de amenazas y comportamiento observado de los atacantes, con el objetivo de identificar aquellas situaciones que requieren atención prioritaria [33].

Este enfoque pretende responder a la necesidad de ir más allá de la severidad técnica, incorporando factores como:

- la probabilidad de explotación,
- la relevancia del activo en el contexto del negocio,
- y la evidencia de actividad maliciosa asociada.

De esta forma, Active Risk permite reducir el volumen de vulnerabilidades consideradas críticas y concentrar los esfuerzos de remediación en los escenarios con mayor impacto potencial.

Antes de la introducción de Active Risk, Rapid7 empleó **diferentes enfoques de priorización de vulnerabilidades, que fueron evolucionando progresivamente** a medida que aumentaba la complejidad de los entornos y de las amenazas. Un *whitepaper* comparativo entre Tenable y Rapid7 describe y analiza estos modelos anteriores, permitiendo entender la trayectoria de madurez de la plataforma [34].

De forma resumida, estos enfoques previos incluyen:

1. **Priorización basada en CVSS**: enfoque inicial centrado en la severidad técnica de las vulnerabilidades, con limitaciones claras a la hora de reflejar el riesgo real.
2. **Priorización basada en exposición**: incorporación de factores como la accesibilidad del activo desde redes externas o internas.
3. **Priorización basada en inteligencia de amenazas**: consideración del tiempo de vida de la vulnerabilidad, de la disponibilidad de exploits y de la actividad maliciosa conocida.

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

4. **Priorización basada en contexto del activo**: integración progresiva de la criticidad del sistema y de su rol en el negocio.

Estos cuatro enfoques sentaron las bases conceptuales para el desarrollo de Active Risk, que los integra en un **modelo único, continuo y orientado a la toma de decisiones operativas**.

Active Risk consolida los enfoques anteriores en una **visión holística del riesgo**, en la que las puntuaciones se recalculan de forma constante a medida que cambian las condiciones de exposición, amenaza o contexto.

Constituye una muestra más de que la tendencia de los fabricantes se dirige hacia **modelos de priorización dinámicos y siempre basados en riesgo**, alineados con los principios ya subrayados por el DHS en 2008, y optimizados por Manion y sus compañeros de investigación en 2018 [20][17].

5 Recomendaciones

Si el lector analizó previamente el anterior **Informe de Ciberalertas – I** [4], recordará que existía una **sección de recomendaciones. Lo remitimos allí para un tratamiento más detallado y contextualizado de las fuentes y de los marcos de referencia** empleados.

El propósito de esta sección es **condensar las ideas clave y conectarlas en un hilo lógico que vaya desde los principios generales hasta las prácticas operativas más directamente relacionadas con la gestión de vulnerabilidades y el parcheo** en entornos industriales.

Como punto de partida, se establecían unos **principios generales de ciberseguridad OT** ampliamente reconocidos a nivel internacional, como los recogidos en la **guía *Principles of Operational Technology Cybersecurity*, impulsada por el Australian Cyber Security Centre junto con otras agencias nacionales**. Estos principios sitúan la seguridad física y la integridad del proceso como prioridad absoluta, promueven el diseño de sistemas resilientes para entornos hostiles, subrayan la importancia de la previsibilidad operativa y del conocimiento continuo del entorno OT, e integran la gestión de los riesgos industriales dentro de la gestión global del riesgo de negocio.

Sobre esta base, distintos **informes sectoriales de referencia en el ámbito industrial, como los informes anuales de ciberseguridad OT/ICS elaborados por Dragones, proponían un enfoque pragmático**, orientado a traducir esos principios en acciones concretas: disponer de planes de respuesta a incidentes específicos para ICS, evolucionar hacia arquitecturas defendibles con segmentación clara IT/OT, reforzar la visibilidad y la monitorización específicas de entornos industriales, asegurar el acceso remoto y adoptar una gestión de vulnerabilidades basada en el riesgo real y no sólo en la severidad técnica.

En este contexto cobraba especial relevancia la filosofía **Now / Next / Never** que volvimos a traer a colación, que proporciona un criterio operativo sencillo para decidir que vulnerabilidades requieren actuación inmediata, cuáles pueden abordarse de forma planificada y cuáles pueden gestionarse mediante medidas compensatorias. Este enfoque permite alinear las decisiones de parcheo con el impacto operativo, evitando tanto la inacción como las intervenciones precipitadas. En cambio, en el actual Informe se proponen otros modelos como el KEV, EPSS, o soluciones propietarias híbridas.

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

A nivel más operativo, las buenas prácticas internacionales en materia de parcheo en ICS, recogidas en guías prácticas publicadas por organismos como la Cybersecurity and Infrastructure Security Agency (CISA), coinciden en que éste debe concebirse como un proceso estructurado y cíclico, que incluya gobernanza clara, inventarios fiables, análisis de impacto, pruebas previas, ejecución controlada, verificación posterior y mejora continua. Y **asumir que no siempre será posible parchear lleva a incorporar de forma explícita medidas compensatorias** —como segmentación, aislamiento, restricción de accesos o monitorización reforzada— como parte integral de la gestión del riesgo.

En conjunto, esta combinación de principios generales, prioridades tácticas y prácticas operativas permitía construir **programas de ciberseguridad OT realistas, sostenibles y alineados con la continuidad del negocio**, adaptados a las limitaciones y a la criticidad propias de los entornos industriales.

A continuación, se verán conceptos sobre **buenas prácticas de gestión de vulnerabilidades, y medidas compensatorias** en los casos en que por causas técnicas o coste/beneficio no sea adecuada la mitigación primaria mediante parcheo.

5.1 Buenas prácticas de gestión de vulnerabilidades

Esta sección compila **buenas prácticas de referencia para gestionar vulnerabilidades y decidir medidas de mitigación** con criterios operativos, especialmente útiles en entornos industriales donde el parcheo puede ser complejo (ventanas de parada limitadas, dependencia de proveedores, requisitos de seguridad funcional, etc.).

Para ello se aportan dos fuerzas complementarias: por una banda, un *paper* clásico de mitigaciones en redes de control (INL/ISA, en el contexto de programas de DHS) que pone el foco en las medidas **compensatorias y en la arquitectura defendible**; y, por otra, la guía del NIST sobre **planificación de gestión de parches a nivel empresarial**, que estructura un programa sistemático y repetible.

El documento **Mitigations for Security Vulnerabilities Found in Control System Networks [35] identifica patrones recurrentes observados en evaluaciones en campo y formula medidas prácticas para reducir exposición y explotación en ICS/OT.** Uno de sus valores didácticos es que organiza la lógica defensiva partiendo del *modus operandi* del atacante: **(1) acceder a la LAN de control, (2) comprender el proceso y (3) controlar el proceso**. A partir de esta secuencia, propone un conjunto de mitigaciones por capas, enfocadas a impedir o dificultar cada etapa.

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

En relación con el **perímetro y la separación IT/OT**, el *paper* insiste en que la segregación entre red corporativa y red de control es una práctica ya habitual, generalmente apoyada en *firewalls*, y que sirve tanto para reducir la exposición directa como para limitar la propagación de *malware* procedente del ámbito corporativo. Sobre esa base, propone ir más allá de la "frontera única" y evolucionar hacia una **segmentación interna por zonas de seguridad**, limitando las comunicaciones entre segmentos a aquellas estrictamente necesarias y bajo reglas explícitas.

En lo que respecta a **accesos y control de privilegios**, el documento enfatiza la necesidad de aplicar el principio de **mínimo privilegio** (en usuarios y aplicaciones), eliminar servicios y aplicaciones innecesarias y asegurar que las políticas de contraseñas y de respuesta a incidentes estén definidas y operativas. El hilo conductor es reducir superficie de ataque y limitar movimiento lateral si se produce una intrusión.

Una recomendación especialmente relevante para ICS/OT es sustituir, cuando sea posible, **protocolos en texto claro** por mecanismos que incorporen autenticación y cifrado. El *paper* ilustra el riesgo de credenciales capturadas en tránsito y como una autenticación cifrada podría evitar ataques de interceptación. Además, vincula autenticación e integridad de comunicación con el riesgo de **suplantación (spoofing)**, que podría derivar en pérdida de visión real del proceso por parte del personal operador.

Finalmente, el documento dedica atención explícita a la **gestión de parches**: recomienda aplicar parches de sistemas operativos y aplicaciones "conforme están disponibles", pero subraya que en entornos de control esto debe hacerse **tras pruebas previas para evitar impactos negativos en la funcionalidad**. En paralelo, refuerza la idea de que las mejoras deben introducirse **en pequeños incrementos**, coordinadas con el proveedor del sistema de control y con procedimientos de *rollback* que permitan revertir cambios si se detecta conflicto con la operación. Esta aproximación incremental encaja bien con una estrategia de riesgo progresivo (priorizar el crítico, mitigar el inmediato y planificar actualizaciones).

Por otro lado, **la publicación NIST SP 800-40r4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology [36], está orientada a establecer un enfoque de "mantenimiento preventivo" para tecnología, convirtiendo la gestión de parches en un proceso de negocio repetible**: con gobernanza, planificación, ejecución controlada, medición y mejora continua. La guía no se limita al acto de "aplicar parches", sino que enmarca la remediación de

vulnerabilidades como un conjunto de opciones y decisiones, donde el parche es una de ellas. Las principales ideas, se recogen a continuación.

a) Objetivo y alcance del programa. El NIST parte de la necesidad de que las organizaciones definan un programa de gestión de parches como función transversal, con roles y responsabilidades claros (propiedad de activos, seguridad, operaciones/IT/OT, gestión de cambios) y una alineación explícita con los objetivos del negocio. La intención es reducir la improvisación: el parcheo debe estar integrado en la gobernanza y en los procesos formales de cambio.

b) Respuesta al riesgo: opciones cuando aparece una vulnerabilidad. La guía formula la respuesta como decisión de tratamiento del riesgo clásico.

En términos prácticos, cuando se identifica una vulnerabilidad, la organización puede:

- **evitar el riesgo** (retirando o sustituyendo la tecnología),
- **mitigarlo** (parche, reconfiguración, controles compensatorios),
- **transferirlo/compartirlo** (p.ex., mediante acuerdos/seguros cuando aplica),
- **aceptarlo** (cuando el impacto esperado es asumible y queda documentado).

Este punto es clave porque formaliza lo que en OT adopta ser inevitable: no todo se puede parchear, pero todo debe gestionarse.

c) Ciclo de vida de la gestión de vulnerabilidades y parches. A SP 800-40r4 estructura un flujo continuo en el que se diferencian etapas típicas:

- **Identificación y conocimiento del activo**: inventario, dependencia de software/firmware y conocimiento de exposición.
- **Obtención de información de vulnerabilidades y parches**: fuentes de proveedores, alertas, *feeds* y evaluación interna.
- **Evaluación del impacto y del riesgo**: análisis de como la vulnerabilidad afecta al activo y al contexto (criticidad, exposición, compensaciones existentes).
- **Priorización**: establecer orden y cadencia de remediación, diferenciando tratamiento urgente vs. tratamiento por mantenimiento programado.
- **Remediación**: aplicación del parche y/o mitigaciones alternativas (configuración, desactivación de servicios, segmentación, etc.).
- **Convalidación y verificación**: comprobar que la remediación fue efectiva y que no generó efectos colaterales.

- **Registro y mejora continua**: documentación, métricas, revisión de procedimientos y aprendizajes.

Ciclo de vida de la gestión de vulnerabilidades y parches según NIST SP 800-40r4. Fuente: NIST(2022)

Un tema interesante que plantea la publicación es la asignación de los activos a grupos. Las organizaciones deben **asignar cada activo a un grupo de mantenimiento** empleando inventarios de software, características técnicas y de negocio, y escenarios de respuesta al riesgo. Un **grupo de mantenimiento** reúne activos con **características semejantes y necesidades de mantenimiento de software similares** para cada escenario de riesgo.

El mantenimiento no incluye sólo el **parcheado** (calendarios, pruebas, restricciones de indisponibilidad o impacto de una vulnerabilidad), sino también **otras medidas de mitigación y respuesta al riesgo**, incluidas mitigaciones temporales cuando no existen parches disponibles.

Las organizaciones deben **definir los grupos con el nivel de detalle más adecuado**, revisarlos periódicamente y **ajustarlos cuando sea necesario**. No deben tratar ciertos activos como "excepciones": **todo activo tiene necesidades de mantenimiento** y debe pertenecer a un grupo, incluso si **no puede o no debe ser parcheado**.

Ejemplos simplificados de **grupos de mantenimiento**:

- **Portátiles de la fuerza de trabajo móvil**: impacto moderado, tolerantes a la indisponibilidad, con controles de seguridad en los dispositivos.

- **Centro de datos on-premises**: impacto alto, parches de firmware, SO y aplicaciones, con ventanas de mantenimiento programadas y fuertes controles de red.
- **Activos OT heredados**: sin posibilidad de parcheado, impacto alto, mitigados mediante aislamiento de red y seguridad física.
- **Smartphones** corporativos: impacto moderado, sistema operativo y cadena de aplicaciones, tolerantes a la indisponibilidad.
- **Servidores locales para pruebas automatizadas**: impacto moderado, generalmente tolerantes a la indisponibilidad.
- **Contenedores en nube pública con aplicaciones orientadas a clientes**: impacto alto, muy tolerantes la indisponibilidad, con controles de seguridad en el sistema del contenedor.

En síntesis, el enfoque clave **es gestionar el mantenimiento y el riesgo por grupos de activos**, asegurando una **respuesta coherente, revisable y adecuada al impacto de cada tipo de sistema**. Posteriormente como decimos, a cada grupo se le asignará una planificación de parcheado determinada.

d) Planificación: mantenimiento rutinero y respuesta de emergencia. Una de las aportaciones más prácticas del NIST es la distinción entre:

- **Parches rutineros (mantenimiento programado)**: organización por "grupos de mantenimiento" (conjuntos de activos con requisitos y similares), definición de eneros, pruebas, comunicación y ejecución repetible.
- **Parches de emergencia**: cuando la explotación es probable/inminente o el impacto es alto, se habilitan procedimientos acelerados, manteniendo (en la medida de lo posible) control de cambios, convalidación y mecanismos de reversión.

Esta separación permite que el "urgente" no destruya el "importante": el programa sigue funcionando sin caer en una dinámica permanente de crisis.

e) Dependencias, pruebas y control del cambio. La guía insiste en que la remediación debe considerar dependencias (aplicaciones, librerías, configuraciones) y requiere un enfoque de pruebas en entornos de no producción cuando sea posible. El objetivo es minimizar interrupciones y regresiones, incorporando procedimientos de vuelta atrás y verificación post-implantación.

f) Medición y mejora (métricas). El NIST recomienda definir métricas que permitan evaluar la eficacia del programa (p.ex., cobertura de activos, tiempo hasta remediación, porcentaje de excepciones, éxito/fracaso de implantaciones, volumen de vulnerabilidades abiertas por criticidad, etc.). La finalidad no es "contar parches", sino demostrar reducción de riesgo y capacidad operativa sostenible. A continuación, un ejemplo de cuadro de mando asociado a los tiempos de gestión de vulnerabilidades:

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

Ejemplo ficticio de indicadores de tempos de gestión de vulnerabilidades. Fuente: NIST (2022)

5.2 Mitigaciones y medidas compensatorias

En entornos industriales, no siempre es posible reducir el riesgo únicamente mediante la aplicación de parches para corregir vulnerabilidades. **Las restricciones operativas, la dependencia de proveedores, los ciclos largos de mantenimiento, los requisitos de seguridad funcional o el coste, harán necesario complementar el parcheo con medidas compensatorias**, entendidas como controles técnicos, organizativos y procedimentales que permiten **reducir la probabilidad de explotación y/o el impacto de una amenaza**, aun cuando la vulnerabilidad subyacente sigue presente.

Las siguientes medidas recogen un **catálogo típico de mitigaciones en OT**, extraído y sintetizado a partir de las publicaciones del Centro de Ciberseguridad Industrial (CCI) sobre la aplicación práctica de la regulación en entornos industriales y medidas compensatorias [37][38]. Estas iniciativas no deben entenderse en modo alguno alternativas excluyentes, sino como elementos combinables dentro de una estrategia de defensa en profundidad.

a) Segmentación de red

La segmentación de red consiste en dividir la infraestructura OT en **zonas de seguridad con funciones y niveles de riesgo diferenciados**, limitando las comunicaciones entre ellas al estrictamente necesario. Su principal beneficio es reducir la superficie de ataque

y contener el movimiento lateral de un adversario en caso de intrusión. Esta medida mitiga especialmente el riesgo de propagación de malware y de accesos no autorizados a sistemas críticos.

b) Industrial DMZ / Borde IT–OT

La implantación de una **DMZ (zona desmilitarizada) industrial** en el punto de convergencia entre IT y OT permite intermediar y controlar los flujos de información entre ambos dominios. Esta arquitectura reduce el riesgo de que incidentes procedentes del ámbito corporativo impacten directamente en los sistemas de control, al tiempo que facilita la aplicación de controles específicos (firewalls, proxies, pasarelas seguras) en el perímetro más sensible.

c) Monitorización pasiva y detección de anomalías

La monitorización pasiva de tráfico y comportamiento en OT permite **detectar desviaciones respecto del funcionamiento normal** sin interferir en el proceso. Su valor reside en identificar actividades anómalas, cambios no autorizados o patrones compatibles con intrusiones, mitigando el riesgo de detección tardía y permitiendo respuesta temprana antes de que el impacto sea físico.

d) Logging inmutable / registro inviolable

Registro centralizado y protegido de eventos y acciones relevantes en OT que proporciona trazabilidad y soporte al análisis forense. El carácter inmutable de los registros reduce el riesgo de manipulación por parte de un atacante y contribuye tanto a la detección de incidentes como al cumplimiento regulatorio y al aprendizaje posterior.

e) Control de acceso robusto y separación de funciones

Control de acceso basado en identidades, roles y privilegios mínimos, junto con la separación de funciones críticas, limita el impacto potencial de credenciales comprometidas. Esta medida mitiga el riesgo de errores humanos, abuso interno y escalada de privilegios, especialmente en sistemas de ingeniería y operación.

f) Acceso remoto seguro para manteamiento

Dado que **el acceso remoto es uno de los vectores de riesgo más críticos en OT**, su protección **mediante autenticación fuerte, control de sesiones, trazabilidad y acceso bajo demanda** reduce significativamente la probabilidad de intrusiones externas y de uso indebido de cuentas de terceros.

g) Gestión de parches y estrategias compensatorias

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

Cuando el parcheo directo no es viable, pueden aplicarse **medidas compensatorias técnicas (configuraciones, reglas de filtrado, desactivación de servicios) que reduzcan la explotabilidad de la vulnerabilidad**. Estas medidas permiten ganar tiempo y reducir riesgo mientras se planifica una actualización segura.

h) Copias de seguridad y recuperación orientadas a OT

Los backups específicos de sistemas OT, incluyendo configuraciones, lógicas de control y datos de proceso, son esenciales para la recuperación tras incidentes. Esta medida mitiga el impacto de ataques destructivos, errores de configuración y fallos de sistema, siempre que los procedimientos de restauración sean probados y conocidos.

i) Bastionado de HMI y sistemas de ingeniería

Refuerzo de la configuración de HMI, estaciones de ingeniería y servidores asociados reduce la superficie de ataque al **eliminar servicios innecesarios, limitar aplicaciones permitidas y aplicar configuraciones** seguras. Se trata de activos de alto valor para un atacante, por lo que el hardening oun endurecimiento contribuye a disminuir tanto la probabilidad como el impacto de una intrusión.

j) Gestión de la cadena de suministro y firmware

La convalidación de proveedores, firmware y actualizaciones, así como el control de la integridad de los componentes, reduce el riesgo de introducir vulnerabilidades o código malicioso a través de la cadena de suministro. Esta medida cobra especial relevancia en entornos OT con largos ciclos de vida de los equipos.

k) Resiliencia y seguridad funcional

La resiliencia del sistema y la seguridad funcional aseguran que, aun **en condiciones anómalas o de ataque, el proceso transite a estados seguros. La integración entre ciberseguridad y seguridad funcional mitiga riesgos para las personas, el medio y las instalaciones**, más allá de la dimensión puramente digital.

l) Procedimientos operativos y formación

Los procedimientos claros y la formación del personal son una medida compensatoria fundamental. **Un personal formado es capaz de detectar anomalías, evitar errores críticos y responder de forma coordinada ante incidentes**, reduciendo tanto la probabilidad como el impacto de los eventos de seguridad.

m) Parcheo virtual / Firewall de capa de aplicación

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

El **parcheo virtual** dedicamos algo más de espacio por su relevancia e interés en OT, donde el equipo adopta a ser más delicado u obsoleto. Consiste en emplear controles de seguridad —habitualmente *firewalls* de capa de aplicación, *firewalls* o sistemas de prevención de intrusiones (IPS)— para **bloquear la explotación de una vulnerabilidad sin modificar el sistema vulnerable**. Según la definición de Fortinet, esta técnica permite crear una "capa de protección lógica" frente a exploits conocidos, interceptando solicitudes maliciosas, patrones de ataque o comportamientos anómalos antes de que lleguen a la aplicación o dispositivo afectado [39]. Desde el punto de vista operativo, el parcheo virtual resulta especialmente útil en entornos OT cuando:

- **no existe aún un parche oficial** del fabricante,
- el equipo afectado **es legado o está fuera de soporte,**
- **o el parcheo directo implica un riesgo elevado** para la continuidad o la seguridad funcional del proceso.

Entre sus principales beneficios destacan **la reducción inmediata de la superficie de ataque**, la posibilidad de protección en tiempo real sin intervención directa sobre el activo y la capacidad de ganar tiempo para planificar una actualización segura. Además, el parcheo virtual permite aplicar políticas coherentes a múltiples activos afectados por una misma vulnerabilidad, mejorando la eficiencia operativa.

No obstante, hay que subrayar que el parcheo virtual **no elimina la vulnerabilidad subyacente**, por lo que debe entenderse como una medida compensatoria temporal o complementaria, y no como sustituto permanente del parcheo. Su uso requiere una correcta definición y mantenimiento de las reglas de protección, conocimiento profundo del tráfico y de las aplicaciones industriales, y una supervisión continua para evitar impactos no deseados en el proceso industrial.

A continuación, a modo de cierre de la sección, se incluye una tabla resumen con los controles indicados.

Medida compensatoria	Definición sintética	Amenazas / riesgos que mitiga
Segmentación de red	División de la red OT en zonas de seguridad con comunicaciones estrictamente controladas	Movimiento lateral, propagación de *malware*, accesos no autorizados a sistemas críticos
Industrial DMZ / Borde IT–OT	Zona intermedia entre IT y OT para controlar y filtrar intercambios de información	Intrusiones desde IT, *malware* corporativo, exposición directa de OT

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

Monitorización pasiva y detección de anomalías	Observación continua del tráfico y el comportamiento OT sin interferir en el proceso	Intrusiones silenciosas, cambios no autorizados, detección tardía de ataques
Logging inmutable / registro inviolable	Registro centralizado y protegido de eventos y acciones relevantes	Ocultación de actividades maliciosas, dificultad de análisis forense, incumplimiento regulatorio
Control de acceso robusto y separación de funciones	Gestión de identidades, roles e privilegios mínimos	Uso indebido de credenciales, errores humanos, escalada de privilegios
Acceso remoto seguro para manteamiento	Accesos remotos controlados, autenticados y trazables	Intrusiones externas, abuso de cuentas de terceros, accesos persistentes
Gestión de parches y estrategias compensatorias	Aplicación planificada de parches o medidas técnicas alternativas	Explotación de vulnerabilidades conocidas, riesgo acumulado por parches diferidos
Copias de seguridad y recuperación orientadas a OT	*Backups* de configuraciones, lógicas y datos de proceso con procedimientos probados	Impacto del ransomware, pérdida de control, indisponibilidad prolongada
Bastionado de HMI y sistemas de ingeniería	Refuerzo de configuraciones y eliminación de servicios innecesarios	Compromiso de activos críticos, control do proceso por atacantes
Gestión de la cadena de suministro y firmware	Control de la integridad de proveedores, firmware y actualizaciones	Introducción de código malicioso, vulnerabilidades de origen
Resiliencia y seguridad funcional	Diseño de estados seguros e integración con la seguridad funcional	Impacto físico, riesgos para personas e instalaciones
Procedimientos operativos y formación	Definición de procedimientos y capacitación del personal	Errores humanos, respuesta incorrecta a incidentes, detección tardía
Parcheo virtual / Firewall de capa de aplicación	Bloqueo de exploits mediante reglas de seguridad sin modificar el activo vulnerable	Explotación de vulnerabilidades sin parche, riesgo en sistemas *legacy*

Tabla resumen de mitigaciones y medidas compensatorias. Fuente: elaboración propia (2026)

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

5.3 Indicadores de seguimiento

La **inclusión de un subapartado de métricas** es coherente con las guías oficiales recientes que enfatizan la **evaluación continua de la efectividad de las medidas de ciberseguridad** (no sólo su existencia formal).

El documento de junio de 2025 de **ENISA** (guía técnica de implementación en el contexto **NIS2 / medidas de gestión del riesgo**) dedica un capítulo específico a las "policies and procedures to assess the effectiveness...", indicando que la organización debe determinar **qué medidas se monitorizan y miden, como, cuando y quién es responsable de medir y evaluar los resultados** [46]. Además, propone métodos concretos (auditoría, análisis de vulnerabilidades —VA—, monitorización de rendimiento, etc.) y recomendar **KPIs**, aportando un listado no exhaustivo de ejemplos.

En la práctica de la **gestión de parches y vulnerabilidades**, el **NIST** recomienda evitar métricas simplistas y "no accionables" (por ejemplo, "total parcheado" sin contexto) y construir indicadores que crucen **la criticidad del activo** con **la criticidad y explotabilidad de la vulnerabilidad**. Ello incluye medidas de cumplimiento por plazo, tiempos medio y mediano de mitigación y segmentación por grupos de mantenimiento (especialmente relevante en OT debido a las restricciones de venta de mantenimiento y la presencia de activos *legacy*) [36].

Como referencia gubernamental directamente orientada a **KPIs de parcheo**, la guía federal canadiense "Patch Management Guidance" explica que una estrategia debe incluir indicadores de desempeño y ofrece ejemplos concretos: métricas de **cobertura** (inventario cubierto), de **eficiencia/efectividad** (tiempos mínimo/medio/máximo para parchear un porcentaje determinado, % parcheado en X días, % completamente parcheado, recuento de vulnerabilidades o hosts sin parchear por criticidad, ratio automático visual, etc.), así como calendarios sugeridos de despliegue por prioridad (por ejemplo, emergencias en 48 horas; alta en dos semanas) [47].

A nivel de **gobierno corporativo**, el toolkit del **UK National Cyber Security Centre** para trabajar recomienda emplear cuadros de mando con KPIs y menciona expresamente indicadores como el "tiempo para implementar parches" o los "días entre detección y remediación" como métricas esperables para apoyar la toma de decisiones estratégicas [48].

5.3.1.1 Catálogo propuesto de KPIs/KRIs

Los siguientes indicadores están concebidos como **ejemplos base** para ser adaptados a la realidad OT (ventanas de mantenimiento, activos legados, convalidación previa y

controles compensatorios). En línea con las recomendaciones del NIST, se recomienda segmentarlos por **grupos de mantenimiento** y por **criticidad del activo**, con el objetivo de obtener una visión realista y accionable del riesgo y del desempeño del programa.

Indicador	Tipo	Definición operativa	Cálculo recomendado
Cobertura de inventario bajo gestión de parcheo	KPI	% de activos inventariados incluidos en el proceso formal de parcheo	(# activos cubiertos / # activos inventariados) × 100
Cobertura de telemetría para evidenciar estado de parcheo	KPI	% de activos con los que se puede verificar versión/firmware de forma fiable	(# activos con evidencias / # activos totales) × 100
% de activos "fully patched" (por familia tecnológica)	KPI	% de activos cos parches aplicables aplicados segundo baseline	(# fully patched / # operativos) × 100
Cumplimiento de la SLA y criticidad	KPI	% de los activos pagados dentro del periodo definido por prioridad	(# parcheados en plazo / # objetivo) × 100
Tiempo medio de remediación (MTTR)	KPI	Media del tiempo desde aprobación/disponibilidad hasta instalación efectiva	Media (días)
Tiempo mediano de remediación (Median TTR)	KPI	Mediana del tempo de remediación	Mediana (días)
% parcheado en ≤X días tras validación	KPI	Velocidad de despliegue una vez validado el parche	(# ≤X días / # objetivo) × 100
Acumulación de vulnerabilidades pendientes por criticidad	KRI	Volumen de exposición acumulada por severidad y activo	Conteo por nivel (crit/alta/media/baja)
Cumplimiento en vulnerabilidades con explotación conocida	KPI/KRI	% mitigadas en plazo para vulnerabilidades activas/explotadas	(# mitigadas en plazo / # detectadas) × 100
Tasa de éxito de despliegue	KPI	% de instalaciones exitosas por campaña	(# OK / # intentos) × 100
Ratio de despliegue automático vs manual	KPI	% de parches desplegados con automatización controlada	(# automáticos / # total) × 100
Cobertura de controles compensatorios en activos no parcheables	KRI	% de activos legacy/no parcheables con mitigación verificada	(# mitigados / # non parcheables) × 100
Tiempo detección → contención	KPI	Tiempo desde detección hasta aislamiento/contención	Media (horas)

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

Tiempo detección → recuperación operativa	KPI	Tempo total ata restablecer operación normal	Media (días)
% de sistemas críticos con MFA	KPI	% de sistemas y accesos críticos protegidos con MFA	(# con MFA / # críticos) × 100
% de accesos remotos revisados/auditados	KPI	% de conexiones remotas sometidas a revisión periódica	(# auditado / # total) × 100

Propuesta de indicadores de seguimiento relativos a vulnerabilidades. Fuente: elaboración propia (2026)

6 Alertas

6.1 Últimas alertas

Con el objetivo de **aportar un marco claro y operativo para evaluar la situación de las vulnerabilidades en los sistemas industriales**, este informe incorpora un apartado específico centrado en las **alertas emitidas por organismos oficiales durante el trimestre más reciente**. Dado el carácter periódico de la publicación, esta aproximación permite **concentrar la información más relevante en un formato sintético y accionable**, pensado para facilitar el análisis y la priorización por parte de equipos técnicos y responsables de seguridad.

Antes de entrar en el detalle de las alertas seleccionadas, resulta oportuno **ofrecer una breve orientación sobre los principales canales disponibles para acceder, seguir o recibir este tipo de avisos**, tanto en el ámbito de **ICS/OT** como en el de **infraestructuras TI** que, en el contexto actual de convergencia tecnológica, **pueden tener repercusión directa o indirecta en la continuidad de la operación industrial**.

6.1.1 Principales fuentes de advertencias

Además de los **avisos específicos emitidos por los propios fabricantes** —que se recogen de forma estructurada en un **anexo al final del informe**— existen determinadas **plataformas de referencia** que actúan como **repositorios centrales, fiables y permanentemente actualizados** para el seguimiento de **vulnerabilidades de especial relevancia** en entornos industriales.

Estas fuentes proporcionan información clave para la **detección temprana**, la **evaluación del impacto y la toma de decisiones informada** en materia de gestión de vulnerabilidades, tanto en **entornos ICS/OT** como en **infraestructuras TI** con posible repercusión sobre la operación industrial. Su uso sistemático constituye un **pilar fundamental de un programa de vigilancia de vulnerabilidades**, que debe completarse con los boletines de los fabricantes cuyos equipos estén desplegados en planta.

Fuente	Ámbito	Descripción	Valor cercano
INCIBE-CERT	Nacional (España) / ICS	Fuente nacional de referencia en **ciberseguridad industrial**.	Información técnica detallada, **CVSS**, impacto operativo y

		Publica avisos de vulnerabilidades que afectan a fabricantes y productos ICS [40].	**medidas de mitigación** adaptadas al contexto industrial.
CCN-CERT	Nacional (España) / TI-OT	Orientado principalmente a administraciones públicas, pero con **aplicabilidad transversal**. Publica alertas de alta criticidad [41][42].	Identificación de **vulnerabilidades severas en sistemas TI** con posible **impacto en contornos OT interconectadas**.
Avisos CISA – ICS (ICSA)	Internacional / ICS	Repositorio internacional más reconocido de avisos para **sistemas de control industrial** [43].	Descripción técnica completa, **CVSS**, productos afectados, **escenarios de explotación** y **mitigaciones recomendadas**.

Origen principal de los preavisos de vulnerabilidades. Fuente: elaboración propia (2026)

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

6.1.2 Consideraciones clave para la interpretación de alertas

Al analizar **vulnerabilidades en entornos ICS/OT**, resulta esencial tener en cuenta una serie de consideraciones específicas del ámbito industrial:

- Las **puntuaciones CVSS**, aunque útiles como referencia inicial, **no siempre representan fielmente el riesgo real en OT**, donde la **disponibilidad del proceso y la seguridad física** tienen un peso determinante.
- Las **alertas procedentes del ámbito TI** (por ejemplo, servicios Windows, bases de datos o middleware corporativo) pueden tener un **impacto directo en OT** cuando están presentes en **estaciones de ingeniería, servidores SCADA o soluciones de acceso remoto y mantenimiento**.
- Un número significativo de **vulnerabilidades en productos ICS** no pueden ser **corregidas de forma inmediata** debido a **restricciones operativas, de certificación o de continuidad del servicio**, lo que convierte las medidas **compensatorias** en un elemento clave de la estrategia de mitigación.
- La mayoría de los **advisories técnicos** no incluyen información sobre **explotación activa en entornos reales**; por este motivo, fuentes y enfoques

complementarios como los presentados en este Informe, resultan fundamentales para una **priorización efectiva**.

Esta sección funcionará en cada edición del informe como una **guía práctica de apoyo** para los **equipos de seguridad, mantenimiento y operación**, facilitando la **identificación de las nuevas vulnerabilidades relevantes y** la toma de **decisiones fundamentadas** sobre aquellas que presentan un **mayor nivel de riesgo (sólo teórico, a la luz de la información recopilada en este segundo Informe) para la operación industrial**.

6.1.3 Alertas ICS de alta criticidad del trimestre

De entre los avisos publicados en el período analizado (**primer trimestre de 2026**), se presentan a continuación en esta segunda entrega, únicamente **las vulnerabilidades de severidad crítica que afectan directamente a entornos ICS**, descritas de manera sintética y orientada a la acción.

Partimos de la premisa de que el lector dispone de un programa propio de gestión de vulnerabilidades ya implantado y/o realiza el seguimiento habitual de los avisos de los fabricantes, por lo que no se consideró oportuno dedicar un fragmento extenso del informe a la descripción detallada de CVEs que pueden no ser en absoluto de su interés.

Por el contrario, **la tabla resume los elementos esenciales para facilitar una rápida identificación del riesgo, invitando en todo caso a la consulta de la fuente original de INCIBE-CERT**, que recopila de forma estructurada los avisos de origen internacional.

Nombre	Data de publicación en INCIBE	Descripción	Recursos afectados	CVES
Múltiples vulnerabilidades en los productos de Mitsubishi Electric	08/01/2026	Asher Davila y Malav Vyas reportaron 16 vulnerabilidades: 1 de severidad crítica, 11 altas, 3 medias y 1 baja. En el caso de que alguna de estas vulnerabilidades haya sido explotada con éxito, podría permitir a un atacante acceder, divulgar o manipular información confidencial, crear condiciones de denegación de servicio (DoS), ejecutar código remoto malicioso, así como eludir la autenticación.	MC Works64 : versión 4.04E e anteriores; GENESIS64, ICONICS Suite, GENESIS32, eMC Works64 todas las 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 seguridad de Siemens de enero de 2026	12/01/2026	Siemens publicó en su comunicado mensual varias actualizaciones de seguridad en algunos de sus productos.	Múltiples de Industrial Edge Services, TeleControl Server Basic, SIMATIC y RUGGEDCOM.	CVE-2025-40805, CVE-2025-40942, CVE-2025-40944, CVE-2025-40892, CVE-2025-40893, CVE-2025-40898
Múltiples vulnerabilidades en productos de AVEVA	14/01/2026	Christopher Wu, de Veracode, reportó 7 vulnerabilidades, 4 de severidade crítica y 3 de severidad alta. En el caso de ser explotadas, podrían permitir a un atacante no autenticado ejecutar código remoto y arbitrario, escalar privilegios y acceder o filtrar datos confidenciales.	AVEVA Process Optimization (anterioremente denominado ROMeo) en versiones anteriores a la 2024.1, incluida.	CVE-2025-61937, CVE-2025-64691, CVE-2025-61943, CVE-2025-65118
Omisión de autenticación en productos de ABB	19/01/2026	ABB reportó una vulnerabilidad de severidad crítica que, en el caso de ser explotada, podría permitir a un atacante omitir la autenticación de los sistemas afectados y apagarlos, modificar sus configuraciones e instalar y ejecutar 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, reportó 2 vulnerabilidades de severidad crítica que, en el caso de ser explotadas, podrían permitir a un atacante omitir la autenticación y acceder a datos confidenciales.	DIAView, versiones anteriores a 4.3.1, incluida.	CVE-2025-62581, CVE-2025-62582
Múltiples vulnerabilidades en productos B&R	20/01/2026	B&R publicó 2 avisos de seguridad que resuelven, en total, 1 vulnerabilidad de severidad crítica y 1 alta. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante hacerse pasar por una entidad de confianza o bloquear el producto.	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, informó de 21 vulnerabilidades, 1 de severidad crítica que, en el caso de ser explotada, podría permitir a un atacante leer ficheros arbitrarios del servidor mediante una solicitud 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, informó de una vulnerabilidad de severidad crítica que, en el caso de ser explotada, podría permitir a un atacante no autenticado escalar privilegios y controlar los dispositivos más allá de su alcance permitido.	Varios de Elevation CX, versiones de firmware anteriores a la 2.4.2.157.	CVE-2026-1201
Asignación incorrecta de permisos en ibaPDA de iba Systems	29/01/2026	Siemens reportó una vulnerabilidad de severidad crítica que, en el caso de ser explotada, podría permitir a un atacante ejecutar acciones no autorizadas en el sistema de ficheros.	ibaPDA, versión 8.12.0.	CVE-2025-14988

Ejecución SQL remota en productos de Johnson Controls	29/01/2026	Johnson Controls reportó 1 vulnerabilidad crítica que, en el caso de ser explotada, podría permitir a un atacante ejecutar comandos SQL de forma remota y, como consecuencia, alterar o eliminar datos.	Varios de Metasys, SST, CCT.	CVE-2026-21654
Ausencia de autenticación en la serie de codificadores de KiloView	30/01/2026	Muhammad Ammar (0xam225) informó de una vulnerabilidad crítica que, si se explotaba, podría permitir que un atacante no autenticado tuviera control administrativo total.	Varias versiones de hardware del 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, informó sobre una vulnerabilidad de severidad crítica que podría permitir que un atacante no autenticado modifique configuraciones críticas del dispositivo o restablezca el dispositivo a los valores de fábrica.	Todas las versiones de Synectix LAN 232 TRIO.	CVE-2026-1633
Ausencia de autenticación en switches Ethernet de Moxa	04/02/2026	Ya publicó un aviso para varios de sus switches Ethernet en el que informa sobre una vulnerabilidad de severidad crítica que, en el caso de ser explotada, podría comprometer la seguridad del 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 informó sobre una vulnerabilidad de severidad crítica que podría permitir a un atacante tomar el control total del dispositivo.	Tódalas versiones de Avation Light Engine Pro.	CVE-2026-1341
Ausencia de autenticación en MOMA Seismic Station de RISS SRL	04/02/2026	La estación sísmica expone su interfaz de administración web sin requerir autenticación.	MOMA Seismic Station versiones anteriores a la vez 4.2520, incluida.	CVE-2026-1632
Múltiples vulnerabilidades en EVE X1 Server de Ilevia	06/02/2026	Gjoko Krstic, de Zero Science Lab, informó sobre 9 vulnerabilidades: 5 de severidad crítica, 3 altas e 1 media, que podrían permitir a un atacante ejecutar comandos de shell arbitrarios e divulgar información confidencial do sistema.	EVE X1 versiones anteriores a la 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 gestión industrial de WAGO	09/02/2026	Diconio informó de 4 vulnerabilidades, 3 de severidad crítica y 1 alta que, en el caso de ser explotadas, podrían permitir a atacantes remotos bloquear el servicio web, ejecutar código arbitrario, eludir los controles de autenticación y obtener credenciales de administrador en texto plano.	Modelos de switches de control industrial con firmware 2.64 o inferior: 0852-1322, 0852-1328.	CVE-2026-22903, CVE-2026-22904, CVE-2026-22906, CVE-2026-22905
Múltiples vulnerabilidades en los productos de ZLAN Information Technology Co.	11/02/2026	Shorabh Karir y Deepak Singh, de KPMG, reportaron 2 vulnerabilidades de severidad crítica, cuya explotación podría permitir a un atacante eludir la autenticación o restablecer la contraseña del dispositivo.	ZLAN5143D: versión v1.600.	CVE-2026-25084, CVE-2026-24789

Carga de ficheros sin restricción en Airleader Master	13/02/2026	Angel Lomeli, de SySS GmbH, informó de una vulnerabilidad de severidad crítica que, en el caso de ser explotada, podría permitir a un atacante no autenticado ejecutar código remotamente en el servidor.	Airleader Master, versión 6.381 e anteriores.	CVE-2026-1358
Múltiples vulnerabilidades en los productos Schneider Electric	11/02/2026	Pest Limited y Robin Plugge, en colaboración con Schneider Electric, reportaron 3 vulnerabilidades, 1 de ellas crítica y 2 de severidad alta que, en el caso de ser explotadas con éxito, podrían permitir a un atacante, entre otras acciones, provocar una denegación de servicio que daría lugar a interrupciones del servicio.	Varios productos de la serie SCADAPacksupTM x70 RTU, das series EcoStruxureTM Building Operation y EcoStruxureTM Building Operation WebStation	CVE-2026-0667, CVE-2026-1227, CVE-2026-1226
Ausencia de autenticación en productos de CCTV de Honeywell	18/02/2026	Souvik Kandar informó sobre 1 vulnerabilidad de severidad crítica que podría llevar a la apropiación de cuentas y al acceso no autorizado a las transmisiones de la Cámara; un atacante no autenticado puede cambiar la dirección de correo electrónico de recuperación, lo que podría llevar a un mayor compromiso de la red.	Diversos productos de 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 severidad crítica, 2 altas y 1 media que, en el caso de ser explotadas con éxito, podrían desactivar la autenticación, provocar una condición de denegación de servicio o el robo de credenciales válidas, incluida la 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 informó sobre 2 vulnerabilidades de severidad crítica que podrían permitir la ejecución remota de código.	Todas las 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, del equipo de investigación 82 de Claroty, informó sobre 6 vulnerabilidades: 4 de severidad crítica, 1 alta y 1 media. Su explotación podría llevar a la ejecución remota de código antes de la autenticación, fuga de información o denegación de servicio.	Frick Controls Quantum HD, versiones anteriores a la 10.22, incluida.	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 y 1 baja. A explotación podría permitir evitar a autenticación, provocar denegación de servicio, crear corrupción de memoria e ejecutar 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. Si fueran explotadas, podrían permitir el secuestro de sesiones, la supresión o desvío del tráfico legítimo para causar denegación de servicio la gran escala y la manipulación de los datos enviados al backend.	Todas las versiones de swtchenergy.com.	CVE-2026-27767

Múltiples vulnerabilidades en el sitio web de Chargemap	27/02/2026	Khaled Sarieddine e Mohammad Ali Sayed informaron sobre 4 vulnerabilidades: 1 crítica, 2 altas e 1 media. La explotación exitosa podría permitir obtener control administrativo no autorizado sobre estaciones de carga o interrumpir los servicios de carga mediante denegaciones de servicio.	Todas las versiones del 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 ser explotadas, podrían permitir a un atacante obtener control administrativo sobre estaciones de carga vulnerables o provocar ataques de denegación de servicio.	Todas las versiones de OCPP Backends de Everon.	CVE-2026-26288
Ejecución remota de comandos en productos Labkotec	04/03/2026	Souvik Kandar reportó una vulnerabilidad de severidad crítica cuya explotación podría permitir a un atacante obtener control no autorizado sobre las operaciones del sistema, interrumpiendo el funcionamiento normal y generando posibles riesgos para la seguridad.	Labkotec LID-3300IP: todas las versiones; Labkotec LID-3300IP Type 2: versiones anteriores a la V2.20.	CVE-2026-1775
Contrabando de solicitudes HTTP en LabX de Mettler-Toledo	05/03/2026	LabX presenta una vulnerabilidad de severidad crítica que, de ser explotada, puede permitir a un atacante omitir la autenticación, afectando a la confidencialidad y la integridad del producto.	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, publicó 4 vulnerabilidades: 1 crítica y 3 medias. Un atacante remoto no autenticado podría obtener acceso completo al sistema y ejecutar código remotamente.	UMG 96RM-E, versiones anteriores a la 3.13, incluida.	CVE-2025-41709
Avisos de seguridad de Siemens de marzo de 2026	10/03/2026	Siemens publicó en su comunicado mensual varias actualizaciones de seguridad en varios productos, relacionadas con un total de 35 vulnerabilidades. En el detalle del aviso se indica que emitió 5 nuevos avisos de seguridad que recopilan 35 vulnerabilidades de distintas severidades.	Helio Flex 180 kW Charging Station, SIDIS Prime, SICAM SIAPPSDK, RUGGEDCOM APE1808 y varios productos 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, publicó 4 vulnerabilidades: 1 crítica y 3 medias. Un atacante remoto no autenticado podría obtener acceso completo al sistema y ejecutar código remotamente.	ENERGY METER 750-230 y 750-24, versiones de firmware 3.1 y anteriores.	CVE-2025-41709
Múltiples vulnerabilidades en Lantronix	11/03/2026	Francesco La Spina y Stanislav Dashevskyi, de Forescout Technologies, descubrieron 8 vulnerabilidades, 2 de severidad crítica, 5 altas y 1 baja. Su explotación podría permitir evitar la autenticación y ejecutar 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 una función crítica para Honeywell	11/03/2026	Gjoko Krstic, de Zero Science, informó de una vulnerabilidad de severidad crítica. El producto expone su interfaz HMI sin autenticación en la configuración de fábrica, y esto podría permitir crear una nueva cuenta con permisos de administración de lectura y escritura.	Honeywell IQ4x BMS Controller en las siguientes versiones: IQ4E, IQ412, IQ422, IQ4NC, IQ41x, IQ3 e IQECO, con firmware desde la v3.50_3.44 (incluida) hasta la 4.36_build_4.3.7.9 (no incluida).	CVE-2026-3611
Múltiples vulnerabilidades en	12/03/2026	Mr Nicolas SCHAFF y el equipo de VOC EDF informan sobre 4 vulnerabilidades: 2 críticas, 1 alta y 1 media que, en caso de ser explotadas, podrían permitir a un atacante	Todas las versiones anteriores a: HMS Networks Ewon Flexy 15.0s2; HMS Networks	CVE-2026-25817, CVE-2026-25823

Ewon Flexy e Ewon Cosy de HMS		ejecutar código remoto, realizar ataques de fuerza bruta y causar denegaciones de servicio al sistema.	Ewon Cosy+ 22.1s5; HMS Networks Ewon Cosy+, dende a versión 23.0s0 ata 23.0s2.	
Desbordamiento de búfer de la pila en AC500 V3 de ABB	13/03/2026	ABB informó de una vulnerabilidad crítica que podría permitir bloquear el dispositivo, provocar una denegación de servicio o ejecutar código remotamente.	Todos los productos AC500 V3 (PM5xxx) con la versión de firmware 3.9.0.	CVE-2025-15467
Múltiples vulnerabilidades en WebCTRL de Automated Logic	20/03/2026	Jonathan Lee, Thuy D. Nguyen y Neil C. Rowe informaron de 3 vulnerabilidades, 1 crítica y 2 altas, que podrían permitir leer, interceptar o modificar las comunicaciones.	Automated Logic WebCTRL Premium Server, versiones anteriores a la v8.5.	CVE-2026-24060
Compromiso total del sistema con los productos WAGO	23/03/2026	Un atacante remoto no autenticado puede explotar una función oculta del prompt CLI para escapar de la interfaz restringida, lo que deriva en un compromiso absoluto del dispositivo.	Varios de la serie 852-X, versiones 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 los productos de Helmholz	24/03/2026	CERT@VDE, en colaboración con Helmholz GmbH & Co. KG, publicó dos vulnerabilidades, una crítica y otra alta, que podrían permitir ejecutar código remoto o realizar una inyección SQL.	Helmholz myREX24V2 y myREX24V2.virtual, versiones de firmware 2.19.3 e anteriores.	CVE-2026-32968
Múltiples vulnerabilidades en productos de MB connect line	24/03/2026	CERT@VDE, en colaboración con MB connect line GmbH, publicó dos vulnerabilidades, una crítica y otra alta, que podrían permitir ejecutar código remoto o realizar una inyección SQL.	MB connect line mbCONNECT24 y mymbCONNECT24, versiones de firmware 2.19.3 e anteriores.	CVE-2026-32968
Múltiples vulnerabilidades Plant iT/Brewmaxx de Schneider Electric	25/03/2026	Schneider Electric reportó 4 vulnerabilidades: 1 crítica, 1 alta y 2 medias. Su explotación podría implicar un riesgo de escalada de privilegios y ejecución remota de Código.	Plant iT/Brewmaxx 9.60 y versiones posteriores.	CVE-2025-49844
Ejecución remota de código en productos de PTC	27/03/2026	Un investigador anónimo informó de una vulnerabilidad crítica que podría permitir ejecutar código remoto en Windchill PDMLink y FlexPLM mediante deserialización de datos no confiables.	Windchill PDMLink e FlexPLM, varias versiones	CVE-2026-4681
Múltiples vulnerabilidades en productos WAGO	30/03/2026	WAGO, en colaboración con CERTVDE, informó de 47 vulnerabilidades, 5 críticas, 21 altas y 21 medias, que podrían permitir evitar restricciones de seguridad, escribir fuera de los límites del montículo y provocar la caída del dispositivo, entre otras acciones.	Device Sphere, versiones anteriores a la 1.2.2; Solution Builder, versiones anteriores a la 2.4.2; Visualization And Control Hub, versiones anteriores a la 5.0.1.	CVE-2025-55315, CVE-2026-25983, CVE-2026-25897, CVE-2026-25987, CVE-2026-25898

Vulnerabilidades ICS críticas del primer trimestre de 2026. Fuente: elaboración propia (2026)

6.1.4 Ejemplos reales de incidentes ICS

La evolución reciente de las amenazas en entornos industriales confirma una tendencia consistente: una parte creciente de los incidentes busca interrumpir operaciones, no sólo robar datos. Esto se manifiesta tanto en ransomware y extorsión como en campañas de intrusión prolongada que explotan vulnerabilidades y credenciales válidas para acceder y moverse lateralmente entre sistemas [44][45].

En Europa, la explotación de vulnerabilidades se mantiene como vector de intrusión relevante y, en la práctica, reduce el margen de reacción de las organizaciones. En el ámbito estatal y hacktivista, la presión geopolítica incrementa la actividad contra sectores estratégicos e infraestructuras críticas, incluidas organizaciones del Estado español, por lo que el riesgo no puede interpretarse como "ajeno" al entorno regional.

Para el ecosistema industrial gallego (agua, energía, alimentación, automoción, logística...), el aspecto más importante es que **muchos incidentes comienzan en IT, pero acaban condicionando decisiones operativas: paradas preventivas, operación degradada, recuperación escalonada y comunicación con la cadena de suministro**. Con el fin de hacer didáctico este bloque, se describen tres incidentes recientes en el Estado español del año 2025 de modo anonimizado, ofreciendo contexto sectorial y geográfico, consecuencias observadas y mitigaciones recomendables.

Las descripciones se basan en información pública y en patronos recurrentes recogidos en informes sectoriales y repositorios de incidentes OT.

6.1.4.1 Incidente en el sector aguas

En una ciudad mediana del noreste peninsular, **un operador municipal de agua y saneamiento sufrió un incidente en el que varios sistemas corporativos quedaron cifrados, afectando a componentes administrativos y de atención al público** (portales web, gestión interna y determinados servicios digitales). La información disponible indica que el suministro y el saneamiento se han mantenido, esto es, **no hubo impacto directo en el proceso físico**. El escenario es representativo porque, aun cuando OT no resulta comprometido, la pérdida de IT puede afectar operaciones por dependencia funcional (gestión de incidencias, facturación, trazabilidad documental, coordinación con contratas).

Desde el punto de vista causal, este tipo de incidentes adopta encajar en cadenas de ataque donde el acceso inicial se obtiene por **servicios expuestos, credenciales reutilizadas/comprometidas o phishing**, y después se produce movimiento lateral y cifrado en dominios Windows. En entornos de servicios esenciales, la consecuencia más habitual es la activación de protocolos de respuesta y contingencia, con retorno temporal a procedimientos manuales y coordinación con autoridades.

El aprendizaje principal es arquitectónico y de gobernanza: cuando existe **segmentación efectiva entre IT y OT**, control estricto de accesos remotos y una práctica realista de continuidad, es posible contener el incidente en el ámbito corporativo y mantener la operación física.

Como **medidas preventivas y de mitigación** aplicables, se recomiendan: **endurecimiento de acceso** (MFA y mínimos privilegios), **separación de dominios y rutas de administración**, **copias de seguridad** offline verificadas y **pruebas periódicas** de restauración, así como planes de contingencia que contemplen operación degradada y comunicación pública coordinada.

6.1.4.2 Incidente en la industria alimentaria

En un polo industrial del sureste peninsular, **una planta de producción alimentaria comunicó un ciberataque que obligó a adoptar una medida típica en entornos industriales: un apagado controlado** para contener la propagación y preservar la seguridad del proceso**. El efecto ha sido un impacto temporal en la producción y en la logística asociada, con recuperación progresiva**. Este patrón es especialmente relevante para Galicia por la importancia del sector alimentario y por su dependencia de cadenas de frío, trazabilidad y plazos contractuales.

La literatura de referencia describe que, en incidentes de alto impacto, las organizaciones pueden escoger "parar con control" antes de arriesgar una parada caótica o una contaminación de dominios (por ejemplo, propagación a servidores de planta, saltos a sistemas de supervisión o bloqueo de estaciones críticas). Este tipo de decisiones no implica necesariamente compromiso OT, pero sí evidencia la **interdependencia**: si las capacidades de monitorización, gestión de identidades o ciertos servicios de planta dependen de IT, un incidente puede forzar una parada por prudencia.

Didácticamente, conviene destacar tres puntos.

- Primero, la rapidez: informes del sector señalan que **una parte significativa de las intrusiones modernas progresa a gran velocidad**, reduciendo la ventana de detección y contención.
- Según, la gobernanza: **sin procedimientos y responsabilidades claras** (quien decide parar, en qué condiciones, como se convalida la vuelta a la producción), la **respuesta tiende a ser improvisada.**
- Tercero, la continuidad: **es imprescindible disponer de escenarios de operación degradada y** de recuperación por fases.

Como **medidas recomendables**, destacan: **refuerzo de acceso remoto** (incluyendo registro y supervisión de sesiones), **segmentación y listas de flujo estrictas entre IT/OT**, **endurecimiento de endpoints** de usuarios y servidores de planta, y un

programa de gestión de vulnerabilidades que priorice activos y exposición real, no sólo CVSS (tal y como se indica en el presente informe técnico).

6.1.4.3 Incidente en la industria pesada (metalurgia)

En un entorno industrial del norte peninsular, **una instalación de industria pesada comunicó un incidente que afectó a sistemas internos y** ha tenido como consecuencia una **paralización significativa de la actividad durante varios días, con recuperación escalonada y comunicación a clientes y proveedores**. Este caso es útil para ilustrar que el **impacto de un ciberataque no se mide sólo por la duración de la parada, sino por la afectación a la cadena de suministro** (pedidos, transporte, calidad, contratos) y por los costes de recuperación.

En entornos de este tipo, las causas recurrentes incluyen **explotación de vulnerabilidades** en componentes expuestos (por ejemplo, portales, VPNs, dispositivos perimetrales) y **deficiencias de segmentación** que permiten que un incidente IT degrade sistemas industriales por dependencia o por accesos de administración compartidos.

También se observa que la **recuperación requiere disciplina**: **inventario fiable**, restauración desde **backups verificadas, revalidación de integridad** y, muchas veces, **priorización de servicios mínimos** antes del retorno completo.

7 Conclusiones

Este informe ofrece una **lectura actualizada del panorama de vulnerabilidades que afecta a los entornos ICS/OT**, combinando una **revisión conceptual de los principales modelos de evaluación del riesgo** asociado a vulnerabilidades con un análisis **práctico de las alertas y tendencias observadas en el período reciente**. El enfoque seguido permite comprender no sólo la **creciente magnitud de la problemática**, sino también sus **implicaciones reales sobre la operación industrial**, la continuidad del servicio y la seguridad de las personas y de los procesos.

En un primer nivel, el documento aborda los **fundamentos que condicionan la gestión de vulnerabilidades en entornos industriales**, poniendo de manifiesto las limitaciones de los enfoques puramente técnicos o basados únicamente en la severidad. Se analiza el papel de métricas como CVSS, EPSS y KEV, así como sus puntos fuertes y carencias cuando se aplican a sistemas donde la disponibilidad, el ciclo de vida prolongado de los activos y las restricciones operativas son factores determinantes. Este marco permite interpretar el riesgo desde una perspectiva más cercana a la realidad OT/ICS.

En un segundo plano, se plantea una **visión sintética de las alertas y avisos más relevantes del trimestre**, apoyada en fuentes locales y especializadas. Esta revisión evidencia una **tendencia al alza en el volumen de vulnerabilidades publicadas, con** un impacto transversal sobre fabricantes, tecnologías y sectores industriales.

El informe subraya que esta situación dificulta de forma notable a la ya de por sí **compleja operativa de la gestión de vulnerabilidades en ICS/OT**, haciendo inviable un tratamiento exhaustivo y homogéneo de todos los avisos. En este contexto, la priorización basada en el **riesgo efectivo** —y no sólo en la severidad teórica— se convierte en un elemento esencial para mantener niveles aceptables de exposición sin comprometer la operación industrial.

A partir de este análisis, se exponen **diversas alternativas y enfoques complementarios de mitigación**, desde modelos basados en explotación conocida o probabilidad de ataque, hasta estrategias apoyadas en segmentación, medidas compensatorias y gobernanza del parcheo.

Más que proponer una solución única, el informe invita al lector a **reflexionar críticamente sobre su propio contexto y** a **diseñar procedimientos de gestión de**

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

vulnerabilidades adaptados, combinando aquellas prácticas de las descritas (o análogas) que mejor se alineen con su nivel de madurez, perfil de riesgo y capacidades operativas.

Reducir la complejidad mediante una aproximación pragmática, estructurada y orientada al impacto real, es **uno de los principales retos actuales de la ciberseguridad industrial en Galicia**, donde desgraciadamente el nivel de madurez en este campo todavía tiene margen de mejora. Si este boletín contribuye a que **alguna organización del ecosistema gallego cuestione sus modelos actuales, explore enfoques alternativos y avance hacia una gestión más eficaz y sostenible del riesgo en OT, el objetivo del Informe podrá darse por cumplido.**

En definitiva, el valor de este trabajo reside en ofrecer **información accionable, criterios de análisis y referencias prácticas** que ayuden a las organizaciones gallegas a evolucionar hacia una gestión más madura de las vulnerabilidades industriales, alineada con la realidad operativa y con las mejores prácticas internacionales.

Ello posibilitará sin **duda fortalecer el ecosistema y el tejido productivo de nuestro país para alcanzar un nivel de resiliencia acorde a los tiempos que vivimos**, de tensión geopolítica y automatización creciente de la actividad cibercriminal.

Bibliografía

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

[2] Instituto SANS (2024). *Gestión de vulnerabilidades basada en riesgos y parcheo de sistemas industriales*. Recuperado de https://www.sans.org/blog/risk-based-vulnerability-management-and-patching-industrial-systems

[3] PRIMERO (2023). *Sistema de Puntuación de Vulnerabilidades Comunes v4.0 – Documento de Especificaciones.* 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] Instituto Nacional de Estándares y Tecnología (NIST) (1901). *Instituto Nacional de Estándares y Tecnología – Sitio oficial*. Recuperado de https://www.nist.gov

[7] Instituto Nacional de Estándares y Tecnología (NIST) (2025). *Base de Datos Nacional de Vulnerabilidades (NVD) – Visualizaciones 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] Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA). (2021). *Catálogo de Vulnerabilidades Explotadas Conocidas (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] Agencia de Ciberseguridad e Infraestructura (CISA). (2018). *Catálogo de Vulnerabilidades Explotadas Conocidas – Feed en formato JSON*. Recuperado de https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

[11] Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA). (2018). *Servicio de suscripción a alertas e comunicaciones de CISA*. Recuperado de https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?topic_id=USDHSCISA_136

[12] Agencia de Ciberseguridad e Infraestructura (CISA). (s.f.). *Reducción del riesgo significativo de vulnerabilidades explotadas* conocidas. Recuperado de https://www.cisa.gov/known-exploited-vulnerabilities

[13] Agencia de Ciberseguridad e Infraestructura (CISA). (2021). *Directiva Operativa Vinculante 22-01: Reducción del Riesgo Significativo de Vulnerabilidades Explotadas* Conocidas. Recuperado de https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

[14] Instituto Nacional de Estándares y Tecnología (NIST). (2022). *Directiva Operativa Vinculante del DHS 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] Noticias de Ciberseguridad. (2025). *CISA amplía el Catálogo KEV para incluir vulnerabilidades más activamente* explotadas. Recuperado de https://cybersecuritynews.com/cisa-expands-kev-catalog/

[16] Sostenible. (2024). *BOD 22-01: Informe de vulnerabilidades clave explotables*. 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 razones por las que la gestión de vulnerabilidades basada en riesgos es importante en OT.* Recuperado de https://www.dragos.com/blog/5-reasons-why-risk-based-vulnerability-management-matters-in-ot

[19] Dragos, Inc. (2024). *Gestión de vulnerabilidades basada en riesgos para tecnología operativa: un marco para priorizar riesgos en sistemas de control industrial*. Recuperado de https://hub.dragos.com/hubfs/116-Datasheets/Dragos_Risk-Based_Vulnerability_Management_OT_Cybersecurity.pdf?hsLang=en

[20] CISA (2008). *Práctica recomendada: Gestión de parches para sistemas de control*. 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). *Sistema predictivo de puntuación de vulnerabilidades (EPSS).* Recuperado de https://i.blackhat.com/USA-19/Thursday/us-19-Roytman-Predictive-Vulnerability-Scoring-System-wp.pdf

[23] Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST). (s.f.). *Modelo del Sistema de Puntuación de Predicción de Exploits (EPSS*). Recuperado de https://www.first.org/epss/model

[24] Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST). (s.f.). *Puntuaciones EPSS (datos CSV).* Recuperado de https://epss.empiricalsecurity.com/epss_scores-current.csv.gz

[25] Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST). (s.f.). *Documentación de la API EPSS*. Recuperado de https://www.first.org/epss/api

[26] Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST). (s.f.). *Guía de usuario de EPSS*. Recuperado de https://www.first.org/epss/user-guide

[27] Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST). (s.f.). *Probabilidad, percentiles y Binning en puntuaciones EPSS*. Recuperado de https://www.first.org/epss/articles/prob_percentile_bins

[28] Qualys, Inc. (s.f.). *Qué es la gestión de vulnerabilidades: detección y respuesta*. Recuperado de https://www.qualys.com/fundamentals/what-is-vulnerability-management-detection-response

[29] Qualys, Inc. (2025). *Cómo pasar de la gestión de vulnerabilidades a la reducción de riesgos centrada en el negocio* (libro técnico). 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). *Resumen de la solución: Calificación de Prioridad de Vulnerabilidad Tenable (VPR).* Recuperado de https://dam.tenable.com/a4d872a3-0f2a-4dbd-99ff-b31c0109b502/solution-overview-tenable-vulnerability-priority-rating-vpr.pdf

[31] Tenable, Inc. (2020). *¿Qué es VPR y en qué se diferencia de CVSS?*. Recuperado de https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss

[32] Tenable, Inc. (2024). *Mejoras en la Calificación de Prioridad de Vulnerabilidad Tenable (VPR)* (libro técnico). Recuperado de https://dam.tenable.com/9cd34a71-a912-40c6-bf85-b31c01120285/white-paper-enhancements-to-tenable-vulnerability-priority-rating-vpr.pdf

[33] Rapid7, Inc. (s.f.). *Prioriza vulnerabilidades como un atacante con Riesgo Activo.* Recuperado de https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/vulnerability-risk-score-sb.pdf

[34] Tenable, Inc. (s.f.). *Comparación de los enfoques Tenable y Rapid7 para la priorización de vulnerabilidades* (libro técnico). Recuperado de https://www.tenable.com/sites/default/files/uploads/documents/whitepapers/TEN_Rapid7PriorPaper_Final.pdf

[35] Agencia de Ciberseguridad e Infraestructura (CISA). (2006). *Mitigaciones de vulnerabilidades en CSNets y sistemas de control industrial*. Recuperado de https://www.cisa.gov/sites/default/files/2023-01/MitigationsForVulnerabilitiesCSNetsISA_S508C.pdf

[36] Instituto Nacional de Estándares y Tecnología (NIST). (2022). *Publicación Especial del NIST 800-40 Revisión 4: Guía de Tecnologías de Gestión de Parches* Empresariales. 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. (s.f.). *Parcheo virtual*. 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). *Avisos ICS — Alertas de seguridad de sistemas de control industrial*. Recuperado de https://www.cisa.gov/news-events/ics-advisories

[44] Soluciones de Seguridad en Cascada (2025). *Informe OT sobre amenazas de ciberseguridad 2025*. Recuperado de https://waterfall-security.com/wp-content/uploads/2025/03/2025-OT-Cyber-Security-Threat-Report.pdf

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

[46] ENISA (2025). *Guía Técnica de Implementación sobre Medidas de Gestión de Riesgos en Ciberseguridad (Versión 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] Gobierno de Canadá (2025). *Guía de gestión de parches*. Recuperado de https://www.canada.ca/en/government/system/digital-government/online-security-privacy/cyber-security-guidance-policy/patch-management-guidance.html

[48] Centro Nacional de Ciberseguridad del Reino Unido (NCSC) (s.f.). *Kit de herramientas de ciberseguridad para juntas*. Recuperado de https://www.ncsc.gov.uk/files/NCSC-Cyber-Security-Toolkit-for-Boards.pdf

Glosario

Acceso remoto

Mecanismo que permite la conexión a sistemas industriales desde ubicaciones externas, frecuentemente empleado por fabricantes e integradores para tareas de soporte y mantenimiento.

Activo crítico

Elemento de infraestructura (hardware, software o sistema) cuya indisponibilidad, compromiso o mal funcionamiento puede tener un impacto significativo en la continuidad operativa, en la seguridad de las personas o en el negocio.

Activos legados

Equipos o sistemas industriales con largos ciclos de vida, a mi cabeza de soporte del fabricante y con limitaciones para aplicar actualizaciones de seguridad.

Amenaza

Circunstancia o evento potencial, intencionado o accidental, capaz de explotar una vulnerabilidad y causar un impacto negativo sobre un sistema, proceso u organización.

Análisis basado en riesgos

Enfoque de gestión de la ciberseguridad que prioriza decisiones en función de la probabilidad de explotación y del impacto real sobre el proceso, en lugar de emplear únicamente métricas técnicas.

Arquitectura defendible

Diseño de sistemas industriales que incorpora segmentación, control de accesos y mecanismos de detección para reducir la superficie de ataque y limitar el impacto de una intrusión.

Binding Operational Directive (BOD)

Directiva operativa emitida por CISA de obligado cumplimiento para determinadas agencias federales. La del informe, orientada a la 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 o entidad especializada que informa de la existencia de una amenaza, vulnerabilidad o campaña de ataque relevante.

Ciberfísico (sistema)

Sistema en el que componentes digitales interactúan directamente con procesos físicos, como ocurre en los entornos industriales y de infraestructuras críticas.

Ciberseguridad industrial

Conjunto de prácticas, tecnologías y procedimientos orientados a proteger sistemas ICS/OT frente a amenazas cibernéticas, preservando la seguridad, disponibilidad y estabilidad del proceso.

CIA (Confidencialidad, Integridad, Disponibilidad)

Tríade clásica de la seguridad de la información que define los tres objetivos fundamentales de protección de los sistemas.

CISA (Cybersecurity and Infrastructure Security Agency)

Agencia federal de los Estados Unidos responsable de la protección de las infraestructuras críticas y de la coordinación nacional en materia de ciberseguridad.

Contexto operativo

Conjunto de condiciones técnicas, organizativas y funcionales que determinan como opera un sistema industrial y condicionan las decisiones de seguridad.

Control compensatorio

Medida técnica u organizativa que reduce el riesgo de una vulnerabilidad cuando su corrección directa (parcheo) no es viable.

Convergencia IT/OT

Integración progresiva de sistemas de tecnología de la información y tecnología operacional, que incrementa la eficiencia, pero también la superficie de ataque.

CVE (Common Vulnerabilities and Exposures)

Identificador estándar que permite referenciar de forma única una vulnerabilidad conocida.

CVSS (Common Vulnerability Scoring System)

Sistema estándar de puntuación que avalía la severidad técnica de las vulnerabilidades en una escala de 0 a 10.

Detección continua

Capacidad de identificar eventos, anomalías o amenazas de forma permanente mediante mecanismos de monitorización.

EPSS (Exploit Prediction Scoring System))

Modelo estadístico que estima la probabilidad de explotación de una vulnerabilidad en un horizonte temporal determinado de 30 días, entre 0 y 1.

Explotabilidad

Facilidad técnica con la que una vulnerabilidad puede ser explotada por un atacante.

Explotación activa

Uso confirmado de una vulnerabilidad en ataques reales observados en el mundo real.

Exposición

Grado en el que un activo es accesible o visible para posibles atacantes, tanto interna como externamente.

Gobernanza OT

Marco organizativo que define roles, responsabilidades y procedimientos para la gestión de la seguridad en entornos industriales.

Endurecimiento

Proceso de refuerzo de la configuración de un sistema para reducir su superficie de ataque y minimizar riesgos. Bastionado.

HMI (Human-Machine Interface)

Interfaz que permite a los operadores supervisar e interactuar con los procesos industriales.

ICS (Industrial Control Systems)

Conjunto de sistemas empleados para monitorizar y controlar procesos industriales.

Impacto

Consecuencia potencial de la materialización de una amenaza sobre operaciones, personas, activos o negocio.

Inteligencia de amenazas

Información analizada sobre actores, técnicas y campañas de ataque empleada para apoyar la toma de decisiones de seguridad.

TI (Information Technology)

Tecnologías orientadas a la gestión de la información y de los sistemas corporativos.

KEV (Known Exploited Vulnerabilities))

Catálogo mantenido por CISA que recoge vulnerabilidades con evidencia confirmada de explotación activa.

Mitigación

Acción destinada a reducir la probabilidad o el impacto de una vulnerabilidad o amenaza.

Movimiento lateral

Técnica empleada por atacantes para desplazarse entre sistemas de una red tras una primera intrusión.

Now / Next / Never

Modelo cualitativo de priorización de vulnerabilidades que clasifica las acciones según su urgencia operativa.

NVD (National Vulnerability Database)

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

OT (Operational Technology)

Tecnologías empleadas para supervisar y controlar procesos físicos en entornos industriales.

Parada de planta

Interrupción planificada o no planificada de la producción industrial, con impacto operativo y económico.

Parche

Aplicación de actualizaciones o correcciones para eliminar o reducir vulnerabilidades en un sistema.

PLC (Programmable Logic Controller)

Dispositivo industrial programable empleado para controlar procesos y maquinaria.

Priorizar

Proceso de ordenar vulnerabilidades o riesgos según su relevancia y urgencia de tratamiento.

Probabilidad

Estimación de la posibilidad de que una amenaza se materialice.

Proceso industrial

Conjunto de operaciones físicas y lógicas destinadas a la producción de bienes o servicios.

Riesgo

Combinación de la probabilidad de explotación de una amenaza y del impacto asociado.

Riesgo técnico

Riesgo asociado exclusivamente a las características técnicas de una vulnerabilidad, sin considerar el contexto operativo.

SCADA (Supervisory Control and Data Acquisition)

Sistema empleado para supervisar, controlar y adquirir datos de procesos industriales distribuidos.

Segmentación

Separación lógica o física de redes y sistemas para limitar movimientos laterales y reducir la superficie de ataque.

Seguridad funcional

Protección de las personas, instalaciones y del proceso frente a fallos que puedan causar daños físicos.

Superficie de ataque

Conjunto de puntos de entrada potencialmente explotables en un sistema o infraestructura.

Vulnerabilidad

Debilidad en un sistema, proceso o configuración que puede ser explotada por una amenaza.

Enero de mantenimiento

Período temporal planificado en el que se permiten intervenciones técnicas en sistemas industriales.

Anexo. Avisos de fabricantes OT

Con el fin de facilitar la consulta directa de los avisos de seguridad publicados por los principales fabricantes de tecnología industrial, se incluye a continuación una **relación de los portales oficiales donde cada proveedor publica vulnerabilidades, parches, mitigaciones y buenas prácticas asociadas a sus productos.** Tanto advisories de alertas, como PSIRT (Product Support Incident Response Team), o soporte a incidencias de seguridad en los productos.

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

Fabricante	URL DOS avisos / 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
Contacto Phoenix	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
ENFERMO	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 no es exhaustiva, pero recoge a varios de los fabricantes más presentes en entornos ICS/OT, de manera ampliada con respecto a la primera edición del Informe. Se aconseja al lector buscar los recursos asociados a sus fabricantes de referencia.

La integración sistemática de la información procedente de estos portales en los procesos habituales de seguridad facilita una gestión más proactiva del riesgo, organizar de manera más eficiente las intervenciones de mantenimiento y garantizar una supervisión continua acorde tanto con el riesgo asumido como con el ciclo de explotación de los sistemas industriales.

CIBER SEGURIDADE GALICIA

Observatorio de Ciberseguridad 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